Reboot Communications
Public Safety Technology Conference April 29–30, 2002
Web site: www.rebootnorthamerica.com

RAJ NANAVATI PRESENTATION

Thank you for that introduction Tom. I appreciate it. I have been asked today to speak about biometrics and present an overview of the technology. Where it works and where it's being used and with the potential for biometrics is respect to terrorism. One initial question I have for the audience before I get started, is to understand your perspectives are from a general perspective. How many people here have actually used biometric technologies in every day life? Actually used fingerprint or iris or face technology? So, we've got a few people here, okay, excellent. How many of you used the technologies prior to 911? So, okay, most of you. One thing I'd like to underscore with the presentation is that the technologies, biometrics, are a very real technology. They can serve a very real purpose in terms of identifying people and preventing fraud. However, there's also been a lot of news and hype about the technology. So, what I'd like to do is separate some of the facts about biometrics in terms of how accurate they are, where they've actually been used from what the potential of the technology is. Sometimes people expect it to do more than it can actually do and we want to set reasonable limitations

on how the technology operates.

So, I'll start out with the definition of biometrics. Biometrics is the automated measurement of physiological or behavioral characteristics. So, that means it's automated. It's not someone looking at a photograph and comparing it manually. It's an automated process. It takes a few seconds. Physiological or behavioral characteristics, something you are, your fingerprint, your iris print, or something you do, signing your name. And it's something that can be used to authenticate or determine identity. That's an important distinction. One to one verification. That means you present your credentials, the system says yes or no. It compares your credentials against what you enrolled and it says, yes, this is a person, or no, it is not the person. That process is very fast.

There's another process called "One to Many, One to End Identification". That's a little bit different. That's when you take your fingerprints, submitted it to the FBI, and it will compare those fingerprints against 20, 30, 40 million people in the database and identify you from that group of people. So, you're not claiming an identity, rather the biometrics identifying who you

are. And that's an important distinction for a lot of the travel applications, because there's different ramifications for using one to one technology versus one to many.

What we have got here, and it's a little bit difficult to read, but it's basically a brief overview of the different types of technologies. Key stroke, facial, retina, etcetera, and there'll be a presentation that's available that can -- you can look at this at your own time, but basically presents an overview of how accurate the systems are, how much they cost, etcetera. We'll go through this in more detail during the presentation.

Okay, the two types of biometrics, behavioral and physiological. For most of the airport applications, most of the terrorism applications, etcetera, people are looking at physiological biometrics. The reason is those are more accurate. Your fingerprint doesn't really change over time. Your iris print, your retina print, etcetera, they don't vary. You might get a cut, they might become abraded or something like that, but they're fairly stable. With respect to the behavioral, those do change. The way you sign your name, the way you say a given pass phrase, how you type, those are

useful in identifying people, but they're not as accurate as physiological characteristics.

I am going to start out taking about AFIS technologies. This is one of the most important technologies in terms of preventing terrorism. AFIS refers to Automated Fingerprint Identification System. That's different than fingerprint technologies that is traditionally thought of. Fingerprint technology outside the realm of AFIS basically refers to putting your finger on a small scanner and the scanner does a one to one match and says yes or no. The AFIS technologies refer to the technology where you put your fingerprint -- ten fingers on a scanner. It takes images of all ten fingerprints and does a large scale match against millions of people. So, the best example of this is the FBI AFIS system where they have, I think at this point, 42 million fingerprints on file. So, when someone gets booked at a police station, or if someone does a background job check or something like that, they capture the prints locally and those prints are then sent to the FBI to do a large scale match. The key with this technology is that it is fairly expensive. It's much more expensive than using the one to one fingerprint, and it does require some amount of

guidance to using the system. The AFIS technologies are not self running, in other words, you wouldn't have an AFIS scanner just at an airport where someone comes up and puts their hand down. You need someone there showing them how to place their fingers appropriately.

There are four major vendors in technology, Cogent, NEC, Printrak and SecuGen, and the technology, the important part with this technology is that it's been around for quite awhile. Many police stations all over the world use this technology. It's not something that was developed a few years ago and just is now being deployed. It's been around for 10-20 years and it's fairly saturated in terms of getting them out to police stations. What we're seeing now more of is people using the technology for non-forensic type applications. For example, welfare systems or national ID. China right now is looking to roll out a large scale AFIS system for their national ID for 800 million people. The Philippines is rolling it out now for 25 million people. Nigeria is looking at national ID for 50 million people. So, the technology is real and it's out there and it's being used in larger and larger systems.

