Webcast: E-discovery Synergy Between Small Law Departments and Outside Counsel
Date and Time: Tuesday, November 7, 2006 at 2:00 PM ET
Presented by ACC Small Law Departments Committee and sponsored by Lexis Nexis

Presenters: Scott Kreamer, Baker Sterchi Cowden & Rice LLC, Jennifer Liebman, Esq., Electronic Discovery Specialist, LexisNexis Applied Discovery; Bernard M. Schulte, Esq., General Counsel, Mitsubishi Fuso Truck of America, Inc.; Todd H. Silberman, Vice President & General Counsel, Express Carriers

ASSOCIATION OF CORPORATE COUNSEL

Moderator: Todd Silberman
November 7, 2006
12:29 p.m. CT

Operator: Todd, please go ahead.

Todd Silberman: Good afternoon everyone or good morning depending on where you're calling in from.

We are glad that you're able to join us today for e-discovery synergy ((inaudible)) law department and outside counsel and we greatly appreciate LexisNexis sponsoring this Webcast for the small law department committee of ACC.

Just to let you know, there is a box on the lower left-hand side of your screen that will allow you to send us questions. So as you listen and read, if you have any questions, just go ahead and type them in that box and then click send and we'll be paying attention to the questions you've got and we'll try to answer them either in due time or immediately of, whichever makes sense with the – with the presentation.

Also, I've been asked to remind you to please fill out the Webcast evaluation form. That's link number one in the link's box. You just double click on that and that'll take you to the form itself, and please make sure you put in today's date so the folks reviewing that form know what Webcast you're talking about.

Otherwise, if you've got any concerns or questions, you can either ask the questions in the question box on the lower left or you can e-mail them to accwebcast@ – excuse me – commpartners.com.

My name is Todd Silberman. I'm Vice President and General Counsel for Express Carriers. I am a Corporate Generalist. I do a little bit of everything here and I have no other lawyers that work for me, which means I am responsible for figuring out all issues that need to be addressed.

I'm going to let other panelists introduce themselves and then we'll get started – (Ben).

(Ben Schulte): Good morning and afternoon. My name is (Ben Schulte). I'm the General Council at Mitsubishi Fuso Truck of America, Inc. and I've been in-house about four years, I'm a member of ACC involved with the small law department's committee, and I've had a good amount of litigation experience including various projects involving e-discovery – next person.

(Jennifer Liebman): Hi, everyone. My name is (Jennifer Liebman). My title is Corporate Discovery Specialist and I am an attorney with the Philadelphia office of LexisNexis Applied Discovery.

I work exclusively with corporate legal departments of all sizes helping them to understand and navigate the e-discovery process and records management obligation. And before joining Apply Discovery, I was a litigator in Philadelphia for close to nine years – Scott.

Scott Kreamer: Hello, everyone. I appreciate the opportunity to participate in this. Again, my name is Scott Kreamer. I am a member of the law firm Baker Sterchi Cowden & Rice. We're – the principal office is located in Kansas City, Missouri. We have offices in St. Louis and in Overland Park, Kansas.

I am a trial attorney. I practice in the areas of product liability and commercial litigation and have had the opportunity, or unfortunate opportunity, depending on how you look at it, of having to deal with a number of issues related to the new electronic discovery rules.

(Jennifer Liebman): My …

Male: Great.

(Jennifer Liebman): … sense on that is that any opportunity to work with electronic discovery is a good one because really it's inevitable, and really that's why we're all here today for this Webcast, why all of you are joining and listening in.

And we've put together a program today that's really going to focus on the obligation of council, both in-house and outside council, when it comes to litigation discovery in the age of electronic information, and more specifically what the synergies are between in-house and outside council to navigate or walk through this process. So the basic context here is e-

discovery in general and why it's so important, why electronic documents are treated differently than paper and we'll talk a little bit about that.

Also, the phases of the discovery process that we're very used to and how they're different now in view of the body of case law that has developed over the last decade as well as the new federal rules of civil procedure that are scheduled to take effect December 1st of this year.

So what we're going to do is walk through the various phases of e-discovery, as it were, talking about some planning stage, how to prepare yourselves, and again what you need to do to work together as a team in-house and outside council as you begin to investigate and preserve relevant information from computer systems and how you actually go about collecting that data in a manner that's consistent with the obligation that the courts have now put upon us with the new rules, and again the body of case law.

