Webcast: Infusing Records Policy Into Technology
Date and Time: Wednesday, April 18, 2007 at 12:00 PM ET
Sponsored by: Jordan Lawrence
Panelists: Dan Cooperman, Senior Vice President, Secretary and General Counsel, Oracle Corporation; John Patzakis, Chief Legal Officer, Guidance Software and Alice Lawrence, Principal, Jordan Lawrence
Moderator: Sonia Cudd, Assistant General Counsel, McCormick & Company Incorporated

ASSOCIATION OF CORPORATE COUNSEL

Moderator: Sonia Cudd
April 18, 2007
11:00 a.m. CT

Operator: Just a reminder, this today's conference is being recorded.

Female: Please go ahead, (Sonia).

(Sonia Kudd): Thank you. Hello everyone. I'm (Sonia Kudd), Associate Counsel (with Business Secretaries McCormick and Company), and I welcome everyone to the webcast on using records policy into technology.

Before we get started, I just want to mention a couple administrative items. Asking questions: if during the course f the webcast you have a question you'd like to ask one or all of the speakers, feel free. You can write it – if you look in the bottom left-hand corner of your screen, there's a questions box. You simply type your question into there and hit "send." Also, we would like to remind everyone to please fill out the webcast evaluation form and submit that.

In today's challenging environment of heightened regulatory requirements and litigation risks, it's imperative for every company to have an effective records management program. Additionally, many, if not most, company records today are electronic. The combination of those two facts have made it imperative for legal and information technology departments of every company to work together to successfully implement and enforce an effective records management program.

Today, we have a distinguished panel of speakers that will discuss how to successfully infuse policy into the technology in order to effectively manage the risk of regulatory compliance and litigation risk. And it's my pleasure to introduce them to you now.

First, we have (Alice Lawrence). (Alice) is a principle of (Jordan Lawrence), a consulting firm focused on assessing, developing and enforcing corporate records policies and practices. With 17 years experience at (Jordan Lawrence), (Alice) is responsible for the executive strategies and implementation process necessary to connect policy to practice. She frequently speaks to legal and IT communities on managing records to mitigate risk while improving efficiencies. (Alice) also pioneered the development of the (Jordan Lawrence web-based enforcement Tool Enforcement Solutions). And (Enforcement Solutions) is actually something that we use here at (McCormick). (Alice's) presentation will provide a very practical action plan to create the foundation from which legal and IT can work to effectively address the challenges of records and information management. Additionally, (Alice) will provide insight (into) establishing a formal hold management process, a key part of any records management program.

We also have (Jon Pat Zachas) – (Jon Pat Zachas) with us today. (Jon) is a vice-chairman chief legal officer of (Guidance Software). (Guidance Software) is a developer of (Incase Enterprise), the leading software for (Enterprise E) discovery, collection, processing and record retention audits. In his current role, (Jon) employs his legal and technical experience in computer investigations and regulatory framework to help educate the market and support their customers on computer evidence and compliance matters related to computer security, electronic evidence discovery and corporate governance, all areas critical to company's today. (Jon's) presentation will discuss current law concerning records retention management, including recent case law underlining the importance of active policy enforcement and a defensible litigation hold process.

And last but certainly not least, we have (Daniel Cooperman), general counsel of (Oracle Corporation). As general counsel for (Oracle), (Dan's) responsibilities include worldwide legal policies, corporate governance, securities compliance, M&A, commercial licensing, intellectual property, employment law, litigation, patent law and legal support for all of (Oracle's) business units. (Dan) also manages the (Oracle) legal department and its compliance program and serves as secretary to the board of directors. This year, (Oracle) celebrates its thirtieth anniversary in developing technologies and applications to the best manage – to best manage and use their most invaluable asset: information. (Dan) will discuss some of the key challenges facing organizations today as it pertains to governance, risk and compliance and the importance of building solutions on a sustainable technology platform to address these broader challenges. Specifically, one of the areas (Dan) will discuss is around the management of unstructured information and the tighter enforcement of policy within content and records management. As all of us could agree, these are all critical areas for legal departments and companies today.

So without further delay, I'd like to turn it over to (Alice).

(Alice Lawrence): Thank you, (Sonia). From the number of participants on today's webcast, it's evident that our discussion focused on bringing records policy technology together is timely and of great interest. But many of you on the call are probably thinking, "We already have a records management policy. We've made huge investments in technology, so why are my servers still overflowing? Why is the discovery so disruptive to my IT department? And why can't I sleep at night?"

My role is the discussion today is to provide some framework and foundation from which legal and IT can work together to address these risks around regulatory compliance and litigation, while at the same time, delivering some real business value. I hope that by the end of our time today, the three of us will have given you a logical and practical path to follow and a realization that effective – managing of records and information is really within reach.

