E-Discovery

INFORMATION IS A VITAL PART OF ANY BUSINESS. AND THAT INFORMATION COMES IN A VARIety of formats—from document and video files to email and instant messages. Nowadays companies regularly store terabytes of data—one terabyte is approximately 1,000 gigabytes—making the prospect of electronic discovery a daunting task.

What will be the impact of the new federal rules of civil procedure regarding e-discovery? Our panelists of corporate and outside counsel discuss how a company can respond to a discovery request; the challenges of managing e-discovery expenses; the importance of having policies and procedures for handling electronic information; and the dangers of saving everything versus having a policy that employees do not follow.

The panelists are Mark Michels of Cisco Systems; Robert Brownstone of Fenwick & West; AnnaMary Gannon of Littler Mendelson; Robert Andris of Ropers, Majeski, Kohn & Bently; and Kenneth Rashbaum of Sedgwick, Detert, Moran & Arnold. The forum was moderated by Editor Chuleenan Svetvilas.

MODERATOR: The new federal rules of civil procedure regarding electronic discovery, went into effect on December 1st. What is a party required to disclose and when are they required to disclose it?

EXECUTIVE SUMMARY

Our panel of in-house and outside counsel discuss the effects of the new federal rules of civil procedure regarding electronic discovery. Topics include what parties are required to disclose and when they are required to disclose it; whether the new rules help manage e-discovery expenses; policies and procedures for managing electronic information; and the challenges of enforcing a document retention-and-destruction policy.

GANNON: Under the amended federal rule, the party's basic responsibility is to produce reasonably accessible information. Under Rule 26, the parties have to meet and confer and come up with a discovery plan as to what is going to be produced, how it is going to be produced, and when it is going to be produced. Hopefully the parties can reach an agreement on all those points. Where we have less guidance is where the parties—this being an adversarial process—are not willing to reach agreement or where there are significant cost issues, which are going to require some intervention from the court to resolve.

BROWNSTONE: Over the last four years, judges have increasingly gone beyond the stumbling block of "Is electronic information discoverable?" to come up with specific approaches. Now they are saying, "It is discoverable, but how do we deal with it?"

The thrust of the recent federal rules amendments is, early on in the case, to get the parties to deal with electronic information issues, for example, IT systems. Who are the most knowledgeable people at each company on those systems? In what format is the data going to be exchanged? The nitty-gritty is now addressed right in the rules and in the accompanying committee notes rather than the parties and the judges fumbling around with the concepts.

MICHELS: From a corporate counsel perspective, these are exactly the questions that we ask at the outset of every case. Some of the challenges that we face today, and will continue to face under these new rules as they are implemented, are that there are few bright lines. When we don't have bright lines, it makes it hard for to us establish repeatable processes in our company, particularly with respect to what we must collect and disclose in litigation.

Trying to find out where responsive information is located in a company can be very hard. Depending on the type of data, it can be difficult to extract the data and get it available for production without affecting our

business systems. That's really going to be the big issue we have to work through with our outside counsel when we are faced with electronic discovery issues.

RASHBAUM: And this is exactly why the committee report is very clear about the requirements for the Meet and Confer, in a way attempting to expedite the discovery process, because judges generally hate delay, and they specifically hate delay in cases due to discovery. The Meet and Confer is really a critical element to try to get counsel to agree early on to minimize what U.S. Magistrate Judge Ronald Hedges called "discovery about the discovery" or "litigation about the litigation."

ANDRIS: Just like litigation before electronic discovery, you are always trying to figure out at the front end what could be relevant and discoverable information and the new rules have probably magnified the need to do so as soon as possible. Trying to analyze a case on the front end, especially if you are on the defense of that case, and trying to understand what the other side might be looking for if they really dug down into the case, is a difficult proposition. Translating that concern to the client so that they can draw some sort of bright line is also a more difficult proposition. Admittedly, it probably couldn't be that bright, and that's why the rules are written the way they are.

