Chapter 6

NEW FRONTIERS: BIOMETRIC INFORMATION TECHNOLOGY AND PRIVACY ISSUES

Moderator: David R. Williamson, Member, National Academy of Arbitrators, London, Ontario

Panelists: David Hodgkins, Director of Human Resources, City of Berkeley, Berkeley, California

Rachel J. Minter, Law Offices of Rachel J. Minter, New York, New York

Samir M. Tamer, Chief Scientist, Ingersoll Rand Recognition Systems, Campbell, California

Hand scanners, iris scanners, and other biometric measurement techniques are increasingly being used by organizations to limit access to designated areas and in place of the traditional punch-in time clocks. In this session, a physicist in the industry discusses how these systems work and the nature of the personal information collected. The panel then explores the attractions that the adoption of this technology has for employers and the reservations and concerns that unions and employees have about the utilization of biometric information technology in the workplace.

Williamson: I am David Williamson, the moderator for this session. I am an arbitrator and member of the NAA residing in London, Ontario, Canada. It is halfway between Toronto and Detroit. The distinguished participants I have are from California and New York. I will introduce them in alphabetical order before we get underway and ask them to make their presentations.

On my extreme right is David Hodgkins. David is the Director of Human Resources for the City of Berkeley, California. He brings a perspective of more than 25 years in human resources. David will address the benefits that accrue to an employer upon the introduction of biometric technology into the workplace.

To my immediate right is Rachel Minter from New York City. She is a union-side labor employment lawyer in New York with more than 25 years of experience. Rachel will address the issues

that the introduction of biometric technology into the workplace has for unions and employees.

To my left is Samir Tamer, a technology physicist with Recognition Systems, an Ingersoll Rand company, in the Bay Area, specifically, Campbell, California. Samir specializes in biometric technology and biometric profiles; he is a scientist and he will begin by addressing electronic hand scanners and iris scanners and explain the nature of the technology in direct layperson's terms. In other words, what it can do, what it cannot do, and how it functions.

Tamer: Thank you. I am not an arbitrator. I am not a member of the NAA. Hopefully the things that I say today will make sense. I am not here representing my company. This is not an official statement from Ingersoll Rand or emissions systems; this is just my opinion as an industry expert.

What I will do is give a quick run-through. This will not be a scientific endeavor. This will be just more of an introduction, a quick overview of some technologies that people are gravitating towards so you can see what is happening in the field. Specifically, what are biometrics and why are they used?

The definition of biometrics has been crafted and worked on over quite a bit of time: Biometric is defined as the automated recognition of individuals based on their behavioral or biological characteristics. Straight off the bat, you see we are talking about people. Sometimes similar technologies are used for animals such as thoroughbreds or cows if you are tracking mad cow disease. In the industry, that is not considered to be biometrics because biometrics focuses on humans. We do allow behavioral or biological characteristics. I will not speak about behavioral today because they are not used as much, however, things that would fall into that category would be some types of voice recognition and most signature recognition. Also, there has been a lot of study recently in gait recognition—walking. There is a big hope that you can do biometrics from a distance, mostly for government applications. If you can spot someone a quarter- or a half-mile away, this is useful. But gait, again, is behavioral. It is something that you can try to learn or break if you do not want to be identified.

Biometrics, in general, is a technology that can compare one sample with another sample. If I stood up here and said, "Hello, I am Samir Tamer," you would have no way of believing that was true. If I gave you my fingerprint, you would still have no way of believing that was true unless you have some reference with which

to compare it. When we talk about identity management, or the use of biometrics for access control or verification, we have to assume that we are trying to verify that the person who is in front of you right now is the same person that you enrolled in the system some time in the past.

Take note that—especially with *CSI* and other pop culture sorts of phenomena—there is an assumption in the environment that biometrics and related technology are infallible. That is not true. Even DNA is fallible—not very fallible, but it is. There is always the risk that one person could be misidentified as another person. There is a risk that someone who is enrolled in the system and is a legitimate user might get rejected for no apparent reason. Also, there are classes of people who cannot work or fit with biometrics. For example, my company does hand recognition. If someone lost both of their hands in an accident, that person will not fit with the system.

