III. PANEL DISCUSSION

Moderator: Jacquelin F. Drucker, NAA Member, New York, New York

Panelists: Lesli J. Bruden, Labor Relations Manager, Qwest Corporation, Denver, Colorado
Martin J. Costello, Hughes & Costello, St. Paul, Minnesota
Joan Feldman, Navigant Consulting, Inc., Seattle, Washington
Theodore O. Rogers, Sullivan & Cromwell, LLP, New York, New York

Drucker: As moderator of this session on high-tech evidence and high-tech discovery, I must say to my colleagues in the Academy that I am no Doug Collins. Doug, who is a member of the NAA from California, is our Academy guru of all things high-tech: hardware, software, e-mail, viruses, and all of cyberspace. While most of us lag far behind Doug in expertise, we all realize that we can no longer do our jobs without an understanding of both the technology and the law associated with much of the high-tech information that is out there. In this session, we're going to address a small part of this rapidly developing field.

Among the issues we will consider in this discussion is the hidden information within the documents we produce, including the embedded data in the documents we send flying electronically throughout the world every day. What are our documents saying behind our backs? Everyone knows by now that a deleted file on a computer very seldom is truly deleted, but what is the status of such data and what is involved in retrieving it?

What about e-discovery? Many of us are involved with employment arbitration where discovery is common, albeit more streamlined than in litigation. In that arena, issues of electronic discovery loom large. In labor arbitration, we technically do not have discovery, but the issue of pre-hearing access to electronic data has been steadily creeping into that world too. Massive amounts of information can be subject to discovery. On a first pass, for example, on an electronic data search, millions of e-mail messages may be identified. What are the obligations of the parties to search for and produce some specific piece of evidence from all of that? And in what form must the evidence be produced? Who pays for this process? And back at the beginning, what is the obligation of par-

ties to preserve electronic data when litigation or arbitration is possible?

Finally, we will look at the expanding use of electronic tracking and monitoring in the workplace. We all have a vague sense that if someone really wanted to, he or she could reconstruct most of our daily activities by scrutinizing the various sources of high-tech information that is amassed about us as we wander through our lives. But in the workplace, for employers and employees, this ability is magnified and raises issues that are addressed in bargaining, arbitration, and litigation.

We have assembled a panel of experts who are going to help us understand these issues. And they will bring us—some of us, perhaps, kicking and screaming—into the 21st century with respect to electronic information. Introducing them in the order in which they will be speaking, I will start with Joan Feldman. Joan is our computer forensics expert. She founded and was president for 12 years of Computer Forensics, Inc. She was a pioneer in the use of electronic discovery, advising both plaintiff and defense bars in litigation. The title of her book says it all: *Electronic Discovery: Finding and Using Cyber-Evidence.* Joan's company, Computer Forensics, was recently acquired by Navigant Consulting. Ted Rogers is the go-to guy when it comes to the legal issues of electronic discovery. He is the managing partner of Sullivan & Cromwell's labor and employment litigation practice representing management. He has written extensively and has educated judges on issues of managing electronic discovery. Today he will be educating us. Lesli Bruden is Manager of Labor Relations with Qwest Communications in Denver. Qwest has a workforce of nearly 25,000 employees represented by the Communications Workers of America (CWA) and the International Brotherhood of Electrical Workers (IBEW). Lesli has extensive experience in the use of Global Positioning System (GPS) data in arbitration. Finally, Martin Costello is a partner at Hughes & Costello, representing unions and is general counsel to the International Brotherhood of Teamsters General Secretary-Treasurer. Martin has had a wealth of experience in dealing with performance-monitoring data in call centers, warehousing, trucking, and health care. Martin's practice also includes criminal defense.

To begin, Joan Feldman has a few remarks to supplement her excellent paper, which you have. Joan?

Feldman: So I'm going to tell you a little bit about computer-based information. It is related to real estate. How is it related

to real estate? Well, it's location, location, and location. The first place to look is the easiest place to look. *Active information* is what you call up when you turn on your computer. It is what is in front of you. It is the first place we would look for computer-based evidence in most cases, especially something like labor arbitration where the business has hundreds or thousands of people and you are generally looking for information that is on file or e-mail servers rather than information that might be on only one individual's PC. I don't mean to dismiss the PC as a source of evidence, but where the evidence is in most of the work that you are going to be doing will be on file servers.

Where people are working in a group in an office and they are sharing information with others, they will be working with a computer called a file server or an e-mail server. That is where there will be a collection of many people's documents. And what distinguishes a file server from a PC? A file server is like a PC with a thyroid problem. It is just a big hard drive. It uses a slightly different operating system; but basically, from our perspective, a hard drive is a hard drive. So is a data server. For those of you who are working on cases involving very large entities—the government, very large corporations—you may also be dealing with an extremely large computer sometimes referred to as a mainframe. That's another source of active electronic evidence. So these are the main repositories. This is where most of your stuff is going to be.

