Federal Reserve Bank of Atlanta *Talk About Payments* Webinar

Biometrics: Technology and Policies

October 29, 2020

As biometrics technology continues to get more refined, what's happening with associated privacy and policy issues? Watch this *Talk About Payments* episode to learn what biometrics subject matter expert James Loudermilk and Dave Lott of the Atlanta Fed's Retail Payments Risk Forum have to say about these issues. They also discuss use cases for the various modalities, including fingerprint and facial authentication.

Send questions about the webinar to David Lott at david.lott@atl.frb.org.

You may view previous *Talk About Payments* webinars.

Transcript

Tim Lloyd: The views expressed in this presentation are those of the presenters and do not necessarily reflect the positions or policies of the Federal Reserve Bank of Atlanta or the Federal Reserve System. Any company or product mentioned in this presentation is for informational purposes only and should not be considered as an endorsement.

It is now my pleasure to turn the call over to our first speaker, Dave Lott, to begin our program. Dave, the floor is yours.

David Lott: Tim, thank you very much, and thank you to everyone for joining us today. For those of you that are outside the Southeast area, you may not be aware but we had a tropical storm, Zeta, that moved through the metro Atlanta area earlier this morning, causing some major power outages—so some of us have had to move to some alternative locations in order do the webinar today, so we appreciate your participation, and certainly hope that anyone that has been in the path of Zeta has been able to escape damage.

I was so excited when I contacted Jim Loudermilk to participate in this webinar, and he immediately said "yes." Jim's full bio is at the end of the presentation, but let me give you some highlights. Jim is currently senior director of innovation and customer solutions at IDEMIA National Security Solutions in the Washington, D.C., area; prior to joining IDEMIA about three years ago, Jim was a technology executive with the Federal Bureau of Investigation. During his 21-year term at the FBI, his latest position was deputy program manager and chief engineer, where he had overall responsibility for the design, development, and implementation of the Integrated Automated Fingerprint Identification System, or IAFIS.

IAFIS maintains the largest collection of fingerprint images and criminal history information in the world. From other conversations I've had with some of Jim's peers, he's pretty humble but they credit him with really bringing that fingerprint system into the 21st century.

Jim was a member of the FBI Biometric Steering Committee, and he represented the FBI with the National Science Foundation Center for Identification Technology Research. Jim is a frequent speaker at biometric and identity conferences.

Jim, thank you again for joining us. Can you tell us a little bit more about your role at IDEMIA, and provide a brief profile of the company? And Jessica, if you could move to the next slide.

James Loudermilk: Thank you, Dave. Let me really focus on the company; you've said plenty about me. IDEMIA National Security Solutions is a separate legal entity and company, but it's a wholly owned subsidiary of the much larger—actually, global—IDEMIA Company. IDEMIA has in excess of 14,000 employees; it does business on all six of the inhabited continents in over 170 countries.

In a typical year, even now in a pandemic, it does about $3.2 billion U.S. dollars in revenue. It's the major supplier of payment cards and SIM cards in the world. Most likely, all of the credit cards in your wallet and the SIM cards in your phone were made by one of the IDEMIA affiliates. And I understand that more than 1,800 global financial institutions are served as well.

As I tell you these things, if I say something that really interests you, I'm not going to be the one to help you with it, because that's not the part of the company I'm with; I'm just putting it out for context. You see in the maps of the United States that we also supply about 30 of the states' public safety biometric systems. We also supply four of the five national identification systems. You can see we are involved in issuing most of—about 80 percent—of the driver's licenses that are done annually. And we provide enrollment services for HAZMATs and TSA credentials and a variety of other credentials nationally. And that's a more than an adequate thumbnail, I think; you can go on to the next slide.

Lott: Thanks, Jim. And for those of you that are joining our *Talk About Payments* webinar series for the first time, let me give you a quick overview of the Retail Payments Risk Forum. We really have two major areas of activity: one is research, and one is education. We do a weekly blog, which you see the link to on the slide there—and we hope that you will subscribe to that—where we discuss payment risk issues or events happening in the payments space. We also have our own web page on the Federal Reserve of Atlanta website where you can access all of our documents, sign up for our webinars—everything that you wanted to know about the Retail Payments Risk Forum is there, so we hope that you will use that as a resource going forward.