Here are some of the deployments where AFIS

technology has been used. The FBI AFIS has, I think, 42 million prints at this point. Another good example, is in the U.S. for welfare benefits. California, New York, Texas, Arizona, a couple other states use this type of technology. Now, if you think about it, it's extremely effective at preventing fraud. New York's a good example. They rolled out with their civil AFIS about, I think now, five years ago or so, and before that, if someone wanted to get welfare benefits, they go up to Queens, give an ID, put their finger -- not put their finger in a scanner, someone would look at their credentials, their driver's license, something like that, identify who they are and give them benefits. Well, it was pretty easy for that person to get a fake ID, go to the welfare office in the Bronx, do the same thing the next day, do the same thing again the next day in Manhattan, whatever the case might be. It was very difficult to prevent fraud. It was based completely on the idea itself. That was the only security method and it wasn't really that difficult to get a fake ID.

They put in the welfare system using biometrics such that when you got benefits, you put your finger on a scanner, took a picture of your image, and compared

it against every other person in the state who is getting benefits. So, it's comparing against 2 million other people. In that case you can't just get a fake ID, go to another location. It's almost impossible in that circumstance to commit fraud. It's a very effective automated way of comparing one person getting benefits against everyone else. So, you go from a scenario where it's very easy to commit fraud and very difficult to prevent it, to a scenario where you're almost automatically capturing all the fraud there. New York State, itself, has stated that they saved, I think, 2 to 3 hundred million dollars by using this system. Now, one caveat with that is that it's notoriously difficult to capture exactly how much the savings is because there are other factors, social and economic factors, etcetera, that go into it, but clearly they have saved a lot of money and fraud has gone down tremendously.

Some of the other programs, I mentioned briefly a moment ago, Philippines, Argentina, there are a lot of programs in Central America for national ID. Driver's licenses is another important application. Right now, for example, California -- when you get a driver's license in California, they capture your fingerprint.

So, you put your finger on a scanner and they capture it. Right now what they are doing is just storing that image. So, they've been doing it since about 1990. They're not using it in a biometric system, they're just capturing images and storing it on file. If there's a case of suspected fraud, they can go back and look at that image to figure out if someone has multiple ID. What they're looking to do now, and this is part of work we're doing for them, is to figure out how to convert that system into a full fledged AFIS system. So, when you put your finger on the scanner, it just doesn't store it somewhere in a database, but it compares it against everybody else in the state who has a driver's license.

Liescan devices, this refers to those fingerprint scanners used to capture images that can be used in that AFIS technology. So, these are relatively large systems. You put your ten fingers on the scanner and it captures images of all ten fingers. There are also systems that can capture one finger or two fingers, and this refers to liescan differs from the one to one smaller fingerprint systems in the fact that it captures a much higher quality image.

Now, I'll talk a little bit about the one to one

type fingerprint devices. These are ones that would be attached to your computer. If you want to log into your laptop, or it'd be something that you would put on a door. So, if you're securing a staler part of the airport environment where only employees are allowed to access, you can put a fingerprint device right on the door and make sure someone doesn't steal a card or a badge and access that facility.

The key thing with fingerprint technology is that it's very accurate compared to a lot of the other biometrics. It's very fast and it's very easy to use and there a lot of vendors out there that make this technology. So, there's not one or two systems to choose from, in fact, there are about 30 or 40 different systems. And also what has been interesting over the last few years, that we have seen some major names become involved with this technology. If you looked at the industry in 1994 and 1995, there was a lot of smaller companies that didn't have a lot of resources to fully develop or deploy biometrics. Right now you're seeing companies like Motorola, Seaman's, Judigzu, Sony, etcetera, become more involved with biometrics, signifying that it's a real technology, that they're looking to roll it out not only in

industrial applications, but also in the commercial sector for consumer based applications. In fact, four or five of the laptop manufacturers have announced that they're beginning to include biometrics built into their laptops. So, for an extra hundred dollars or so, your laptop will come with a fingerprint scanner built right into it to log in, you don't type a password, you just put your thumb right on the scanner.