We'll talk a little bit about the processing of electronic data and how the review options and format of production and how you actually go about producing an electronic data set in litigation. We're going to end with some practice tips and advice that will sort of recap everything that we're going to go through in this presentation and give you some solid takeaways to when you leave this presentation actually start putting into motion the best practices that we're going to lay out for you today.

Todd Silberman: (Jennifer), this is Todd. Also, so you all are aware, we do have a number of links that provide you some additional information and forms that we hope will be useful and there in the links' boxes there on your screen. If you just double click on those, they'll pop up for you.

(Jennifer Liebman): Thank you, Todd. And as we go through the presentation where some of these links are coming particularly into play, I'll point out what documents will be most responsive to the areas that we're talking about. But generally, you know, why are electronic documents being treated differently than paper, why is there all of this attention to e-discovery. And really the term e-discovery is simply discovery – the discovery process that we know and love under some different circumstances and that is proliferation of electronic information.

So it's the same basic steps, the identification, preservation, gathering, review and production of responsive information in the litigation or investigation context. We're talking about a little bit of different circumstances now because more than 99 percent of all new business information is created and stored electronically and only about a third of that at most is actually ever printed to paper.

Some studies are saying that we're looking at about 60 billion e-mail messages sent daily in the US and really that number is just increasing exponentially. And if you think about the number of e-mails that you – that you all receive …

(Jennifer Liebman): … on a daily basis – is anyone hearing an interference?

Operator: Please note that – please place your phones on mute so ((inaudible)) that are not speaking.

(Jennifer Liebman): Thank you.

Think about the number of e-mail messages that you receive and send on a daily basis and you can just imagine the sheer volume that is being sent daily in the US alone. So all of this information is very rarely printed to paper – where is it – and the storage of electronic documents create some new issues with regard to our obligation to investigate and preserve.

So instead of opening up file cabinets or looking through paper files for relevant information, we've got to consider a whole new realm of sources of data, and that includes laptops, of course, and desktop computers. You've got server data, backup tapes.

Many people today are using flash drives or little transportable media that can hold up to two gigabytes or more of data, CDs, PDAs, et cetera. And when they're talking about a flash drive, really that's what an iPod is, and I've even heard now of people using iPods to actually store information for business or other work-related uses so don't forget about any potential sources.

Electronic documents are also different than paper because they're dynamic, much more easily movable, changeable, and frequently deleted often with no proactive act on the part of the deleter. So sometimes you've got data residing in computer systems that are set to automatically rewrite or overwrite data; same thing with the hard drive. When you delete information it does remain in available space in your computer even after it's been deleted and can be recovered by a forensic analysis if that data hasn't been overwritten using software, or if that space hasn't been used for new incoming data.

So the sources of data are really an important consideration, and then the most distinguishing feature of an electronic document is the metadata, the existence of this data

about the data and what that is and you all are probably very familiar with that term. It's been used in the press, it's been used by lawyers now frequently as they use the word discovery, and what this is, is a backend field of information about the electronic document. And the metadata can contain upwards of 200 fields of information, such as when a document was created, when it was last modified, who it was sent to, et cetera.

All of these things – the dynamic data of electronic documents, the existence of metadata, where they're stored, they all – all of these factors impact our ability to investigate and preserve this information as required by the federal rules, in fact, as required by our longstanding discovery obligations.

So what we've seen develop is a body of law where the Zubulake line of decisions really spearheaded the e-discovery law, so to speak, and that was a series of about five decisions issued by Judge Shira Scheindlin of the US in the Southern District of New York and those new federal rules of civil procedure really adopt the rules and the precepts that were developed by Zubulake and that's what you're going to see play out in terms of changing obligations which are really mostly procedural.

So given that backdrop, what are the obligations and what duties do in-house and outside counsel have when they're looking at an e-discovery-related litigation, which as of December every case is going to fall under the new rules regardless of the status of the case and you're going to have to start accounting for the existence of what the rules are calling "electronically-stored information," or ESI.

(Ben Schulte): (Jennifer), this is (Ben Schulte). I just want to put in a comment here that if you haven't read through the committee notes and the rules themselves get a copy. They're available out there.

I know that if you have LexisNexis, (Weslaw), anybody, you can get the committee notes. It is very revealing to see what was done in reaction to Zubulake to make it consistent and clear what the obligations of the corporation are, and we'll be going through that a little bit.

But when you're interacting with your outside counsel, they're going to be familiar with this. You don't have to be an expert on e-discovery but you have to have a good, basic familiarity with what those obligations are in the early stages to make sure that you're not buying yourself a problem later on.