Let me give you a little bit of background to put some framework around the perspective of my thoughts. (Jordan Lawrence) is an objective resource for organizations that look to assess, develop and enforce policies and process around records and information management. The foundation of our thoughts and methodology is a compilations of statistical benchmarking data, best practices that we've accumulated through each client project. Our perspective is real world, not jaded by conflicting business – interests.

It's been said that you can't solve problems with the same thinking that got you into the problem. Since 2000, in the wake of (Arthur Anderson) and (Enron), attention to how companies manage their records, their technology – it's exploded. High-profile cases, increasing regulatory requirements fuel that fire. After seven years of hyper-attention to records and information management, our company is really getting their arms around these challenges. Judging from the continual flow of cases related to records management, most are not. The few that have, have tackled this from a different perspective.

The amendments to the (Federal Rules of Civil Procedure) make it essential for the legal and IT groups to work together. Specifically, counsel and IT must have an effective process for executing, documenting legal holds, and counsel is not expect to discuss how electronically-stored information is managed. You're both in need of what we refer to as a "(Rule 26 Data Map)." You quickly recognize that you both have a significant stake in the decisions and technology that's going to govern the records and information throughout your organization. In order to fulfill these objectives from the – from your unique perspectives, you need better information before you make the decisions.

Companies that are effectively addressing these issues have really started by capturing the critical information that's necessary to make effective, well-reasoned decisions about their policies, their process and their technologies. Approaching it in any other way, we believe, is putting the cart in front of the horse.

The first step is to understand, really, what are the record types in my organization? It's seldom that we find an organization that has universal agreement on what the record types are enterprise-wide. You need to understand who owns them, controls them, both from the official owner, the custodial owners. What are the applications that they reside in? Where do I find these records? You need to define the content, the value of the information. Does it contain sensitive information? Personally identifiable information? What's the reference value of this information? And then, of course, when can this information be deleted or destroyed?

We refer to this information collectively as the "DNA of records," and for our clients, we begin with an assessment. We collect this information from several different areas: senior management, subject matter experts that focus around content management, e-mail records, subject matter expert around litigation, the legal team that supports this effort in the event of needing to find records. And then, most importantly, we go to the business representatives, the folks that create – touch these records on a daily basis. On average in an assessment, we speak to over 130 people throughout an enterprise and collect about an average of 50,000 data points in just under 45 days.

Generally speaking, without looking at specific industries, your organization probably maintains roughly 625 unique types of records. A record type by definition in our world is sometimes referred to as a specific document or a form, like a – an application or a (1099), but it's often more logical groupings, like a benefits folder, a terminated employee file, a paid loan file, those types of things. Again, I'm sharing averages, but – you know, in more regulated businesses like financial services, you'll tend to have more. However, whatever the number of unique record types is, there is always redundancies, typically on a scale of four to one, four versions or formats exist in other platforms or systems throughout an enterprise.

The next step in the assessment process is to evaluate the contents of this information, tag you records according to this specific retention management disposal requirements that govern you. Specifically regulatory requirements like (FAFDA), (Gramleach Blyly) for financial services company, (HIPPA), Sarbanes-Oxley. Unfortunately, when organizations fail to collect this type of critical information and help use it to guide their decisions, it often results in poor choices. Additionally, without this information, it's virtually impossible to create a policy that becomes actionable by your IT department.

So what does this type of information mean for IT? With this level of detail, the results of the assessment give them the picture of where information exists in the organization and what they need to protect. Most organizations focus on protection of data around their HR records, that the personally identifiable information. Statically, we've seen 80 percent of records that contain this information actually exist outside of HR. Identifying where information's retained redundantly, where collaboration occurs. That enables IT to leverage some technology, eliminate the redundancies. And understanding of the true business value of records and information clearly give IT the objective knowledge they need for their information lifecycle management policies and things like that.

And finally, we find, you know, an average of over 50 percent of legacy information has no business or regulatory requirement to be retained. Shedding this unnecessary information translates into real hard-dollar savings of storage and management costs. It also means your systems are going to operate more efficiently.

So what's it mean for the legal department? The assessment value for them is – you know, it gives them the information they need to discuss in this (Rule 26) conference the data map of where information is, how they're going to preserve it. It enables legal and IT to tie together their parallel initiatives and objectives that occur in companies to marshal resources more effectively. The assessment will clearly draw out opportunities to reduce the sheer volume of records and information that's currently be retained. Proactively and appropriately disposing of this legacy information is probably the most significant action any company could take to reduce their risks and costs associated with discovery.

So at this point, your organization has this information. You've either updated it, supplemented or created a policy that's truly (optionable) by your IT department so they can do something with this information. The records and information management policy is now ready to be infused into the technology stack where it makes senses. Records and information classes have been defined. They've been mapped to applications they reside in. The content and reference value of the information has been defined. Naturally collaboration patterns that surround records can be leveraged.