What is relevant discovery is a question that lawyers fight about and will continue to fight about all the time. It's just that now we have a lot more sources of information, and there are much graver consequences for companies that don't have the right protocol installed and for lawyers that don't go in and understand their clients' systems—what they have, where it is—and give them the proper advice for preserving it.

GANNON: That's the key point, because even before we get to the Meet and Confer process, the client and the attorney have to get educated about the client's electronic data, just as you mentioned—what they have, what format, whether they keep back-up tapes, and where they keep them. You need to have both counsel and IT representatives sitting at the table long before counsel is going to be talking to opposing counsel about electronic discovery. So the very first step is to sit down and say, "What do you have?"

MICHELS: Well, there certainly isn't a lot of time to make that happen, either. At the same time you are trying to learn the facts of the case and get the initial discovery under way, you are now tasked as an in-house and outside counsel to understand all of your data systems and figure out where potentially responsive data are in a very compressed period of time. That could be daunting for many companies.

RASHBAUM: It may be helpful to the company to have a way to communicate to counsel efficiently what the IT architecture comprises, what information is maintained, how it is maintained, how quickly it can be produced, what policies and procedures currently exist as well as the practices for maintaining data. A good suggestion would be to have someone responsible for being the liaison with counsel.

MICHELS: Which sounds great in theory. The challenge, of course, is that the IT staff in most information-driven enterprises is stretched very, very thin. They've got at least two day jobs, and when the lawyers show up and say, "By the way, we'd like to take a little bit of your time," that can become a fascinating interaction.

BROWNSTONE: Being a combination of a lawyer and an IT leader, a lot of my involvement during discovery is translating during a conversation between a lawyer at our firm or in-house and an IT leader at the client. My work has increasingly become working with clients not only when they are in litigation mode, but also prophylactically—trying to help them think through what their systems are and who's responsible for them. With some clients, no one even has a playbook, so to speak, or a menu or systems map of what and where the systems are.

It's very inefficient for a company to pay a lawyer rate or even a consultant rate to do an investigation about where all the company's

FORUM PARTICIPANTS

MARK E. MICHELS is a Managing Attorney at Cisco Systems, Inc., the worldwide leader in networking for the Internet. Since Joining Cisco in 1996 Mr. Michels has held a variety of legal management positions. He currently is a member of Cisco's intellectual property dispute resolution team responsible for discovery management. Prior to joining the intellectual property team, Mr. Michels co-managed commercial litigation and dispute resolution for Cisco. Before joining Cisco, he was in private practice where he focused on government contracts and international regulatory and criminal matters.
mmichels@cisco.com

ROBERT D. BROWNSTONE is the Law & Technology Director at Fenwick & West LLP, a 250-attorney firm providing comprehensive services to technology and life sciences clients. A member of four state bars, Mr. Brownstone advises clients on e-discovery, electronic information management, and compliance. A nationwide speaker and prolific writer, he was featured in *ABA Law Practice* magazine's September cover story. Before coming to Fenwick in 2000, Mr. Brownstone had a 13-year career as a litigator, law school administrator, law school teacher, and consultant.
rbrownstone@fenwick.com

FORUM PARTICIPANTS

ANNAMARY E. GANNON is a shareholder in Littler Mendelson's San Francisco office. She advises and represents employers in employment law matters, including the defense of wrongful discharge, employment discrimination, and workplace harassment litigation; and advises clients on all aspects of the employment relationship. Ms. Gannon is a frequent lecturer on employment law topics and was Technical Editor of *Preparing for and Responding to Crisis in the Workplace.* She has held faculty appointments at the UCLA's Graduate School of Management and at the University of Oregon.
agannon@littler.com