(Jennifer Liebman): Thank you and that's a great point.

So reading and understanding the new rules as well as the committee notes is really step number one. If you haven't done it yet do it now and do it together in-house and outside counsel. Work through the new rules, walk through them together, and even present educational seminars for each other, as the need may be.

And you're starting point is to bring together a team of people who can work in all of the different aspects of this process, which includes IT representation, records management, compliance if there are folks available in your corporation serving in those capacities. So it's not just a task to be owned by legal, per se'; it's really critical to bring IT records management and compliance folks into this process.

And if your office does not have folks that are really serving all of those roles, and that's not uncommon, then you need somebody who's going to be able to wear a variety of hats. So if you've got a corporate secretary who's also serving as general counsel or an assistant general counsel, then there's the hat of records management potentially included within that in-house counsel role.

So partnering with IT and your records manager to learn about the clients, the company's IT systems, infrastructure, and capabilities is critical. Start early by putting together a data map. And really that's just a roadmap to tell you as counsel where and how data is stored within the corporate organization so that you know where to look and where to go when your obligation to investigate and preserve kicks in when a litigation is imminent.

It's a good idea to early on designate and prepare a 30B6 witness and this should be somebody who can attest to the company's record retention policy, assuming there is one, also to litigation hold procedures that were undertaken, and to IT capacities and infrastructure generally. Maybe that's one person, maybe that's a series of individuals, and that's a case-by-case decision that in-house counsel and outside counsel need to assess together.

Scott Kreamer: And (Jennifer), it's Scott. I just wanted to offer a point or two with respect to the 30B6 witness.

That is critically important, and just to kind of bring this to home, so to speak, you know, here in Kansas City in the heartland, you know, there's a lot of country music and country

music, although I'm a big aficionado of it, offers many words of wisdom in some of the titles of the songs. And just to impart some of that wisdom to you all there's a song that the – that the title of which is "You're The Reason Our Kids Are So Ugly," and when you've got a 30B6, you know, corporate representative, you know, in the context of any matter, whether it is in the context of, you know, e-discovery or anything else, it is very important that you work in conjunction with your outside counsel in preparing that person to testify because those are admissions on behalf of the corporation and it is imperative that that person be prepped properly because if he's not your case can get ugly in a hurry.

(Ben Schulte): This is (Ben Schulte). I want to add a couple points here.

One is that we're talking about the early planning stage before litigation or even an investigation begins. Unless you have a very large volume of cases, you may not have one outside firm that you use exclusively and that you have a relationship with. If you do that's great. You can get a lot of guidance.

In general, especially in a small law department situation, you may have to rely on yourselves to do all of this so the relationship with the IT department becomes the in-house lawyers' job. It's their responsibility.

The second comment I wanted to make before we move on to this next slide is if you are in a small in-house situation, if you have a company where you are the only one who knows the documentation retention program, if you're the one who develops it and implements it and enforces it and you don't want to put one of your IT people on the stand, it's OK if it's your choice to – in my instance, I've done this – is put myself out as the 30B6 witness. Even

though you're a lawyer, if you're not, you have to weigh whether you're going to be actively involved in the litigation itself. If you're not and there's no problem with that where you're just going to be the corporate representative anyway even, there's no reason not to be the 30B6 witness, especially if you're protecting someone else.

Scott Kreamer: And (Ben), that's a good point because, again, when you have the face of the corporation out there, you want that to – you want that person to be able to communicate a very good story of what the policies and procedures are of that corporation. The 30B6 doesn't have to be the person with the most knowledge, you know, with respect to a particular area. It's just somebody who is speaking on behalf of the corporation who has educated themselves into the particular areas of inquiry.

(Jennifer Liebman): And along those lines, the links include a set of sample 30B6 deposition questions that can be used obviously to ask questions of a 30B6 component, but also to prepare your own witnesses for the types of – the type of testimony they may be required to present.

So now we're sort of moving into the preservation phase. So early planning's really critical in order to set you up to be able to comply with your preservation obligations, which are very (weighty) given the nature of electronic evidence, in that it's stored in many different places, subject to automatic overriding, and often affirmative proactive steps need to be taken to actually preserve the electronic data; whereas with paper, as long as nobody was throwing it away, you could rest assured that it was remaining preserved.