Now keep in mind I said "where it makes sense." It's not – it may not be practical or even necessary to fully integrate policy into the technology stack everywhere. In other words, you don't have to try to tackle everything. We recommend you do an analysis, focus on the greater risk areas. You don't – but don't lose sight of the people. You can't integrate policy into human behavior like you can into software. But people in those lower-risk systems must be accounted for, and this can be accomplished by using policy-driven notices to business people as well as to IT representatives that are responsible for those systems.

For our clients, we provide a Web tool called "(Enforcement Solutions)" that acts as that central federation point to integrate technology to command the automated notices. This model of the central portal servicing as the central federation point, has really proven to be certainly the most practical, cost-effective way to infuse your policy into technology, but also a real logical step. This approach is system and media agnostic and can truly cover all record types across the enterprise, and most significantly, it's seamless to business people. We know if you try to implement or institute a new process or technology that requires your business people to re-engineer how they do things, you're going to seldom be successful.

Hold management is one of those requirements that a lot of companies overlook. When litigation investigation is reasonable anticipated, companies must have the ability to identify and secure relevant records. The inability to communicate (and an act precise) and documented legal holds on relevant records is at the heart of many of these familiar cases. Following the steps I've outlined, counsel will have a 360-degree view of the enterprise, understand what records exist, where they are, what media, what applications they reside in, who the owners are, who the custodians are. Leveraging this knowledge, counsel can then enact and immediate and verifiable legal holds that cover all users, all record types, all systems and all media.

Additionally, proactively going through this type of formal process should enable the organization to defensively dispose of obsolete records and information. Again, we find on average typically 50 percent of legacy records and information can be disposed of. Having half of the information you have in your organization today can really translate into significant collection and review savings if and when your organization becomes involved in discovery. And finally, of course, you need to keep your policy up to date.

Working together with good information, legal and IT can dramatically reduce (their) costs and risk associated for your corporation.

If you have any questions, as (Sonia) said, you'd like more case studies, please feel free to contact me at any time. I'm now going to turn this discussion over to (Dan Cooperman).

(Daniel Cooperman): Thank you, (Sonia). (Alice), I enjoyed that presentation, and I'll pick up on some of the themes that you struck.

First of all, before I begin my remarks about infusing records and information management policy into technology, let me provide a little background on (Oracle) to put my comments into some context. (Oracle) is the world's largest enterprise software company. We develop and support database, middleware and application software to help our customers manage and grow their businesses. We're just known, perhaps, for our database technology, which enables to storage, manipulation and retrievals of all forms of data but (were) not confined to the database. We provide a complete technology stack that includes our middleware solutions to enable customers to quickly integrate diverse business applications as well as software applications that enable efficient management of all core business functions, such as customer relationship management, financial management, human resources and supply chain management.

All in all, (Oracle) is a pretty complicated global enterprise. We operate in 145 countries with 87 operating subsidiaries. Almost half of revenues come from outside the United States and nearly 60 percent of all of our employees work outside the United States. So for the issues I'll be discussing this morning, records management and (e-discovery), having 87 operating subsidiaries creates a lot of places to look for records and imposes a myriad of requirements and considerations around how to manage our own records and information.

In the 30 years that I've practiced law, I've observed the significant evolution in the role of the general counsel. In the '70s and '80s, the general counsel was principally a legal advisor who provided counsel to senior executives, directed litigation and was a regulatory expert. In the '90s, we saw a stronger orientation to align the legal department to maximize (business/client) satisfaction and focus on managing outside counsel with a view toward cost savings. Today, there's a notable shift in the role of the general counsel toward acting as an activist general manager where we manage key enterprise-wide initiatives, such as records management, privacy and security, compliance and ethics programs and board governance. The reason I mention the changing role of the general counsel is to emphasize that it is the general counsel and the legal department who will often have to take the lead on issues that might once have been the province of the IT department.

Indeed, it's an exciting time to be a general counsel, but it's also quite a challenging time. In today's pressure cooker environment, corporate counsel and IT must be partners. Governance, risk and compliance management is the new normal. Since 1981, the U.S. federal government alone has introduced over 114,000 new regulations that affect businesses. And of course, in the context of how organizations manage their electronic records and information, few of these regulations have been as significant as the recent changes in the (Federal Rules of Civil Procedure). The 2006 Litigation Trends Survey from (Fulbright and Jaworski) shows and increasingly active environment for litigated disputes worldwide. The percentage of companies surveyed with over 50 pending lawsuits more than doubled from 2005, and among respondents from the U.K., that figure tripled.