The other place where people look for computer-based information if they can't find it in an active state online, on a file server, or on a hard drive, would be on a *backup*. Most backups these days are still created on backup tape. In some cases, information is backed up to a giant hard drive. The motivation for a backup is to protect against anything that might take down the system—so you can recover from a disaster. What has happened as electronic discovery has evolved is that parties have turned to backup tapes if they cannot find the information that they are seeking in active files or systems.

One of the problems with getting evidence or documents from backup tapes, however, is that there is no organizing principle for how it got onto the tapes. I was a system administrator in a law firm for 11 months; and that means I never have to go to hell again. [Laughter.] We backed up files because we wanted to save our people from data loss. It was a big deal—we could say, "I can get that back for you, no problem." But the way we organized things on the backup was based on whatever would fit on the tape. So if

you are turning to backup tapes as a source of evidence, then you have to understand that there is not an easy way to figure out what is on the tapes. It is not designed to be an archive. In electronic discovery, however, it is sometimes treated that way. So active, online is first; network backups, next.

Where else might you find evidence? Just about anywhere. From my perspective as a forensic analyst, every piece of Mylar out there, whether it is a PC drive, a piece of Mylar in a phone, or a piece of Mylar in a floppy diskette, is a resource for me to look into for evidence. Over the years these devices proliferate. They change over time. We all know what a floppy diskette was and then we started saving things to CDs. Now we have those little thumb drives. Anybody use an iPod? That is a hard drive. So the next time you see somebody sitting at your computer, rocking out, they may actually be downloading the contents of your computer. So this is another place that we can look.

I want to show you something else about electronic information because it is so much fun. And you can do this at home. I am showing you a computer file that was created in Word. For most of you, this is what you would look at on your screen. If I were to print it out, you would get everything on the screen on paper. But this is a computer-based file so in this case, this file was created using a redlining feature that Microsoft calls "Track Changes." Let me show you what I can do to this file within Word. I simply go into the "Tools Menu" and click on "Track Changes" and it will then show me the markups. If you have received a document from someone as an attachment and you are looking at it in your version of Word, you can go into it and look at their markups. Everything that you see that is red with a strikethrough, obviously, would not normally have been sent to you, and you didn't see it in that other version. In addition, you get pop-up notes so you get to see who did the change and when they did it. So this is an example of embedded information in a file. It is an extra.

Let me show you something else about a file. You can do this in any file. When you go back to your office open the File Menu, click on Properties, and you will see a host of information about the document you're looking at—information that is never printed out, that you usually don't care about but it will have the author's name and usually the license holder of the software. It will have a company name in many instances. If I go to the statistics tab, it will tell us when this document was originally created, the last time it was modified and then saved, and the last time it was accessed.

For many of us, we don't really care who wrote it or when it was created, except do we? Is timing ever an issue? [Laughter.] Right? We first used this in a case in the early days back in 1995. We worked on a case where a woman related to her supervisor that she had been diagnosed with cancer and she was going to be taking time off for treatment. Within a couple of weeks, she was terminated. There was no particular reason given except that there were some documents that showed hints of disciplinary problems from two years back. The woman knew that this was falsified, so we asked for the computer-based files to be turned over. We were able to look at the creation dates and, indeed, most of them had been created two or three days after her manager had learned of her diagnosis.

Not every file that you have will have "Track Changes" markups. But every file in a Windows environment will have its creation date, its last modified date, and its last access date. But you get it only if you go after electronic files. If I hand you this on paper, chances are good that you are not getting that information. So although you may have a fear of the computer, take a deep breath and embrace this richness because it is a valuable source of evidence.

Let me give you one more example of an embedded file—a very easy one. This is a spreadsheet and here is a yellow pop-up note that some people use. You might use these pop-up notes in your documents and here is one referencing an employee's alcoholism. This is another example of embedded information. Such information is often referred to as "metadata"—items like this that are inserted and embedded in the document. We distinguish between "meta data"—date of file creation, modification, or most recent access—and "embedded data"—user inserted changes or entries.

There is one more thing that you may see in your cases. When employees are out on the Internet, whatever they are doing, they are leaving a historical trail behind. Here I am in Internet Explorer. Go up to this little symbol—in XP it looks like a recycle symbol with a green arrow, in Windows, it looks like a sun dial —it is your history section. The default setting in Windows Explorer is to keep a history of where you have been on the Internet for three weeks, but it can be set for longer or shorter periods of time. This is always fraught with peril for me—please don't fire me Navigant. [Laughter.] What you see here is what I was doing. I was on my company Web site; my company will be happy to hear that. There

are also file properties associated with this showing how many times it was visited and when.

We worked on a case where we were able to show that a woman was working on her real estate business 6½ hours out of an 8-hour day at her law firm legal secretary job. That discovery made her sexual harassment case go away. [Laughter.] It did. So the Internet will come up in some employment cases, particularly for "after-acquired" evidence.

