Title: The New Federal eDiscovery Rules: How Your eDiscovery and eRecords Management Practices Should be Revised for Compliance
Date and Time**:** Tuesday, August 29, 2006 at 2:00 PM ET
Duration**:** 60 Minutes

ASSOCIATION OF CORPORATE COUNSEL

Moderator: (Sean Cheadle)
August 29, 2006
1:00 p.m. CT

Operator: Please go ahead, (Sean).

(Sean Cheadle): Good afternoon everyone and welcome to today's ACC Webcast presented by Jordan Lawrence and Guidance Software, entitled the new Federal e-discovery Rules, How Your e-discovery, e-records Management Practices Should Be Revised for Compliance.

Today's program will last approximately 50 minutes, which should allow some time at the end for you to ask questions of our presenters. And you may submit these questions through a chat box down in the lower left panel of your browser. You can enter a question at any time throughout the program by entering the text, and then clicking send. These questions will be addressed towards the end of the program.

You may also send questions to an e-mail address entitled questions@jlgroup.com, that would be handled by the Jordan Lawrence Group, of which we have a speaker here today. You can send those both, during and after this presentation. The presenters will attempt to

get all of these questions today, and we'll be able to follow up even after the program with answers.

And my name is (Sean Cheadle). I'll be the moderator for today's program. I am in house counsel at (Telladyne Cougar), reporting to our corporate parent, (Telladyne Technologies, Incorporated). (Telladyne Technologies) is a leading supplier of sophisticated of electronic components, instruments, communication products, and serving aerospace, defense, marine and environmental markets. (Telladyne Technologies) is the parent corporation to over 30 independently owned, operated subsidiaries, for which I serve as the program manager for (Telladyne's) enterprise wide records management program.

At (Telladyne) in 2002 we initiated an enterprise wide records retention policy and retention schedule for approximately 17 business functional areas. This policy brought all of our companies on to the same playing field, but we were still left with the daunting task of how to enforce the policy and the retention schedules. That's when we discovered Jordan Lawrence and it's enforcement solutions Web based tool, a robust software designed to allow companies to issue destruction notices, and legal hold notices to all of its users, nationwide and worldwide, which ensures the users log in and act upon the requests.

Our mantra at (Telladyne) has been records retention really means records production, whether for audits investigation, litigation, companies must be able to produce the records requested through discovery. There is a presumption that if you can't produce, then you haven't really retained. This production means – becomes extremely troublesome when they discover a request for electronic records. And under the new federal rules, we all need to counsel our clients in the best practices, to help our companies reach a safe harbor. Today's

program will help us all better understand how to counsel our clients, and preparing for e-discovery under these new rules.

A few reminders, again, the program is being recorded, and if you have trouble logging in, or any other technical difficulties, again, please e-mail ACCWebcast@commpartners.com as you see on the screen. COMM Partners is commpartners.com. Again, you may ask questions through the chat box. And I want to remind you to fill out the Webcast evaluation form which you can find on the links panel, about midway on your browser screen on the left hand side. If you just click on that number one Webcast evaluation, it will pop open a new window, which is an entry form, an online entry form.

Now I'd like to introduce you to our speakers of the day, (Jeff Hatfield) and (Patrick Zeller). (Jeff Hatfield) is Senior Vice President of Compliance strategy at Jordan Lawrence, and plays a key role in helping companies establish and enforce legally defensible corporate records programs, covering all records platforms. (Jeff) joined Jordan Lawrence in 1994, and has since worked for senior management at over 300 national and international companies, assisting and developing and implementing high impact records controls solutions and systems.

He is an accomplished speaker, has been published in numerous trade publications and conducts seminars for general counsel, information management, audit and compliance groups. (Jeff) is a member of the Sedona conference, a non profit research and educational institute dedicated to the advanced study of electronic documentation retention and production. (Jeff) has more than 12 years experience as a records management executive. Prior to joining Jordan Lawrence, (Jeff) was an executive with the Federal Reserve Bank of

St. Louis responsible for the design and implementation of securities and item processing systems. (Jeff) received degrees in finance and engineering from the University of Missouri, Columbia, the University of Missouri, (Rolla) respectively. He also holds an MBA in international business management from St. Louis University.

(Patrick Zeller) is Guidance Software's assistant general counsel. Prior to joining Guidance Software, (Zeller) practiced litigation in the Chicago office of (Safe, Arth, Shaw), where he co chaired the firms electronic discovery task force. His practice primarily involved commercial litigation with a strong emphasis on i-technology issues, and electronic discovery.