It's not surprising then, that the 2006 (Benchmarking In-House Counsel Management Practices study) from the (BTI Consulting Group) shows that an average overall legal spending climbed yearly five percent in 2005 to reach $27 million. A typical Fortune-1000 company spent about $17 million on outside counsel and large legal departments directed over 60 percent of legal spending to outside counsel with more and more spending going towards the collection and review of records and information.

In this pressurized environment for corporate counsel, it's tempting to take a quick ad hoc or project-based approach to compliance requirements in general and to records and information management in particular, whether these requirements are mandated by external governing bodies or by a company's own internal initiatives. But to the point (Alice) made earlier, this type of approach to records and information management has not been particularly effective for organizations. Over the long run, as the number of compliance-driven projects increases, the cost and complexity of taking a piecemeal approach will escalate. This is because of the complexity of the interaction between mandates, regions, technologies and functions.

So for example, let's take compliance with the financial integrity regulation such as Sarbanes-Oxley. Requirements from this mandate flow across the different operating units around the world, affect processes that are underpinned by various IT systems and touch a variety of business process owners. In addition to a program to address the documentation testing and certification requirements, you also have to implement a program for compliance and ethics to ensure that employees are properly trained that whistleblower and hotline support is provided for all employees.

Another example comes from mandates such as California Senate Bill 1386, (HIPPA) and the (EU Data Privacy Directives) that mandate the protection of personally identifiable information. Other requirements like the Patriot Act also stress data privacy and protection but impose new requirements around anti-money laundering. So each mandate can and often does spawn a discrete response across different regions, systems and organizational functions.

An auditor or security officer or accounts payable manager may be called upon to perform duplicate tasks and provide duplicate information to address different mandates. Likewise, IT managers might be called upon to investigate and deploy multiple tools to address similar requirements. With a piecemeal approach, it is difficult to sustain the cost efficiencies as well as gain an overall understanding of the risks an organization faces. In the long run, we end up with complex and inconsistent processes that make it difficult to address the next new requirement that might come along.

To effectively address records and information management governance risk and compliance risk in general, corporate counsel and IT should consider taking a holistic approach. So many facets of governance are intertwined that an organization that looks at governance initiatives in their entirety and not as individual pieces will ultimately do a much better job of infusing policy into technology and leveraging technology to meet compliance and business objectives alike.

Specific to records and information management this, what I'll call a "platform approach," greatly enhances an organization's ability to manage information in accordance with policy and be able to execute verifiable holds when required to do so.

For the sake of time today, I want to focus specifically on the challenge of tying policy to unstructured data. What is unstructured data? Unstructured data refers to data that is not contained in (ERP) systems and therefore, does not have a structure that's easily readable or searchable. Examples include contracts, e-mails, voicemails, memos, Web conferences, data sheets, instant messages, planning documents, forecasts, sales quotes, et cetera.

The challenges of unstructured data are similar to those of structured data, but even more pronounced, given the exponential increase in the data volume and the larger number of systems involved. Most of these systems are controlled by individual departments, so IT doesn't have centralized control over policies and procedure, in particular, security and record-retention policies. Unstructured data is not easily searchable as data is typically scattered across hundreds of servers, and there is little (auditablity) of changes to different contents. It is no wonder then that (e-discovery) is a topic of such concern for companies today. In a 2006 survey by (Fulbright and Jaworski), the vast majority of firms, 81 percent, who responded reported being either not at all prepared or only somewhat prepared for (e-discovery).

My guess is that most organizations attending today's discussion already have some sort of records retention policy (and accompanying) schedule. When you examine the policy and schedule, you need to review several questions. Does it address unstructured content? Does it include detailed information that (Alice) discussed? Who owns and controls records and information both as an official owner and as custodian of the records? Does it tell you where the records are held and on what applications they're located? Does it define the content and value of information? Collecting all of that information is the first factor for success.

Once you have this information, however, then you need to include two other success factors into your program design. First, as I'm sure most of you would agree, not all everything is, or should be, treated as a record and, therefore, subject to formal records management policies. Second, and this is the (got you), while everything is not a record, everything you have is subject to discovery. So it's critical that you understand this difference and apply an aggressive retention and destructive policy – destruction policy to get rid of non-record information that provides no useful benefit to the organization just as soon as possible.

Given a records and information inventory and a definition of what is and what is not a record, legal and IT should develop a clear understanding of the organization's current technology infrastructure, clearly defined legal and compliance requirements of technology for records and information management. With this information, legal and IT can begin to build a sustainable and effective platform for managing records and information and improving governance in general.

So assuming that you're gotten through these three critical success factors, where do you begin to see the benefits? Let's take a look at how the discovery process can be improved.

This schematic illustrates the benefits of a comprehensive program that links policy with technology. By doing so, you reduce the volume of information and the associated cost and risk of the discovery process. Beginning with the complete spread of electronic information in your organization, you can characterize and classify it based on the assessment and inventory process. Note that this may include both unstructured and structured information, depending on how broadly you cast your net. So this first process establishes a smaller set of potential information.