ROBERT P. ANDRIS is a partner in the Redwood City office of Ropers, Majeski, Kohn & Bentley. Over the past 20 years, he has litigated and tried a broad spectrum of copyright, trademark, and patent cases including web-based infringement actions involving metadata and key words. In 2001, he was lead trial counsel in one of the first California cases brought under the Anticybersquatting Consumer Protection Act. Mr. Andris is also a registered patent attorney whose national litigation practice regularly involves the discovery of electronically stored information.
randris@rmkb.com

> **"Now we have a lot more sources of information, and there are much graver consequences for companies that don't have the right protocol installed."**

information is located. People say that lawyers are from Mars and IT people are from Venus, but there needs to be interplanetary communication throughout. Otherwise there are going to be a lot of pain points for the company because, for every litigation, it is going to have to pay for a lawyer to spend hours figuring out where computer information is. If someone in legal or in between legal and IT can get some kind of protocol or systems map in place, theoretically, you could avoid going through the same set of questions every time you hire an outside attorney.

MODERATOR: Do the new federal rules provide any indication that e-discovery expenses can be manageable?

MICHELS: That is the $2 billion question. I say that because some surveys say that the market for electronic discovery is approaching $2 billion. These same surveys suggest that at least for the next couple of years, the e-discovery market will grow 30 percent annually. What this really means for companies with large amounts of electronic data is that they have to look carefully at managing this expense. Adding in-house IT staff to address e-discovery issues can have a great return on investment. You can certainly pay lawyers to help manage e-discovery vendors, but IT professionals usually bill at a much lower rate.

Working with our outside counsel at the outset of the case, we set the data collection parameters that enable us to budget for these expenses. The early Meet and Confer should be a benefit if the parties can agree up front on what electronic data are required to be produced. If the parties can't agree on what is reasonable, then my lawyers will need to articulate very well to the court why our position is the most reasonable approach.

GANNON: That is key, because the revised rules do anticipate that you can go to the court and ask for some cost shifting, which is something that you can use with your opponent saying in effect, "Unless you narrow these requests, we are going to go to court, because the anticipated cost is X. And you may wind up with an order that we produce it, but you pay for it. So you want to rethink your request."

In the *Zubulake* case, there was one discovery request, which asked for all emails that were sent and received by five specified employees over two-and-a-half-year period. That does not seem terribly unreasonable, but it has been reported that UBS estimated the cost of restoring and searching the back-up tapes would be $166,000, and then they had an estimate for attorney and paralegal review of retrieved emails of $107,000. So that is a quarter of a million dollars to answer what seems like a pretty simple discovery request. And that is why it is a $2 billion industry.

BROWNSTONE: One of the basic new provisions in the federal rules provides the opportunity for the responding party to say this evidence is not reasonably accessible; there will be undue burden and cost. If you can show that, then you place the burden on the other side to show due cause. As AnnaMary Gannon points out, that's a prelude to saying, if the court orders production, then the requesting party better be paying for some of it, because it consists of back-up tapes, which are vats of unsorted, undifferentiated information.

So this is a great development that frankly is an attempt to rein in some of the excesses in lawsuits where the judges have ordered a very costly and time-consuming restoration process to take data that was on tapes for disaster

recovery if the building falls down or all the servers crashed, and turn it into an evidence vault that's very expensive to open up.

RASHBAUM: There's a cautionary note here, and it's that I've seen a number of companies use their back-up tapes as archives. They go to them frequently enough that they can no longer be deemed not reasonably accessible, and then the cost will be on them, perhaps, to restore them. And restoring a back-up tape is an onerous task—very time consuming and very expensive.

> **"The early Meet and Confer should be a benefit if the parties can agree up front on what electronic data are required to be produced."**

GANNON: If you should have preserved it earlier, and had you preserved it, you would not have to go to the undue cost of going to the back-up data, then you are probably going to be stuck paying for it. At the least, you have a more difficult argument to make if you intend to convince the court that your opponent should be required to undertake the cost of going to back-up data because you did not follow your duty to preserve.