Biometrics is not infallible because it does not inherently return a yes/no sort of a decision. If it says "How much like Samir does this person look?" It might give you a number such as 80 percent, but is 80 percent good enough for you to unlock a door for me? I do not know. But each site, each employer, each user of biometrics has to make a decision as far as setting what we call a threshold. What is your threshold for how sure, confident, you need to be? This is going to be a tradeoff in any situation. That is, a tradeoff between absolutely positive that this is the right person versus 15 people who were authorized to get in the door but were rejected because you were not 100 percent sure. This idea of a variable threshold in biometrics is a significantly important idea.

What is the timeline for biometrics? Most people in this room probably just started hearing about biometrics used for commercial applications. The reason is that commercial applications did not develop until the early 1970s with the first hand scanners and the first retina scanners. In the 1990s and after 2000, there was a huge proliferation of commercial devices from other biometric modalities that I will address shortly.

Now let us reach back to the distant past. When were biometrics first used? The first records that we have of it are from the 1400s. At that time in China children had both of their hands and feet pressed for foot prints and hand prints as a means to identify children. There is not much of a record about why and how often China did it or how well it worked, but it is documented that it happened.

The next milestone was in the 1850s when a fellow in India named Sir William Randolph Hershel was forming contracts with locals and he wanted to scare them into abiding by the contracts. He had no real authority to do so but he required a handprint on the document as proof that the individual promised to do or perform the contract. It was nothing more than a ruse. He was trying to trick the people into abiding by the contract but it worked because they did not know what the power of doing this thing was. They assumed bad things would happen to them if they did not sign along. Over the course of several years he had contracts with many different people and he actually noticed that the handprints and the fingerprints looked different from each other, and he could actually tell who signed this contract and who signed that one. That was the beginning of the recognition that you could discern one person from another based on fingerprints.

Also during the 1850s in the United Kingdom there was a big push toward something called Brittilian measures, which were used only for criminals. If someone was arrested and the police worried that they were given a false identity, then calipers were used to measure the prisoner's cranium and arm length. There were 15 or 20 different numbers. A list of these were maintained in an index system in a card file and checked against to see if any other person matched. This worked great except for the fact that it did not work because in 1902 there were two people who had exactly the same measurements and their names were very similar. This went to court because the individuals claimed not to be related but, in reality, they were twin brothers who were lying. Simply because the Brittilian measures were working out exactly the same for two different people debunked the entire science of it and people departed from its use.

No matter, for around the 1890s fingerprints came into use and have been going strong for more than 100 years, although the technologies that are used to capture and match fingerprints to each other have changed and continue to evolve. By the 1940s, tens of millions of fingerprints had been collected.

Let's switch focus from history to biometric systems. How do biometrics fit into systems? Security—this is the first one that everyone thinks about. Suppose a door is locked to keep bad guys from entering. If you give a key to individuals whom you want to enter, your authorized users might lose the key and then the bad guy picks it up and he has a 100 percent chance of entering. He will definitely get in. Instead of a key, you can have cards such as

proximity cards or mag-stripe cards, similar to your credit card. There is a huge array of different types of credentials for use in unlocking a door. The problem again is, once you lose it, the bad guys definitely get in.

Try something a little different such as a password, maybe a personal identification number or PIN. You can add a challenge response such as "what day did you come in to work last week?" or you could use something silly but useful as long as that something changes. This is a different level of security rather than only something that you have for entering through a door. The problem is that it is still easy to look over someone's shoulder as they type in their PIN or it is even easier to ask them. If you have two people working together, they may share their password.

There was a desire to have something that worked better in the sense of ensuring security, and that is where biometrics enters.

Biometrics is not something that you have or that you know, it is something that you are. I am not going to say it is who you are because we are not talking about personality, but we are talking about fingerprints, hand size and shape, iris patterns, and the look or shape of your face. These are all commonly used biometric traits that are measured by a machine that then automatically makes a "yes/no" decision as to whether you are the same person that they (an employer) believe was enrolled way back when.

Thus, security sites will often have a combination of the three security items. You may have a card or some kind of credential that you insert into a reader and then type or input a PIN number; after you have entered your PIN, then you have to give a fingerprint. At this point you are fairly certain that this is the right person. This approach—card, password, and biometric with fingerprint—is being rolled out by the U.S. government to all federal employees now as the personal identity verification (PIV) program. The cards are already being issued to 17 million federal employees; contractors to the federal government will be required to use this system as well.