(Zeller) previously served as an assistant attorney general, and director of the Computer Crimes Institute for the state of Illinois, where he prosecuted a wide variety of crimes involving sophisticated technologies issues, and supervised a multi jurisdictional computer forensic laboratory. During his time, he was named a computer crimes fellow by the United States Department of Justice, and served as a trial attorney for the department's computer crime and intellectual property section, where he prosecuted and advised prosecutors and law enforcement agents on Internet and high tech criminal investigations. (Zeller's) experience also includes lecturing on Internet and high tech crimes at numerous law enforcement training being used nation wide, including the FBI academy. He is widely regarded as one of the leading mines in the emerging field, and his specialties include e-discovery, internal investigations, computer intrusion, economic espionage, online fraud, intellectual property and trade secret issues.

Mr. (Zeller) is an adjunct professor of the John Marshall Law School's Information Technology and Privacy Law LLM program. His class topics include computer crime, information warfare, and economic espionage, and e-discovery, computer evidence, and computer forensics. He also holds several certifications in computer forensics.

As you may know, the Federal rules of civil procedure have been revised especially with respect to e-discovery rules, and these changes will take effect later this year. (Jeff) and (Patrick) will discuss these rules, changes, in how to adjust your company's internal electronics record management systems, and electronic discovery practices to meet the rule changes. As with Sarbanes-Oxley and exporting, non compliance to modern e-discovery requests can result in substantial penalties and damages and litigation. Today's program is really your first line of defense.

At this time, I'd like to turn the program over to our first speaker, (Jeff Hatfield).

(Jeff Hatfield): Thanks, (Sean). And thank you to everyone for coming to our Webcast today. I think everyone appreciates the urgency of this topic, and as (Sean) said, today we're going to talk about how to make some concrete adjustments to your company's internal electronics record management systems, and electronic discovery practices, in order to meet these rules changes.

The information covered today will help you prepare for the rules amendments, and specifically to be able to take advantage of the Safe Harbor Provision. My job today is provide you with some actionable ideas that can be put into place by mid October so that you can be better prepared at your company. Now, the new amendments now incorporate

electronically stored information under the same standards that have long been applied to other media. And companies must have demonstrated consistency in their processes for properly identifying, for managing, protecting and destroying records of all types. And it must be as part of their normal course of business.

So today, I'll provide you at a high level with some very practical steps that could be completed within just a few months. And following, my presentation, (Patrick Zeller) will go into more details about the amendments.

On December first, the updated Federal rule of civil procedure take effect. These amendments really make it critical for companies to establish or update their corporate records policies. And more importantly, ensure they are consistently applied and executed. Companies will need to have consistent management practices. They must be able to convincingly prove that they properly retain records, that they can enact hold on records when required. And that they dispose of records under a sensible and routinely enforced set of rules. The Safe Harbor part, under sub section 37F means that companies who can demonstrate that they have consistent and diligent processes for managing and protecting their records, are going to be in a much better position than those who can't. Unfortunately, however, based on our 2006 survey of ACC members, and based on our own work providing assessments for records initiatives, we found that more than 80 percent of companies are no where near where they need to be. And these lapses in records management will become the killer legal strategy that these companies will have an incredibly difficult time defending again. And generally, aren't even aware where the problems are.

Now, while companies are struggling to prepare themselves for the rules amendments, they're also dealing with the related issue of the sky rocketing costs of e-discovery. Now, to truly reduce e-discovery costs, you need effective technology. But you also need to have a very comprehensive understanding of the records you retained. You need to have the critical metrics regarding records, again, on all media types.

Also, with the abundance of technology available today, many companies are faced with complex decisions regarding records related solutions. In fact, many companies suffer from solution confusion. Intuitively, you need to under the problems that you're trying to solve with technology, before you can actually deploy technology. So again, you need to have the facts regarding all of your records.

So these factors really drive home the reality that these issues demand attention, not only from legal but from the collective senior management team. Records retention, discovery, proper destruction practices. These have all landed in the direct view of the courts and the investigators, and of course, your adversaries. Exploiting these deficiencies and inconsistencies can translate into settlements, sanctions or fines and penalties.

Being prepared to meet the new rules means meeting very straight forward requirements. These fundamentals have always been present for sound records management and risk mitigation. But the new amendments have made it more critical to have greater knowledge about your records, and have greater consistency in your processes. Meet legal obligations and to reach the protections as offered by the Safe Harbor Provision. Companies need to ensure that they maintain records long enough to meet any regulatory requirements. And they must ensure that records are quickly accessible throughout this period of time. And

now, under the amendments, companies must understand the processes that manage the records and their information.

