LiveCast 5: Sep 3, 2020

Spotlight on Face Recognition Technology

The following is an AI generated transcript of the above mentioned LiveCast episode and therefore may include typographical errors. The purpose of this transcript is to provide quick, searchable reference to the various issues discussed based on keywords you choose to enter.

SUMMARY KEYWORDS
face, face recognition, biometrics, technology, algorithms, africa, fingerprints, passenger, question, government, enrollment, operator, application, deduplication, identity, system, duplicates, problem, issue, Patrick grother

14:40
Greetings Ladies and gentlemen, I am Joseph Atick, the executive chairman of ID4Africa. And I would like to welcome you to this restart this new season of our life casts, which is starting with a very exciting session on face recognition. But before we speak about This session, I've got a few announcements to share with you quickly. I am sure some of you have seen the announcement we made earlier in the month regarding the fact that we've moved our general Annual Meeting from October 2020 to 27th to 29th, October 2021. This decision was made in consultation with the host government, because of the continued restrictions on large scale gatherings such as ours, and the lack of transportation, airlines that would be servicing the country. So while we are disappointed that we will not be seeing each other face to face in this year, rest assured, we are not sitting idle. We are leveraging this medium to advance our collective agenda. We will in fact, see each other 30 to 40 times before we meet again, in Marrakesh, in 2021. We have a whole series of live guests that are being organized with fresh content with a pertinent material with experts that are going to be sharing with us and joining us. In fact, I give her Africa has become the voice of Africa on identity matters. And this voice is being heard, in fact, all over the world. With us through the live casts through this medium, we welcome more than 90 countries, representatives, and delegates and attendees from more than 90 countries. So we're excited to see the breath that we are going into. So in addition, in addition to our live casts, which are being organized 30 to 40. In this coming year, we will also be bringing to you in November, an exposition a virtual exposition, a completely new concept in how technology will be brought to you. But anyway, we will give you more information about that when in due time. Back to this month, I want to attract your attention to a few important announcements regarding the two sessions that are coming up after the

face recognition session. We have a big event coming up September 16, which is which is on inclusion happens to coincide with the D day. So this is the September 16 celebration. We believe inclusion is what is the largest, most important challenge that is faced in Africa. It's not interoperability, it's not trust, it's really achieving inclusion so that everybody can be counted can be brought in. So we're going to talk about the root causes of exclusion, the barriers to inclusion, and share experiences from countries that have actually made significant progress in the inclusion agenda. So stay tuned for that, please join us. And then on September 23, we are launching a new series, which we are excited about. And this new series is in fact, we call the country progress report. And we start with a spotlight on Nigeria. As you can see, we will be bringing in company identity stakeholders from Nigeria on a roundtable where we will have an open and frank discussion among all of them to understand the demand and supply side of the identity ecosystem in the country, and extract lessons that could be really useful for other countries. So we will be doing, of course, many, many countries in Africa in due time. This takes a lot of effort to organize bringing in all of the political as well as the operational people that are in charge of the strategy and vision of the country regarding identity. But it's a very important activity. And it's the only one that you can find in any forum. It's only here for Africa.

19:24

There's a lot more we don't have time to go over them in October, for example, but the best way to stay informed in our life gas is our life gas page. So please bookmark that. Keep visiting it and see the new announcements that we are making regarding what's coming on the program. I also asked you to please do me a favor and subscribe to the YouTube channel. Go to the YouTube channel of our different Africa, the media channel, and subscribe. Why because we will be putting out a lot of valuable content that we really want you to have access to as members and partners. This identity community. So anyway, now we're going to go back to our session today. We're very, very excited to have assembled an illustrious panel focused on face recognition. We are going to start with a major keynote by Patrick Grother. Patrick does not need introduction, Patrick is somebody that I've known over 15 years. But he's well renowned for being the person who knows more most about face recognition and evaluation in the world. So we're really pleased to have Patrick with us, Patrick will deliver a keynote you will you will get an opportunity to ask Patrick questions directly. We've also received questions from you, which we will be sharing what we've shared with Patrick, and maybe he will have time to answer those. Afterwards, we are going to have basically rapid fire case studies, we'll have four different case studies where face recognition has been used with success for development, so positive applications. And then we are going to bring an in conversation session with Pam Dixon, and Teki Falconer, who are going to be engaged with me in what I hope would be fireworks type of debate and discussion on the responsible use of face recognition, and the need and the need for regulation or not. At that time, you as members of the panel, you can raise your hand, and you can attract the attention of an operator from ID4Africa will prepare you to get on the panel to share your views, we'll have the community voices session section segment it all in all, we'll have an exciting two hours, filled with important fresh content from experts that are worldwide in their reputation. So I without any further delay, I would first thank the entire panel for being with us for the contribution. And then we'll come back to you one by one. And then I would like now to ask Patrick, to step to the stage and take control and share his screen.

22:31

Thank you, Joseph, thank you very much for the invitation to talk today. It's a it's a privilege to be here. So I work for an organization called NIST part of the US government under the US Department of Commerce. We have been involved in face recognition for maybe 20 plus years now, our most famous activity is the face recognition vendor tests. Here you see an overview of the various activities within that what I'm going to talk about today are various products that come from our benchmarking activities. We track the technology and and report it openly. On our website. You can Google NIST FRT to give you pretty much all the information that you'll see today. And I'm happy to share these slides afterwards. So what is face recognition actually doing? It's doing what other biometrics do it compares essentially two samples, and it's called this kind of activity is used in border crossing gates of the kind shown on the left there. But the goal is is to deduce whether the two images you can see here are the same person or different person. And that is a non trivial task, you can perhaps look at these two faces and and have difficulty determining this. I will tell you the true answer in just a moment. But how would face recognition proceed with that both images would get sent to a a black box, a identity extractor that produces what's called a feature vector or maybe a template, which is a representation of identity information in the face. We do that to two images. And then we compare them that's the center black box that produces a score. And in this case, these are different people. They're my colleagues and one is a system of my colleague. And so the correct response would be to produce a low score and to say it's a different person. Now, that technology those blank boxes nowadays are built with convolution, neural networks AI and machine learning. They are not commoditized. This is not something that is open source has a lot of trade secrets, a lot of intellectual property in there. The feature vectors, the encoding of the face is maybe two kilobytes, sometimes the smallest point two kilobytes. And they can be produced on a typical CPU in less than one second. That's, that's how face recognition proceeds as it's called. And I said that face recognition is not easy. There are errors, there are particularly false rejection area areas where I don't match a photo of me. And in that case, I wouldn't get through an E passport gate. And there's been a revolution in the accuracy of face recognition. Now over at least a decade. This graph shows the reduction in false negatives, over a three year period from one typical algorithm, which happens to be idemia in Paris. And though they've evolved our algorithms, along with all the other developers, and the error rates have come down from 13%, which one in six to one in seven transactions failing? Down 2.6%. And that is because the technology is much more capable of handling poor images. And this, this is not an easy data set that we've used here. This is a operational data set. So this result is quite impressive. We track the technology, we publish open benchmarks, this is a essentially a screenshot of our website, you can see algorithms listed listed on the left side from different suppliers. And on the columns of this table are different datasets from different kinds of images. And the error rates, their lower is better. That table extends now to 400 rows. And, and it's interesting to monitor the technology that way.