Another example of a place where biometrics are used to allow the good guys in and to keep the bad guys out is San Francisco International Airport (SFO). How many of you flew into that airport coming to this meeting? Most of you. SFA has more than 200 doors from unprotected, public areas into protected areas, where people like you and I could enter and access baggage that goes underneath the airplane. In other words, you would have access to the airplanes themselves. Many of those doors are protected

by biometrics with the use of hand geometry readers installed in 1991. The numbers that I have seen quoted are that at any given moment they have 30,000 active users. Every day at SFA they have more than 15,000 users. This is a lot of people trying to get into work every morning, a lot of people moving back and forth. Recall the error rates that I talked about earlier, there is a tradeoff. How many of these 15,000 people get stuck at the front door because the reader did not work for them that day? You can readily see how this would be an operational consideration for a director of security. How many people does the director want banging on his door saying "The reader did not work." If your paycheck is tied in some manner to entry, then you are even angrier.

Biometrics is not some sort of panacea for security. It is one part of a system in the same way that a lock on a door is one part of a system. If you have the best lock in the world on the front door but the back door is unlocked, then that is not a very secure environment. If someone can hold the door open and six people walk in, that is not a very secure environment. When we talk about implementing biometrics in a system, we also talk about designing the entire system at one time with one cohesive plan to ensure that you do not miss a loophole where people can slide through.

Another big program that has been rolled out in the last few years is the U.S. Visit Program. All non-citizens have to stop and give their fingerprints when entering via airlines. In years past they gave two fingerprints and a face image. Now this has been ramped up to 10 fingerprints to ensure greater accuracy for identification. Suppose you find a fingerprint in a cave in Afghanistan but you do not know whose it is and you do not know which finger it is. Now every foreign national entering into the United States will be providing all 10 fingerprints and the fingerprints are checked against the U.S. Visit Program database.

In other countries there have been efforts towards establishing or using national identity cards, especially in the Middle East where a few of the Arab states have introduced national identity cards based on a fingerprint or on iris recognition. These are huge programs where you have tens of millions of people enrolled. As you may surmise, this has been less than exuberantly accepted within the United States and United Kingdom in terms of privacy issues. In the United States there are two things that people have a sincere visceral reaction to: one is a national database approach using biometrics, which reminds Americans of a "Big Brother" keeping track of them, and the other is simply the notion or concept of a

national identity card, regardless of whether it has biometrics on it. These are hot button issues in the United States.

Aside from security, using SFA as an example, the other significant application for biometrics is in time management and payroll systems. For example, I leave my office around noon and drive to San Francisco. What if I ask my buddy to clock out for me at 5:00 p.m. like we always do? I will be working, right? What if someone is a good friend and I am going to Lake Tahoe to do some skiing. Can you clock out for me an hour later? This is easy to do and some percentage of the population in every workforce does seem to do it. One of the numbers that I have heard quoted is that payroll costs decrease by about 5 percent when you introduce biometric systems as a way to stop "buddy punching." I do not have a means to verify that number, but that is the number talked about within the industry.

Standing alone, biometrics is not a payroll system. You have a "yes/no" box that indicates that this is the right person, but with what does that box communicate? It talks to the back-end software that calculates how many hours you've been at work and then, depending on the state or jurisdiction, whether you are eligible for overtime for these particular hours. At some places, more than 8 hours a day is considered overtime and at other places more than 40 hours a week is considered overtime. This may not seem like a big deal to us, but when you come home and your paycheck is wrong, that is upsetting. Biometrics devices get blamed for this kind of stuff but it has to be viewed as a system, the interaction of a biometric device with some sort of back-end software, where each has to work correctly for the entire system to work. If there is one weak link in the chain, then the entire system has problems.

Someone posed a question as to a hand print, which is often used interchangeably for both hand geometry and for palm print. These can be affected by fingernails. Palm print, generally, looks at only the texture of the palm and would not look so far down the fingers as to even know that there were fingernails on there. Hand geometry units are generally larger than palm print devices and are either dark gray plastic or a beige-colored metal and work on the size and shape of the hand. In general, when we talk about people not being able to get in a door because they are falsely rejected, that is due to either the individual has not used the system in six months or their body has changed. People gain weight, lose weight. If the individual has a large bandage or something similar, that would definitely affect hand geometry systems

because the system is looking for size and shape of each finger, the palm, everything.