Next, by differentiating between record and non-record information and applying aggressive retention disposition policies to the non-record information, you further reduce the information available for discovery. You've kept only what you wanted that has value to the business, eliminating anything outside that definition.

Next, by ensuring that the records-management policies are communicated as part of an overall program which educates both the authors and the custodians, you're able to take advantage of the normal disposition cycle, (and an effective) way to place holds on information to avoid allegations (of spoliation) and more management.

And finally, you're left with at more reasonable set of electronically-stored information to review and potentially present to court.

This infusion of policy into technology enable the organization to consistently and non-selectively enforce policies across all contents, whether it's structured or unstructured. Counsel will know what information they have and be able to defend why they don't have certain information by demonstrating the consistent execution of a records and information management policy in the normal course of business. Counsel also will have the ability to suspend normal destruction cycles when required to do so.

For our colleagues with an information technology focus, here is a high-level view of the technology solutions side of the connection. At the bottom of the diagram, we see the various sources of electronic information that can be subject to discovery. The universal records management application becomes the central policy management solution that supports all aspects of record and retention requirements, including the ability to group or federate the source systems, control both electronic and physical records, issue and monitor notifications to custodians and users and support efficient discovery.

I'm hoping that this has spurred some of you to begin thinking that creating and executing a program like this is really doable within your organization. Putting together a program is doable, but it isn't easy. As someone who's doing it right now, I can assure you it takes a commitment to get it done. You need to make sure that you have the support from your lines of business since they know where everything really is, your information technology executives since they will be required to create and operate the supporting systems and your finance, legal and compliance organizations to make sure that everyone knows the risks and rewards of the program.

So the question becomes how can you increase your chances of the getting the necessary commitments and getting the job done in a reasonable timeframe at a reasonable cost? The answer is to take advantage of those who've done it before. There are experiences that you can leverage to accelerate the program's success. We've talked about a number of these so far today, but here are a few key take-aways.

First, capture the critical information from the right people. You must make sure that you do the inventory correctly, otherwise your downstream decisions are filled with uncertainty and risk.

Second, apply retention policies to all content across multiple repositories, not only records. You need to create a culture to assess, retain and dispose of everything in the appropriate time.

Third, don't keep what you don't need. This will stretch your IT budget and reduce your discovery costs. (Alice) mentioned that in her experience, over 50 percent of information currently stored is not a record and not required by the business.

Fourth, apply policies consistently and universally. Under the (Federal Rules Amendment), a good policy that isn't enforced might as well just not be there.

Next, centralize policy administration and disposition processing through a central federation point, reducing the chances that holds and releases are missed and that you've inadvertently failed to apply your policies properly.

And finally, apply legal holds promptly and universally to minimize user disruption. Regardless of the size of an organization, the business process continues in the face of litigation, audits and the like. As soon as you suspect and issue's come up, you need to trigger the notifications and do so in a manner that supports the normal business flow. And remember, a program like this or any similar program really isn't worth a darn if you can't show that it operates in the normal course of your business.

So to summarize what we've discussed, first you must have the critical information needed to make well-reasoned, well-informed decisions about policy, process and technology around – around records and information management. Second, a piecemeal approach to records and information management and governance in general will only lead to more complexity inconsistent processes and lack of visibility over the long run. And third, the key is to simplify. Look for the common requirements and see if there's a way technology can aid you. With a platform approach will come increased security, a better way to handle content, both structured and unstructured content and reduce risk while building business value.

And so with these final considerations of knowledge, vision and technology that are shown on this slide, I'll now turn it over to (Jon).

(Jon Pat Zachas): Thank you, (Dan). So my portion of the presentation is going to talk more about some of the details in the law around records management and as well as (e-discovery) litigation holds, specifically, the importance of enforcing existing policies, something that (Dan) alludes to. We need to establish the objectivity of these policies and that they have a proper business purpose. So we'll see how active enforcement is a key aspect to accomplishing that.

Second, the need to execute timely, effective litigation holds. Really a key part of the records-management process is an effective litigation hold process. We need to establish the (defensiveabilty) of these policies and processes (and) litigation hold mechanisms are critical to doing that to show that they're utilizing good faith.

And finally transparency, both of our records retention destruction policies as well as our litigation hold process policies. We've seen in recent months, especially since (the Federal Rules) have gone in place, a number of courts that have issued several decisions regarding the process scrutiny. (These courts) are looking at what the (e-discovery) litigation hold process (that these) companies have, what their records management policies are and the – having these processes established, documented with a good reporting mechanism is the key to defending those policies.