Also relevant to 37F, they need to certain that legal holdovers can be immediately legally and precisely executed. And that the needed records are appropriately collected and prepared. Finally, they must be able to demonstrate that records are systematically, non selectively and properly destroyed. Now meeting these obligations does not have to be as daunting of a task as many companies believe, but you have to know where to begin. And the logical starting place is to perform an enterprise wide assessment of the company's current state and related to how you manage records.

Now such an assessment should collect and analyze deep knowledge about current policies, about your procedures, about your practices related to your company's records. And it should lead to understanding what records are actually held, what are the appropriate retention and disposal practices. And what is the best use of technology, especially in regards to how you manage things like e-mail and e-discovery.

So let's take a deeper look into the types of information that should be gathered in an assessment. Better information leads to better decisions. Better information leads to better prioritization. And better information will lead, in some cases, to abandoning legacy ideas, old processes, even vendors and services that no longer are the most appropriate use of your time and money. Within six weeks, your company should be able to extract, what we call, its record type DNA. This means literally, that you will know every record type held, all of the related descriptive information, all of the facts about usage patterns and various other metrics. At a macro level, your assessment should include gathering and analyzing and

benchmarking information about your records for four primary areas that we call record type tagging, facts and metrics, media and application and people.

You must learn who uses each record type and for how long and for why. And which records are common subject to litigation and to audit, and for other outside uses. You need to gain information regarding which media types are used, including electronic records, e-mail based records, paper records, digital images, and so on. Along with which records are redundantly maintained, and are, thereby driving up your costs and your risks throughout the company. Additionally, when we conduct this type of assessment, we found a lot of value in looking what other organizations are doing, regarding regulatory tagging issues that effect things like retention, rapid discovery, privacy, secure destruction, and other similar requirements.

So this type of internal knowledge and benchmarking information that leads to better compliance, and this is what leads to corporate governance. It provides you with the ability to build your rules that meet the requirements of these new amendments. In regards to the amendments, it's also critical – it's critically important to look at any planned initiatives around new technologies. You can't go to the meet and confer sessions without accurate knowledge of your IT processes.

Also, in order to get the sufficient data and adequate perspectives, assessment participation should certainly include records users. Those are the front line individuals within the business that work with records day in and day out. But you also need to have the perspectives of senior management, senior management who, for example, have knowledge about future IT initiatives, and other individuals with specific subject matter expertise,

including those who are responsible for litigation and those who manage specific IT applications.

This is the information you'll need to have in order to adequately find and produce needed records. This is the type of knowledge the courts are going to expect you to have. And this is the information that you absolutely have to have, in order to ensure that you're able to protect your records and your data.

So preparation for the new rules means that companies need to take an objective look at what's going on. Some things that used to make sense probably don't any more. And in order to truly revise your e-discovery and your e-records management practices for compliance, you should be prepared to abandon some old ideas and processes.

For example, the over retention of records is, in many cases, at the very heart of the real world records related problem the companies face. The amount of electronic information that companies maintain is swelling at exponential rates. And this over retention of records generally stems from a few specific causes.

For example, companies simply don't have adequate standards and records management processes. It's seldom that a company's record practices are an actual extension of their policy. There's often tremendous inconsistencies across departments, and across lines of businesses, and across media types. Policy is not connected to practice.

Or many times, it's more of a conscious decision by companies, realizing they don't have adequate controls, and fearing they might not have a record that they need, they're keeping

way too much stuff, and they're keeping it for way too long. Or it could be a due to a vendor's influence. Influence by vendor's who's business models benefit directly from the company (over retaining) records. Now any of these can create enormous problems in terms of costs and efficiencies and compliance. But the notion of keeping everything to be safe, and to ensure compliance, often makes it impossible for companies to comply with records management obligation. And it can expose your company to unnecessary risks and costs, at a very minimum, over retention makes it increasingly more difficult to demonstrate consistency.

When we advise our clients when they are considering vendors that will provide them with records related services like records storage or e-discovery, we advise them to carefully consider the potential vendor's business model. Does the more volume of records or information your company retain have a positive financial impact on the vendor? Is their fee structure related to volume? If so, we recommend and counsel our clients to proceed very cautiously. And we can provide additional examples for anyone who wants to contact us. So again, preparation is about figuring out what works, and what doesn't work.

It's also about getting parties talking in the same language, headed in the same direction and doing it as fast as possible. You must have the combined efforts of legal and IT to explain and to defend your practices, and to be able to clearly demonstrate what records are retained and why?