So if we could get into the heart of our webinar today and move to the next slide, these are some of the areas that when Jim and I were prepping for the call we thought were major areas that we wanted to cover—but we want to be responsive to our audience, so we've got a poll question for you. Tim, could I get you to launch the poll question for our members?

What we're asking in that poll question is for those key areas that were listed, which one is the most important to you? Is it authentication? Is it the various biometric modalities such as fingerprint, voice recognition and others? Is it about the challenges of enrollment and the importance of enrollment? And then we get into some of the more policy issues associated with the security of biometrics data, privacy, and trust. So we'll give you a little bit more time to answer that.

Jim, I think we could probably spend a whole hour on each one of these items. What do you think?

Loudermilk: Easily, and in some cases, a full day or two. In fact, earlier this week, I was in a three-day international conference on face recognition alone. But we're not going to do that today.

Lott: No, not today. Tim, could I get you to publish the results so that we can see where the audience is leaning toward?

Jessica Washington: Dave, excuse the interruption; this is Jessica. If Tim could put forward the slide, that would be great until further notice. Thank you.

Lott: OK, authentication. More than half of you indicated that, followed by data security; the smallest was the biometric modality, so we'll run through those quickly and also address the issue of trust. Thank you very much for that feedback.

So let's just jump to the next slide, and jump right into the issue of authentication. Identity authentication is absolutely critical, and it's something that has existed since the beginning of humankind. In the early days when there wasn't a lot of movement between communities, it was pretty easy to recognize and authenticate someone. But as mobility increased among communities, it became more and more of a challenge. The first incidence of fraud that I could find recorded in the Bible is the story about Queen Jezebel in 1 Kings, where she forged her husband King Elijah's signature on some documents in order to essentially confiscate a vineyard that the King had his eyes on.

Jim, you've got some other references, don't you?

Loudermilk: Well, there are two that I particularly like. One is in the Hammurabi code, where they talk about barbers cutting the sign of the slave into the hair of subjects and penalties for doing that wrongfully; that happened about 1700 BC. And another one is in the book of Judges; after a battle, to distinguish the friends from the enemies, they gave them the password "shibboleth," and those who could say it properly were considered friends and allowed to pass, and the ones who mispronounced it "sibboleth" were immediately killed. And it says in the Bible, "And there fell on that day forty and two thousand." And that dates to about 1300 BC.

So these issues go back a long way; they really started when people began to occupy cities, and as I'm sure this audience knows we've been occupying cities a lot longer than there's been writing. The walled city of Jericho has been continuously occupied for more than 9,000 years.

Lott: And as time has progressed, we've seen additional types of authentication, from back in the medieval days when we had the wax seals being placed on documents with the imprints from the royalty rings or things of that nature, to protect against an envelope being opened as well as to authenticate that. Then we had notary publics, who designated officials to authenticate the signature of people bringing documents.

In warfare, again going back to the early days, we had the beginnings of the challenge questions—knowledge-based answers, if you will—where the sentry would provide a challenge word and then the subject approaching the gate or what have you would have to respond with the proper code word. And then, of course, we've moved into the technology aspect of it with behavior biometrics and fingerprints, facial recognition—all of those that we'll discuss a little bit more.

But in terms of looking at the elements of identification on the next slide: Jim, do you want to cover that?

Loudermilk: Yes, I'd be happy to. There are an awful lot of aspects of identification that are useful for different kinds of applications in the national security and criminal justice environment. You look at biographical information like names and addresses and height and weight and so on; you look at behavioral information which includes such things as the way we walk—when you have applications that are able to sense it, the way people use [computer] mouses and keyboards and pressure on the keys; then there's the biometric information. It would be helpful if we could get that next slide up... I finish talking about it.

A lot of different kinds of biometric information are available; I won't dwell on that. Then there's digital exhaust, but not in terms of "how can you be known in general," but "how do we know you?" You know your friends, your colleagues, your family; you just know them. You know them by looking at them. You don't ask to see their identification.