So in terms of some recent developments in the law in this area, you know, in the (e-discovery) realm, you hear a lot about the (Zubilick) case. In the records management realm, the (Reamus around) this case had a lot of importation developments and nuances and (geared) guidance around (defensibility) of records management policies as well as areas where a company – the pitfalls for a company that will be subjected to sanctions if those policies are not applied routinely and effectively.

(In the Reamus around this) case, the company established these annual purge days that were done annually or semi-annually at the company where the employees were directed to put a day aside and to dispose of electronic records and other documents in their possession. The problem with that is these purge days seem to be coincidentally tied to pending litigation matters. So they certainly were – was not a process – certainly not the kind of process that (Alice) talked about and (Dan) talked about that was ongoing, systematic and routinely applied. And that's what the court found, that these policies – or procedures that (Reamus) put in place at the time, where (certainly) not defendable, (they were not systematic).

The second problem with those policies is there weren't documented, so these – end custodians were asked to basically purge their – the records they didn't need, but there was no documentation around it. The court wasn't able to determine what the records were saved, why decisions were made, and again, that's a key aspect to (defensibility), you know, to be able to show the parameters for why these record – these policies were carried out and what the decision-making process was.

The key element of having a policy in place is that you do have that – that (defensibility), you do have that transparency which documents the effectiveness and the consistency of those policies.

And then finally, the third key aspect is, again, executing proper litigation holds. The (Broccoli versus EchoStar Communication) just one of many cases which specifically provides that when you have an ongoing policy, that must be (overridden) by effective and timely litigation hold.

The one aspect I want to talk about the (Federal Rules) today is the so-called "Safeharbor Provision" – it's not actually referred to as to "Safeharbor." Some refer this as a "lighthouse" or "guidance" on how to avoid – potentially avoid sanctions under the (Federal Silver Cedar framework). So there are certainly caveats in terms of the limited effect of the Safeharbor (applying) only to the (Federal Rules) and not to common law. But those caveats aside, what's interesting about (37F) is that it really is more of a records-management focus on the (Federal Rules). And see here the convergence of (both e-discovery) and records management, and (Rule 37F) is really the key area we see that convergence.

There's two important elements of – (37F) in order to invoke its protection. One, you must establish that any efforts to destroy electronically-stored information, or ESI, must be pursuant to the routine operation of IT systems. So again, what (Alice) talked about establishing a process, that is key to establishing the routine operation, but there are cases specifically mentioning that applying a records-management policy is defined as routine operation by the courts, which then would apply here to (37F).

And then, the second element in the good-faith element. If you look at the actual text within the comments to (Rule 37F), good faith really is talking about the litigation hold process. So if you have a process that is applied evenly, routinely, it's enforced on a routine basis and there's a very effective litigation hold process in place so that – that the data's preserved, really, at the outset of litigation. Then you'll potentially will be able to invoke the (Rule 37F) Safeharbor.

And, you know, there's also an interesting aspect of – (we've seen that Safeharbor) has addressed the issue of litigation holds almost as if there is a inverse correlation, meaning that if the data – if there isn't a litigation hold process, then there's going to be even more scrutiny, you know, of the company's processes and sanctions (will be) much more likely. And we see that in some – some recent cases that implied, around the time (the Federal Rules) come in place, or actually (post-Federal Rules), and we see a lot of courts that are looking hard at a litigation hold process. Was there one in place? What was the efforts done at the outset of litigation or when the duty to preserve kicked in to preserve this data in a systematic fashion? We see in the (NTL) case, the court heavily securitized the processes or lack of processes that were in place. It found that, in reality, there was no litigation hold process at all, which resulted in sanctions.

(Samsung Began versus Rambus) – that also discussed the litigation hold aspect because the company there was trying to both purged its data (pursuance) policies while preserving relevant information. And what the court, both in the (Rambus) as well as the (Wachtobers Health Net) case – what both courts really kind of criticized was the constant custodian self-collection where the custodians were just (asked) to preserve the relevant information. And in the (Samsung) case said basically that kind of token effort is not going to suffice. The same kind of ruling in the (Health Net) case. So we see courts really putting a lot of scrutiny and carefully looking at what not only litigation hold process was, but how that process was executed by the companies in the context of litigation.

You know, another case, also very notable, that addresses or (is caught in one) of these process-scrutiny cases is recent case of (Pescoff versus Ferber). And you look at this paragraph and it's where the court is talking about – there is a discovery motion where the plaintiff was alleging that the company didn't do a adequate – didn't utilize adequate efforts to preserve the data in the face of litigation. So what the court says is that they're going to schedule a subsequent hearing, and at that hearing, the company (will then) come in and essentially (defend) their process. Court wants to see what was done in the face of litigation, what the search criteria that was applied – basically it wants to see whether the company had an adequate process not only for putting the hold in place, but executing on that hold and actually preserving and collecting the data. So at this hearing, the defendant will really need to establish a defendable process.