So working together to assess your records retention policy so that you know on what basis data is overwritten in your clients or in your corporate organization's IT system and how to actually go in and stop the overwriting of that data for purposes of preservation when you're required to implement a litigation hold. If you've done all of that investigation or research on the front-end, when you're obligation to preserve kicks in, you will be well-prepared and well-versed on the locations of data that may be relevant to your particular matter and the processes by which you need to go ahead and preserve that data along with the metadata that's associated with that information.

So there's a lot of questions around when does the obligation to preserve kick in, and the rules say when you know, or reasonably should know, that litigation is on the horizon – and maybe, (Ben), Todd, Scott, you have some particular circumstances where an obligation kicked in that you wouldn't expect based on the facts. I mean, you have – typically, if you get an EEOC notice or a letter from counsel putting you on notice, (they) are the easy cases, some questions come into play when you've got different facts or a claim that's made on an insurance policy, for example, any insight there?

Male: (Ben)?

(Ben Schulte): Well, I wanted to make one quick comment, (Jennifer), that for the instance where information is generally overwritten by the system itself, you have to be sure to talk to your IT people about that because the new rule says that – it says specifically you don't have to put the company at a standstill just to prevent information from being overwritten. If it's in good faith and overwritten in the normal course, then you don't have to take extraordinary

steps to protect that pattern. That's usually financial data, sales figures, things like that that are constantly being updated in your system.

If it's possible to do that, and this is where working with your IT department comes in – if it's possible to do that, then you should be able – then you should do that just as a proactive step, which leads me to my second comment, which is that in figuring out your holds – you should have a holds' procedure, but in figuring out what needs to be put on holds that's where talking to outside counsel early and often is key because they're going to know local practice better than you are ever going to know because they're in that jurisdiction all the time hopefully and they may have some insight, they may have some vendors that they use. They may be able to help you figure out exactly what that is. Plus, you should be working on a discovery plan with counsel once you know litigation is coming.

Todd Silberman: And to expand on that before we move to the next slide, I've got a couple of questions that I wanted to share with the panel here.

The first one is can updating record retention policies with ESI preservation and discovery guidelines come back to haunt a company; can you comment on the balance of documenting policy versus digging the company into a hole to respond to a certain manner.

Scott Kreamer: Well, this is Scott again and just to comment on that, one of the things that courts look to when you've got a discovery dispute amongst the parties is whether or not you do have a document retention policy.

There are a number of cases that are now filtering down through the courts with respect to preserving electronic discovery, electronic documents and the failure by a party to follow or to preserve that evidence has resulted anywhere from the imposition of sizable sanctions in the amounts of millions of dollars to adverse jury instructions being provided. That the lack of evidence is – you can infer from the lack of evidence that the company destroyed those and that there was an negative, you know, connotation with respect to that particular destroyed document.

So, you know, if you follow your document retention policy, you know, establishing that after every 60 days, that documents or e-mails or whatever it is are in a normal course and scope of your business destroyed, then you can go before the court and you can argue, look, Your Honor, we didn't have any idea that there was any pending litigation, our normal document retention policy is A, B and C, we followed A, B, and C, there wasn't any ulterior motive, there wasn't any willful destruction of this evidence. So I think courts are really pressing companies to have that document retention policy.

Now certainly, there is a problem that if you have a written policy out there and you don't follow it you could be in trouble, but the lack of a policy I think poses greater risks to the company.

(Ben Schulte): This is (Ben) again. To answer the question another way, if you've got a policy, great, if you don't have one, get one. But if you're in the middle of litigation or you know litigation is coming, that is not the time to either start implementing or enforcing the policy. That will get you in trouble because they will look at the timing of it.

If you happen to – if you don't have a policy, I would say immediately look at all the literature you can find. Find a (foreign) policy. There are books, there are info packs on the ACC Web site, there are a lot of ways to go about doing it. Don't delay. Document everything you do when you're not in the middle of a case. If you do want to do it while you're in the middle of a case, then you have to immediately have the policy but implement a litigation hold.

So is there ever a negative from having that document retention policy in place, EDI or paper documents, and the answer is no as long you're careful about how you go about doing it.

Scott Kreamer: And one other thing that I have seen from the – from the frontline, so to speak, is the fact that many plaintiffs' counsel attorneys are out there and it may be the – maybe the factual basis of their case isn't that strong but they'll try to create a stronger case just through electronic discovery disputes.

If, for example, information hasn't been preserved, they will try to parlay that into a – into some type of a discovery motion and sanctions being imposed against the party, and now all of a sudden the case that didn't have much merit, you know, may have some merit if we're not careful on our end in protecting that information and documenting what we do to the court.