On the other hand, with strangers—where you have some reason why you need to actually know who they are; for example, whether or not you're going to accept their credit card, allow them to claim a senior discount at a movie theater, or purchase controlled substances (alcohol, for example)—now you need some actual identification. This particular slide has examples of lots of different pieces of identification. None of them are mine, but I have every last one of those documents and more, and sometimes have to carry all of them at the same time. They've got a tremendous amount of information on them, and they're highly duplicative.

Let's go to the next slide and talk a little bit about some of the challenges with such identification documents and note that the official documents typically include a photograph. So these documents, these credentials, they're expensive to produce. Those of you involved in issuing cards know that while the raw card stock is available for as little as a couple of dollars, the cost of actually producing it with all the labor involved is typically in the realm of $15 and up. They require a lot of time to obtain. If you've ever lost or had your wallet stolen and had to go reproduce the contents, you know this takes a tremendous amount of time and effort to do. There's a lot of standing in line, too, at the DMVs and other places.

And then when you have to present it, it reveals a lot more information than either the police officer or the clerk really needs to know, depending on the situation. If I am purchasing beer at the supermarket, they do need to know in Virginia that I'm over 21. They don't need to know whether or not I'm an organ donor, what my blood type is, that I have a motorcycle endorsement, that I have to wear glasses. They don't need to know my home address or anything else; all they really need to know is I'm old enough. As I said, the information's highly redundant, and then you end up in the realm that an awful lot of people we provide our information to—organizations—have proven that they're not really able to protect it.

And then maybe last for now—we'll come back to it, I suspect—they're ineffective in cyberspace. It's relatively difficult to show your driver's license to the computer unless you have additional equipment. Let's go to the next slide. I'd better move locally as well.

So once you have these credentials, one of the issues is, is it really you? Counterfeit credentials are readily available. I'm sure all of you know that there are dozens of sites that will happily sell you a high-quality but fake driver's license for any country on earth, and any state in the United States. So, there are counterfeit credentials that can be told apart—they all include security features—but many of the security features require training and sometimes require special equipment to use.

Perhaps more problematic than counterfeit credentials are valid credentials that are fraudulently obtained. Now the teenager that wants to claim to be 21 so that they can illegally consume alcohol—they're probably not going to be able to fraudulently obtain valid credentials. But states, terrorist groups, criminal organizations, highly skilled criminals—they are able to come up with the breeder documents, and they use them to obtain fraudulent but valid credentials. One thing that can be done at the biometrics office is the ability to uniquely link that document to you, to where only you can present it as yourself, and you can't repudiate it if you do present it.

So let's move on to the next slide, please. Or if David will talk about some authentication factors.

Lott: Yes, the authentication factors really fall into one of three buckets: something that you know, such as a password; something that you possess or you have, such as a mobile phone or some type of payment card, and then something that you are, which is where biometrics falls into play. Sometimes you hear the term "multifactor," and we'll talk about this a little bit in just a minute. And what that means is that the authentication process is using two or more elements from different columns. So, for example, if I'm having to use a biometric to log in, but then I'm also having to respond to a one-time password or some sort of verification code—those are two different factors and so that would be considered a multifactor approach.

And then as we see on the next slide, back in 2011, the FFIEC issued regulatory guidance to financial institutions with regard to their online systems that basically said that there's no single authentication methodology that's 100 percent foolproof. Anything can be hacked or compromised, given enough time and money. But clearly, if you engage multi-factors, that makes it much more difficult in order to compromise that.

And so basically, they provided this guidance that for online systems, you should be utilizing multifactor authentication. But we know that from the e-commerce side of things, with the merchant and their effort to authenticate the legitimacy of an online order, there's that contention, if you will, between how far do I go in authenticating that customer versus running the risk of making them abandon the process. So, Jim, isn't it about finding the right balance, as we see on the next slide?

Loudermilk: Yes, I think that that's true. You could make it so onerous that people won't put up with it and turn to some other provider for whatever the experience is that you're offering, whether it's a financial transaction or something else. Or you can make it so weak that they have no confidence in it.