The three -- well, the two most used applications for fingerprint technologies are logical security, securing a laptop or a computer access to certain files, or physical access applications. The physical access one has gained a lot of press recently because under the *Aviation and Transportation Security* Act, the TSA now has to provide a plan for deploying biometrics to secure employee access areas at airports. So, they are going to be deploying 20 pilots to figure out how effectively this technology prevents unauthorized access to certain areas.

The three different types of fingerprint scanners, the two most popular ones are optical and silicon. Basically, optical scanners -- it's like a copy machine or a camera. It takes a picture of your fingerprint. The silicon ones are a little bit different. With

those technologies, you actually put your finger right on a silicon chip, so those can be put on a cell phone, they can be put right onto a laptop, and what happens is, the silicon chip measures the electrical capacitates of your finger and it can identify where there's a ridge or where there's a valley on your fingerprint. The key with that technology is that it's a much smaller form factor than the optical ones. You don't need a miniature camera, rather you just need a silicon chip.

There's also a third type that's not mentioned here. There's only one vendor that has it called Ultrasound Technology. It's made by one company called Ultrascan. That actually measures your fingerprint by sending sound waves that bounce off your finger, and if you've got a ridge, the sound waves will hit your finger and bounce back faster than if you have a valley in your fingerprint. Then, based upon that, it can identify the print of your finger.

All these technologies, optical, silicon, ultrasound, once they capture an image of your finger, they then extract certain features to create a template. So, many times they're not storing the fingerprint images themselves, rather they're taking

the image and extracting certain minutia features and storing that in a template. So, it takes up a lot less space than the full image would.

Another application that's been around for quite awhile is hand scan technology, as opposed to fingerprint where you're taking a picture of the tip of your finger, this one you put your whole hand down on a platen and it measures the shape of your fingers, height of your knuckles, that kind of thing. It sounds a little bit unusual. You wouldn't think that that would be a differentiating factor, but it actually works quite well. And this technology has been around since the late 70's and is used, basically, to open up access to certain facility areas. Columbian Presbyterian Hospital uses this. There are a bunch of locations listed down here. Walt Disney World uses this type of technology. Certain airports do. I think one good application to point out is the INPASS application. If you're going through immigration and customs at a bunch of airports, for example, between the U.S. and Canada, instead of having to wait in line, you can pre-register the INPASS program whereby you get a card. You put this card in a machine, you put your hand down, you're identified, and then you clear

through immigration without having to wait in line. It's a much faster process if the line is 40 or 50 minutes long, you can go right through that system. Now, there had been some glitches with the technology -- or with the system in terms of how effective it works and that kind of thing, but the important thing to note is that there are 40 or 50 thousand people enrolled. It's been running for many years and the hand geometry technology that's been used has worked perfectly.

Some of the other applications. Disney World's an important one to know because that's a consumer application. If you're a season ticket holder to Disney World and you want to access the park, you actually use a two finger geometry, as opposed to putting your whole hand down, you put two fingers there. The interesting thing to note there is it's a consumer application. Average people are using it. It's not some high-tech facility where they're trying to prevent terrorism or some severe type of fraud, but what happened in the past was, someone buys a seasons ticket, gives it to his neighbor, his neighbor gives it to his neighbor and the whole neighborhood would go for free whenever they wanted the whole summer. Using this technology you can't go in unless you are the correct

person. Now, it's not ironclad security. It's not absolutely perfect in terms of it preventing a hundred percent of the fraud, but Disney World didn't care about that. They want to reduce fraud a little bit, lower the chance that someone is going to buy one ticket and give it to 50 people. It's not worth the headache anymore. And what happens? If someone even does happen to have the same hand shape as someone else, they take their friends, they can go in there, they're still at Disney World. They are going to have to pay ten dollars for a pizza and twenty dollars for soda, it's not going to be any different. Some of the other applications, banks have used the technology for physical access. University of Georgia has actually deployed hand geometry since, I think, about 78' or 79'.