In summary, think about your hierarchy. Think about your objectives. You know that what you might be looking for might not have anything to do with the Internet. But maybe it is in a detailed database of salaries or attendance records. So you have to think about *what* you are looking for, and then think about *where* you are going to look for it. For key witnesses, we do suggest looking at hard drives, especially in labor cases, and then think about the historical information that might be available to you. Now I am going to turn this over to the expert on the legal issues of electronic discovery—Ted?

Rogers: Thank you. So you are the arbitrator and there's a fight going on between the parties in the matter over which you're presiding: They're quarreling over how much should be produced, whether that meta-data is going to be allowable, and how far you should go in requiring production and who should pay for it. Thankfully, guidance is coming from the courts and other sources that can help in that regard. Adjudicators are struggling with these issues and coming down with pronouncements all over the place.

A little cautionary advice—Joan mentioned the fun in going into the document that's been sent to you. There is a decision by the New York State Bar Ethics Committee that it is unethical for a lawyer to delve into a document that has been sent electronically by an opponent to see what the changes were and what the history was in that document. It is a little akin to the authority that developed with respect to misdirected faxes.

There are a number of sources of guidance if you need some touchstones. At the moment, there are proposed amendments to the Federal Rules of Civil Procedure that have been wending their way through the procedural hoops. They should be adopted by December [2006] and they give good examples of how the courts in the federal system are going to handle disputes relating to electronic discovery. A think-tank developed what are known as the Sedona Principles. They consist of some very good common sense. They are set up like the codes of professional responsibility.

There are 14 basic principles and then a long explication of the various considerations under each principle.

The American Bar Association (ABA) recently issued Civil Discovery Standards that delve into how the ABA thinks a judge should assign or shift the costs of production to the party demanding the production. Finally, there are decisions—one much noted in New York is *Zubulake v. UBS,*[1] and one that was not an employment case is *Coleman Holdings v. Morgan Stanley.*[2] This was a case in Florida that was much noted last Spring where Ronald Pearlman sued Morgan Stanley. At the moment, Morgan Stanley has a $1.4 billion judgment against it because of electronic discovery failures.

The backdrop of all of this for someone like me—a management lawyer—is that there is a lot of opportunity for mischief in electronic discovery. This is especially true where one party has a lot less electronic data than the other. Because a large organization will have tens of millions of pieces of information, if the opponent wants to torment that party, or drive up the costs, the opponent will insist on extreme levels of information production. This really scared us in the management bar a few years ago. In the *Harry Potter* movies, there is a character called the Dementor. The Dementor is a ghost-like waif that will surround someone and suck all of the joy out of him. [Laughter.] Electronic discovery was doing that to litigation. It was really sucking all the joy out of practicing law because the first thing that would come in was a document request saying, "Give us all your documents relating to X." So someone calls up the Information Technology (IT) person who says, "Well, we've got 50 billion bits of information. That's probably conservative. Plus, we've got these back-up tapes in some mountain in Colorado that, day-by-day, has the last ten years' worth of information." That IT person will also hopefully tell you that if Joe Blow had a really hot e-mail on April 1, even if he deleted it the next day, if you went to the backup tape for April 1, it would be there. So that could leave you with the prospect of calling out to Colorado, shipping a trainload of tapes back to your home office, and putting the tapes up for review. That is obviously impractical and, fortunately, as time has passed, the courts have recognized that, too.

---

[1] *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422 (S.D.N.Y. 2002)

[2] *Coleman (Parent) Holdings Inc. v. Morgan Stanley & Co., Inc.*, No. 502003CA00504XXOCA1 (Fla. Cir. Ct. Mar. 1, 2005).

So what are the amendments to the Federal Rules that provide some guidance on being sensible? First, the rule changes will require parties to talk about, and report to the judge, how electronic discovery is going to be handled at an early stage. That is something that could be imported into arbitration quite readily. Rule 26(b) states that a party need not produce electronic information that is not readily accessible. So as a first-cut principle, a party does not have to go out to Colorado and get those back-up tapes. Later on, if there is clearly something out there that is vitally important that might be found on a back-up tape, then you can initiate discussions about doing it and who is going to pay for it.

Rule 26(b) establishes procedures for addressing inadvertent production of privileged material as well. That goes to our earlier discussion of "Track Changes." If indeed the parties are going to produce loads of information to each other, it would be impractical to expect that every single one of those documents will be reviewed for privileged information, so there might well be some inadvertent production of privileged materials. The rules effectively say that by producing in such a massive way, parties can agree there isn't a waiver.

Other aspects of the rules get to how the information is produced. First, interrogatories can be answered by providing access. That is the same as the rule with regard to paper documents. Rule 34 goes to document production that occurs in arbitration all the time. It essentially endorses negotiation. The party requesting can specify the form. So the party requesting can say, "I want all the meta-data—all the background for each one of your documents"—all those auto-generated materials that Joan discussed earlier. The party producing may say, "We're not giving that to you because this is a contract dispute. The drafts of the contracts were looked at by counsel, that meta-data will have indications of changes made by counsel that are privileged, and it's just too much of a pain in the neck to go through and separate it out. So until you come up with some reason like a suspicion about back dating, we're not going to do it."