But perhaps most importantly, your assessment must lay out the roadmap for which initiatives must be considered and approved, all based on your needs for reaching safe harbor. Unfortunately, time is not on the side of many corporations right now. Information

collection needs to start fast, it needs to get finished fast. And any gaps must be filled quickly.

So what do you after 45 days and you've completed this assessment? At this point, you should have gathered information from hundreds of participants, and you've probably collected 20 or 30,000 different data points and insightful knowledge about your current corporate records practices, about your plan initiatives and about the details about your hundreds or maybe even thousands of record types.

Now you're really well positioned to make the policy and practice updates that are required to meet the new rules. You're able to put processes and standards in place that really work and are taken seriously and are complied with in your normal course of business. And with this deep record type knowledge, you can easily apply your retention schedule to every record type maintained, regardless of the media that they're held on. You'll be in a much better position to make measureable, operational and financial impacts on your company.

For example, in many instances, over 75 percent of the electronic records are unnecessarily retained. And we also know that typically, 50 percent of paper records, and a significant number of backup tapes held at offsite facilities are all obsolete. And they have no regulatory or operational reason to be retained. This is a serious waste of money but most important, it's a serious risk and litigation.

So what's a solid process and sensible record naming and retention practices that are applied and enforced, these volumes of obsolete records can be drastically reduced, and it's good practice, and it's just plain smart to complete this type of clean up of old obsolete

records, keeping in mind any obligations that you have, such as legal holds. Also your decisions about initiating, changing or upgrading technology can then be made with facts and not opinions.

And perhaps most importantly, your policy intentions, your required capabilities and related obligations are well positioned for strict enforcement, just like any other corporate policy. Consistent enforcement of your policy is the holy grail, but it can't happen without factual, comprehensive information first. And this information will take your company all the way to the point where you really want to be, within safe harbor.

Keeping in mind the end objective of consistent enforcement of policy, we concentrate on analytics and information about compliance issues, legal issues, media solutions and technology issues, even operational issues. This information is benchmarked and best practiced, so that our client has actionable information, along with a very clear direction.

So at this point, the heavy lifting has been done. And with this information, it can often make sense for you to bring in your outside counsel, for example, for a review, or to ensure that you're adequately prepared for these amendments. You're also now ready to make good decisions about technology. And there's a lot of good technology out there, technology that can be very effective in helping you achieve compliance, as well as meeting other critical business initiatives. In fact, we spent a lot of time on this and have identified a few select companies that provide solutions in this area, and we refer to them as being enforcement certified.

Next, I'd like to share a quick example of some of the insights gained from some recent assessments. This is only a small, simple portion of the data collected but for these clients, the resulting actions were hugely beneficial. This is a small group of recent clients. The assessment that was done, the assessment for records initiatives, uncovered the number of unique record types for each of these clients, of course, but then some more interesting and variable (surfaced).

For example, the first client listed had more than 1800 unique record types, but they were actually retained over 5,000 record types. This means that many of those record types were being held in duplicated versions and often on multiple media types. What we found was that this level of redundancy was the major contributor to their inability to identify, to produce, and protect records effectively, when they were needed in discovery.

You'll also notice this company's distribution of electronic records between IT areas and users, for example, employee controlled applications, like Microsoft office, or similar software. With this information, and the supporting details, this company is now better prepared to look at, possibly migrating and fully controlled records to more formal processes, to help reduce the amount of employee discretion related to employee controlled records.

I also want to focus your attention on their e-mail findings. Of all of the countless e-mail communications, this company processed each week, their assessment identified over 400 valid business e-mail record types, along with of course, the junk e-mail and non essential e-mail communications. But now, they're taking these true business record type categories, and are preparing retention standards, that now comply with their real obligations. They're

doing this rather than the previously, arbitrary 90 day retention for all of the e-mail that no on complied with anyway. They'll keep that 90 day time limit for the non business e-mail communications. But now, they're able to begin auditing for compliance, and consistent application of their policy.

So with the proper assessment information, establishing your policy and enforcement processes, even establishing record naming and retention standards, truly is a simple step by step process. And it's surprisingly uncomplicated and can be completed within weeks, or a few months at most. And this is probably a happy surprise for most executives.

Consistent application and enforcement of policy and enforcement across all records repositories is hugely beneficial, legally, operationally, and financial. And remember that enforcement happens when policy is connected to practice, and this needs to be expanded throughout your company as soon as possible.