And you know, one question I often get is "What does that involve?" Well, it certainly involves best practices technology. Another question related to that is "Does this mean that you need to outsource everything or can this be done, as (Dan) alluded to, with a strong relationship between IT and the legal department?" And I think absolutely that that is, I think, in many ways, the best practices. When you have IT that is closely working with legal and they have the right tools, the right technology in place, they have the right training and this is a preset, throughout process, that actually is a very ideal situation because your IT department understands where your data is. There are so many nuances to a – a corporate network, so many complexities, and there's no one better than your internal IT staff, again, with the right training, right technology to be able to go out and collect that data to timely execute litigation holds.

This is really critical and (lies) a new set of rules under (Rule 26F), which basically requires early attention to (a discovery). This is no longer a reactive process. This is something that really needs to be tied into your records-management systems and your records-management processes so that timely, effective litigation holds can be executed. And we see that being done when legal and IT are on the same page with the right technology and right processes.

So once the duty to preserve is established and the interplay with your records-management systems, sometimes people, the reaction is to panic and say, "Wow, we got to go out and just save everything and collect everything." And one thing that strikes me in reviewing this area is that, you know, law's pretty clear that the duty to preserve evidence only applies to potentially relevant data. So there's no duty to collect everything. There's no duty to – to incessantly stop your – your backup recycling systems. No duty to get hundreds of full-disk images of every custodian. And this is not only (reflected in Zubleg) and other cases, but also in the (Federal Rules). If you read the rules, especially under the comments sections, talks about the need – the duty to preserve relevant data to execute preservation efforts that are narrowly tailored. The (Rules) also incorporate that (manual) – a key (area to manual for complex) litigation, which recommends a process where – where specific custodians are (collected from), using specific key words, date ranges, file types all which really talk about a very narrow and targeted collection process. So – and again, these other cases too. And we talk about there's plenty of legal support. (FlexAmercia Trepp) was a very important case talking about targeted search strategies.

And -- the caveat though, is that in order to accomplish this, there has to be a good process in place. Over collection, we see a rising in situations where there's not a process, where IT doesn't have the tools and hasn't really put a process in place to begin with and just goes out and takes a broad stroke or having consultants parachute and getting – having to get full-disk images because there's no other way for them – they only get (bite of the apple) -- that consultants. Again, that's one of the limitations of the process. But where you have a process for litigation holds in place to collect the data with best practices enterprise technology, you're able to go out and actually (cull) the point of collection, run more targeted collection efforts across your various data structures and resulting in a much more efficient process. You remember that (funnel) slide that (Dan) had. That's key is that when you over-collect, the funnel becomes far too wide. If we have a good process in place, you're able to narrow the collection. Then – with good technology, then you're going to bring more efficiencies and less cost to the process.

So a little bit about (Guidance Software). We're an enterprise software company based in California with offices around the country, and we are the leaders in computer forensics software and also enterprise computer investigation software. We address, on the enterprise level, (in-case) enterprise enables us to search and collect from any computer connected to (wide area networks), such as desktops, servers, e-mail (storers). And our area of specialty in the enterprise is addressing the (unstructed) – unstructured data on (a distributive) basis. You saw that slide from (Dan) talking about – how 70 percent of the – of the data in an enterprise is unstructured, and that is really the area of focus for (Guidance Software) and (our in-case) enterprise (e-discovery) collection of processing software. We're able to search and collect that undistributed data – that unstructured data across the enterprise. It's applicable not only for (e-discovery) collections and processing, but also for internal investigations and also records retention audits. We can search thousands of computers in a short timeframe to identify violations of policies as well as to enforce records-management policies.

And finally, one of the key benefits of (in-case software) is that because of our legacy of servicing government, law enforcement, corporate security consultants, there's been literally tens of thousands of cases that have relied upon the (in-case software). Many of these have resulted in that case law where the software (has been vetted) both the law enforcement and (e-discovery) cases, so this translates well to a defendable process for utilizing this technology in the corporate environment for compliance purposes.

For my (contact information), kind of did an overview of the law. And – but we have – a couple of white papers which go into the – areas more in depth, so if you want a copy of our white paper on ("The Law Around Records Management Enforcement") and the importance of that as well as ("Best Practices for E-Discovery Collections in the Enterprise"), you can e-mail us at (legal@ncase.com), and these are some of the other references we have for some key resources that we utilize extensively at (Guidance Software).

So with that, I will turn it back over to (Sonia).

(Sonia Kudd): Thank you, (Jon). With – we have a few minutes left, and we'd like to go ahead and address some of the questions. Just so everyone listening in knows, all of the Q&A will be posted by next Wednesday, April 25th. Along with the replay of the webcast, there'll be a handout which will include all of the Q&A. So to the extent that we can't get to everyone's questions in the next few minutes, know that your question will be addressed in that handout.