(Jennifer Liebman): And that's a great point and that's what all of the case law is showing us is that there is a substantial risk to not having a retention policy because, A, your – any sporadic loss of information will be construed as spoliation even if it was accidental.

Also if you've got a policy that you're not following, that is just as bad – likely worse than not having any policy at all because again it gives rise to the allegation of spoliation and the circumstances, you know, play that out because the evidence is missing.

And what you see, you know, there's the Morgan Stanley case which came on the heels of the Zubulake line of decisions where the company didn't have a formal records retention policy that provided them with a roadmap to where and how long data resided on their systems and certifications were made to the court that everything was turned over, when, in fact, they kept discovering new volumes of information in different places.

And ultimately the court said this was gross discovery abuse, read the allegations of the complaint to the jury and said you may accept them as true, and what resulted was a $1-billion judgment not based on the merits, based solely on discovery abuses. The case is cited on the preservation slide. Play that out as well.

And there's really so much to be said about records retention, litigation holds, what to do, what not to do, what the risks are, and anyone who is looking for additional information can follow up with the links that are provided, and also with any one of us who have a lot of experience working through these issues.

So the preservation piece leads us right into collection because once you've taken the steps to proactively preserve the information that's likely to be relevant to your particular case, now you've got the collection process to consider, and this is typically when or before a document

request is filed. You want to actually start pulling all of the information together so that you can get it ready for review.

And here it's critical for in-house and outside counsel to start working together to talk about what issues will arise when you have your initial scheduling conferences with opposing counsel in the court. So the new rules of civil procedure are requiring counsel to meet and confer early on, right away to talk about e-discovery, electronically-stored information, where it is, how much there is, how you're going to narrow the scope of what's being requested, whether there is backup tape information and issue, whether there are legacy data, and that's information from old systems that are no longer in active use.

And you also have to think how are you going to actually do make a collection of data because to simply copy electronic information onto a CD often is not going to give that information the protection it needs to actually pass evidentiary scrutiny, meaning you want to make sure you maintain the forensic integrity of this information. That's keeping the metadata in tack. Many IT departments are able to do this, they just need to understand the different issues with metadata and the tools they need to copy data so that the metadata is maintained in tack.

Todd Silberman: (Jennifer), this is Todd. Can you explain how detailed a data map needs to be?

(Jennifer Liebman): You know, a data map is – think about it as a guideline for you to understand where information is stored so that you know where to go to get it when your obligation to collect and preserve information kicks in. So it can be as detailed or as high level as works

for you and it's really going to depend on the complexity of your computer systems and of your particular business organization.

So some companies may have 40 different subsidiaries and affiliates and maybe they have data from those companies hosted on the headquarters' servers, and then you're going to have a more intricate data map. And if you're talking about just data that resides within a corporate office, it may be very simple and talk about exchange servers or e-mail servers, file servers, backup tapes, and then just what people in the field or end-users may have assessable to them, desktops, laptops, PDAs, et cetera. It's really a very case-by-case decision and the detail is very tied to the detail on complexity of your business and IT organization.

(Ben Schulte): (Jennifer), this is (Ben Schulte). One comment I want to make is that a lot of – I mean, this is overwhelming to me and I have experience with the area. When you look at the slide – the previous slide and this one, processing data for review, all of this activity looks like the in-house counsel has to become a expert in IT and that's not really true. What it means, though, is that you have to work with outside counsel and evaluate you're – the case – the seriousness of the case.

You could be a very small law department with a very big company that may or may not have a lot of in-house IT people, especially if things have been outsourced, you may want to consider along with your outside counsel outsourcing a lot of this procedure. And that can be done. If anyone went to the ACC meeting in San Diego, probably a third of the vendors there were talking about e-discovery, and if they weren't they had something to do with it, or they had a relationship with somebody who did.

So the resources are out there and it may not necessarily be in the lawyer's best interest to focus on doing that themselves. A lot of that depends on the seriousness of the case, the size of the company, and like you said, what data is out there and might need to searched.

Once the allegations come in, once you have your holds in place, you have to sit down with outside counsel and figure out what sorts of documents is the plaintiff going to need to prove their case, assuming you're the defendant what you're going to need to defend the case.

And at that point, you both have to sit there and make an evaluation as to what you need to bring to bear. Also, your IT department is not going to be able to throw huge amounts of manpower because in this day and age they just don't have it to spare and they don't understand that 30 days without an extension might be a requirement. So the outsource route is something that you have to seriously consider, especially if you're going up against an aggressive opponent.