Voice scan technology. Basically, this identifies you based on you saying a certain pass phrase. So, you'll say, my voice is my pass word, something like that. The system will then record that phrase and extract certain features used to identify you. It works on cell phones, it works on speaker phone and that kind of thing, and it works more accurately than people give it credit for. Questions we also get asked

are, does it work if you have a cold, does it work if you're tired, that kind of thing. And it does. It's not based just upon how your voice sounds, but it's also based on the vibration pattern. So, when you speak, based upon the shape of your larynx and your throat, there is a certain vibration pattern given off there that the system can identify. There are a bunch of vendors that provide the technology. For the most part it's used in telephone based applications. Calling up your bank to transfer funds or something like that. It's just now becoming introduced into the commercial sector. So, over the next few years you'll see a bunch of banks coming out with systems that they'll offer. They're not going to make it mandatory, but if you want to transfer funds in your account, or Fidelity, or whatever the case might be, you can use this technology to make sure someone at your office didn't overhear you, guess your PIN, and try and transfer funds out of there. So, it's more secure than the existing applications.

Another biometric technology is signature scan. This doesn't look at the static signature, rather it looks at how you sign your name. So, you sign your name and it will measure the pressure, the speed, the

time it takes you to sign your name, how long you pause before you come down on a stroke, when you cross the T versus dotting the I, that kind of thing. Again, this technology is not -- it's clearly not as accurate as fingerprint. Your signature is not as stable. It changes over time. You can change it if you want to, but it's better than not using the technology. So, if you're looking at something, for example, re-signing on a credit card, using this technology makes it more secure. It's better having signature scan with the person looking at your signature, than just using some clerk getting paid minimum wage looking at your signature. That's not very secure, if it's secure at all. There are several applications, for example, there are certain banks that use this for loan verification. So, when you're signing for your loan, it'll take your biometric signature and compare it against your enrollment. And you -- generally many from mortgage pulling applications use the technology. That's an internal application, so people that work at that location will actually use it.

Facial scan technology. This one has probably been in the media more than any other technology recently because of the potential for capturing

terrorists. The one benefit facial scan has over all the other biometrics, is that it can be used passively. Now, it's a benefit, it also can be considered a privacy invasive negative. In other words, this can be used for surveillance technology. It's interesting to note there are several locations that are using it now. Outside of England, outside of London, in a suburb called Newham, they're using facial technology and this type of veneration right now. So, they have a number of cameras positioned throughout the city. What happens when you're walking down the street in public, the camera will focus in on you and take a picture, extract certain features from that picture, and be compared against the police database. And what they'll do is identify whether you're someone who's in that database who's got an outstanding warrant. So, it's a technology that can be used without your permission, even without your knowledge. Basically, the way it works is a similar concept to fingerprint. You enroll in the system, it takes a picture of your face, captures that image and then extracts certain features. So, it's not looking at the whole image when it's doing the biometric match, but extracting certain features. Different vendors do it differently. Some look at

neuro-network technology, other ones will extract certain points and say, the distance between the eyes and the nose is this much, etcetera, etcetera. But, the basic concept is it creates a template, uses that for matching. Facial scan technology can be used both on one to one, just saying this is the correct person, yes or no, but also on a one to many contacts. There's several DMV's right now, motor vehicle departments, that are looking at this technology. West Virginia and a few others where when you apply for your driver's license, they'll take your face image, they're already capturing your image anyway, extract certain features for the template and then do a match against everybody else to see if you have another ID under a different name. There are a few major vendors of this technology, Physionics, Isonic Images, I think the latter one is here today.

The technology has changed a lot recently. They're now beginning to roll out into larger scale government applications. For example, Mexico announced, I think, about a year ago that they're going to roll out facial technology for nationwide voter registration. So, everybody that votes in Mexico will get their face image taken and they compare it against

a database. Now, one important thing to note is that the technology has a lot of positives. It can be used very easily, it's using a photograph, not some new type of device or something like that, but it's not quite as accurate as fingerprint. So, if you have a database of 5 or 10 million people and you need to pull that one person out of the database, fingerprint will work pretty effectively. Face technology might narrow that database to a 100 people or 200 people, but it won't necessarily pull that one person out of that database.

Some of the applications, the public sector ones, a few driver's license bureaus, the Mexican voter registration, another application that got a lot of notoriety was it was used at the Super Bowl in 2001. So, people who went into the stadium, there were cameras around there that would take their picture, extract certain features, and compare it against a police database. So, if you had an outstanding warrant, if you were a felon, something like that, ostensibly the police in Florida will be able to know that and go in and arrest you. Now, they didn't make any arrests there and there were a lot of concerns, especially from privacy groups, about the technology being used there. There were some signs apparently,

but not posted in a fashion that people could really know what was happening, and it wasn't clear that they were being used in this face technology application. So, one could argue good and bad things about it, but it does demonstrate a technology that can be used in surveillance and that's why it's been mentioned a lot at airports. You could set up face technology cameras throughout the airport, and when people are walking by, take their image and compare it to a database.