27:19

Recently, of course, we've started wearing protective face masks. And it was interesting to know what would happen if you were to hide some percentage of the face. So we covered faces digitally, with either solid masks or textured masks. And then we ran the the algorithms on those. Now, that was never going to be a very good thing for face recognition. But in the best case at the top there, the failure rates have increased, say from point 4% to 2.4%. So that's taking the technology back maybe two or three years. It's a setback compared to what it was some algorithms However, at the bottom of this screen are entirely intolerant of face masks and the failure rate can be very, very high. So some

algorithms are probably usable and some algorithms are probably not and we are evolving this this kind of data as we go continuously. So the larger market segment will face recognition is one to many identification. There are a number of applications typically document fraud, Visa fraud, National ID duplicate detection, but also in casinos in aircraft boarding in video surveillance. And humans are not normally used much in those applications. They would adjudicate some errors. Of course, there's another class of application this criminal investigation where face recognition is being used with a human in conjunction. How How, how does this proceed? Essentially, we do a one to many search by doing many one to one comparisons, two kinds of errors can occur a false negative where the person is not found in the database, and also a false positive, where a person is erroneously returned by a search. And there are cases reported where false positives and true positives occur. And they've been reported in the press. So as a demonstration of how well one to many can work. What we did is we enrolled images of the kind on the left, and we enrolled 104 million of those from our bank 32 million people. So that's the population of Mozambique, and I think Angola approximately and the idea is to search an image of the kind on the left and look at the accuracy. So we did this with a demonstration using an algorithm from NBC in Japan. And those algorithms, that algorithm is successful at returning the correct image from a search with a 99.6% success rate, the point 4% miss rate. So that would be a result appropriate to an investigative search. But if you are going to do high volume searches, you have a low false positive rate. And that error rate will drop, you have to increase the threshold. And in this case, with a 1% false positive rate, you can still identify 99.4% of the people in our database. So that is a remarkable result, given that the images are far from passport compliance, aka compliance. We maintain, again, a leaderboard different algorithms on different data sets. And we track the technology continuously and publish the results. So what is the state of the industry has been an expansion of the industry, enabled by better algorithms that are very accurate on high quality images that are tolerant of poor quality, increasingly, that are tolerant of aging also increasingly, and can operate in very large databases. China, the Europeans, Japan and Russia are very active in development. The technology is not commoditized some algorithms are much better than others. So buyer beware. We can still do better with the cameras to improve quality. So there are standardization activities going on. On the right side of this slide. The issue of demographics, which I'll get to on the next few slides. And twins also are not separable. I'll get to that in just a second. And also there are opportunities to attack face recognition, as with other biometrics face is perhaps problematic because it's easy to steal another person's face.

32:05
If you're going to launch an impersonation attack of them, many systems are not defending against that currently, some are. And there are some other attacks. Also human capability when a human is employed, to look at face results. human capability is poor, and also potentially bias. So what what do I mean by performance bias, we can look to Apple no less for some data on this. After they released their iPhone x. They quickly added a web page indicator indicating that the false positive rate on twins and siblings and children was a lot higher than the one in a million false positive rate than they had marketed the phone ads. And that effect is shared with traditional face recognition hosted on other platforms. And so we produced a report looking at these various issues on demographics in December last year. And we noted that false positive rates vary with age, that's the cells in each of these blocks, and also geographically with where people were born. And of course, it varies with the algorithm. What you see here is a measure of false positives for an algorithm out of the UK. And you can see much

higher false positive rates in elderly Chinese woman than you do in white males from Eastern Europe. And that is has security implications for something like border crossing and other applications. And what you would like is for those false positive rates to be much more uniform, not varying with age or with sex, or with geography with race. We produced a lot of data on that there is some developer activity to mitigate these differentials. In all cases, these differentials are not necessarily material, it depends on the application. So it's very important to walk through the consequences of errors in face recognition systems, false negatives and false positives. And I've given three different applications here. I won't go through them in detail. But you have to think through your volumes, your probability of fraudulent behavior, and the the, the kind of algorithm that you're using different implications for different applications and they need to be thought through quality of course matters. There are many, many ways to take very bad photographs, and eventually you will undermine performance. There are standards efforts, long standing efforts going on within ISO sc 37. On image quality on passport image interchange, and on face aware capture recently, those bottom two standards there are now under development and worthy of considerable attention in the future. I shall mentioned twins. Twins are quite common, one in 30 births in the United States. And twins vary considerably with geography across the world. So they're not uncommon. They're more common in I think, in West Africa than they are in East Asia. And face recognition algorithms will routinely confuse identical twins. So here we have three algorithms being used in a one to many search. And they are all returning the twin as the person in the database. So that is something that needs to be considered and planned for an operating. It also happens with fraternal twins, but they do not score as highly. Some fraternal twins are different sex and they are not falsely matched typically. twins are a problem for face recognition. Replacing say 10 fingerprints because with fingerprints, we don't see false positives in related individuals. And in face, it implies a limit on how low we can go with false positive rates. But because twins exist in society and national scale databases, or local databases,

36:52

and found other family relationships, we can't get to very low false positives. And that is not something you expect to happen with fingerprints or with iris recognition. And that brings me to one slide on modality comparison. So why face over for example, fingerprints, versus Iris. And a reference this table to the sort of definitional properties written down 20 years ago for biometrics that they must be unique, they must be available, they must be socially acceptable, they must be permanent. And more or less different modalities have different compliance to those ideal traits. So if we look at uniqueness, a single finger will not be as unique as a face nowadays 10 fingers will be highly unique, not always available. So that's the second the third column there. That some fingerprints, sorry, the demographics column off to the right there. But in elderly people using certain kinds of sensors, you don't necessarily see good fingerprint images. So there are demographic issues. false negatives, particularly in the elderly, false positives in face recognition. And, and different social acceptance. On the right side there, I co wrote a very nice study of that when they were formulating the 9303 passport regulation document. And different sensors, different capabilities, different speed. All of the cells in this matrix have a nuanced discussion. And particularly, there are applications where any particular property is not really relevant. So for example, some same day airport applications wouldn't need to worry about aging of a biometric. So yeah, I'm happy to sort of entertain any questions either today or offline about that kind of matrix. And you could reach me, my email at work is that and our face recognition vendor test, also has an email. Thank you very much. Thank you. Thank you, Patrick.

39:28
I think we have time for taking questions. There have been several questions from the audience that have come up. And they can be lumped together. In fact, one area that people are wondering about, Patrick, in your opinion, do you think face alone, maybe plus some certain exception handling is sufficient to deal with one to many deduplication at a national scale, without invoking any other biometric?

39:57
I don't think so. India made its choice A decade ago now to use Iris and fingerprints. Obviously, face recognition is much better today. But contemporary algorithms are not capable of disambiguating twins. There are approaches that can solve that using high resolution imagery and skin texture. But but a national ID program would need to address the possibility of twins today.

40:30
And do you think the issue of fraternal relations not twins, is that something the algorithms will come to the accuracy levels, that we could tell that they are related but not the same person?

40:44
I think so. They, for blood relatives give higher similarity scores, they may well be below threshold and face recognition would work anyway. But in something like a surveillance system, it would be possibly problematic.

41:03
Now, I mean, this is on the side, should there be any privacy implications in that, like, knowing that I am the brother of somebody? Is that something that we should worry about in society that there is a technology that can tell who is related to me? Is that a dimension, perhaps, is something that I'll leave for the other panelists, but have you explored that as a potential issue?

41:28
We haven't done privacy analysis or even work on privacy enhancing technologies. That's something we want to do in the future. But you know, there are ethical problems, the DNA community have looked at, you know, the ethics of of being able to associate individuals that you didn't know, were related. face would be less powerful than DNA in doing that, of course. But

41:52
yeah. And

41:56
but from a technology point of view, you cannot really tell that that these are related or it just happens to be somebody with a with a similar score. I mean, there isn't a special signal that we can, we can extract, right?

42:12

Yeah, that's right. Unless identical twins, and particularly young, identical twins, you wouldn't be able to conclude a familial relationship

42:22
during your relationship. Okay. There's a lot of questions now on the chat about 3d face, has NIST been interested in exploring or will be exploring 3d face, we want to we haven't

42:35
all of our venture to run with traditional 2d photographs. 3d obviously has advantages for accuracy for spoof detection. We want to work in that domain, we are limited by the amount of data that we have. Okay.