While it's true that federal law in most circumstances limits our financial liability to $50 with various transactions, that doesn't mean that consumers are entirely comfortable with it. I know from my time in the FBI, where I would deal with a variety of financial institutions, that they would find that some of their customers really appreciated additional efforts to protect their identity and protect their financial information. And any of you that have ever been involved in identity theft and had to go through the very complex and extended process of clearing your name and clearing out other transactions, would really do almost anything to avoid ever having that happen to you again.

So while there are some disadvantages to strong practices, not the least of it being people not being willing to put up with it, you need to find the right balance—which, increasingly, particularly now in the time of pandemic, people are coming to believe needs to involve biometrically linked information, but biometrically linked in a way that does not require them to be touching things or coming into close contact with other people. We might go to the next slide.

Lott: Yes. Jim and I have a common colleague in Anil Kumar Jain at Michigan State University—actually, Anil cochaired a biometrics conference that the Federal Reserve Bank of Atlanta convened here back in the fall of 2015. I think Jim would agree with me that he's probably the foremost biometrics expert in the world. He's come up with a formulation—Jim, do you want to take us through that?

Loudermilk: Yes; I won't read that full slide; it will be available to them afterward. But the key points—this was like 20 years ago, when he was formulating this—he said that the ideal biometric, it ought to be universal—that is, something we all have. We all, or nearly all, of us have fingerprints. We have eyes, we have ears, we have faces, so it's something that we all have. And it ought to be unique; nobody else ought to have it.

Now, that is more easily said than done. Fingerprints are unique; there's no doubt about that. Over more than 100 years, the United States has been collecting fingerprints for criminals and, frankly, for almost 100 years has been using it for employment checks. Since this audience is in the financial sector, you probably all had a fingerprint-supported background check. They're unique; the iris is unique. The face is not—identical twins, for all practical purposes, have the same face.

Similarly, they have the same DNA. So as useful as face and DNA are, they're not [inaudible]. They ought to be permanent, so that if I check your fingerprints today and then check them again in five years, I ought to get the same result. And they ought to be easily collectible. Some things are—certainly it's very easy to collect an impression of your face, you can do that with a digital camera in moments. DNA is not so readily collectible, and it's highly intrusive.

So those are the key things, and then you get into system development considerations: How quickly does it perform? How accurate is it? Is it publicly acceptable? For most people, fingerprints have a connotation of criminality. Now, we're coming away from that in an age when large numbers of people use their finger to unlock their mobile phone, but even so, it's less acceptable and so on. How easy can you circumvent it—*can* you circumvent it?

So, a lot of considerations in that. Let's move on to the next slide, which addresses the issue of there being tradeoffs in just what biometric you want to select. This is an older slide that was developed for law enforcement purposes, and also military, and it trades off the fact that some are highly accurate, but you really have to get up close and personal to make use of them—whereas others can be collected at more of a distance. The voice can be collected at a distance—there are challenges; your face can certainly be collected at a distance, although if you're too far away, there won't be enough resolution in the photo to be able to confidently identify who it is.

But today, in the time of pandemic, using the face or some other measure that could be collected at a distance is fairly popular. People don't really want to be up close and personal. Let's go on to the next slide.

Lott: Let me just interject here. That was a great discussion on the authentication issue and some of the challenges that it presents, so let's get into some more details of the different biometrics. You've touched on some of them already.

The key physical biometrics that are being used in financial services you see on this slide here—with, of course, the exception of DNA that Jim mentioned. But we're seeing these more and more in everyday use, and we'll talk about them in more detail. Jim, from a law enforcement standpoint, which of the biometrics are admissible in a court of law for identifying an individual?

Loudermilk: Every one of the items shown on this slide has been introduced, but they haven't been generally accepted. Some of them haven't been used; voice hasn't really been accepted anywhere, although it has been introduced on multiple occasions. There's even a term for it in the legal world: "ear witness testimony" (well, that's humans, not machines, doing it).

Fingerprints and palm prints have been regularly used in courts in the United States, and really most of the world, for over 100 years. The face, oddly enough...while eyewitness testimony is frequent, it's also very unreliable. There have been lots of instances where at crime scenes, there's photographic records of the subjects that committed the crimes—or at least, apparently committed the crimes.