The courts now –the courts will expect companies to know what types of records are held across the company and where. They expect companies to be able to preserve records and be able to produce them quickly. It's critical that you keep this information up to date, that you can retain records based on consistent retention practices, that you can access the records. And that you can enact legal hold orders for any record or for all of the records. And of course, the destruction is done consistently and on selectively.

So this leads to an obvious question, are you ready? If the answer is yes, that's great. However, an issue as important as this might deserve an objective audit, or maybe an assessment for validation. If the answer is no, then the next question is, what are you doing

over the next 120 days. This issue is pressing, and you can be prepared within the next few months. As an ACC alliance partner, we are obligated to provide real solutions to assist you. So I encourage you to visit our Web site after this session, for a special assessment offer for ACC member companies. It's a fast, cost effective, and a comprehensive way for getting ready for these rules amendments.

And that concludes my portion of today's Webcast. Now I'll turn over the program to (Patrick Zeller) from Guidance Software.

(Patrick Zeller): Thank you. As (Jeff) mentioned, my name is (Patrick Zeller). I'm assistant general counsel with Guidance Software. And I will be discussing electronic discovery and the amendments to the federal rules of civil procedure.

Specifically, I'd like to address the five major changes to the rules that call for a systemized approach to e-discovery. Before I address the federal rule changes, I'd like to briefly discuss the traditional e-discovery model, to provide a context to this process, which companies must adapt to comply with the new federal rules.

Next slide, please. The traditional approach to e-discovery is very disruptive and expense. It's disruptive because it's a very manual process, where each computer is taken from each employee and a bit, by bit forensic image is taken of each computer. The average laptop contains 40 to 60 gigabytes of electronic data. This includes many types of data that are irrelevant to a typical e-discovery case. For example, this includes the windows operating systems, help files, or the paperclip that seems to haunt many computers, machine files, or

dll files, essentially areas where users cannot save data or information. So they're rarely relevant to civil litigation.

Active user files on the other hand, may be very important. These are e-mail, Word files, WordPerfect, PowerPoint and spreadsheets that contain data and information saved by your employees that may be relevant to your litigation. This active user data is a much smaller universe of only one to two gigabytes of relevant information.

Next slide. Project based e-discovery is usually outsourced to consultants on an ad hoc case by case basis, and they're usually hired by outside counsel. There's huge costs to collect this data because it's a very manual and time intensive process. Costs for this type of collection can exceed 3,500 per gigabyte. Generally this work is ad hoc, because it's ad hoc, or done on a case by case basis, the IT department and records management is usually not included in the process. There are also issues of compliance with the new federal rules of civil procedure, because the company will not have an internal process to comply with the rules, and I will talk about this in some more detail in just a minute.

The business model of more e-discovery vendors is premised upon the assumption that the company that are providing services for it does not have a process. Expensive outsourcing is a symptom of this lack of process.

Next slide, please. The process based approach, on the other hand, involves a strong partnership with IT and the legal staff working together, which means for, you know, simply a better, more defendable process. There is substantial return on investment or ROI with costs of only $10 per gigabyte because it uses automated software to search and collect

relevant data, instead of a very labor intensive and disruptive manual process. The process is tied into records management and facilities compliance with the federal rules.

Next slide. The federal rules have been getting a lot of attention, because as (Jeff) said, they take effect on December 1, 2006, assuming Congress will not intervene and make any changes, and so far it doesn't appear that they will, which I think is some good news. There are updated definitions and terminology to specifically address electronic data. There's a new definition that was specifically created for electronically stored information. Everybody – it's also referred to as ESI. Now there's no question that relevant electronic data must be produced, preserved, and produced in discovery.

If most of your litigation is in state courts, don't think you're safe, because state courts will likely adopt similar rules fairly quickly. Sanctions will also nearly be automatic for failure to comply with new federal rules.

Next slide, please. The new federal rules call for a systemized process, and I'll discuss these five specific provisions in more detail. These provisions – you know, the overview of these provisions is that they call for systemized process. But specifically, there's a framework for early attention, a safe harbor for data destruction, which is some good news for companies. The section that everybody is referring to is need a file production with meta data requirements and I'll go into this in much more detail in a minute.

There's also some more good news that follows some of the existing case log, and that is the duty to preserve is narrowed to relevant data. And then, there's some – a little bit of bad news, what we're calling the doomsday scenario which could allow opposing counsels expert

to access your computer system, to search for data if a defendable process is not demonstrated.