In the absence of agreement, production must be made either in the form in which it is ordinarily maintained, which would give all that meta-data, or in another reasonably usable form, which most people take to mean that you cannot produce the paper, but you can give it in a form that is computer searchable, but without the meta-data.

Rule 37, the sanctions rule, was interesting, although it is obviously not applicable to arbitration. Some of the district courts felt it was taking away some of their authority. The rule says that a district judge may not issue sanctions against a party for failing to produce electronic information that is lost. It is applicable where data are lost in the routine operation of the system and absent a showing that there was a failure at the early stages to take steps to preserve information.

One of the first issues addressed in the Sedona Principles is an advocate's obligation to instruct witnesses and IT people to put a hold on those documents that reasonably could be considered to be germane. Controversies may arise as to how far that hold goes. Does it mean that you may no longer destroy any e-mail against the off-chance that there may be something conceivably relevant to a counterclaim in the future? These principles try to flesh that out—trying to strike a reasonable balance between not crippling a corporation every time there is a $10,000 dispute by making it hold on to all information, yet, nevertheless, making sure that reasonably related information is kept.

The Sedona Principles also deal with disaster recovery tapes. One interesting principle is their endorsement of the sampling of data to find whether or not a tape has some potentially pertinent information in it. This is where I think electronic discovery is going–sampling and a use of keywords. You can't be perfect. You cannot, in an electronic system of these immense sizes, find every single document that bears on an issue. But you can come to a negotiated solution as to where information that would be most germane is likely to be found.

Where have some of these issues gone in real application? *Zubulake/UBS* was a sex discrimination case. The defense counsel from the Southern District in New York was more diligent than I would have been at the time, frankly. He quickly issued a memorandum to the right people saying, "We have been sued by so-and-so, please preserve all your information." What came out in the course of discovery was that some items were, however, destroyed. The plaintiff, realizing that she had an opening, kept pushing. Ultimately, there were four separate decisions on the issues of discovery issued by the judge who wanted her case to be a landmark. She addressed when a notice to preserve data should be sent. She said the duty arises when a party should have known that evidence may be relevant to future litigation. I do not endorse that standard as

a management lawyer. It is pretty aggressive. But certainly a duty to preserve does attach once a case has been brought. Whether it attaches if a lawyer's letter comes across is another issue. Once the duty to preserve attaches, the litigation hold is required.

The judge became upset about the fact that records were destroyed. She determined that she had the right to issue sanctions if the records had been destroyed with a culpable state of mind. She found that a culpable state of mind means ordinary negligence. Then she issued an instruction to the jury that documents had been destroyed and the jury could infer that those documents had significant information. The result was a $29.3 million verdict, $20 million of which were punitive damages.

The *Morgan-Stanley* case involved a judge who was upset with the way the defendant had handled discovery. Someone who was in charge of the technology effort had put in an affidavit affirming that they had produced everything, but then they continued to find cabinets and cabinets filled with old back-up hard drives. They repeatedly came into court saying, "I'm sorry, judge, there's more." Finally, the judge issued a default judgment. It is on appeal.

Under the heading in the paper, "Practical Suggestions for Counsel," there are suggestions that you might want to think about as you oversee disputes. A "litigation hold memorandum" is something that should be issued promptly and if the other side raises a fuss about it, then you should be interested in why. One of the most difficult situations the management bar faces in the employment field is the case where an existing employee is raising a claim. For example, suppose an existing employee has a lawyer write a letter saying that his or her client has been discriminatorily denied a promotion. All right, the book says you should issue a litigation hold memorandum and send it to all people who might have information relevant to the claims raised. All should be asked to please hold information. Obviously, you immediately get the buzz around the company that so-and-so has raised a claim. The next thing you know, something negative happens to the claimant and there is a new claim for retaliation because everybody knew. So in the situation of existing employees, you may find that the litigation hold memo should go to only a very circumscribed group who already knew about the problem and who are most likely to have relevant information.

Learn your client's computer system. Joan Feldman and her peers, both in-house and outside, are around and can help in a dispute. It may well be useful to have the company's computer person come in. That is where it should be resolved. If they are involved, issues are likely to be resolved somewhat happily. There is a huge incentive for both parties to sit down and negotiate how to approach it. You can organize a not terribly expensive search for electronic data by coming to agreement about those persons in the company whose e-mail accounts should be searched. Who is likely to have relevant information? Then you can agree on a protocol of search terms, the last name of the claimant, first name, nickname, etc. Then the company can run the search and find out how many hits there are. If it is reasonable—2,000 pages—then the company will review and produce whatever is germane.

Such an approach is working reasonably well from the plaintiff's side as well. Responsible plaintiff's counsel in these cases don't want to get a million pages dumped on them any more than defendant counsel wants to dump it on them. So we are finding some success in that.