MICHELS: Once again, the federal rules suggest the bright line, but the state of technology is always changing. So determining what is "reasonably accessible" can be a moving target.

ANDRIS: Judges have the power to issue an order that the other side pay production costs. Frankly, the court's always had the power to do that and manage litigation expenses, so again, these rules, not just with respect to managing the costs of production, but all of these rules in some ways are more clarifying than they are novel. These issues have been out there for a number of years, judges have talked about them, and cases have gone different ways on the same set of facts. And that's not to say that it's not going to happen under these rules as well. I'm sure it will.

But it's put people on notice that you can't hide your head in the sand anymore. You are going to have to deal with this issue. So companies looking at this should step back, talk to their in-house counsel, talk to their outside counsel about ways that they can sit down and manage this effectively, because sooner or later everybody is going to have to deal with it.

MODERATOR: Another challenge for companies is managing their electronic information. What policies and procedures are you recommending?

GANNON: Finding out where all the electronic information is can be a very expensive process. Corporate counsel, perhaps with the help of outside counsel, can develop document-retention policies for electronic data that address this issue in advance of any particular litigation.

Once a complaint has been served, there is little enough time to analyze the case and determine who the key players are, without also having to learn the intricacies of the client's IT resources. If there are document policies developed with IT so that they can hand you the playbook, and say, "Here is what we've got, here is how far back it goes, this is readily accessible, this we have to manipulate in order to retrieve it," then you could say "thanks" and get going. This is also why firms have developed electronic discovery teams that are a combination, usually, of lawyers and IT technicians who will go in and talk to the client's IT people.

RASHBAUM: Policies and procedures are critical for several reasons, not the least of which is they can excuse a variety of sins. If you can't produce something, then you have a good reason for it and it's documented. The *Arthur Andersen* case taught us that the policy can actually end up resulting in not only a court decision in your favor, but arguably the avoidance of a monetary sanction or an adverse inference instruction where the jury will be told they can presume that the missing documents will be adverse to your position at trial. So we need proactive counsel. The time to have those policies is not when the process server or government investigator is knocking at your door.

BROWNSTONE: The ideal combination would be: number one, a retention/destruction policy accompanied by implementation protocols; and, number two, a computer-use policy addressing that, among other issues, any device supplied by the company and used for work belongs to the company as does any information created on it, also making clear that there's no expectation of privacy. At least for U.S. companies, that policy eliminates the expectation of privacy and comes right out and says that if the company is subject to a discovery request or a government inquiry, it can freely look at what the employees have.

FORUM PARTICIPANTS

KENNETH N. RASHBAUM is a partner in the New York office of Sedgwick, Detert, Moran & Arnold and Chair of the firm's E-Discovery, Data Management & Compliance practice. He counsels corporations on compliance with federal, state, and judicial norms governing electronic data management, privacy, and security. Mr. Rashbaum is a member of the Sedona Conference's Working Group 6, where he focuses on international electronic information management, discovery, and disclosure. He is on the editorial board of the *Journal of Privacy and Data Security Law*.
kenneth.rashbaum@sdma.com

RASHBAUM: Retention and deletion in policies are no longer just the province of litigation. There is a regulatory network now that requires certain data be retained for certain periods of time. Statutes such as HIPAA [Health Insurance Portability and Accountability Act] and Sarbanes-Oxley, which has a seven-year time period, and state laws, which also include data breach prevention acts, which will mandate the deletion of certain personal information or sensitive information after it's no longer needed for business use.

MICHELS: We have computer-use policies and, of course, we have record-retention policies as well. The real challenge is applying the policies on a daily basis. It can be very difficult to figure out all of the applicable regulatory regimes but once you have record-retention protocols in place that will help manage the expense of maintaining corporate data and also the expense of discovery in litigation.