Next slide, please. There's a clear theme of early attention, rule 1626 in form 35 present a framework for parties in the court, to give early attention to issue related to e-discovery. And this is good news for companies. The earlier counsel can address what data is relevant for litigation, the easier it will be for companies to preserve, search and collect the relevant electronic data. Also, for counsel, they need to be prepared at the rule 16 conference, to discuss ESI preservation at the onset of the case.

The next slide addresses the Safe Harbor Provision, and this has been betting a lot of attention because it also provides some good news for companies. Rule 37F states that there are no penalties for deleting electronically stored information due to routine operation of your IT systems. But there's an if, and it's, you know, it can be a big if, reasonable steps were taken to preserve that data. So there's two key elements here, if it's due to the routine operation, if you lose that electronic data to your routine operation, rotating backup tapes, whatever the scenario may be and you have good faith. Deleting ESI must be part of a routine operation and done in good faith, and you need to have a systemized framework for early attention like a litigation hold must be in place.

The consensus here is that good faith will only give you one bite at the apple, because once you're aware, that you've deleted electronic data, I mean you're covered, but you're only covered for the first time, the second time, you lose relevant electronic data, you could lose your good faith in a sense.

The next slide, this is what everybody is calling need a file production, rule 34B permits the requesting party to specify the form it would like ESI to be produced. The default is if parties can't get together and agree, the producing party must product the electronic data in the form that is stored on their computer systems. Usually that form is need a file, that's why everybody is referring to the section as the need a file production.

The key comments include that the form of production is more important to the exchange of electronic information than it is for hard copies of materials or documents. This ESI is normally stored in a searchable format. It should not produced in a form that removes or degrades the searchable features. There are several cases that address meta data and its importance in discovery, including the (Nova) case.

Meta data is usually defined as data about data. Examples of meta data include blind copies of e-mails, formulas and Excel spreadsheets, track changes and Word documents, and also the dates and times files are created and modified. I believe the practical result of these provisions is that non sophisticated plaintiffs counsel will be asking for meta data, and will be asking for need a format production, simply because it's mentioned in the rules.

Next slide, please. Some more good news, preservation is only require for relevant data, despite what plaintiffs counsel may ask for, and I think everybody has received some of those outrageous requests, asking a company to stop deleting all data in every format. There's really no way to comply with such a request, other than to shut down the company. The (Zubilake) decision discussed clearly that there's no duty to preserve every shred of paper, every e-mail document, backup tape, because such a rule would cripple a large corporation. And this idea is essentially codified in the new federal rules. It mentions that there should be

a balance between competing needs to preserve relevant evidence, and to continue routine operations critical to ongoing activities of the company. Stopping a party's routine computer operations would paralyze the company's activities. However, there's previously been no way to separate the wheat from the chaff at the point of collection without a systemized process.

Next slide, please. The (Zubilake) court's decision of a defendable process, Judge (Schinlin) and her opinion discuss the idea of running a system wide keyword search, and then preserving a copy of each hit of information for preservation. She advised – she also advised soliciting key word lists from opposing counsel, so they would not be able to complain later about what terms were being used.

Rule 26F in the upcoming changes mentions the example that parties may specify topics for such discovery and the time period for which discovery may sought. Section 26F in the notes, also sites to another section in complex litigation manual which is section 40.5, where it discusses lifts of subjects for consideration. Identifying the types of materials to be preserved, the subject matter, the timeframe, authors addresses, and key words. N case enterprise has the ability to search a company network to include e-mail, hard drive, a network space, using keywords, dates and times, file types and other search criteria to collect relevant data for litigation.

This is an example of how you can make the federal rules work in your favor. It's the ability to turn the tables from questions of whether you have a process to utilize your established and defendable process, to limit the scope of requested discovery.

Next slide, please. Rule 34A, what we refer to as the doomsday provision, as you may have been able to determine from the name, this is not necessarily good news for companies. Essentially rule 34A may allow opposing counsel's expert access to your company's network, for inspection and copying of electronic data. And this is the last thing you want as a company to have an expert running searches through your system. Although, at first glance, the rule might be as bad as you think. I mean the comments really try to limit the use of this rule. The comments state that the provision is not met to create a routine right of direct access to a person's electronically stored information, although such acts may be justified in some circumstances. There are some cases, courts have granted such access as this and cases of spoliation , or failing to establish a defensible process. On the other hand, courts have not allowed inspection where a company has a defensible process of being able to preserve relevant data.

If you were wondering how long it will take the courts to apply the new rules of federal procedure, I can tell you that the (Dippen Host) case applied the new federal rules back at the end of June. It has a good discussion. And again, applied, the rules, at the end of June.