First, (Dan), if – this question would probably be best directed for you. "Have you identified tools that help your company move away from piecemeal and towards a more holistic approach?"

(Daniel Cooperman): Well, I think the key here really identifying the components of a – what I call a "the platform" – (the platform), and moving away from the reactive approach to individual regulations. The way to do that really is develop systems ((inaudible)) management and identity management being sure that the appropriate (access) controls are in place within the company. And then with respect to structured and unstructured data ((inaudible)) capability in a repository to read and search (that data), again whether it's structured or unstructured in its nature and that the corporation has appropriate compliance systems (and a) records retention policy that is (formally posed to) technology, but also in governance requirements. That's, you know, the whistleblower lines (are) hardwired into the company's culture and that there's a – there are training systems that are available to employees and in an automated fashion, you know, web-based training for example, that assures (there) – the access and availability of the training tools, but also imposes requirements that employees are (required) to take the courses, if you will, on the governance and compliance (systems) that will familiarize them with the key aspects.

And then finally, some type of a business intelligence system that allows reporting to senior executives, compliance managers, legal department and so forth and analysis, so that you can do analysis of the information that's available to you. I think those are the key components to the platform, and there are readily available software tools. I'm not going to do a commercial here, but there are readily available software tools for each of these important components of the complete platform.

(Sonia Kudd): I would agree, (Dan), and actually, that might be an easy segue to one of our other questions, which I'm happy to try and answer is how to balance the need for getting rid of or purging irrelevant information, you know, records that are beyond their retention date with just prevailing employee habits of keeping everything. And I know that that is – is sort of that packrat habit is in a lot of people and that's – it's definitely a large challenge, particularly with things like e-mail and things that are electronic that people don't have a sense of the space that it's taking. They can sort of – it is somewhat of a cultural challenge, and the way that we've addressed that or that we handled it, and I think it's an effective way, is that it's critical that the tone from the top is – that it's important to comply with this – with the records management program, as with all of the programs. At (McCormick), we have that message of trying to communicate to the employees not just "do it because we tell you to do it," but really explaining why it's so imperative that we have an effective records management program. And that comes from our CEO and then is supported by all of the direct reports and heads of the business units all the way through to say that this is important. As well as we have ruled it under our ethics policy, so to the extent that, you know, the records management program is subject to those annual certifications of saying that they're in compliance with all of the company's key policies and procedures.

And we've actually found it to be a fairly smooth transition. When you do have that support and that tone from the top, you'd be amazed that even the packrats realize that it's important to comply with that new program and with those retention periods.

(Jon), maybe you could address whether records may be subject to different retention periods depending on whether they are electronic or paper, et cetera, various media forms.

(Jon Pat Zachas): You know, in terms of the difference between paper and electronic documents – I'm not aware of any – any differentials in terms of the timeframe. (I mean), they certainly are – the area where you need to focus on is what industry you're in (by because you see different) regulations (that just want to match institutions), auditing firms and the like, but one thing we see in the (Federal Rules) is that (really the policy to courts) is that generally now (in electronic) data and paper documents are on equal footing, (generally) you would think that the retention schedule (would also) apply.

The one difference though is that it's – in many ways, it's a lot easier to manage the retention instruction on electronic data. You have entire back-up tapes. You've got your e-mail servers. You've got other technology that can purge data. So we tend to see a more (finalities) and transparency (and ability) to manage and purge electronic data.

(Sonia Kudd): Excellent. Thank you. I think we might have time for one more question. (Dan), as part of your presentation, you talked about content and record. Could you discuss a little bit or try and clarify the difference between content and a record?

(Daniel Cooperman): Sure, and I think actually that (Alice) touched on this in her introductory comments. You know, a record – record needs to be classified and characterized in some way, and I think one effective way to do that is through the effective use of metadata labeling, so that in fact, the – it can be classified by content because the content is, of course, what we're searching for. We're searching for content (and because) we want to find relevance to, let's say, a matter in litigation. So the – we'll have to agree in the conferences that (Jon) had described in court what kinds of search techniques we're going to follow. What are the key words we're going to be using? What are the techniques we're going – we're going to (be doing) with respect to receiving the entire universe of records within the corporation.

So the record itself is where is the – the content is located. It is the physical embodiment, if you will, of the content. The content is the expression. (The way) those two are related through technology is the classification system that's being used.

(Sonia Kudd): Great. Thank you so much.

I'd like to thank all of our speakers, (Alice), (Jon) and (Dan), for the great information that you've presented today. And again, I'd to remind the listeners that we will be posting our answers to all of the questions sent in during the webcast by next Wednesday (and the) handout to the webcast, as well as I'd also like to remind all the listeners to fill out the evaluation form and submit that. And with those administrative points, I'd like to thank you again for attending the webcast.

END