But I remember several years ago talking to the FBI's chief expert in this area, and I remember Richard telling me that he had testified many times, but more often than not his testimony had been why someone had to be excluded as a subject—that the image quality was sufficient to say that the person was too tall or too short, or in some other fashion couldn't possibly be the person of interest—if you could go back to that last slide, please—couldn't be the person of interest, but seldom did the cameras or the placement of the camera allow him to make a positive identification.

So occasionally the face will be used for positive identification, but more often it's used to exclude people. DNA is used all the time; iris recognition has occasionally been used. Voice recognition is used in Spain and several other European countries; it is not accepted by courts in the United States, to the best of my knowledge. I know at the time I was there, the Federal Bureau of Investigation would use voice recognition for investigative lead generation. They've actually got a unit that does that analysis and does such identification; that was one of the elements involved in the search for Osama bin Laden, and some other terrorists.

But the FBI will not allow its experts to testify in court, and the reason for that is they don't believe that there's enough scientific evidence published in peer reviewed journals that would allow them to withstand a Daubert hearing at the federal level, or a Frye hearing at the state level. Those are the legal processes where expert testimony is examined to determine whether or not it's going to be admitted into court. So fingerprints, for sure; iris, for sure; DNA, for sure. The others: maybe, maybe not—not for sure. We can move on.

I know the audience is less interested in the details of biometrics, but we might talk a little bit about binding the credential to the person, because that's important. What's used here is essentially the DMV example, where you come in, you present your documents, and they scan them through a system—sometimes in real time, sometimes not. My company and others make equipment that will verify technical security features in documents. I know we have one that will verify the technical features of about 5,000 different documents, so a lot more than just driver's licenses.

But even after you have verified that it's a valid birth certificate, and perhaps gotten online with the state's bureau of vital records and determined that yes, indeed, that it not only is a correct document, that it was issued and there is such a person, you now have the issue of, but is that the person that's in front of me presenting them? If one of the documents is a passport, or a driver's license from another jurisdiction, or an earlier license issued in Georgia, you have the option then of taking the person's image and using face recognition to determine is this the same person.

While you could use fingerprints or various other biometric technologies, typically you don't have access to repositories that would allow you to do that. But in any case, you can uniquely bind that credential to the individual that's in front of them and be sure that, yes, it's a real person; yes, these credentials are valid, and the person in front of me corresponds to the credentials that have been presented. So this is a very important step, and it's a step that we're starting to see across the United States and parts of the world as states are issuing electronic driver's licenses.

Now, you still have to have the physical license as well, but some of the states—Louisiana and I've forgotten one other—will now issue it to every one of their citizens that has a driver's license, that [the citizen] they can just present their mobile phone as their credential and the officer can determine through near-field communication, or the merchant can, that this person does have a license and that they're old enough. And it can be restricted in how much information is revealed. Let's move to the next slide.

Lott: Jim, you just talked about how critical the enrollment process was in binding that identification to authenticate that person to a document, whether it be a digital document or a physical document. So that leads to the question of: how accurate are biometrics? If we could move to the next slide.

There are certainly weaknesses in passwords, and knowledge-based questions—we need to back up one slide, please—that for their weaknesses, the reality is it's binary; it's either yes or no. You either enter the right password or you don't. Whereas there's some gray area in biometrics, isn't there? Can you talk a little bit about accuracy and how that is handled within biometrics?

Loudermilk: So you raise an important point. In 2009, the National Academy of Science, in response to a tasking from the Congress on this very subject, included the statement that biometrics are inherently probabilistic, which means that they're not absolutely accurate. But that allows you to think, "Well, maybe they're pretty flaky"—and that's not true either with a well-designed system.

I don't want to get too far into the minutiae, but let me take one of the less accurate of the biometrics, namely face matching. There is a report out this month from the National Institute of Standards and Technology, where it looked at the face and algorithms to do face matching—in fact, it looked at hundreds of algorithms to do face matching. And I won't try to take you through the intricacies of hundreds of different algorithms, but let me just say that at a false match rate of one in a million, there were about 35 different algorithms that were in the 99 down to like 98.5 percent accurate [range]. So they're highly accurate for one-to-one matching; they're not as accurate when you're trying to identify a person out of the crowd. But even in that situation, with a false match rate of one in 100,000, there are several algorithms that are 99.6 percent accurate or better.