Fingernails can cause a problem and lead to a false rejection. I work at a hand geometry company so I can speak to this. Fingernails are tough for two reasons: one is that they change in length constantly. One day you can walk in with fingernails like mine and the next day with artificial fingernails so the algorithms very actively go in and look for that and try to handle it. In general, algorithms will not be effective 100 percent of the time but they will probably work 99.99 percent of the time. There is always room for improvement and it also depends at what security threshold the devices in question are set. If a site administrator seeks to have security a priority over convenience, then some people will be inconvenienced and that is a tradeoff that must be made on a site-by-site basis.

In hand geometry we are focusing on the size and the shape of the hand, the way in which it is looked at or illuminated in the infra-red. If you walk up to the device, you are not going to see flashing lights or anything interesting like that, although it is flashing but not in the visual spectrum that we can see. The image is broken down to a silhouette, which means no fingerprints, no palm prints, no texture, no hairs. Rather it is the physical size and shape—lengths, widths, heights—characteristics of that nature. This is good and bad because information is lost such as the texture of the palm. We are looking at only the bulk-size shape of the digits. The upside, though, is that it is more privacy-enhancing in that I can see most of your hands, at least in some measure of a pose, but it is physically not possible for me to somehow know what your hand geometry template would be like.

Hand geometry is also used in what we call verification mode, one-to-one authentication. In practice that means I walk up to a door and claim "I am Samir" and then I put out my hand to prove it. That is an inherently different approach than me walking up to a door and it looks at me and identifies me as Samir. In one-to-one authentication I am making a claim of identity and then proving it, but in the later identification process the system is searching a database and seeing if I am one of the people in the database. In the biometrics sphere this is a big issue—authentication versus identification.

I will move on to fingerprints, which is the de facto standard. When someone says "biometrics," they are thinking "fingerprint" in general. This is looking at what we call minutiae points, which

are the fine lines on your fingers, the places that come together, places that bifurcate. There are different types of minutiae points that we define. We look at the X/Y location of these things with respect to each other. Imagine looking up into the night sky and you see stars. It does not matter if you are in the southern hemisphere or the northern hemisphere, if it is a constellation you can figure it out because you are handling rotations in your mind and magnification differences. Fingerprint recognition is the same thing—a constellation of points that the algorithms rotate and figure out on the fly.

Face recognition. This is something that is very popular because there are existing databases within the government similar to fingerprint databases. Again, if you go to Afghanistan and you get a picture of someone from a distance, you would like to be able to spot that person as they are entering the country. Face recognition has garnered much attention from governments. The other amenable thing about face recognition is the non-contact nature of it, meaning that you do not have to physically walk up and touch something. Hygiene is an issue with anything you have to touch. With face recognition, you walk up to the door and look at it and presumably the door slides open. If you have to grab the door knob and pull it open, then you just lost your benefit because now everyone's touching the same door knob. Face recognition is used for both authentication and for identification, so there are big search databases.

Iris recognition: This is a new kid on the block. Extremely accurate. Very cool. It used to be difficult to use in that you had to do a little dance and line yourself just right in front of the sensor. The sensors are getting a lot better. I have seen demonstration systems recently that can tag you from 10 to 15 feet as you are walking and looking towards the camera for a good image. Iris recognition almost always is used without cards or passwords or anything like that, so there is a cost savings.

Vein recognition: Another really new and interesting thing. There are two types. One is finger vein. You walk up and stick your finger either on top of something or into something. The other type is palm vein, where you push your hand above something and there is another type where you grab a handle and push your hand upward into it so that the device is looking at the veins in the back of your hand. In both cases you are flooding the area with infra-red light and the oxygenated blood in your veins absorbs the infra-red light such that those areas in the image look black and

you have a field that is mostly white but with some black traces. This looks like a spider web or a road map and from that you can place a pattern of finishing algorithms on it to discern one person from another.

Privacy is a significant issue in biometrics. If you are enrolled in a system to pay for your groceries with a fingerprint without needing to bring cash or your credit card, then you walk up to the counter, show your groceries, place your fingerprint in a device and it charges your credit card. There are privacy implications as to what that supermarket does with your fingerprints. Currently, there are no problems and the data are held locally, but you can imagine if the FBI wanted to see every fingerprint that a grocery records in the next 12 months? These are the kind of things that have to be spelled out and understood both by the people creating these systems and by the people installing them, because left unchecked, governments will ask to do things, because they will see a need for it. It is all about balance—balancing privacy, balancing convenience, balancing security.