One more point is interesting. The Internet Explorer antitrust issue was mentioned. My firm actually represented Microsoft in the antitrust cases and I should say that Internet Explorer is a fine product and I think we are all much better off with the situation the way it exists right now. [Laughter.] But in the antitrust field, one assumes with good reason that when e-mails are produced, they are going to be bad for the defendant. This is because salesmen are out there saying, "We're going to kill the competition, we're going to cut the prices," etc. In employment litigation, by contrast, e-mail evidence can very often help the corporate defendant as much as the claimant. Joan mentioned one situation. I had an arbitration involving a national origin discrimination claim where the plaintiff's counsel got enthusiastic about the case and thus made some assertions in the claim that the harassment was so bad that her client was miserable coming to work—her life was a holy hell for six or eight months before she quit and it was so bad she had lost weight. Well, we pulled the e-mails and when you see an individual's e-mails at work for a day, you get a sense of what her life is really like. On Monday morning, she e-mailed her friend saying, "Boy, that was fun going out to such-and-such bar on Friday. Where are we going tonight?" And she is joking. As to the

weight-loss claim, we had an e-mail from her to a friend of hers saying, "I've been going to Jenny Craig and it is really working." [Laughter.] And that ended the case.

It is not always the defendant staving off producing e-mails because they're afraid of what's in them. They are just as often trying to stave off production because of the cost and huge distraction. You must be alert to gamesmanship by advocates, but I also would urge, having made many mistakes in my own practice, that just because it is a computer search and it is a computer doesn't mean that there can't be all sorts of good-faith foul-ups. Failure to produce is not necessarily due to evil intent.

So that is essentially the legal background. Now maybe we will get back to some of the more fun things.

Drucker: Before you leave the microphone, I have some observations and then a question. From my own experience in employment arbitration, I have seen success in the use Ted describes of search terms and sampling. This is encouraging. I also note that as employment arbitrators we must be prepared to resolve questions concerning who bears the burden of the cost of electronic discovery. With respect to sanctions, it is important for us to be familiar with Rule 37 because there is some question about whether arbitrators in an employment or commercial context have the authority to order sanctions. Certainly, if we do, we have no broader authority than a court would. My question goes to the application of the litigation hold in unfair labor practice or duty of fair representation cases. Would you suggest that parties use that approach in those contexts?

Rogers: I haven't thought enough about that issue. If you did that, however, you would have a global hold in my opinion.

I don't want to sound like Pollyanna, but I think things are getting better because, frankly, a lot of corporations faced with a lot of litigation are being driven to systems where they are simply not destroying anything anymore. Storage costs are getting cheaper and systems are becoming more transparent. So it may be that this issue will go away.

Drucker: Thanks, Ted. Now we turn to Lesli Bruden, Labor Relations Manager with Qwest in Denver.

Bruden: Good afternoon. Qwest, as you probably know is a telecom company that covers 14 states in the Western United States. Jackie has asked me to discuss some of the practical considerations of the new technology.

For the past three years I have been the company representative in advisory bench arbitrations. There are two types of cases that have involved electronic data rather extensively—GPS and "cramming" cases.

Before I get into them, I would like to review with you some of our contract language. In preparation for this session, I went to our current Qwest contract as well as some of our older contracts and those between the union and some of the other telecom companies. Surprisingly, within our Qwest contracts, there was a lot of consistency in the language on the use of electronic data in call monitoring, call recording, and call sampling dating back to the pre-1989 era. There was no consistency across companies, however, on electronic data gathering. At Qwest, we have one side letter that is devoted to call monitoring but we have another broader side letter regarding electronic data gathering. Both are longstanding, dating back to the pre-1989 period.

The electronic data letter concerns any type of electronic data gathering that might come up presently or in the future and it sets out the requirements that the company must go through before it can implement that type of electronic data gathering in reference to performance monitoring. Under our letter, we are required to notify and provide information to the local unions and to the employees before we systematically implement electronic data gathering for a particular performance metric.

This letter also requires us to share the electronic data with the employee in a timely manner if it is being used for developmental or disciplinary purposes. Finally, the letter also specifically addresses the use of electronic data for disciplinary purposes. It indicates that an employee cannot be disciplined as a result of electronic data that has been collected except for fraud, privacy of communications, gross customer abuse, or when developmental efforts have not been successful.

A number of my cases within the Network Group—the field organization at Qwest—have involved GPS. Four years ago that was not such a familiar term with most people, including arbitrators. In December 2002, Qwest began deploying our Global Positioning System across all 14 states and placing GPS units in the field technicians' Qwest vehicles. We were using a contract provider—@Road—which provided us with live feedback on the locations of our Qwest vehicles through a Web site. This vendor also provided us with Exception Reports that would include information

that allowed us to more effectively manage the productivity of our technicians. We placed these devices in more than 6,000 Qwest vehicles and then, as I indicated, @Roads provides us with the live data. They guarantee that the GPS location data for an individual truck is plus or minus 10 meters from where the truck is actually located.