Scott Kreamer: One of the things that I have found that courts really look to is just an overall evaluation of the circumstances and what is reasonable in light of the information that is needed, the type of case that you have.

You know, if you have a – if you have a big case, you know, a substantial amount of damages are alleged, high document, you know, a lot of – a lot of documents out there, a lot of electronic information, courts are going to require you to engage in greater detail, greater efforts in order to recover information, and maybe that's going back and trying to hire forensic experts to come in and try to reestablish deleted e-mails. It could be, you know, something to that extent or it could be something just, well, talk to the key players that were

involved in this transaction and, you know, and get the information that is on their hard drives or on backup tapes.

And again in parting wisdom found from our country music lyrics, you know, the song that is her teeth was stained but her heart was pure, if you've got good intentions, you know, and you follow through with those, that may not be enough. You know, you have to look to what was reasonable under the circumstances, be able to articulate to the court, you know, the series of steps that were taken, and present your position to the court.

Todd Silberman: There was just a question and this person was on the – on the – had the same question that I was about to ask actually, can you quantify the costs for e-discovery using an outside vendor.

Scott Kreamer: The costs can vary significantly depending on the type of information that you need.

There's has been significant advancements in the – in the area of recovery – forensic recovery of information, such that some folks now can, you know, for $5,000 can go back in, recover on backup tapes, you know, information that had been deleted or other information.

Now, counter that with, you know, a high – a high profile piece of litigation that involves a lot of people, a lot of documents, you know, in that instance, you know, the costs can easily run in the tens of thousands of dollars.

(Ben Schulte): Scott, this is (Ben Schulte) again. One thing that you have to consider when you're looking at cost issues is whether the – whether the electronic documents are readily assessable.

The good thing that they did put into the new rules is that if you, as the responding entity, say that documents are not readily assessable, and the notes define what that means – I'll on that in a moment – but if you say they're not readily assessable, then you are not going to be subject to an order to produce those and expend all the money to recovery the information until you've had a chance to explain to the court that – why the cost is prohibitive, why the case isn't worth it, why the information is available elsewhere. So the procedures have built in some protection from the potential cost.

As far as what is considered not readily assessable, when you get into the rules a little bit you'll see that – for instance, backup tapes, while you may have the backup tapes you may not have the equipment to download an entire duplicate set of books or whatever accounts are on those tapes on another box – on another physical machine without disrupting your business.

At that point, you have to assess, can I get a vendor to do it, how much is it going to cost me. If it's going to be cost prohibitive, you say they're not readily assessable and you may have to justify that and the vendors will address those issues usually.

(Jennifer Liebman): And this is (Jennifer) speaking in behalf of LexisNexis Apply Discovery.

We get asked very frequently by clients, corporations, attorneys to cost-out certain projects such as backup tape restoration (or) also onsite data collection, et cetera, so that the parties can go back to the court or each other and say this is what it's going to cost, reasonable or not, depending upon the circumstances.

And for purposes of data collection generally and to address the question about e-discovery and using an outside provider, call the providers. They will give you cost estimates and budgets and you can work with your outside counsel or conversely in-house counsel to establish what would be an appropriate budget for any given project depending on the case and the providers will work with you to achieve a solution that assists you within the confines of your budget.

And a simple data collection job, if you feel that you don't have the resources internally to properly collect electronic data and handle it, those services are often very inexpensive, relatively speaking, and are frequently billed on an hourly basis depending upon the time it takes to travel to the site and actually copy the data. It takes about an hour to make an image of a computer and that's how those services are typically charged.

Todd Silberman: Well – and let me – let me ask another question in terms of using outside vendors and having them assist with what they review.

You know, we've got this neat question box down here where people are instant messaging and I think there was probably a time where instant messaging was the same thing as a phone call, but with these new rules, we all see a shift in this to where instant messages are going to

be – have to be produced as well. And when we're producing all these things, particularly through vendors, do you all see any impact on attorney/client privilege?

(Ben Schulte): This is (Ben Schulte). To answer the first question, instant messages don't disappear. They may disappear off of the user's screen and they may not be able to go back and get them but they do live somewhere, they are recoverable, they are documents. Almost anything is considered an e-document.

And to take it a step further, there's a lot of concern now with voicemail systems, for instance, where you can get your voicemails sent to you as e-mails, or where even your voicemail system is digitally recording those messages, so even though you delete the message, it may not be overwritten on a hard disk somewhere and might be recoverable. All of that is considered an electronic document.