So they are highly accurate when properly implemented; fingerprinting, more accurate than that—DNA as well. Iris is more accurate than that. Where you have some oddities, however, are demographic effects, particularly with the face matching, not so much with fingerprints or iris—in fact, not at all with fingerprints and iris. But with faces, the very young are quite difficult, and when I say the very young, I'm really talking about under 16 and with the most recent technology, under five years of age. They're not reliably identified from one situation to the next.

And then there are differences in demographic groups, with people from certain Asian countries and African countries being as much as 100 times less accurately matched as people from some other demographics. Oddly, we usually think in terms of whites and blacks. It turns out that of the first 150 most accurate algorithms, in all cases black males are more accurately identified than white males, white females or black females, and there are a variety of different variations in that.

But even having said that, there are algorithms that have been carefully studied by the National Institute of Standards and Technology that were found to have no measurable demographic variations at all, so they can be highly accurate. It's really a function of what system you use. The caution I would add for anyone thinking about using these technologies is, you really need to know your algorithm and it would be prudent to only consider using algorithms that have been submitted to NIST testing, which is very thorough and is published so that you know exactly how well it performs.

Lott: Yes, that's great information. And I actually wrote a blog back a couple of weeks ago on the NIST evaluation process and some of their key findings. So related to that: I often hear from individuals remarking that, "Hey, I can easily change a password if my account gets hacked, but I can't change my fingerprint." So, Jim, what protections are there against biometric databases being hacked? And if we could move to the next slide and talk about templates.

Loudermilk: Well, there are a number of issues. A lot of issues are in play there, and some of the protections really depend upon the system manager and whether or not they provide the protection. All of the systems don't do the matching with the actual original fingerprint or photograph or iris impression; what they do instead is extract a template, a much smaller template, and you need to do that for a variety of reasons that have to do with how well the system will perform and how rapidly it will perform, and the ability to store enough of the information to be productive. But they'll extract a template, which first of all is not interchangeable with all different systems; it will only interact with the same manufacturer's technology, and more often than not the same release level of the technology.

It's not really invertible; you can't go back through the template to the original image. Not all systems, but sensible systems responsibly implemented will also encrypt that information so that even if you somehow were to gain access either to the source fingerprints, in the case of this template, or to the templates themselves, you wouldn't be able to do anything with it unless you had the key that would allow you to decrypt it and do something with it.

Beyond that, an awful lot of the scenarios are unrealistic. You may have read of the Italian minister whose fingerprints were captured at a distance, and some dummy fingers were put together that allowed a German hacker group to fool a low-level system—that's really not something that can be scaled. It's not very practical. The more realistic case where fingerprints are used is that there's a confederate that works with you to give you access to their fingerprints.

The idea that someone would follow you around until you leave your fingerprint impressions on hopefully a clean surface that they can then come and do a late lift and build a dummy finger, and then maybe somehow later on, when you set your telephone down for a while, I'll pick up your cellphone and use that dummy finger to open it—that's just not a realistic scenario. No one would do that in the real world. They'd wait until you opened it and hit you over the head if they were going to do it at all. But again, it just doesn't scale.

So an awful lot of those scenarios—they're pretty far-fetched. But there are protections that are available that a well-designed system will put in. There are very few instances of even claimed erroneous release of biometrics from a database, and there are no known instances where someone got hacked biometrics from the database and then actually used them to someone's harm. That's not to say it won't ever happen someday, but it hasn't happened yet.

Lott: Yes. Never say never, right?

Loudermilk: Right.

Lott: Well, we've got about 10 minutes left because we wanted to save some time to address some of the questions that are coming in, so let's quickly move through some of the modalities themselves. If we could jump to the next slide on fingerprints.

Jim, you've talked about that a lot, and given your extensive experience dealing with fingerprints there at the FBI, is there anything else that you want to mention with regard to the modality of fingerprints?

Loudermilk: No, but I'll throw in a startling fact. The FBI has on file criminal fingerprints for felony level offenses on 78 million people as of the end of last month and has several fingerprints that were used in background checks for another 58 million people. So fingerprints are very commonly used. Now we can move on to something else.