Assuming that a company is using the data appropriately —only keeping it onsite, getting rid of it after an employee leaves the company, only keeping what's necessary to run the system—there are still questions about how the data are stored within the company. Is it on a computer with a password? Is it in a room that is locked? Is it encrypted on the hard drive? The most interesting is, do you have biometric data adjacent to personal data, like your name or your address? If you break into a company and steal 10,000 fingerprints, what are you going to do with them? If you can link each of those fingerprints to the name of a person, then you can start thinking about stealing the person's identity. There are understandings within the industry that these have to be addressed and you have to do the right thing, but I do not know that laws exist or whether precedent exists dictating it one way or the other.

I have been asked what is the probability or likelihood that my handprint could be confused with someone else's handprint. In other words, how unique are my handprints or irises? The quick answer—it depends on the threshold for a biometric system. It depends on how sure you want to be where you set the system. If you have a really tight security threshold, you can make the handprint truly unique, but that means that the authorized person is not going to get in the door as often as they might like to. To place this in context, for hand geometry we usually talk about .1 percent to .5 percent as uniqueness. On the other end of the spectrum

is iris recognition, where we talk about one in a million. It may seem obvious to use the iris but the other side of uniqueness is, how often do the good guys get rejected? Iris recognition has a higher rejection rate, that is, a false rejection rate, than some of the other technologies. With iris recognition you can obtain really good uniqueness numbers but the false rejections are not good. Again, the tradeoff of security versus convenience.

Fingerprint is a smooth transition where you can have high uniqueness numbers such as 1 in 10,000, but you are going to pay a price for that in terms of false rejections. If you operate in a super-high security area, iris is a great choice. Alternatively, use several fingerprints, not one, because if you require two fingerprints and both of them match for the same person, then you start getting into those really high security areas. There are other issues that come into it—costs, the ability to use in indoor and outdoor environments, and the robustness over time between days, months, and years.

Williamson: We will have the opportunity to come back and ask Samir questions at the end. I would like to move along so that Rachel Minter can present us with her views as to some of the issues that biometric technology has for unions.

Minter: This may not surprise anybody after listening to the technology that unions are not happy. A term that has been coined to talk about the use of this kind of technology in the workplace is "geoslavery." People do not yet understand the significance of having this data kicking around and being used in the workplace. I was going to do this later; but the last question just called out to this quote from EPIC, which is the Electronic Privacy Information Center. EPIC states that you have to ask the question: Why are you using biometrics? If it is just to have people clocking in and out by using an iris scanner or fingerprint scanner, then that is like using a sledgehammer to crack a nut.

There are many large-scale societal privacy issues being discussed about where we are going and whether we are on a slippery slope. What is going to happen to this data, both from third parties and what the employer is able to glean from it? There are many issues that unions need to be bargaining about to protect employees when this comes into play. I have a paper in the conference materials and it has all the cites. The issue of bargaining obligation on biometrics is still kind of open but there are a handful of cases. One of the cases cited I am litigating in New York City before the Board of Collective Bargaining, dealing with New York

City's unilateral implementation of a biometric hand geometry scanner made by Samir's company, the Hand Punch 4000. Nothing personal, whatever I say about it, but it has not gone over particularly well, and there are a lot of reasons in terms of the impact, the way people feel about it, and what is going to happen to the data.

In this instance we had a group of highly skilled people—I represent a 6,000-member union comprised of architects, engineers, and construction project managers. Nobody at the Department of Design and Construction ever punched time clocks and now they come in and there is this hand geometry scanner and they have to insert their hand in the device when they come in and go out. Now, of all the groups to implement this with—these are people who, if they are working 7:30 to 3:30 but the contractor needs to call them on the cell phone about something at 7:00 a.m., they will take the call. Alternatively, if they are working on a plan and almost finished, they will stay until 6:00 p.m. and do not request overtime compensation. These are dedicated people, so it did not go over well.

Why are the employers implementing biometrics? As a union in a post-911 world, it is very hard to take a position against increasing security, but that is not what is going on in this case. In fact, they installed the things after two checkpoints and they are at their workstations so this had nothing to do with security. This is for timekeeping. Biometrics is now a multi-million dollar industry. Check the Web and you will see ads where there are biometric systems that prevent "buddy punching." That would have to be very prevalent to justify something like the $240 million that the city has put into this project.

Now there is City College that is going to start with the white-color employees—the accountants and their IT specialists—with the new biometric finger recognition system. They sent out the marketing materials and I got a quote. Bio-scan technology combats the most rampant payroll pilfering activities: time theft and buddy punching. These two practices have embedded themselves in every private and public institution. This is the mindset.