42:54
Now, if I may ask you, Patrick, on page 34 of your slide deck, your answer very quickly, rapid answers to many questions that came in prior May. Could you please share your screen again, and just run through these answers so that people will be satisfied that the questions were answered? I'll try. Yes. 34.

43:21
Yeah.

43:25
Yes. So please, please explain. If you if you if you may run through some of these answers.

43:30
The question is, can we look at school calibration procedures to remove demographic bias? There are some studies going on in that area. It is a researchers, you this is properly the responsibility of the vendor community, I believe. And the idea would be to suppress false positives. I think that's that's good potential retraining algorithms. There's also got potential company in Europe is published on that aspect. Second question, how age related face changes affect the accuracy rates? Yes, unfortunately, we change appearance over time at some graceful rate. That change in appearance will depress the similarity scores. Eventually it will undermine recognition. The algorithms are more tolerant of that than they used to be. I don't think it would affect our matching speed. The third question live capture against a photo captured from laminated or protected paper document. Miss doesn't have a study on that. An organization associated with homeland security in the United States has recent data on that publication is pending. And that was for using a US driving license to go through an airport identity To check and I think the results are quite encouraging. Again, it depends on using a modern, good algorithm can face recognition work on the newly born? Yes, the best data on that has come from an Australian government study using passport photos. There are some human factors issues with getting a baby to look at the camera, and to stay still. And the Ozzie study does show that you can't do tenure recognition. Aging is too rapid and error rates to creep up but over the short run one year or two years, face recognition has shown quite remarkable accuracy and even in the very young, there are some more false positives in the very young. How can face avoid bias the next question? How can it be audited to certify it is free of race and gender bias? Free is a quite a strong word I'm not sure we'll ever

get to a point where it is free of all age, race, gender bias. Control testing is needed. You need to be able to show that these underlying factors have been mitigated. And potentially, I think the vendor community believes that retraining is necessary on more diverse data. image data, relative accuracy of face compared with Iris and fingerprint is again a quite a complicated discussion. As I mentioned face doesn't get too low false positive rates. But things like Iris and fingerprints have problems getting to very low false negative rate. fingerprints can be damaged. In elderly people with an optical sensor, they may be difficult to take photos of iris recognition, sometimes the capture devices somewhat difficult to use and enrollment doesn't always succeed. With both eyes. There are advanced optical designs, obviously for both Iris and fingerprint that address those issues. But face recognition algorithms will enroll most faces that are occluded by face masks, or about a time. When would you ever use face when you already have finger? capture speed is possible if you've got some high volume access control application, maybe where you're concerned about social acceptance, or you've got different concerns about spoofing? I'm not sure what my last comment means that but there are reasons to use face when you have finger to do with lower false negatives. And concerning with with the threat environment or the concerns that you have with security.

48:15
You better it let's go back to the question of bias, gender racial bias of the technology. From your expert opinion. Do you think this is fundamental to the dimensionality of the space representational phase? For example, if we, if we over trained in one one racial group than the other group have would be insensitive or would be making hire mistakes. But when we shift and train to the other racial group, aren't we going to have potentially certain algorithms, which will begin to show the inverse bias? It's not something that's related to the to the size of the space or even even when we went in diverse data set? Maybe there is a fundamental limitation are we hitting fundamental limitation or not? That's my question.

49:11
I don't think there's fundamental limitations here.

49:16
The

49:18
Face Recognition would be better if it could see different features in a face image. skin texture is one of them features in the periocular region around the eyes. there there's information that is not being captured in contemporary photos, like passport photos. But I think if more diverse training data was available to the developer community, they could address existing biases today the false positive biases Yeah, the false negative differentials in face recognition we found are quite small photo Face Recognition algorithms are capable of dealing quite well with overexposed and underexposed photos with poor photography, essentially.

50:14
How difficult is it for a player like Facebook, for example, to assemble a really diverse database and show that there is no fundamental bias in the technology once and for all? This is what I'm not yet

arriving at the conclusion or being convinced of, basically, because the data does exist with the big players. And unfortunately, none of them were tested in your tests.

50:42
Yeah, we we did evaluate Microsoft, I don't think Microsoft would have witnessed the number of images that Facebook has, obviously. So Facebook is in a unique position to be able to answer some fundamental questions here. Most of the time, we don't know how much data that the the leading biometrics providers actually have. Vimeo, NBC Talos, cogent. We don't know how much data they have, what access to data they have, it's, it's probably not enough, you talk to a machine learning person, and they always want more and better data? Well,

51:27
I think we need to call upon those that have the data, we make a call for action to Facebook, if any of them are listening to this, we need to establish once and for all, whether face recognition has fundamental bias, because of the limitation in the dimensionality of the informational space of the face, or whether it's just simply we do not have enough data to do the training, and therefore establish racially diverse algorithm. So I call upon Facebook, because they seem to be the ones that have that data. If they don't want to participate in your testing, maybe they can come up and show us independent data, that there is no bias in the because this is a political issue right now around the world. We're wondering about gender, we're wondering about face racial compositions age. So if this can be resolved scientifically, we shouldn't be turning around and avoiding head on site asking this question. So would you be interested in testing Facebook's algorithm? Of course,

52:33
yep. We our doors are open to anybody worldwide with an algorithm. We have no mechanism to compel them to participate.

52:41
Okay, so hopefully, they're listening. And hopefully they will join this call, which is very, very important to the future of this technology. Okay. Actually, we've taken we've taken a lot of time. We there are a lot of questions that are coming in as well. Unfortunately, we don't have time to answer them live. But as you have given your contact information, hopefully, those people will contact you and can get some answers. For those who are interested in Patrick's his presentation, please email us and we'll arrange for you to have access to it. Patrick, thank you so much for your contribution, we can go on for several hours on this topic. Thank you very much.

53:29
Thank you,

53:30
okay. Next, I think we are going to start the case studies. Then we will ask Sita to come to the stage and talk to us about how face recognition is being used today in a positive manner for travel. Jihad Boueri.

53:57
Thank you very much for this opportunity hearing today. And for this very useful information. What I'll be showing here is how we use this ecology for the airport business. So, my name is Sita and the cheetah is not a manufacturer for any kind of face recognition system is an IT company specialized for the transport industry. So, what I will be showing you in this presentation is the case study on how we are using the face recognition for the messenger process and Next slide please. The introduction of myself so I am responsible of the Middle East and Africa region so we can get through the airports of India you can easily and mainly in Africa. Nice Okay he study I have selected is for the Beijing International Airport Why? Because we wanted to show how this technology or face recognition is being used at a very, very busy airport second busiest in the world and accessing millions of passengers passenger a year the airport had the challenge, they wanted to facilitate the passenger processing, they wanted to facilitate the experience of the passengers at the same time is easy to implement and that works across all the airlines without the need to integrate with any different time and that can also took a big advantage and being interested after COVID-19 for this take place as we will see in the coming slide.

56:01
So,

56:04
okay, what is the solution about smart, smart using your face to go through the steps of the ascension journey, how it works, first you have to enroll in Rohan means, you scan your passport, you take your face picture and you have your boarding pass as the data we need to gather and we create what is called a passenger token. This token will match your face is your boarding pass with your personal details. So, your face becomes your boarding pass and you face become the enrollment can be done at any station to your mobile phone can be done at the counter at the airport at the kiosk at the airport at any stage and the solution then we work with easy to integrate will work with integration with the government when the game during the process. So, by showing your face, you just access every step of the airport from the chicken to the security to the plane let the application provide API. So as I mentioned easy to integrate and GDPR compliant which is very important. Next slide please. So, I will not explain who will take you through the process you will be seeing how this technology is being implemented. But at the end of this project, there is efficiency in the potential processing experience for the passenger. When you speak about efficiency to give you an idea about the speed you can in 20 minutes and ever created was 400 passenger and 62 people at the airport we concentrate on servicing the needs of the passenger instead of doing Vietnam and processing. So that was an idea. Permission will be used at the airport passenger journey and there is a team of three minutes that will be self explanatory. And again, we'll be happy to answer your queries. So let's start.