Scott, I'll let you handle the second question.

Scott Kreamer: Certainly there are concerns about attorney/client privilege. To the extent that you are retaining services of an outside vendor, that would be protected with your attorney/client privilege.

Although I'll mention this, there was a recent decision November 1 out of the North Carolina Superior Court in which there was a dispute and there was – regarding e-discovery plaintiff on a trade secret case wanted extensive amounts of trade – of electronic documents. The defendant basically argued some of the things that we've argued, you know, burden expense, you know, time, et cetera, and the court basically just divided the costs.

It said that, all right, look, we're going to hire an independent forensic expert, you guys have to split the cost of that. And so courts are being kind of creative. And, you know, in the old days where, you know, you would just simply charge the other side for copying, you know, documents are gone. You know, courts are now requiring parties to share expenses with respect to this.

Touching back on the attorney/client, you know, it's important after you – I mean – and to the extent that you've hired your own forensic folks to restore the backup, it's important that you guys take the time to review the information that's being produced. There are some provisions in the new amendments that talk about inadvertent disclosures, but, you know, we're probably running a little short on time to get into that area.

(Jennifer Liebman): And just to summarize, again, from the perspective of the national e-discovery provider, we are not seeing your data so it's not being disclosed to us for purposes of privilege. Also, many times providers will be happy to enter into confidentiality agreements or NDAs. You can also do things like data filtering to pull out from a data set proprietary or other top secret information by using keywords geared toward actually finding that information, and you can lock down data when it's released to a review environment so that certain people can see only certain data sets to protect IT or other business-related information.

So that's a lot about collection. The only point we didn't really discuss is chain of custody, which is a critical concern. You want to make sure you're documenting and adhering strictly

the chain of custody protocols and the links contain a sample chain-of-custody log and some of the concerns that you need to look out for.

So just to summarize the review and production process, that's where you really need to work together to decide what's the best format or way for counsel to review this information and it has to be put into a database. So in the same way you take your stacks of paper to the copy center to have multiple working copies made for review, electronic data can be processed to a working format where it can be reviewed electronically, coded or tagged electronically, date stamped, marked for privilege, redacted, and produced in an electronic format.

The variety of solutions out there are many and that's where you really need to focus on whether you're going to be doing the review together, whether there may be some level of in-house review for privilege before the data goes to outside counsel, and if you (want) a Web-based or a shared type of an application in order to accomplish that review, and then also how you're going to track the progress and efficiency of the review so that you know you're going to meet your end deadlines. And there's lots of tools out there to help you accomplish that and working together and talking with outside experts or what other people have done is very helpful to you in that process. You want to consider, you know, your production deadlines first and foremost, also what format you're going to be producing your data in.

And that's a really very high-level overview of the phases and steps of the discovery process and what you as in-house and outside counsel need to look out for and how you need to collaborate in this process. So now we're going to shift into some practice tips and advice to

give you some (walkaways) or takeaways for action items to help you comply with your obligations under the new federal rules.

(Ben Schulte): (Jennifer), one last comment. It's (Ben Schulte) again. That last slide we looked at can be overwhelming as well and the key is working with local counsel to assess the value of the case. If it's not a (venture) company case you may not need to go very elaborately.

If you have one e-mail server and your IT department can give you access to people's e-mail and you can do a word search and you're willing to be the 30B6 or somebody in your IT department is willing to be the 30B6 witness, you can accomplish a lot on a shoestring. It depends on the value of the case, what your litigation budget looks like, and it depends on local practice and that's where you really need to have that synergy with your outside counsel. They may have an in-house expert. They may have one of their IT guys who will serve as an in-house expert. You can get creative with it, and if it's a big enough case, you hire everybody you need to hire to come in and do whatever they need to do.

Scott Kreamer: Moving on to the – to the practice tips and advice to clients, and I'll lead this off with one of my favorite music song titles again and that is "I Ain't Never Gone To Bed With An Ugly Woman But I Sure Woke Up With A Few." Now there's multiple levels of advice that can be found in a – in a title of (a) song of that nature.

You know, first of all, with respect to each and everyone of your respective companies, certainly, you know, you don't enter into business dealings, you don't sell products, you know, expecting to have, you know, litigation that arises out of it, but litigation does arise out of it and precautions need to be taken.

You know, certainly, you know, if a – if a case does arise, you know, you've got the need to make sure that you've got quality people that you can rely on, that your outside counsel understands the obligations created by the new rules of civil procedure relating to electronic discovery because, you know, you may think that you're going to bed with somebody pretty good-looking, but, you know, in the morning, you know, things can change, you know, and that's what we want to help you all avoid is some of those problems.