ANDRIS: Once a lawsuit does get filed, if your company doesn't have an IT department that can respond to discovery requests and digging through data, at the very least, what you need to consider is bringing in an outsourcing company along with counsel and make sure that counsel understand your IT systems every step of the way. One of the big killers as far as litigation costs are concerned, is multiple review of the same document. It's like paper documents but in these e-discovery cases, there are so many different sources. It is critically important to have a logical and thought-out procedure for reviewing electronic documents, both for privilege and substance, just because of the vast numbers.

MODERATOR: Given the regulatory issues and laws on saving certain types of information, some companies' initial response may be to simply save everything. What do you think of that reaction?

RASHBAUM: Keeping everything is how a number of companies have gotten into trouble. The best example of that was Morgan Stanley. There was way too much information for them to be able to search efficiently, and there's nothing that I'm familiar with that requires that in any event. You just build a haystack much, much larger and it's harder to find the needles.

> **"Finding out where all the electronic information is can be a very expensive process."**

BROWNSTONE: What about email deletion? Email tends to be the biggest vat of information, whether there's a government inquiry or a civil lawsuit. So can a company of a large size effectively develop and enforce an email deletion policy that involves a combination of age-based rules and size limits on in-boxes? Is that feasible? Is it desirable?

ANDRIS: These issues typically arise in a discovery dispute or when you are at trial and someone is wondering why something has or hasn't been produced. It all comes back to being reasonable in the context of not only the litigation, but also the day-to-day business of the company. A company can feel safe in drawing a reasonable line, and deleting information, be it emails or other documents, over a specific period of time as long as it can explain that and stop deleting, if need be, under the rules.

Some of my larger clients would literally shut down if they had to keep every email. They receive millions of emails on a daily basis. I would bet dimes to dollars that probably at least half, if not a considerable amount more, of the email that most businesses are exchanging on a daily basis is either personal in nature or comes from an outside source that wasn't solicited.

GANNON: Suppose a client's policy is to send a notice once a month to its employees, "Anything in your in box over 90 days will be deleted over the weekend. If you want to save it, now is the time to do it." And 90 days isn't terribly long, but it forces the employees to go through the jumble and sort and save that which they want for whatever business reason. Will the court find 90 days a reasonable period?

RASHBAUM: This is all starting to shake out. What the courts are going to find reasonable is going to depend on the circumstances and the development of a set of best practices. We are now in the formative period and the judges are still learning this.

BROWNSTONE: An employment decision about a year ago analyzed Echostar's aggressive 21-day purge on email. If an email message sat in an individual user's sent items folder for 7 days, it was automatically moved to deleted items. If it sat in deleted items for 14 days, it was deleted from that folder in that individual inbox, and then it was *not* saved on back-up tapes. It was double deleted. But Echostar's purge-suspension process was deficient.

Interestingly, in that case the federal court said that theoretically, even a 21-day policy may be defensible, provided that, as Rob Andris pointed out, when there is a dispute of which you are aware or should be aware, you have a way to stop the purging process. In other words, you have to follow a policy that includes a "litigation hold" aimed at preventing deletion by individual users likely to be witnesses, such as those in HR if it's an employment case or those in the pertinent product department if it's an IP case. But can you enforce both an aggressive purge period and a legally defensible litigation hold? If you do, maybe that will push the courts to opine on different fact settings and rule that what was done was reasonable.

GANNON: Any policy and procedure that you have for employees requires training on the policy and procedure, as well as an audit process to determine that there is compliance. And compliance goes two ways, not only that the employees are deleting email and other electronic data from their in-boxes, but also that they are not secretly backing stuff up.

Some employees want to maintain an accurate record of everything they do in the course and scope of employment, so, before deleting data from their corporate computers, they transfer it to a personal computer or storage drive. That creates a number of issues because the information still exists, and we may need access to employees' personal computers.