On the next slide, this is to give you an example of a large scale e-discovery collection, where end case, e-discovery was used to search over 1,000 work stations, and desktop computers, a dozen file servers, with over 28 terabytes of total data were searched. We collected the e-mail files on the work stations, searched all of the user created data for key words and collected all of the responsive information. With a systemized process, this was completed in two weeks, with no business disruption, while the employees are working on their computers, this collection happens in the background, they don't see it happening. And this was completed for a cost of about $140,000.

With a non systemized process, where the work is outsourced to consultants, the estimate that this company receive for the same collection would take three months with extensive business disruption, and a cost of over $3.5 million.

Next slide, please. NK software is currently being used by the SEC, the FBI, the Secret Service, the FTC, a number of foreign and state and local governments. Because our software has been used since 1997, there are a number of federal and state cases that specifically reference the defensibility of the software. These cases include validation under both the (Daubert and Fry) tests regarding the validity of the software.

The next slide, please. The three key benefits of NK software include the ability to search and collect individual files and documents across a network in native format, while preserving the key meta data. And only NK Enterprise can do this. We can cull at the point of collection to vastly reduce the volume of data by collecting only potentially relevant documents, without disrupting operations. And the process is automated and systemized. The software collects and culls around the clock and scales to any size network.

And the last slide, please. Guidance Software was founded in 1997. It's the leading product for computer investigations. One hundred percent of our software was developed in the United States. We have offices and training facilities worldwide, and provide technical support in Asia, Europe and the United States. Our headquarters is located in Pasadena, California. We have 350 full time employees, and 40 full time software developers.

Is there a – there's my contact information. My legal department has recently completed a white paper on the federal rules. If you would like to receive a copy please send me an e-mail. My e-mail address is up on the screen with white paper in the subject line, and we'll see that you receive a copy. Thank you.

(Sean Cheadle): That's great. (Patrick), can you still hear?

Operator: (Patrick), please go ahead.

(Patrick Zeller): OK. Can you hear me?

Operator: Yes, you're on.

(Patrick Zeller): OK. I'm finished.

(Sean Cheadle): (Patrick), this is (Sean); can you hear me?

Operator: Yes, (Patrick) can hear you; (Sean), go ahead.

(Sean Cheadle): OK, there we go. Well I've been sorting through some of the questions, and I would like for (Jeff) and (Patrick) to address a few of these while we have time. Some of them are kind of grouped together, one is – and maybe (Jeff), you could take this question, are you aware of any requirements to maintain records of instant messages?

(Jeff Hatfield): In practice, I mean – I'll have to refer to (Patrick) in terms of what's come up in the courts and so on, but I mean absolutely. I mean if its containing information that's relevant that falls under any of the other types of requirements that a company would normally have, yes, absolutely. And the same thing with voicemail, and granted they're more difficult to control but those are types of information and could be looked at as different types of records that do have to be part of your program.

(Sean Cheadle): OK. And can you define for the audience, record types on slide 12, and elaborate on – well go ahead with that one.

(Jeff Hatfield): The record types in that example. Yes, any – you know, unique types of records could be things like contracts. It could be things like terminate employee files. Or what we see a lot of times in e-mail with our clients, or things like purchase order requests and approvals or family medical leave act requests. So those would all be type of – different types of unique record types.

(Sean Cheadle): OK. And for (Patrick), I believe this question would be for you, we've got a question on whether these rules changes would have any impact on ADR, such as arbitration and whether you think state courts are going to be quick to adopt the changes. And is there any international impact?

(Patrick Zeller): Good questions. A lot of that we're going to have to wait to see. The consensus is that state courts will be very quick to adopt. A lot of federal courts are all ready applying the rules, even though they haven't gone into effect. Usually state courts quickly adopt federal rule changes.

(Sean Cheadle): OK, great. And (Jeff) can you explain the, I believe it's on slide six, the verified legal hold orders?

(Jeff Hatfield): Sure. Being able to verify legal hold orders means that you can actually track and monitor what has happened. As is the case with most companies, when there's a need for a legal hold maybe an e-mail is send out, or maybe some sort of communication might be sent out, there's a few people in the organization that are suspected to have control over those types of records. Very seldom, do we find that there's an actual verification that that hold order was applied and enacted. So when we say verified legal hold orders we mean that the hold order has gone out to the area within the company or to the individuals and some sort of response, some sort of documented response has come back that indicates, yes, we are in compliance. We've received the instructions, we've carried them out.