The screen that our dispatch center manager sees shows symbols representing Qwest trucks, with arrows indicating motion. When he places his cursor over a particular vehicle, he sees information that identifies the truck, the date, the time, and the status of the vehicle—whether it is moving or stopped. If it is stopped, the information shows how long it has been stopped. Our dispatch center uses this kind of tool to ensure that we are meeting company commitments, both regulatory as well as individual customer commitments. Supervisors can also see which technicians are located near a particular job where help may be needed to complete it on schedule.

Technicians are required to stay current with our dispatch center. Disciplinary situations arise, often by a customer complaint, when we discover that the technician was not where he or she was supposed to be. GPS comes into that kind of disciplinary situation. Our supervisor will use GPS to see where the technician's truck was when it was supposed to be reporting to a customer premise. Depending on the results of that review, they may look at further data to see if there is a pattern of problems with respect to the technician's locations. GPS is compared against our dispatch center data. By comparing the dispatch data with the GPS data, we may uncover patterns of discrepancies in terms of the technician's whereabouts.

Ultimately, if discipline is assessed, I will be using screen shots to demonstrate the technician's locations. Reports produced by @ Roads demonstrate the whereabouts of a particular truck with the individual technician identified as well. The reports provide summary data such as the amount of time that the truck actually spent moving during a 24-hour period and the amount of time it was stationary. Ultimately, the information I would be interested in is the actual movements of the truck, which we can track over the course of a day from the company garage to the various points, including addresses where the truck stopped, and for how long, and finally its return to the garage.

If discipline is assessed and it goes to arbitration, I have two hours to present our case to the arbitrator with up to two witnesses. I summarize the information to compare the dispatch results, the GPS results, and the employee's electronic time card along with other more traditional evidence.

With respect to our call centers, we have had "e-talk" software in place for one to two years. It is a combination of audio recording and systems monitoring. Yesterday we talked about systems that could track every keystroke an employee made during the course of the day. This is a very similar system. It combines the audio recording of our sales consultants as they are working with customers, combined with the work that they actually do on the systems as they are talking to the customer. This system is useful where violations of sales ethics are suspected and an employee has been disciplined or terminated for cramming, slamming, or failing to make the appropriate disclosures. Qwest cannot review every call that is taken by its employees, but we do a sampling procedure whereby one hour of each employee's day is recorded and then a small portion of that one hour is reviewed by our quality assurance people.

As they are listening to the recording of the call between a customer and an employee, our quality assurance supervisors are viewing a screen. As the sales consultant is making the sale, the required disclosures that they must make to the customer pop up on the consultant's screen. As they pop up, the consultant is required to proactively close the box in order to proceed and to be able to see the rest of the screen. As the sales consultant is selling a package, he or she is also required to make a disclosure with regard to our flat, basic rates.

Cramming involves adding unauthorized products to a customer's account without their permission. In the past, cramming cases involved more typical kinds of evidence—call recording, customer account notes, computerized sales orders, and customer testimony or customer statements. With the advent of "e-talk," if the particular call in question was one of the sampled calls, that process is going to become simpler and we won't have to involve our customers in these arbitrations.

With these cramming cases, we found that if we had only one or two occurrences, then it was very difficult for the company to support a termination. So we have adopted what we call "one bite at the apple" policy—the first time the employee is found to have

crammed a customer, they get a warning of dismissal. If it happens a second time, then they will face termination. Of course, if we see a pattern of seven or eight occurrences over a short period of time, the employee may face immediate termination.

In conclusion, electronic data is very helpful in terms of presenting actual evidence of the employee's misconduct. But it needs to be used carefully, particularly in my advisory bench arbitrations where I have only two hours to present the evidence. It also becomes very important that that electronic evidence is shared with the union during the course of the grievance process and that, in fact, it was shown to the grievant at the time of the investigatory meeting. They are entitled to the best opportunity they can have to recall the particular events. I am advising my client groups, don't hide the ball. Show them the GPS. Show them the dispatch records. We want to give the employees the best opportunity they can to recall what happened on these particular days. We will produce that information during the grievance meetings as well as arbitration, if necessary. Thank you very much.

Drucker: Thank you, Lesli. Joining us now is Martin Costello from Hughes & Costello to give us the union viewpoint.

Costello: Good afternoon; and thank you. One of the panel members mentioned that we could tell by the heavy eyelids in the audience that this panel has the coveted position of Friday after lunch on a holiday weekend. [Laughter.]

It reminds me of an arbitration hearing I was involved in—this is a true story; you can't make this up—where the arbitrator began to nod off during the union's case in chief. To add insult to injury, it was during the union's opening statement. I didn't know what to do so I whispered to the court reporter, "Wake up the arbitrator." The reporter turned to me and said, "You wake him up; you put him to sleep!" [Laughter.] You can't make this stuff up. But I do want to say for the record that no arbitrator in this room was involved in that case.