In our situation the office of labor relations actually conceded that there were no rampant time and leave abuses at this agency. Everything keeps coming back to "Why are we doing this?" It is a policy decision. Now it also happens that we have the highest tech mayor in history—the former head of Bloomberg industries. There are other technological initiatives that raise privacy

concerns that are now going on in a similar time frame. For example, the taxi and limousine commission has mandated not only GPS in cabs, they now have a new system where drivers have to enter their Social Security number into the meter and it cuts them off at 12 hours. The City does not want people driving more than 12 hours, but all the drivers working double shifts are cut off. There are also cameras in the schools and in the future facial recognition technology could be used to catch images from the stream in the camera in the schools.

Policy seems to be along the lines of what we consider to be tracking and not security. People felt strongly about the "Big Brother" aspects. They felt their privacy was violated because you are sticking a body part into a machine and holding a piece of cardboard into a time clock. People have a very visceral reaction and do not want to give it over to the employer.

A lot of the cases focus on biometrics, and we are not talking about GPS, which is location awareness technology. A lot of the litigation and the publicity also have been about GPS in the mobile news units for a local television channel. They put it in snow plows on Long Island. People feel like they are being treated as five year olds. It is very demeaning and the implication is that people are scum and thieves.

There was a case—I believe it was last year—where 20 building and engineering inspectors in the state of Massachusetts were suspended because they refused to accept GPS-equipped cell phones that the employer was going to give them for the purpose of tracking their movements during the day. There is a reported case involving Otis Elevator where the employees disabled the GPS devices that were in the company cars.

Think about when you are tracking people. You do not decide anything biometric, it is time and attendance data. What does it tell you? Employee X usually palms out on the third floor before he goes home. Yesterday, the system shows that he palmed out on the fifth floor. What was employee X doing on the fifth floor? Sounds like a trivial thing but that is what you can know. If you have RFID or biometric sentinels at the entrances—for example, it is lunch time and somebody palms out of the exit to the building—the employer knows that she went to the diner down the street and not the company cafeteria. Small things, but this reveals a lot of information.

There is the concern about what happens with third parties hacking into the systems. It is not like they get your computer ID

or swipe your card, which you can change. You cannot change your retina, so if somebody gets hold of that information, it is going to be really annoying and inconvenient. This is on the Web site from the federal government's National Technology Institute—they have FAQs about biometrics. One of the questions is "Can I change my biometrics?" The answer is no, so if somebody steals your retina scan, you are going to have a problem with that.

Samir talked about hygiene. There was the "ick" factor, which also goes to the fingernails and if you have a large bandage on your hand that changes the hand geometry. We had an instance where a woman had a wound and a big bandage on her finger and she is trying to clock in. It was not even security. She unwinds the bandage and sticks her hand into the scanner. Everybody behind her in line completely and totally freaks out. The labor relations director then sends out an e-mail saying, if this happens again, it is the responsibility of the person behind that person in line to come and notify facilities management that the unit needs to be cleaned. She was somewhat embarrassed when that got introduced as an exhibit at the hearing.

We had all kinds of things that should have been affects bargained. For example, the Yom Kippur episode where you have to scan out to certify your timesheet at the end because after that you are off city time. You are sitting there waiting for your scan time to show up on the electronic time sheet. You are sitting there for 20, 30, 40 minutes, so everybody gives up on Friday. They go home and they do it on Monday except this guy suddenly realizes it was a Jewish holiday Monday and if he did not certify his paycheck then he was not going to get paid. He was going to end up getting a paper check and have to go to the bank instead of direct deposit, which was this whole other level of problems. He sat there for 40 minutes on his own time just so he could certify his time sheet. Endless problems. The City refused to bargain about any of them. Some of them were funny, if you were not annoyed about it from a labor relations perspective.

There are privacy issues. I mentioned hacking. Samir probably could tell you more about how hackable this stuff is. I am not a technician, but I still believe it is all hackable. That is one issue. The second issue is other third parties other than identity thieves. For example, you have an iris scan and insurance can learn something about you from your retina or your iris—glaucoma—or they do a vascular scan and somebody is having circulation problems

or nerve problems, does the insurance now know about you and does it compromise your ability to get insurance coverage?

[*Editors' Note*: Due to an audiotape malfunction, the presentation by David Hodgkins and the question and answer session that followed were not recorded.]