58:57
Beijing capital International Airport is Asia's busiest airport and the second busiest in the world, serving more than 100 million passengers a year. To deliver an outstanding passenger experience. The airport's bold ambition was to design future proof solutions by evaluating the latest technologies in the market and selecting Sita smartpath to serve passengers at different touch points.

59:23
The biggest initiative is a four is creating a more seamless passenger journey or passenger experience. So the passengers going through an airport to seamlessly move from end to end and go through the physical thoughts points with as little friction as possible

59:58
biometrics is enabled. technology and technology that started within the border control and now is moving into other physical touch points within the airport.

1:00:07
The Self Service check in process is reduced to just a few seconds. At the same time, airlines don't need to change their existing software. It couldn't be simpler. The passenger checks in at SITA's intuitive kiosk, which quickly takes their photo and matches their face with the photo and their passport or ID once confirmed, smartpath creates a secure single travel token. for passengers checking in at an airport desk or backdrop. smartpath again makes it easy to create their single travel token a quick glance in the camera and the process is complete. The passengers face is now their boarding pass. See this self service backdrop, known as dropping fly is a simple and quick process. Passengers glance into the camera to verify their identity with no need to present a boarding pass. Flight details collected at checkout automatically update the Self Service backdrop, the passenger just needs to attach the easy to use bag tag received a jacket and place their bag on the conveyor belt. Now airline agents have more time to help other passengers and create an even better customer experience. As passengers move towards the security checkpoint, they simply look into the camera at the entrance of the restricted zone. Once their face confirms with the record created a check in the gate opens and off they go. At the security checkpoint, the same process is repeated.

1:01:33
Now it's time to board the aircraft. Once again, passengers just need to quickly glance at the camera in less than five seconds, the boarding pass is verified, and smartpath automatically updates the airlines departure control system. When everything is in order, the gate opens and the passenger boards their flight smartpath reduces overall boarding times and improves the experience for passengers and operational efficiencies for airlines. Good

1:02:01
if there was one question, but in the meantime, Jihad wasn't so clear to me in your video, you are doing one to many right you are not doing just authentication of faces, the person does not need to utilize a token when they are boarding Is that correct?

1:02:20
What do you mean?

1:02:23
Return on the faces capture the password. And the server there is a token created the face to be passed to the boarding pass. So when the passenger just by showing his face the information about his

boarding pass and his password will be sent to the airline or will be sent to immigration if it is at the finger issue.

1:02:57
Right. But they don't need to show a boarding pass and verify the face against simply they just

1:03:04
Yes, exactly. They don't need them is to be paperless. And they just just show they face in so they insist to double check. But in general as a technology it was without showing anything.

1:03:20
Okay, so that's that's the future the future would be yes. No additional token your face becomes your passport. Okay, that's something that we will explore in the future. Because the error dimension would be interesting to see if you mix with somebody else, etc. But we don't have time today. Thank you very much you had for this interesting. I want to move to the next application which I believe is from Tech5 are you on?

1:04:19
First of all, I would like to thank Dr. Atick and ID4Africa for giving us the opportunity to talk about our use case. This is again, one of the non controversial use of face technology, as we have seen it and we've been in this field in industry see a lot of value of face and that's what I'm going to talk about. He's got in the next slide. I'll give a quick introduction of who I am and what our company does. So, as you can see the company's name is technology for inclusion tech phi. We started this company I co founded this company with the whole principle of Serving inclusion and making sure that the digital identity is in the controls of the owners. This is only for the credibility sake that I have been involved personally in very large scale programs. And all the results that we talk about. And the use case comes from a real study that has been done under these programs. So we have more than 350 million active identities, processing 200,000 transactions per day, and the programs that have been been involved with at least you know, a few 100 million and some of them are about 50 million. So if you go to the next slide. So the problem statement was, how do we use face recognition in a traditional national ID duplication scenario, the program that I'm going to talk about actually started 10 years ago, when this was considered as a secondary biometric fingerprint and Iris was given the primary way this in the deduplication process, and as Patrick has already colored and mentioned, is that face has evolved significantly in the last decade. And I would say, in last five years, we have seen that face and probably play a big role in certain programs or use case. The customer that we are talking about, as I said did make a good move of enrolling IQL compliant images and we are talking about 190 6 million people enrolled and ongoing. So, the whole objective was to see how we can use facial recognition in cases where you cannot use face or fingerprint to do this duplication and stop whatever you know, fraud or issues with deduplication that may arise because of this shortcoming. Next slide please. So the use of facial recognition in national ID as I said, there are one may ask Yeah, why wouldn't a person have his fingerprints or Iris capture during enrollment, because the typical enrollment scenarios in socialized system would be you captured kit face you get to 10 fingerprints and then you capture irises. Now, the issue is of course, because of quality. And there may be reasons why people do not have good quality

fingerprints, or Iris, especially due to age and the demographics, then there are operational or systematic errors, where the operators Mark somebody is an exception, when as an exception means does not have capturable, fingerprints or Iris, or it could purely be a fraud, where the operator is colluding with the enrollment citizen and then trying to bypass the system by not offering the biometrics never use for deduplication. The reason why we use face is because that was the only available modality in this case of duplication. The other reason was that it is now accurate, and we believe that it would solve the problem. It requires very less hardware these days, and the hardware footprint requirements have gone down. And last but not least, any citizen that enrolls primarily, even if they're trying to fraud, they usually do not avoid giving their face because it is printed on the card. So you have to have a face number one, number two, most of these services for visual verification as well as authentication services use face these days. So avoiding face was a little tricky for some of these foresters. So what we did, we had 190 6 million

1:08:43

records, of which we filter down based on the above criterias people who do not have fingerprint or Iris, people who have fingerprint is a low quality, or somebody who is suspicious like one finger me or one Iris only kind of scenario. We filtered out 4 million plus Records, which is about 2% of the total population. Then we did a full face only deduplication. It took us about what worry and hours. You can imagine this is 780 4 trillion comparisons, we use three of the shelf computers, CPUs, and 16 cores. what we ended up doing is we set up a threshold at a log factor of 10. That resulted in 1.25% duplicates from the 4 million subset, which basically means an effective duplicates, duplicates that were found was point 02 5% of the total population. Next slide, please. Now when we say it's only point zero to 5% of the population, but then you have to look at from the perspective of you know, all fraudulent Li created IDs are stealing from the citizens or from the other genuine citizens. So stopping this fraud. And putting some data is always the goal of a national ID system like this. So what we have been able to do is that we have been able to clean up the database when I say cleanup is find the duplicate suspicious cases. And we have been able to create this deterrent and actually close the loophole, which lets these citizens or fraudsters try to defraud the system one or the other way. Of course, the the other benefits that come with the good quality face enrollment and deduplication is that it provides the secondary services based on the national ID like ekyc, then you have the cases where somebody loses their IDs driven services, they could use facial recognition instead of fingerprint, for a lot of reasons that Patrick has already mentioned, the ease and social acceptance. And last but not least, it has also been used in scenarios for natural disasters, where for whatever reason, the other biometrics were not available for matching. What what actually ended up by doing this, we were able to, you know, find and manually verify a significant statistically significant portion of the database are duplicates found, and then they will decimate it to the local authorities to confirm and take corrective action to go to the next slide. So what are the takeaways? Again, I don't want to repeat everything that Patrick said, because he pretty much covered all the questions I would have mine or somebody would ask me. Yes, I mean, face is not more a normal a secondary biometric. He, as a company, since we have face finger and Iris are actively doing our internal research to benchmark these against each other. What we have found so far, and I'm speaking in purely practical scenarios, that a face recognition algorithm is pretty much equivalent to a two finger aphis in from an accuracy perspective, including failure to capture failure to enroll factors included. So it can it already shows that, you know, there were those days when two finger systems were used for many large scale programs. Now, you could in theory, use fingerprints, of

course, considering the fact that you cannot be separate twins. On the other hand, what this also helped us and you know, it's helping the local government to do is that change the whole aspect of perspective towards fingerprint not using fingerprint as the only modality for deduplication slash, you know, use face for conclusive decision if a person is duplicate or not. And last, but not least, I would say the face has proven its efficacy. So we are offering this as a standard offering, you know, in our deduplication supranational IDs, and I'm sure that many governments will consider the same. So with that, I would like to conclude our short presentation and

1:12:55
take any questions you may have. Thank you, Rahul, there is a question for you. Basically, the somebody in the audience was wondering, were there multiple images of the same person associated with the same record? Or was it just one image per person associated with the record?