One of the keys that we talked about earlier relates to the – developing the document retention policy. And just to highlight this again, the importance, many courts nowadays expect this. It justifies that you can use it and rely on it heavily to justify why documents are no longer around, why they have been destroyed. It helps save time and money.

You know, for example, if you have a document retention policy – we're involved in a case – in a significant piece of litigation in which there was no document retention policy. As a result of that, we are having to go through and perform document sweeps in order to justify to the court that we've – that we've engaged in good-faith efforts to respond to discovery. And those documents sweeps that we're doing, going through people's offices, literally looking at papers, looking at electronic information, is a costly proposition, but it's something that we were required to do because there was no policy that was – that was in effect. Furthermore, that document-retention policy can help to avoid sanctions.

(Ben), do you guys have a document-retention policy?

(Ben Schulte): Yes, we do. As a matter of fact, we had a written document-retention policy before I came in here four years ago and a lot of those deadlines for review are statutory.

The finance people are more familiar than I was with how long they needed to keep certain records and we have a system where every department head is required to bring a box back from storage that's been put in archives and review it before they clear it for destruction. So I know where my bottleneck is, where what I have to do to put a litigation hold on something on the paper side. On the electronic side – and I'm looking at one of the questions, which I think plays into this – the electronic side it's much more difficult to get a document-retention policy.

E-mails are an example. My company does not have an automatic destruction cycle on our e-mail – on our e-mail memory – a lot of companies do – where every 60 days all the old e-mails go away. For us, it is up to the individuals to delete old e-mails, to immediately delete non-business e-mails, but if somebody has a record that they refer back to or a correspondence that they're keeping in e-mail, they're allowed to keep it. The only thing we tell people is, if it's more than a year old get rid of it because we'll have had it backed up and retained on tape form at least twice. So we keep e-mail backup tapes. That's not practical for a lot of companies that have a huge number of e-mails or multiple servers or a host of things.

One of the questions was or comments was that the practical tips aren't very practical when you have all these different versions of these documents that might be out there. One person sends an e-mail, 16 people may have it. They may have it on their laptop, on their hard

drive and how do you produce that or determine that you do or do not have it and that becomes a question of company policy.

It is our company policy that no business documents are retained on the hard drives of laptops or desktop computers, that we have our IT department set up so that all of the retained documents are on specific backup servers. That's a document security issue. It's a practicality issue for our disaster recovery as well.

Again, the problem is, if you allow – and you may have to for business necessity – but if you allow your personnel to have company data in various places just as if they had a paper file, you have to go to everyone who's got a file cabinet to look for a document and you have to look for those documents where they are likely to be kept. The discovery burden – and, Scott, you can talk about that a little bit too, I'm sure – the burden is not to look at every piece of paper in the company to make sure you didn't miss anything.

Scott Kreamer: Well, that ties directly into, you know, the preservation plan.

Once you have litigation, whether or not it's a notice of a claim or it's the actual filing of a lawsuit, you know, preservation is key, and again, it's a coordinated effort between outside counsel, between the lT department, and between the in-house legal team. And it is – it is vitally important that all people are operating on the – on the same page, that the outside counsel understands, you know, the type of information that the company has, the folks that they can go to, to talk about certain issues, about the location of those documents.

And (Jennifer), do you have any comments to add with respect to the preservation?

(Jennifer Liebman): Excuse me. Yes, the idea is to have a game plan that essentially covers all of the different forms of or record sets of data being created by the company and then coming up with a method for how that information is saved and deleted, realizing that on the end-user level there are some impracticalities associated with saying, you know, destroy your e-mail every 30 days because you have situations where employees don't always, you know, comply with those rules.

So it's just whatever is going to work best for your particular business, and given your infrastructure, it's a very case-by-case decision and solution that should be decided by in-house and outside counsel, and in many cases together with an expert in the area to formulate a policy that's going to work with your business practices.

Scott Kreamer: And the bottom line is that, again, take a reasonableness approach to this based upon your resources, document everything that you do because that'll be important at the end of the day when you're going before the court to explain, you know, your actions and to – and to argue your company's position.

Todd Silberman: Scott, I think you got the last word. I believe we are out of time.

Scott Kreamer: Well, thank you very much.

(Jennifer Liebman): Thank you, everyone.

Todd Silberman: Thank you to all the participants.

END