Lott: I know we're having a little bit of lag time with the slide advancement here, so if we could jump to slide 22 with regard to facial recognition. The early facial recognition systems from my research showed that they were first implemented back in the 1960s, in casinos and some other venues, but the consumer application really didn't start until the last couple of years, with the introduction of some of the newer models of smartphones. Jim, can you quickly give us an overview of the technology—and in particular, what impact has COVID had on this with the face mask that's going to cover generally at least half of a person's face?

Loudermilk: So, that's still emerging; it's not altogether clear. NIST has published one report so far on this where they looked at a variety of different kinds of masks, which were artificially applied because they didn't have a reference database of people wearing masks that they could do testing against. And they found that the shape mattered, that the low masks—particularly ones that went below the nose—had very little adverse impact on the accuracy of the algorithms, whereas the round masks and the high masks that covered the nose had a significant impact. The very best algorithm only had a 2 percent performance difference with masks.

But in general, we're looking at about a 5 percent performance impact, and there were some that just had dramatic adverse impacts. Now, this is going to get better with the passage of time. A number of companies have come up with new algorithms that take into account masks. There are Asian companies—Chinese in particular, where the wearing of masks in public has been common for a very long time—that perform, or at least they claim they perform, really well in the presence of masks. The NIST testing did not substantiate that, however.

It's going to get better. It's not going to be as good; it's just not. And we're going to be wearing masks for a while now. Hopefully, not a long while now; as best I can tell, and I do have a vested interest in knowing, we're probably a year away from any kind of return to normality like we're used to. Hopefully I'm wrong and it will be sooner than that; but this too will pass, and we'll go back to normal. We won't be socially acceptably wearing masks like we are today.

Lott: I understand that. All right; how about iris recognition? You've mentioned that a couple of times already. Can you give us an update?

Loudermilk: Iris is a truly fabulous technology. It doesn't take much space for the templates; matching is really fast; it's highly accurate. There are absolutely no demographic effects at all, and the scientific community has looked hard. It doesn't vary with race; it doesn't vary with age—it's great. So why don't we use it all the time? Well, because at least thus far, iris is more difficult to capture. It's difficult to enroll, and it's difficult to acquire in operational settings. You'll have problems with occlusion, where eyelashes, hair across the face, various other things get in the way—blinking affects it.

And then, at least until very recently, it's expensive. Of the typical equipment that would be used...I left something out that's important. You don't capture iris in visible light. People of dark skin—or, maybe more accurately, I should say [with] people with brown eyes and black eyes, you can't readily see the vein structure, the pattern structure, in the iris—so it has to be captured in the near infrared, not in the visible. Because of that, the equipment is much more expensive, and until recently you were looking in the $5,000 to $20,000 per camera range to do this, with sufficient accuracy for the used technology.

There have been some mobile phones that used iris to unlock the phone, but that's really a different problem than the general purpose use of iris for identification. So it's a wonderful technology. You'll see it in border crossing applications, in some places. But it's an expensive technology.

Lott: If we could move to the next slide on voice recognition; again, I know we've talked about this before, and I guess from my perspective, it really has had limited implementation in the financial services world. Most frequently, it's being used in call centers, primarily dealing with high net worth clients or with commercial wire transfer transactions, where there's a high dollar value or risk associated there.

Jim, are you seeing anything different?

Loudermilk: So it's great in the call center, in the situations you describe, particularly when you couple it with a Caller ID from a known phone number—very effective in those cases. But there are problems with it. The voice recognition, particularly over the telephone, is inherently discriminative. It turns out that when the telephone system was invented, and really largely has carried through up until today, that bandwidth was a significant consideration, much more then than now.

But the voice information in the telephone is in about a 4,000 Hertz (and lower) band. It turns out the identifying characteristics for males are all below 4,000 Hertz—they range from about 300 to 3,200 Hertz for males—whereas the identifying characteristics for females are primarily up around 6,000 Hertz. So if you've ever wondered why it's more difficult to recognize women—not family, they're easy—but people that you know, but they sound a little funny over the phone, it's because the technology inherently discriminates against the females, so that's a problem with it.