1:13:13
So the it's a typical fraud case where people try to re enroll with a different identity and try to get a duplicate card? So it is one person one face, but two different identities?

1:13:28
Okay, but in terms of the program, the program does take only one photo of the of the individual?

1:13:36
Yes, it takes one picture of the person at every enrollment instance.

1:13:41
Okay, so you don't have a notion of of multiple photos with using the latest photo versus an older photo. This is not a recidivist program. This is just one enrollment, one photo.

1:13:53
Yes, ideally, we would love to have that. But as you can imagine the scales and then the cost involved in the, you know, in the approach, lets you have you have to work with with one time pictures that were captured in the first instance. Right.

1:14:07
Okay. Just one last point. Can you mention what is the profile of the country that this is a developing country? Is this a developed country? Can you say just quickly what this is?

1:14:19
Yes, it is a developing country. I think it's one of the leading economies in the Asian you know, part of the world and it has a very successful program. So, as I said, the only credit I will give is that they started to capture IQ compliant pixels from the get go, which is a big advantage.

1:14:41
Okay, thank you very much roll we run out of time. I think we're gonna continue to the next case study which I believe is Innovatrics.

1:15:00
Thank you. Good afternoon. Thank you for inviting me to this conference. It's an honor to be here. I would like to focus on the way how we used facial recognition in election. More specifically, how we use it for trust it. What is registration. Next please. My name is Matus kapusta. I work at innovatrics as the head of government unit in robotics is a biometric technology company. I joined innovatrics at 2008. And that's when I joined biometric business. The first African project we did in 2010. It was in Nigeria, it was focused on ghost workers. Among government employees, it was Nigeria in Mena state. We did also enrollment and issuance of cards. Then first aphis. focused on election with its together with a system integrator in Burkina Faso, nine years ago. Then, we did a similar project in Guinea for the first time in 2015. It was still based on fingerprints. But in 2017, things have changed a lot. We have developed our own facial recognition. And the first large scale project was in Indonesia, where we deployed the solution for 180 million population, faces and fingerprints together for Indonesian police. In 2019, you know, innovatrics, was chosen as a solution provider for Kenyan election, we have provided the complete solution including the software for enrollment station, and central site. For 2020, this solution was reused. And in robotics acts acts as an international operator for presidential election in Guinea. Elections are scheduled on October 2020. Next, please. Our customer in Guinea, is sending sending is an acronym for national independent electoral committee. It's a it's a committee which is responsible for election organization in the country. All elections including local elections, parliamentary elections, presidential elections. The there are 20 commissioners and all the relevant political parties are represented in the committee. behalf about 7 million eligible voters, the enrollment is done within a period of approximately 2020 days on 44,000 Mobile stations across the country, and there is a central voter registry. And we have provided a solution for collecting the data from mobile stations for deduplication, which is done by our our abs ABS means automated biometric identification system where we use fingerprint and face and then the reporting module where we have to print a cup of millions of pages of electoral reports and voters ID cards. Our responsibility is to deliver the solution which provides every registered an eligible voter with one valid ID card, which will result into one vote election. Traction solution is with fingerprints it's proven for more than 10 years. But recently we have faced some issues. And the first issue is that we have seen a lot of cards. A lot of voters with two valid voters card even if we did a deduplication there are still some duplicates and this has various reasons. It can be the failure of the deduplication for example, the fingerprints are very low quality, or there's insufficient number of fingerprints and rolls. Also when we use the text tool, the duplication in this case, in French language especially the transcription is very variable. So it was not easy to do the textual the duplication and illiteracy rate

1:20:02
in Guinea, among especially old people is up to 80%. So sometimes the people they have difficulties to pronounce and spell their names and the names of their parents. Also, the date of birth is very unreliable, and there are no reliable birth certificates in the country. Very often, this happened also when there was a favor in the enrollment for example, operators, they did some shortcuts they wanted to the job make the job easier, so they skip and Roman fingerprints are intentionally. Sometimes we have also seen inconsistent enrollment. So we upgrade your enroll face, and fingerprints from different person. Why this is a problem. On the voters cart, we have just the facial photo. in Guinea, we have more than 10,000 polling station. And there is no technology for biometric verification. The only

verification is done by the local committee, where we verify the face on the cart with the actual face of the water. So it is very important to create a trusted voter registry, please Next slide. Our solution to this problem or was interaction of the face recognition technology to the existing solution with with fingerprints. First of all, we did a general want to also search based on face for every voter. And this has a pretty good accuracy. And even some of the data are pretty low quality. But we have found a lot of duplicates, then we focus on the people without fingerprints, we did the same job but with a lower threshold. It's a smaller group. So we found another duplicates and without a lot of false four matches. Then we did also an extra check for voters which are inside the same voting centers. Usually those people from the same location, again with lower thresholds. And we combined facial and textual duplication together, we have our interface which allows the operator to analyze the duplicate cases and to decide based on scores and textual similarity about whether it is a match or not. Our findings, our key findings are that operator the register people without fingerprint intentionally we have seen the same people with and without the fingerprints, we have stopped we have improved the the enrollment software, so it's not easy to register somebody without fingerprints. And the ratio was significantly reduced from approximately 2% to zero point 35. We have seen a lot of enrollment with the same face, but different fingers. Oh, we have identified approximately 1000s of duplicates, and we have removed them from from the electoral list. And it's also important, it's very important to train operator on those specific cases. Because if they don't consider them as a standard duplicate, they can be easily easily mistaken as identical twins, instead of being the regular duplicates. It's not sometimes it's not easy to recognize what is identical twin as a hit and what is the real duplicate registration.

1:23:43
Please Next slide,

1:23:44
please.

1:23:49
The next issue which was presented also widely in local media, it was the presence of children in the electoral list, this is something which is very visible. As you can see, there is a electoral card from 2015 you can see the the young boy and this is a big issue. apparent children were enrolled with fake IDs, there is no trust system for for identity card. And this problem was strongly reflected and the political parties were blaming each other that they are registering children to increase the their their number of votes for for the part and the credibility of the electoral process was threatened.

1:24:43
Next slide. Can I just quickly Okay, we developed the module for for minor detection where we trained our algorithm which was able to identify something we called a minor similarity score and for every voter which was registered We have calculated minor similarity score. And if the minor similarity score was above the threshold, we have removed the person from the electoral registry either automatically or manually based on the threshold. And we have found through approximately 70 1000s of minors which were removed. And in some regions, it was up to 3% of the population. And this was successfully validated by operators and also or it from a cause.