Another case involved telephone conversations that were tape-recorded for monitoring purposes. What was said in a particular conversation was critical to the case, but the tapes were rotated and, after a certain period, recorded over. We represented to the court that the tape in question had been recorded over in the normal course of business. Two years later, well into the litigation, we discovered, almost by accident, that a coworker who had heard one side of the conversation thought something was fishy, pulled the master tape and preserved the particular conversation. The employee told no one, but kept the tape in her drawer for two years.

BROWNSTONE: Even if you impose onerous automated prevention mechanisms, you are not going to be able to completely stop a given individual or individuals from keeping "local copies" of emails and files. But that suggests why it's even more important to have an overall policy and IT structure enabling people to centrally store what should be saved. Then when you are analyzing a case at the beginning, you have a better shot at seeing what you have—good, bad, and indifferent—so you can advise corporate officers accordingly: this is one we better settle, or this is one we should fight tooth-and-nail.

My teammates and I advise clients to consider insisting on central storage, knowing full well that you are not going to be able to enforce it 100 percent. If people have a way to just drag and drop into a set of folders not subject to an automatic purge, then, in a later discovery dispute, the company will be best positioned to show thorough collection and production. In other words, the company will have the best shot at fending off an opponent's request to get at the contents of many employees' individual computers.

ANDRIS: When one of these cases gets filed—given the scenario that local copies can be held in different places and formats—it seems to me that because of these new rules, it is even more critical that you not only identify all of the individuals who might be involved in the case, but also to interview them and find out what electronics they have, whether they have their own PDA with their calendar or have they been sending files home like AnnaMary [Gannon] said.

> **"Retention and deletion in policies are no longer just the province of litigation."**

RASHBAUM: We have been advising clients and people in our firm who work at home or who work on laptops on the road, that any information created in the context of business has to be uploaded into the firm's central server within X period of time or as soon thereafter as a practicable. I have one client who was keeping files on an iPod, which was terribly inefficient, but he didn't want to carry a multitude of devices.

When you do have notice of a potential claim, what devices do you include in your preservation notice? As storage technology is changing, clients and counsel have to keep up with all of those different things—USB drives, different kinds of PDAs all have to be included—because people will be keeping critical data on those devices.

MODERATOR: Are you worse off if you have a document retention-and-destruction policy in place and employees are not following it?

ANDRIS: It is more problematic to have a protocol in place that isn't followed. More hay can be made out of that at litigation before a magistrate judge or before a jury, that here is what they themselves said was the minimum they should be doing, and they didn't even do that. Thus I advise my clients that they better think long and hard before they implement a policy and if they do, that they will follow through. Five, ten years from now, looking back in the harsh light of litigation, somebody is going to be on the stand having to explain to a judge why this wasn't done and why you threw out information that you said you should keep.

RASHBAUM: This is exactly why we work with clients at the site to draft policies and procedures. The work group will involve records management, IT, legal, and HR in most cases, and a representative of at least a couple of groups of the front line users. We have actually mediated shouting matches with people saying, "This will work and we have to do it," and others saying, "There's no way my people are going to do that." The best practice is useless if it's not going to be followed. So in that way, we facilitate hammering out something that is practicable, and it makes a difference when they have a part in drafting it.

BROWNSTONE: When initiating a retention/destruction regime, I don't think a company can be fully compliant with its regulatory requirements, let alone its litigation discovery requirements, unless it develops an implementation process The ideal group with which I like to meet has at least one IT leader, at least one lawyer, and one C-level officer.

In some instances, clients have been scared off if I tell them to consider deleting everything in the last of these three buckets: what you need to keep for legal reasons, what you should want to keep, and then everything else. The alternative—over-saving—is quite problematic.

ANDRIS: As long as someone at the company can explain why what they are doing is reasonable within their industry and within their business, you've at least got a shot at explaining it to a judge and a magistrate and making them happy during a discovery dispute. If you are a Fortune 500 company that knows all about this, you are going to have a much tougher time in explaining why you didn't have something like this in place.