Now, the important thing to note is it's not terribly accurate used in a surveillance application. If you think about it, if you're sitting right in front of a camera, the camera is three feet in front of you, you've got good lighting, you're looking directly at it, you're cooperating, you capture a good image there and the system works pretty effectively. However, if you're walking down an airport, the camera is up in the ceiling looking down at you, you're not looking directly at it, there's a shadow, there's bad lighting, etcetera, you capture a pretty poor quality image. That's not very effective at matching people. So, that's an important differentiator when looking at this airport applications. A lot of the ones people are talking where it's sort of a passive system, people

just walking through, those won't work. They won't work at all. If carefully captured, the image -- for example, someone goes up to a ticket counter, or someone goes through the security check point, where they have to pause and look at the camera, it'll work much more effectively there.

Iris technology. This also has been in the media quite a bit. It's sort of similar to face technology, in that, it takes a picture of your face, but then instead of looking at the whole face, it focuses on your iris and creates a template based upon that. The iris is an interesting part of the body in the fact that it is very, very stable and it contains a lot of information. The little patterns in the iris, etcetera, are unique. Your left iris is completely different from your right iris, so you've got two points of identification there. It's stable, it doesn't change over time. Unlike fingerprints, you don't really get cuts on your iris. Most eye related diseases, that kind of thing, don't affect the iris pattern, so it's extremely stable and very useful in terms of identifying people based upon that pattern. Although it is a little bit challenging to capture the image, the technology has improved a lot over the past

few years, but still requires someone to pause, look right at the camera, and focus in for a few seconds. The technology is improving and I suspect that it will be a lot easier down the road. One interesting application of this technology a few years ago, was at Bank United for ATM applications. What they had was an ATM, there were about three or four of them set up in Texas. They had ATMs that uses iris technology in a one to many fashion. So, if you didn't have a bank card, no ATM card, no password, no PIN, nothing, you walk into the ATM vestibule, you look at the machine, identify -- look at your face, look at your iris, it captures the image, does a one to many match, and asks you how much money you want. So, it was a real project. It was up and running for about a year or so, but it was extremely effective. It demonstrated how the technology is not only accurate, but how it's very convenient. You can walk into a -- you know, if you're out swimming and you walk right into the ATM and get your money. You don't need a wallet, don't need anything at all.

Now, there's one company that owns this technology, Iridium, they've licensed it to a few people, including Panasonic and a few other folk, and

it's generally used in physical access applications, or it's being used more now in the transportation sector. There are a few logical access ones, although they focus now more on the transportation sector in the past few months. For example, Heathrow Airport in London. They're using the technology to capture iris prints. There is a pilot going on -- or a project starting in Toronto area, at Pearson Airport, using iris technology. It's not as mature as some of the other technologies, it hasn't been around for 10 or 20 years like fingerprint has, or face technology. The other technologies probably developed about in the mid-70's or so in university and military type settings and have become commercialized over the past decade. Iris technology is not quite as mature as those, so it hasn't been used in large scale systems. The largest application of iris technology right now is at the Singapore/Malaysia border crossing where they're using it for about 50 thousand people per day. So, it's a fairly sizeable application, but not something that's been used with millions or tens or hundreds of millions of people.

Retina scan. It's similar to iris technology. Instead of taking a picture of the iris, it takes a

picture of the retina. The difference here is that the retina is at the back of eye and it's a little bit more complex capturing that image. There's one company that makes that technology, but they have discontinued the current product and they're working on the next version, so for all intense and purposes, the only one that's available right now is iris technology.