1:25:31
It's, it's fantastic. It's a unique application of face where it's not just recognizing people are actually recognizing that they are minors, and therefore they shouldn't be in the electoral list. Sorry, we ran out of time for you, thank you matters for your contribution. And then please, operator bring the last case study, which is from Veridos. While we're bringing that I also want to tell you to stick around because we're going to do a quick poll after the Veridos presentation, and then we're going to start a debate. So please,

1:26:07
Susanne,

1:26:09
I'm here, thank you very much for the opportunity to present here my case study on mobile ad. So please go to the next slide. From birth and throughout your entire life, identity matters. So we know that it's very important for governments and border control agencies to provide secure identities to citizens, and also secure the whole lifecycle of identities, so that citizens can have access to services and also participate in society and an economy be as varied as provide worldwide identity solutions to set to the government's like identity documents, border control solutions, and government services. I myself work in the innovations department of Veridos. And I'm developing new products, especially related to biometrics. Next slide, please. Imagine the following problem, you plan a holiday trip abroad, you booked your flight, and then you find out your passport is invalid. Next slide, please. So imagine even it's a Friday evening. So you have to at least wait until Monday for the opening hours of your registration office, then you prepare all your documents. And then finally, you can visit the office and apply for a new passport. Next. So once the document then is ready, again, you can schedule a visit at the office, and then you finally go there. So this obviously is usually consuming quite a lot of time. And also it might involve travel costs for the citizen to go to the office. Next. So we developed an application called Virtual ID, where we especially want to simplify the application process for the citizens. So it's an app, it can be downloaded from a Google Play Store. It's therefore instantly accessible. It shows a clear process, so you exactly know which documents you want to provide. And therefore you don't need to visit the government office for the application, you just use the app. So of course, this no visit to the government office must be accepted by a government and be fortunate to find a pilot customer, which was willing to change their policies in order to enable that. Also, in the current times of the pandemics, it's good as a solution to reduce visits to crowded places to ensure safety of citizens. Next. So we use face matching to verify the identity of the citizen. So the citizen takes a selfie via the smartphone. The selfie is then sent to serve us on the government side. And there, it's matched against a reference picture from a national biometric database. That can, for example, be the identity document database. When the match is positive, the citizens get a confirmation. And then they are allowed to use the service like for example, renewing of a passport. This service can be also realized on authentication with another technology. But we believe that face recognition technology here offers a very broad power because it's highly convenient for the user, they do not have to register in advance, and they immediately can use the service when they need it. Also, we make sure that it's a secure process. So we have lightning protection to secure the capture of the image. And of course, also the channel towards the government and the data is encrypted and the data is secured when it's sent. Next, here

you see an example how the solution can look like. So as a citizen and our first step, you download the app then you select a service like for example passport, then a second Step you have an option to renew your passport. In a third step, you're asked to enter a new, unique identification number, that number then later on is used to identify the record and the national database. There are also your biometric images. And the fourth step, you get instructions on the face recognition technology, how to perform the face matching, then a fifth step, you take your selfie, in a six step you're asked to pay. And then finally, you get a confirmation, what are your application was done successfully.

1:30:35
next piece, you have performed a pilot project last year, and it was on a total pilot as a customer in Europe. And the use case was done, you'll have driver licenses. So the customer approved also a change of policy in order to enable that service. So in the current process, when citizens apply for your driver's license, they physically have to sign the application. So there's physically a second shot could be removed to the last step of the process, meaning to the pickup of the document. So the application process could be completely done digitally. And therefore, such an application can be used. Also our customer that's own the national biometric databases, and therefore they expect that they can offer it also as a GDPR compliant service, when it really comes to our country wide rollout. And also, the customer gave us positive feedback. So they see that they can use the solution also for other services, like scheduling appointment, reporting, lost or stolen documents, and also to enable other driver licenses services. Thank you very much.

1:31:46
Thank you. Thank you, Susanne, we've got a couple of questions for you, from the audience. First question, is very good to ID IQ compliance.

1:31:56
Currently, no. So we have is our pilot customer, there's not an obligation to renew the picture. So we did not address the step yet. However, this is a very important topic, how to ensure that you really also exchanged the picture, there are different possibilities. One possibility could be also to work together with a photograph or lobby, they are able allowed to take a cow compliant pictures, and to ensure the channel from the photograph. So they take it and securely send it to the government. So then you really have a picture there.

1:32:31
The second question for you is, where's the face print stored is the mobile or in the cloud server.

1:32:38
So what we face matching itself, of course, is performed at a server site, also for security reasons. So we just captured a selfie and then send it to the server and they are performed the matching so that the image from the database never leaves the database, this would not be possible for security reasons.

1:32:57
Okay. And basically, this is a derived identity, but you have to have the national identity database against which you are going to be confirmed confirming you can't just onboard anybody.

1:33:08
At least, this is an issue, it will work with countries that already have national biometric databases, which, if you look at it worldwide, there are quite a lot. But if you don't have it, you have to think about different services to enable such service. So let me see a benefit for the countries who have this national biometric database, because it's a service that basically can add on and can immediately use it as citizens are already registered in a secure way.

1:33:36
It's a new service based on an identity that they already captured. So it's fantastic. Okay, all right. No more questions. Thank you very much, Susanne for for this overview. I'd like to ask the operator to run a poll very quickly.

1:33:56
Okay, so we'd like you to vote very quickly. On two questions. The first question is compared with other biometrics, how do you see face recognition threat to your privacy on comparison. I'll let that settle. Settle a little bit until 60%. Okay, okay. Let's stop that. And move to the next one. Record the number record the result. 15 59% believe this is a higher threat 22% believe it's the same threat as the other modalities. And then 19% believe this is less since it uses public information. Okay. Keep that in mind. We're going to use that never please run the next question. Okay. What do you think is the best way to safeguard against misuse of facial recognition technology? Okay, please vote. This is an important question and it's going to inform our dialogue. Okay. Fantastic. I think we can end the polling here. 60% believe legislation 38% believe Gen data protection is enough. And then 2% believe industry self regulation. Okay, this is very, very interesting. Okay. Now, that goes apart. And please operators bring in the last section of the panel, which is Pam Dixon, and Teki Falconer.

1:37:13
Hello,

1:37:19
I'm happy to have both of you here. You've been patient you've got went through and listen to the limitations of the technology. And you've heard some positive applications, the technology. And you also heard about what you're owed, what our audience believes about the threat of face recognition, and what we should be doing about it. So let me start this session by asking the following question, and then I'll follow a variant of it too Teki. There's not a single day that passes without me opening up the newspapers or online and seeing a headline about face recognition continues to be attracting a lot of headlines, mostly positive, mostly negative around the world, some localities or even in countries are trying to ban it or restricted. Why do you think this is happening? In your opinion, do you think we have when we're not arriving at in from dialogue? Or do you think there is a real threat here and something needs to be done about?

1:38:19
I think both are true. I do believe that the science is now in in regards to face technologies. And we now know that there is significant risk of both age gender and racial utilizations that are biased and unfair.

So this is a problem that needs to be grappled with. And it has not yet been grappled with. This is particularly true in a law enforcement context. And I think that is the other reason that you see people being very concerned and quite vocal is that a lot of the uses that are the most objectionable, carry the most risk, which is law enforcement use that is not by consent, and it is mandatory. So when people feel like they don't have choices, and they don't have autonomy, they tend to have very emotional responses, which gets to your question about, you know, is this hype, etc? I don't think it's hype. I just think that it's a very emotional response, the the move to bands and whatnot. And governments are going to have to listen a lot more. And I think there's going to have to be a center found I don't think the the dialogue is completely informed yet. But at the same time, I also think there are a lot of risks that are not being addressed.

1:39:50
Hold on to that thought. Let me go to Teki and let's get the view from the continent. Teki. What about Africa? Do you think face recognition is making negative headlines there? And what is the nature of the concerns that people have in Africa that go beyond what let's say, Panda said for the rest of the world.

1:40:08
Definitely on top of the list for Africa is racial bias. And we're very much aware of the findings. And as Patrick highlighted, you would see some demographic changes. And we know the impact that has had on on people of African descent. And that is really a high risk there. Another major concern has also been around the political landscape of Africa being and maturing democracy, and, and the ability to actually have governments over set themselves and more or less limits some other rights, like the right to freedom of expression, and another issue. So there's also been a lot of concerns because we currently see deployment in the security sector as well, where national security agencies are deploying facial recognition technologies. And there's always a concern of some form of covert surveillance, as well, which is a big issue. The third one has to do with the whole issue around data sovereignty. And most of these technologies are not being developed by organizations or companies that are African oriented or country specific. And they are being developed by developed countries. And most of these companies are there and are subject to laws in developed countries. And so the there's also that concern around whether this is another form of neocolonialism, whereby, you know, information is being collected on Africans to train these AI systems. But at the end of the day, it could be used, you know, to undermine our political systems, or the independence of these countries. So these are a number of issues that are coming up. And of course, the the privacy angle of it, the transparency issues around what is being deployed, how it's being used, and, and who has access to it all these come into play, when when we're talking about facial technologies in Africa.