And then, that helps you manage going forward as the matter continues to at some point, be able to look back and monitor what has actually happened in terms of these holds, what record types have been effected. So those hold orders can then be released, and those records can be put back into the normal practice.

(Sean Cheadle): Great. You also mentioned a 424 e-mail record type, can you define that?

(Jeff Hatfield): I think it was on the example we were looking at for the company, where we looking at the different types of records that they had. What we found with that company was they had, I think, I said over 400, I think the actual number was 424 types of business related e-mail. So again, back to what I said earlier, those might be things like purchase order

requests, or family medical leave act requests and verification. So those are just another type of record, standard record types that showed up on that example on that company's e-mail.

(Sean Cheadle): And could you recommend any guidelines on where do find retention periods? State courts or state laws don't always reference a retention period for some record type.

(Jeff Hatfield): Well there's – yes, I mean there's different sources, sometimes you have to go to the specific citations, perhaps. The thing that we have found is most – and there might be multiple requirements, so just because you find a state statute or administrative code that references, or retention period for a type of record, does not mean that that's the absolute best one that should be applied in your case. We have to look at a lot of different factors. And when you're looking at retention requirements, you should be looking at the federal state. You should be looking also at your tax requirements, your legal requirements. And a lot of times, just your basic operational and business needs. So all of these things have an impact on what types of requirements, you're adhering and what standards you're applying.

(Sean Cheadle): Great. And (Patrick), the second time you lose data in the same case, are you going to be held responsible?

(Patrick Zeller): The – I mean here the consensus is it's that first, you get one bite at the apple. If it's a similar, you know, set of circumstances and you lost data a second time, you're going to lose that good faith argument. I think if it's a new set of circumstances, it's a new issue, something different, you know, I still think you have some good arguments.

Part of the challenge here is we have to wait and see how the courts are going to interpret a lot of these things.

(Sean Cheadle): Great. And this is kind of related, let's say that you're new to your records management program in house, and you need to implement it quickly say in the next 90 days, where do you guys start? And what do you think the staff size would be required to support these goals?

(Jeff Hatfield): Well I'll take that to start with. I mean certainly, you start with some sort of assessment process like what we discussed today. That is what we have found has been beneficial for companies. When we work with clients, you know, our job is to provide assessments to set strategies, and many cases, actually develop entire records programs. We've found that, you know, a lot of companies don't even know where to begin in this case. So the assessment is an excellent point to start because you are gathering that type of information that you need. You're able to determine what initiatives are most important, where the risks are, where the costs are, and then how to proceed from there.

That's, you know, probably what I would recommend. Whoever is asking a question, if they want to talk to us offline separately, my contact information is up on the screen, I'd be happy to walk through this are more length.

In terms of the staff size, when we do assessments, you know, it varies. You know, like I said earlier, sometimes we'll have 100 or more participants for a company. And those participants range from people in senior management, subject matter experts as I described, the records users, maybe one or two people from each of the departments that have the

hands on day to day information about records. And that's who you're gathering this critical information from, and that's the starting point you really have to be at in order to build your program, so you have consistency, and you have enforcement.

(Sean Cheadle): Great. And I would ask a question of you guys, (Patrick) in particular, you mentioned meta data, can you define it, and can you tell us what types of cases you most see meta data being discoverable?

(Patrick Zeller): There's five or six cases now, maybe even seven that specifically addresses issues of meta data. And one of the – I think the best way to explain meta data, it's sort of imbedded information that travels with a document. It's a lot like track changes in a Word or WordPerfect document. So there's dates and time information, there's who created it, there's, you know, all kinds of information that's hidden in those documents. More and more people are arguing that the meta data is relevant. It's definitely an issue. It's specifically addressed in the federal rules. So I think we're going to have it – you know, it's just going to be an issue that's raised more and more in civil litigation, that meta data is important and needs to be produced.

(Sean Cheadle): Great. And I think a final question would be for (Jeff), are there samples available that you're aware for legal holds? You know, what kind of company communication would be considered sufficient?

(Jeff Hatfield): Yes, sure. I mean if whoever it is wants to contact me, again, separate from this, we can talk about that.

(Sean Cheadle): OK. That's great. I think we're running short of time. If there are continuing questions flowing in or if I have missed any, our panel will review those and get back to the floor, to the audience. I'd like to thank you all for attending and remind you to please fill out your Webcast evaluation under the links. I see some people are having trouble entering that, but tech support is helping you open that window. And there are the PowerPoint presentation is over there in the links box, as well as a survey of corporate records. So those are great resources. And thank you for attending today's program.

END