What I'm going to talk about is what I call, "Big Brother at Work: Workplace Electronic Performance Monitoring." Needless to say, I have a little different slant on it than the employer speakers you have heard up to now. Sitting as an arbitrator, you have to determine whether you are even going to receive this electronic data into evidence. There are two considerations. One is the foundational consideration: Does it meet the standards that you would set for the receipt of any evidence in a hearing that you would conduct? And second, because of the way these data

are obtained: Is it proper to receive it even though it may be reliable? So you have to resolve the reliability question first, and if it passes that, then the question is whether it is procedurally proper to receive this evidence. To complicate matters, it may be admissible for some purposes and not admissible for others. We have seen, for example, with the Qwest side letter, that sometimes these data are not admissible for disciplinary purposes.

A proper analogy might be to many drug and alcohol policies that provide, as Lesli said, the one bite at the apple. The employee appears to be under the influence, so there is probable cause testing. Then you have a test result that shows that the person is under the influence of alcohol. On a first offense, the employee is then allowed to go into the employee assistance program. The data are not used to fire the person; it is protected. Some of the policies go on to say that the data are private—the employer may not disclose it to the police, for example.

I had a case where an employee showed up for work intoxicated. The first clue the employer had was that the employee smashed into the company fence in the company parking lot with his car. Management looked at him and he appeared to be under the influence so they invoked the right to test and he tested 0.24—three times the legal limit. He hadn't punched in yet, so he decided that he would take a sick day and leave. The employer called the police. Not only did they call the police, they turned the test result over to the police. The company drug and alcohol policy prohibited that. There is also a statute in the state that makes that a violation of employee privacy and it is inadmissible in any criminal proceeding. Nobody involved in the case seemed to know that. The prosecutor did not know it. Neither did the judge. So because the employee had a bad driving while intoxicated (DWI) record, he was charged with felony DWI. His lawyer advised him to plead guilty to felony DWI, which he did. That is when I first heard about the case. And I also find out that the lawyer charged him $30,000 to plead him guilty to this felony DWI. I would have pleaded him guilty for $5,000, you know. [Laughter.] The reason I tell this story is so that you can see how the disclosure of some of these data that we're talking about here can have severe consequences if they go outside the realm of the permissible pursuant to the contract, such as into an arbitration hearing where it should not properly be brought. It is you, the arbitrator, who have to be the first line of defense.

So what are you looking for to make the admissibility decision? Let's take a look at the "bits and bites"—the basics of performance monitoring. What is it? What is it required to do? And how does it work? Then we will look at some real life applications.

Concerning the basics, this may be a review for everybody, but it never hurts to review. With electronic monitoring of employees, their whereabouts, their activities, their productivity, and everything else that they do can be monitored. We might think that employees can be monitored only quantitatively—how many pieces in the warehouse did the employee pick? But employees can also be monitored qualitatively—did they pick the right pieces? Was a mistake made? Considering Lesli's presentation, the questions are not only "Where is the truck?" and "How long it has been there?" but also "Should it have been there at all?" and "How fast was it going?" You noticed that the Qwest screen showed how many miles per hour it was traveling. So we have both a quantitative and a qualitative analysis of what the employee is doing.

What are the devices that do the monitoring? We have already heard about global positioning systems, automatic order selectors, use of bar codes and scanners. All of these devices depend on a computer to upload the information. The peripheral is a device that the employee has or accesses. That UPS driver who wants your signature on a device—that is the peripheral. Or the peripheral might be a sensor at a door so that when an employee passes through, it picks up the employee's badge that has a chip that is uniquely encoded.

There are two concepts that you might not be familiar with—"transaction" and "time-stamping." The devices record what we call "transactions." A transaction is anything that an employee does that activates the device. That might be scanning a product at a checkout, or opening a door, or passing through a room, or driving to a location—those are all transactions. Time-stamping is the ability of the computer to note that the activity occurred, when it occurred, where it occurred, or how long it took. You put those two concepts together and add the software that instructs the computer on what to do with the data. For example, it might be to generate a particular kind of report, a map of the employees' whereabouts, a score of their productivity as compared with a standard that's been set in the warehouse, or in comparison with the rest of the workers.

The largest investment, of course, is the computer itself, but all companies have computers. The peripherals are not only rela-

tively inexpensive but also have other uses as well. They monitor not only employees, they also monitor inventory, for example.

Now, the arbitrators in the room before whom I have practiced can attest that there is not a biased corpuscle in my body [laughter], so they know that I would not make any comment at a gathering such as this that would favor the union position. So I can truthfully say, these systems always start out with a good and valid business purpose. For example, we want to see that our truck routes are efficient, that we can have that on-time delivery, that we are not wasting gas, and so on. You can apply that logic to whatever industry you want. But this leads directly to monitoring the employee because management cannot achieve the business purpose unless they know what the employees are doing here, there, and everywhere. Right? The next step, of course, is that because management has the data on individual employees, they can use it to counsel with those individual employees who are not meeting expectations. So quickly the system becomes a means of surveillance, which is used against the employees.