1:42:37
It's quite actually a rich and complex set of concerns when you add sovereignty, when you add the potential for the public feeling that this is a new version of colonialism, etc. Without them understanding that potentially the benefits, I'd like to pose you both for a second and ask somebody from the community, anybody that wants to join the panel, from the community voices to join specifically about this issue, which is we're still talking about which is why should there be concerns about face recognition in Africa or in in the world in general, so anybody that wants to join the panel, operator, please elevate them. As, as a panelist, you have to turn on your video, because we have here total

transparency, you can't speak without your face being shown. No pun intended. But anybody I see somebody raise their hand, they want to join the panel to talk about why we should be concerned about face recognition and why the headlines perhaps are justified in in painting the concern? operator, can you please elevate the individual to to community voice Balaji they're having problems bringing that person up.

1:44:05
Hello, I'm here. Thank you.

1:44:07
Okay. Please introduce yourself. I've never met you before, but I'm pleased to see you with us.

1:44:13
met you before Joseph fatigue. This is Paul Macharia. I'm based in Kenya

1:44:22
in a long day, so

1:44:25
it's okay. It's Hi. How are you? I'm happy to be here. I think in my experience working with biometrics, especially in the healthcare setting, I think they're concerned is fear of the unknown. Maybe there are many unknowns in this emerging technology. But in my other thinking also, it's what now COVID-19 and other circumstances are making us work with because now contract based biometrics seem to be not very acceptable for lack of a better word, when we use biometrics for identification in like the healthcare setting, infection control is a big concern. Thanks.

1:45:14
Now, so, in fact, you're bald, you're advocating something positive, you're basically saying, fact, we need face in the health arena because of the restrictions on contacting surfaces. If I understood that, that's your comment that, yes, there, there are concerns. But in fact, we shouldn't forget that there are certain legitimate needs, such as the use of faith in health in order to avoid contamination and contacting surfaces, do you understand you correctly?

1:45:46
That's what I mean, Dr. teak that we need face recognition in a healthcare setting because of the biggest concern infection control.

1:45:57
Okay, so now Teki going back to you, we see that, obviously, the concerns that you've raised are legitimate concerns. But when I talk to a doctor, who is actually in the field dealing with with, with infections and disease, he he would be saying that, yes, I understand. But my priority is dealing with with managing the identity of patients, and therefore I could afford to take the risks that you mentioned. And you think this is a short term vision, or there are certain justifications for for using face, because of the world that we're in right now. And the fact that we need to be in a contactless environment.

1:46:48
And Joseph, clearly there, there is a good reason to use fees. And, of course, having started on the basis of the risks does not mean that we cannot use fees. But the challenge is that there is really no transparency around when we should use face, and when we should not. And clearly, we should attribute the risks associated, which has been identified and raised by Patrick. And that should inform the context under which we're going to use face for instance, yes, if there is a health risk, and there is the need to use face, it is acceptable, but we must put it within a context that continues to protect the individual in place and minimizes risks to other areas. So the fact that, you know, using facial technology will enable a doctor do or perform the services better, or enable us protect the the larger society if you're looking at COVID. And in this case, let's say that somebody has COVID, and they're supposed to stay at a particular place to minimize the infection, then you you look at the greater good. But the challenge has always been for the continent around the the lack of correlate a framework that really provides this form of guidance, and the likelihood that, you know, now some businesses are thinking about deployment of biometric technologies, including facial technologies, for instance, we have some banks that are using it, and what context, are they planning to deploy it? Is this sufficient reason is that is that a good reason? Or could there be other methods that will minimize the risk associated with the use of official technology? So I'm not necessarily against the use of these technologies, but I believe that the context should define when we should use them.

1:49:03
Okay, that's great. So we're now getting into the nuances, what we're basically saying that, you know, the technology is not good or bad. It's the use cases that could be bad, and that we should protect society from them. If I understand where we're heading. What is the process for a community or for a country and obviously, cultural influences could be different one, one continent, one country to another? How do you go about establishing what are acceptable uses of face recognition? And do we have any sort of experiences from the past for something similar that we can rely on any models that we can rely on?

1:49:43
Yes, I think there are a lot of models that could be used. Right now. They're not being used though. So that is one of the reasons we're seeing so much chaos in terms of policy. So I think one of the important things we we have to mention are bands and moratoriums, also best practices, we see a lot of best practices written, we also see an increasing number of bands in certain jurisdictions. But, but there's a big giant middle section, which has really been left alone. And that is where all the richness and personalization, if you will, is done. And this is this comes in the form of the model of safety regulations. So if you think about dangerous chemicals, one can think of lead, for example, lead is actually not a banned substance in Africa, there are very stringent rules in regards to lead and paint must have only a 90%. It must be 90%, lead free. These are rules in in most African countries. And very similarly, face recognition can have rules that include risk minimization, risk assessments, certifications, required documentations, after it's been put on the market, there would be ongoing surveillance or observation by regulatory authorities, such as data protection authorities and others. And in this way, you can start to build a very robust framework of protections, when all the stakeholders agree that face recognition is appropriate to use, but not all use cases are going to be appropriate. And that is, I think, what Teki

really talking about the community and those unique situations need to be decided by the stakeholders that are there. And it is when governments and businesses and others make, you know, just autocratic decisions, that creates real tensions in the use of any technology, but especially face recognition. So the Trust has to be earned here.

1:52:09
Yes, I understand. But you know, who does that role? I mean, when we look at harmful material, I mean, we've got bodies like the Food and Drug Administration, which basically does not allow any consumable to go on the market without them, classifying it, or categorizing it. In any given country. If we think about face recognition in that context. Who do you think is the right body to pronounce that this is harmful in this application, and will not be allowed in our country? Or this is acceptable, what bodies that it's not just data protection?

1:52:45
No, it's not just data protection, I think there are going to have to be multi stakeholder groups that come together within governments to make these determinations. But I would say that data protection authorities must be present. And in countries where there are not yet data protection authorities, then someone with that kind of expertise needs to be present. And the role of civil society is very important here. civil society needs to provide feedback and expertise, as do all of the stakeholders. But it really needs to be a very respectful and productive conversation. I think one of the problems that exists right now, is this very adversarial, lack of communication. And I think it's just adding to the problem rather than solving the problem.

1:53:38
Yeah. Okay. So pause, pause here for a second, I want to elevate somebody from the community to join the conversation on this specific topic. I understand there is candidates that raise their hand, please, operator elevate this candidate. And we're talking we're continuing essentially to talk about how we can establish if certain applications certain use cases of face recognition are legitimate for the community, it seems that there is a vacuum right now in many countries, there is no body that's already established. So we have to do it on an ad hoc basis of stakeholders, civil society. government regulators. Yes, please introduce yourself. unmute your your microphone. Who do we have with us?

1:54:31
Hello?

1:54:31
Yes. Can you hear me? Yes, please. Hello?