Here are a list of a couple of the biometric applications that have been used in air travel. Obviously, since 911 there has been a big focus on this technology as a way of preventing terrorism, etcetera, but all of these applications here had been in use prior to 911. So, the technology is making a lot of headway, it was in actual use. The INPASS one we talked about, Keflavik Airport in Iceland use it for identifying passengers as they're walking through the airport. They use face technology. Border crossing, that one is in Israel at the Gaza Strip. They're using facial recognition combined with hand geometry to identify day workers as they were crossing the border. Clearly, a very, very high security application where you have to know who is crossing through that border. And, in fact, that application is still moving forward. They're just at the initial stages of rolling that out

now after about four or five years of getting government approvals, etcetera. Ben Gurian Airport in Israel uses hand geometry right now and I think they're extending that to fingerprint shortly. And a few other airports in the U.S., Reagan National, started using fingerprint technology not too long ago.

We've got a few minutes left, so I'm just going to talk pretty quickly about what's going on with biometrics in the transportation sector in terms of how the technology can be used to prevent terrorism. Here's a few of the bills that have been in the news recently and are focusing on the *Aviation and Transportation Security Act*, with respect to biometrics. Obviously the Act covers a lot of different items for airport security, but with respect to biometrics, there are four basic areas, controlling employee access to certain areas, identifying crew personnel, back ground checks against the FBI database, and identifying passengers in a trusted travel program. And the important thing to note with respect to biometrics is that the technology was specifically called out in the legislation in quite a few places. So, again, it was not something that was thought of as, well, maybe we'll use it at airports, we'll take a look

at it, but we're not sure, but rather they have to roll out biometrics at 20 airports in terms of pilots. They have to be used for employee background checks with the AFIS fingerprint systems, and they're used in a bunch of different areas for passenger identification, etcetera. You'll start to see some more news involvement from this from the TSA shortly as some of the deadlines become due in terms of figuring out how to deploy the biometric technology at airports.

We were hired, actually, by the FAA originally and TSA when it was formed, to go through and do a detailed analysis of how the technology can be used there. And I'll go through briefly and talk about a couple of the findings. We talked about surveillance a moment ago. Again, one of the key findings is facial technology is effective at airports if used properly. Most of the deployments, most of the discussions about them, haven't really focused on how the technology is used. You've got to be very careful about the enrollment process, careful about verification, control the enrollment protocols, etcetera, make sure there's correct lighting, and have a good understanding of what the goal of the system is. What are the critical success factors? Are you looking to capture every

terrorist in the database? Well, it's not going to work then, it's not going to come close. Are you looking to use it as part deterrent, part some effectiveness of capturing some people? Then it will work.

Trusted travel program, one of the challenges here is how do you enroll people in a trusted travel program? If you have tens, if not hundreds of millions of people flying every year, how do you enroll them in some process where they're going to have their credentials checked, and then be issued this card? That's the critical factor of that type of project because if you're not checking their background and authenticating that when they issued the trusted travel card, what good is the system? If I can commit fraud and get a fake travel card, it doesn't do much good.

With respect to access control, this is one of the more straight forward applications in terms of how biometrics are used. It's very easy to replace a card slide, you just basically take it off the wall and put a biometric system on there, it has the same type of protocol, etcetera. One issue with this is going to be interoperability. What do you do if you have a flight crew, etcetera, that's accessing a certain portion of

the airport at Logan, they fly down to J.F.K. Airport, they don't want to enroll in a different fingerprint system. You want to use the same product, same technology, same formats. That's one of the challenges with that, to make sure that all the airports in North America utilizing the same technology, same standards, etcetera. That's something the industry hasn't quite addressed. There are a lot of standards out there and they've begun to address that issue, but it's by no means something that you can plug in different products and it will work without any issue right now.

And this a little bit more detailed information on the watch list applications of how the technology might work, etcetera.

Well, one last thing I'll leave you with. With respect to the watch list. It is really critical to make sure that the way in which a system is deployed is carefully looked at. Facial technology, fingerprint, etcetera, will work extremely effectively, and we've seen that it's been used in a lot of applications around the world with tens, if not hundreds of millions of people using biometrics every day. The critical thing is to make sure that there is an appropriate way of utilizing systems if you do find a match. If

someone does come up as a terrorist or an FBI watch list, that there is a set protocol in place how to handle that scenario. There have been some deployments, for example, where the fingerprint would come back saying, yes, this person is on the FBI wanted list, and there was no protocol for what to do next. There has to be somebody there to be able to handle that backup. So, that's important, to make sure not just a core technology itself, but the system and the processes around those are deployed very carefully.

MODERATOR: We're going to have questions and answers for a few minutes here and Raj can answer your questions. Any questions from the audience?