Unions are lax in letting that happen. The Qwest letter is a good example of the union doing the right thing in that the information may be used for some purposes but not for others, so they have reached an accord and accommodation on this. I come from a family of 11 children. We used to like to tell our parents—both of whom went straight to heaven because they had their purgatory here, on earth—"Well, you can't make us." And our parents would say, "Well, maybe we can't make you do it; but we can make you wish you had!" [Laughter.] Well, that's the disciplinary approach. If electronic monitoring simply comes down to discipline, that approach hurts both sides. I remember when we were kids, we got hurt for refusing to behave as our parents wanted, but our parents were also disappointed in that they did not achieve what they wanted us to do. Similarly, if the threat of discipline is the employer's approach to achieving its ends, they will never get the employee to be productive. It is expensive and wasteful to do things that way. It should be the last resort, not for some touchy-feely union kind of reason, but because it is good business for the union and the employer to work together to learn why the company has to be productive and how the union and its members can help the company preserve their jobs and how everybody can get along together.

Let's turn to some real-world applications. In King County—the Seattle, Washington area—it is not only the employer who has the

GPS data, but the public also has the data. They can go online and find out where their bus is. Somebody with their cell phone can determine where the bus is and when it is coming. In some political environments of the world, publicizing where the bus is could be dangerous. I am exaggerating to stress the point. But there are ways in which such data, given to the public, can be misused.

I had a GPS case where a bus driver in St. Paul, Minnesota, was fired for being way out of his territory. He went through the suburbs and then to the exurbs with the bus. They were tracking this the whole time and they had a map with the data to use against him. His defense was that while the management-plotted location of the bus was true, his bus had been hijacked. A hijacker at gun point forced him to offload all the passengers and drive all the way around the county. He also had a backup story in case the hijacker story was not accepted. His backup was that he was an alcoholic, that he was totally drunk and had blacked out and couldn't remember any of this anyway. [Laughter.] The arbitrator put the end to it when he asked the grievant, after his rambling explanation, "Do you have a problem with drinking?" The grievant responded, "Oh, no, I like to drink!" [Laughter.]

For delivery drivers, the scanning devices and GPS data can be either synchronous, where management has the data in real time to observe what a driver is doing and how long it is taking to do it, or asynchronous, where the data is not immediately available but it can be uploaded and a report can be generated.

With respect to health care personnel, each of their ID badges has a unique chip that sensors identify when the health care worker, for example, enters a patient's room. They don't have to scan it in order to show they have been in and out of a room, how long they've been there, and so on. It is all automatic. We have seen some serious cases. We are all familiar with the occasional homicide where a health care professional administers lethal drugs to a patient. These ID chips have been used to track the health care worker's patterns with the decedents. But less high profile disciplinary matters don't necessarily make the news. There have been cases where employees are stealing from patients, or stealing drugs or other supplies from the hospital. Depending on how sophisticated the sensors are and where they are located, valuable evidence can be derived from them.

Other types of employees subject to electronic monitoring include supermarket checkers who, through the scanners used in

the checkout lines, can be evaluated on quantitative and qualitative dimensions. Warehouse forklift operators are also subject to meeting quantitative and qualitative productivity standards. The way their performance is tracked depends on the type of equipment in use. In one type of system, the operator gets the order, which is pre-sorted; they sign on electronically and they sign off when they are finished. A computer-generated report shows how quickly and how well they did the job. That is compared with a standard. A disciplinary structure is then superimposed on that to determine whether the employee's performance is good enough to keep his job. Then there's voice-directed picking, which is even more sophisticated. That's the so-called vocal-X system where the employee wears a headphone and says, "Ready," and he or she is given the order. The employee then picks the order and signs off verbally. In between, each item that is picked is monitored.

Finally, we come to the unkindest cut of all. The Wisconsin State Attorney General's Office has developed productivity standards for its lawyers. Each case file has a bar code. When you scan in the bar code, you're on that file. Then there are additional bar codes to indicate that you are doing research, you are drafting a letter, you are drafting a pleading, or doing something else. The end result is the attorney's report of annual billable hours.

Thank you very much.

Drucker: Thank you, Martin. Let me ask Lesli and Ted if there is anything that they would like to add or comment on from the management perspective with regard to the points Martin raised.

Bruden: Actually, I thought you were very even-handed from a union perspective. That was great! And I would agree that these systems do start with a business purpose but I would contend that they continue with that purpose, as well. For instance, with GPS, it did start as a dispatching tool and it has become a productivity tool. But we don't expect our supervisors to sit in front of a monitor all day. They have to spend their days out in the field. Nevertheless, I have heard that same concern from the locals.

Rogers: The thing that comes to my mind in response to Martin's observations is that electronic monitoring for productivity, accuracy, or efficiency is simply inexorable. You are like King Knute beating against the tides if you try to oppose it. ESPN baseball has that little box now that shows whether the umpire got it right on strikes and balls. That has got to be terribly embarrassing and the umpires did make an issue about it, but it's too late. In tennis, the

same kind of report is generated. We are finding it everywhere and I don't know that there is anything to be done but enjoy it. [Laughter.]

Audience Member: May I ask a question of the experts? Is there a method for you to track how much real study time we put in versus what we bill for? [Laughter.]

Drucker: Thank you for that critical question, Gene. And thank you to our panel.