And there are a lot of other technical issues with voice about how close the microphone is, the acoustics of the room—is it near-field or far-field communications? Is the same kind of microphone used to capture the reference sample that's now being used to capture the probe? As I indicated earlier, the FBI at least will not allow testimony to positive identification because we just don't believe the science is in place to fully support it. It may well be there someday.

On the negative side, in some respects of the technical biometrics, it's the oldest. If you have access to it, there's research dating back to the early 1940s, just before and in the early days of World War II, where the military was trying to do speaker identification from the voice. Some of that research is still classified; a lot of it's eligible to be declassified, but there's no motivation to do it. With all that time, 80 years spent on this problem, it still hasn't come along very well. So, it's hard to say when this is going to actually be a mature technology.

Lott: Yes; still a challenge. Let's skip over behavioral biometrics, that we've mentioned before. That's kind of an emerging modality, used primarily by online and gaming e-commerce merchants in order to try and validate customers—and jump into a couple of the issues, because we only have a couple of minutes left and we want to be respectful of everyone's time here. So if we could jump to slide 26, and talk about privacy real quickly.

Privacy is certainly separate from the issue of security. There are some states that have developed some level of privacy laws, and, of course, in the healthcare area, we have the HIPAA regulations. Federal legislation, consumer protection, doesn't seem to have gone anywhere over the last decade with regard to this. Do you see anything different, Jim, really quickly?

Loudermilk: No. It's a touchy subject, maybe not with the majority, but with a subcommunity, it just seems too personal and seems a little invasive. From my perspective, I really don't mind having my fingerprints or my face in a database. There's nothing that you can do with it unless you have identifying information, biographic information. There is no way to associate my fingerprints with me except with a fingerprint matching system that already has that information in it. I don't find it as spooky.

Similarly, it's hard to hide it. For a long time, I tried to not have an internet presence when I was working at the FBI because of some of the things that I did. And I found that while I could control what I did, I couldn't keep my children and my relatives—and for that matter, my friends—from posting pictures that were taken at social events. So, it's really hard to completely hide your online presence, even if you want to. So it's a concern, but I don't think it should be a terrible concern for most people.

Things that you can do, if you have a system that uses biometrics, is be transparent about it; don't hide what you're doing, or why you're doing it. Be sure that it's appropriate, that it's lawful, and that you protect the information that you put in it. I think we talk about that some more in another slide, too, where the various...

Lott: Yes, if we could move to the next slide, because I know the trust and consent issue is critical and very important to you. We've got about a minute left, so can you recap real quickly, in a minute, Jim?

Loudermilk: Maybe; for government purposes, consent's not too relevant. No criminal is going to consent to being identified, and you're not going to get their driver's license unless they agree. So consent's not relevant, but notice is certainly relevant. I think for all commercial purposes, consent is relevant and notice is relevant—they need to trust you. If they don't trust you, they're likely to take their business somewhere else, which is a pretty terrible thing when your commercial welfare depends upon it.

Lott: Right; well, we're about up on the hour, so I'm afraid we won't be able to address any of the questions on the webinar. But we will—Jim and I will get together, and we will respond to those that posted those questions.

Jim, I can't thank you enough for your time today and all the time that you spent with me preparing for the webinar. I know that those that joined us today got lots of great information and insight. I also want to thank those that did join us. Our next *Talk About Payments* webinar is going to be on November 19 at 1 p.m. Eastern time, where we're going to be examining the change in consumer payments behavior as a result of the COVID health crisis, and I hope you can join us then.

Tim, I'll turn it back to you for closing us out.

Lloyd: All right; thank you, Dave. And I'd like to thank both you and Jim for sharing your time and your expertise with everyone. I want to let you know that a survey is now available to everyone who's joining us via webinar—you can just go ahead and click that link if you've got a few moments to fill it out about today's program—and everyone will also receive the survey link via email. You only need to fill it out once, but please just take a few minutes if you can to do so.

And thank you again for joining us. This concludes today's Federal Reserve Bank of Atlanta *Talk About Payments* webinar. Have a great day.

RELATED LINKS: Presentation • Q&A • Talk About Payments: The Year in Payments • Talk About Payments: Exploring Check Use by Businesses and Consumers