QUESTION FROM THE AUDIENCE: One of your slides talked a bit about the integration of smart card technology with biometrics, and I wonder if you could take a minute to talk a bit about how that works, and specifically with respect to online versus offline transactions, and how that's rationalized against the business case for smart cards?

MR. NANAVATI: Sure. Well, historically smart cards haven't been that popular in the U.S. or in Canada, so it's something that's just being looked at over the past year or so. Biometrics can be used in a variety

of scenarios on smart cards. You can store the biometric template on the card, put the card in the machine, and do a match locally. You can store just the identifier information on the card and store the fingerprints in a centralized database, put the card in the machine, it then pulls the fingerprints off the database. There are actually some technologies now where you can have that silicon chip I mentioned, right on the smart card. So, you have the smart card IC chip, you have the fingerprint chip right on the card. You put your finger -- you put the card in the system, put your fingerprint on the card, and you do a match with your template never leaving the card. So, there's some very effective ways of making sure you don't have security flaws in that type of system. In terms of where it's being used, the initial place to look at is probably the Department of Defence program in the U.S. In May of 2000 they awarded a 1.5 billion dollar smart card project which had a heavy emphasis on biometrics. The goal of that system was to provide smart card ID cards for all U.S. federal employees. Now, it's taken a while to develop the standards, etcetera, but just about two or three weeks ago they awarded some of the initial projects for that to develop the prototypes.

And going to your question, they actually addressed that issue. What are the different scenarios for using biometrics? So, in the prototypes they asked, store the biometrics on the card, store it centrally, store it locally, etcetera. I think over the next few years you'll start to see those applications developing, but a lot of it has to do in terms of technical architecture. What the business case is. In a private sector program it might be different from the government sector. With this common access card project in the Department of Defence, the key issue is interoperability. If you get a card issued by the Treasury and you're going to go access the Department of Agriculture building, they want the same card, same formats to be used. So, that will be a lot different than if Visa includes a biometric on the card or Amex includes it on the blue card. So, that'll dictate more so than sort of one general format. It might be on the card, it might be stored centrally, etcetera.

QUESTION FROM THE AUDIENCE: You mentioned fingerprint readers on cell phones. Are these things available now, or when do you think they will be happening?

MR. NANAVATI: I'm sorry, is what available now?

QUESTION FROM THE AUDIENCE: Fingerprint reader on PDAs

and mobile phones?

MR. NANAVATI: It is available now. There are cell phones, for example, in Europe. Sajamorfil makes one where the fingerprint device is imbedded on the back of the phone. It's actually imbedded into the battery. But it's a fairly new application using it on PDAs. There are a few companies that have plug ins to the palm pilot where you can snap on a piece and put your fingerprint. CIC makes a signature technology where you can sign your name on the palm and identify yourself that way. So, there are few applications out there, but they haven't really proliferated a lot because there's not a real business case for it as of yet. It's enough of a challenge getting this technology to the general awareness and utilizing it in certain applications for access to log on in welfare, etcetera. The next phase over the next few years will be utilizing it more in cell phones and PDAs, but it's just a natural lifecycle for the technology. We're still at the fairly nascent stage of utilizing biometrics. So, once it becomes more common, you'll start seeing it in cell phones and PDAs more often. But, if you want to get a cell phone today, or a PDA today, with either of those technologies, sure, you

could buy it.

QUESTION FROM THE MODERATOR: As you mentioned, the different cards, both for identification and for this purpose and for that purpose, is this going to be like our credit cards and mileage cards and we're all going to end up with a stack of biometrics identification cards for different purposes that will fill three wallets as we walk around?

MR. NANAVATI: That will be dictated more by the given applications, so right now you probably have some kind of frequent flyer card. What they might do is store the biometric on the card, itself, or they might have some kind of system where it's stored centrally, and you use that card to identify yourself. But, there won't be cards that are utilized just to store biometrics, rather it will be part of another application. So, right now, theoretically, you could store a fingerprint on the American Express blue card. There's enough room for that, the fingerprint template is relatively small. There's nothing preventing that from happening today, except for the fact that there aren't any applications. No one has really looked at utilizing that. It's really part of the existing card infrastructure when technology is used, and probably

won’t be something where you have twenty different fingerprint cards or something like that.