1:54:35
Hi. My name is Chesley, right. I am the founder and CTO of infiltrative software suite. And we have our social responsibility aspect of our functionality is to mitigate issues around race and gender equality. And we're currently doing some development around being able to accurately detect transgender people as well, but to speak to what we're talking about right now, I'm actually getting ready to do a presentation for AI Expo Africa tomorrow on this very subject of being able to provide cybersecurity and

equality and biometric technology. So one of the things that I did, because I like to hold myself accountable, not only as a technologist, but as a business owner, and as a black person in this space, I created some international trademarks that would that would hold that speak to the government and legislative aspects of what should happen around biometric technology. So essentially, if anyone develops biometric technologies, whether its facial recognition, tech trends, if it does not have functionalities that mimic gait, race, and gender equality built into them, they should not be used. It's just It's just that simple. It's just that direct, but there should be an auditing body or some type of accreditation body, per government around the world that does this.

1:56:08
So it's basically this content. If you guys want me to share my screen, I can't do that. Yeah. Okay. It's okay. This is not correct.

1:56:18
This is not do no harm of the application, essentially, what you're talking about, we cannot allow an application in society which harms a certain group of society in the society.

1:56:29
Currently, Joseph, absolutely correct.

1:56:32
Okay,

1:56:32
thank you. And it starts with the development teams as well. It starts with the development teams, the development teams themselves need to be diverse, so they can, in turn, show diversity in the development, the software that's being developed itself.

1:56:47
Right. One last question to you, where do you come to us from which country

1:56:51
I am in Atlanta, Georgia in the United States?

1:56:54
Welcome, welcome. Thank you very much. Thank

1:56:56
you for allowing me, guys.

1:56:58
Thank you. Okay. We we want to continue with this discussion. We thank our guests. continue the discussion with Pam and Teki now. So go back to the second. And I want to look at the numbers in front of me. So I don't cite it. We asked the question, what what, in your opinion, is the best way to deal

with the menace potential minister of face recognition? The first question 60% of people felt that they there was an elevated menace more than other biometrics. And so we asked what was the best way to deal with that matters. And, and 60% believe that there has to be laws specific to face recognition. 38% said, no data protection laws are enough. And then only 2% believed in industry, self regulation, I will relate to you the results that I had done, I had done this this survey in London, about five years ago. And I can tell you that industry, self regulation, at that time, was at 22% 22% believe that industry, self regulation was enough. Today, we are essentially seeing that nobody is advocating for industry self regulation. So we move that out of the out of the equation. So we'll focus on whether it is it is law specific to face or whether it is just data protection. So let me let me start with taking this time and get your perspective. Do you really agree that we should be working with legislators to make sure there is an informed face policy? Or should we be putting our energy to inform the data protection laws?

1:58:52
And I believe it's actually both I wish the survey had given me the option to prioritize. And in fact, from where I sit, I think it's all three, industry regulation, some form of regulation attributed to technology, and then data protection. And the reason I'm saying this is because data protection, of course has the overall but then it's it has a very specific rule, which is looking at the individual the personal data and use of it and, and transparency around it accuracy and the rest. But as I mentioned, when you look at the African context, there are other bigger issues around data sovereignty. There are other issues around manipulation to limit other fundamental rights. And so you would actually see that you probably may need and I agree with them, you may need a broader

1:59:59
The

2:00:00
scope of stakeholders to address each of these issues that continue to be a concern. legislation is a good start. But I honestly do not believe that it is sufficient. And especially looking at the context in Africa. If, for instance, where are all these technological companies, ownership of these technologies, where are they based, they are not based in Africa, they're not based in Ghana, or any of our 55 countries, most of them are not based there. So even if you, you look at a regulatory intervention, by way of law, you have to enforce these laws against these companies. And you may not have the necessary structures and tools to be able to go after these, especially the the big tech giants. So for Africa, we really need to sit down and look beyond them and look at where the real issues are, and create some form of system or framework that brings to play the laws and the regulations, which will enable some form of regulators but rather build a larger ecosystem that recognizes certain values, as far as these technologies are concerned, and are willing to to apply these values for the greater good of everyone.

2:01:26
decades, wonderful, wonderful overview of what you think should be happening. Instead of repeating that, could you give us an overview of what is actually happening in some countries around the world? How are they dealing with the situation? Are there models that Africa could use to guide what the next steps should be? Perhaps along the along the lines of what tech is mentioned?

2:01:51
Yes. I think that it's very important to understand that most countries are moving ahead with uses of face recognition in law enforcement and national security context, period, End of discussion. This is without discussion, typically with citizenry. And without discussion of specific use cases. And this is leading to increasing tensions. But I again, I'm going to point to a certain powerlessness that people feel when this happens, and I do think this is of concern. The second thing I would say is that because of the impact of COVID-19, we're also seeing a lot of movement toward the use of phase systems so that there's no touching involved. But I urge caution here, because we need to ensure that all of the use cases have been run through and discussed amongst all stakeholders, including citizens, those who are not citizens, but within the country, government officials and so forth. But the thing is, is that what we also are seeing is a real breakdown, I'm taking mentioned something very important, which is the idea of, you know, something very practical that governments, stakeholders, companies, etc, can implement on the ground. So I, myself do not prefer self regulation. It's very failure prone. But I do like the idea of regulator approved codes of conduct that have oversight to them so that everyone who's supposed to be subject to the code behaves, we're seeing some of this in Africa, coming from Morocco, and also Mauritius. I know, there are other African countries that are also looking at doing regulator approved codes of conduct. This is a really important area of development that I think is right for Africa.

2:03:50
I mean, Pam, what is the United States doing in this area? You're based in the United States? What are they doing? We hear a lot of local and state creating contradictory things and bills that are competing, what's happening very quickly. Up me. Yes, the question to you I mean, the United States

2:04:09
is an absolute mess right now, because we're seeing a policy structure that focuses on bands that are very limited, actually in scope, and also best practices. So the actual middle ground where you really need controls, such as certification audits, as the the guest was mentioning, and all of those really robust safety mechanisms and controls, those are not being discussed. So we're avoiding in the United States, we're avoiding looking at the whole lifecycle of facial recognition. We're avoiding looking at the whole ecosystem of face recognition systems. This is a huge gap, a huge problem. And there's a lot of misunderstanding about what is and what is not a problem. And I must say the tone is deeply adversarial. And that's a problem. We need to be able to talk to each other Find the center

2:05:01
was I want to elevate somebody to the panel that I think will be a firework as well. Operator, please elevate Maxine. Maybe Maybe you can briefly while we are waiting, Maxine, tell us what's happening in Europe.

2:05:21
Europe is very interesting. We had France, regulators say, hey, look, there's schools in the south of France, you are not going to be able to install face recognition. Or for children, you also see the Information Commissioner's Office at the UK, making an announcement that they are going to be looking, and it's a very brief announcement, they're going to be looking at regulating and controlling law

enforcement uses certain law enforcement uses of facial recognition technology. So I think in Europe, and also the European Commission has announced that they are going to be regulating face recognition technologies. Eu wide that's to come this year, hopefully. But Europe is making advances. Okay. Okay.

2:06:08
I understand. Thank you, Maxine. Welcome.

2:06:10
Hi, Joseph, how are you? Nice to see you. Very well, thank you. I feel like we've been having this conversation for 20 years, but it's finally now risen to the top of everyone's minds. And I think it's fabulous, because I think it's really important. And I just wanted to make a few comments, and maybe the panelists can respond. One, I think the idea of banning technologies like banning books, you just can't do it, right? The cat is out of the bag. Facial recognition is here. And I think the knee jerk reaction, particularly in some areas of the United States to say we're gonna ban this technology is, is kind of silly and ineffective. And I think the notion of self regulation, which is something that I've advocated for for 20 years, is just not happening. I mean, I think that the industry has had lots of time to build in safeguards is one of the earlier guests mentioned, into the technology itself, something that again, I've advocated for for a long time, and it's not happening. So I think what we need are really public private partnerships to create standards, it'd be on on both on a global level for interoperability, and then within individual, sovereign areas that speaks to the particular concerns that any of those areas have.

2:07:24
Okay. Any reaction from from the panel to what makes sense? Thank you, Maxine,

2:07:33
just from a US perspective, what I would say about bands is that there, if you look at other regulatory models, such as drug safety regulations, or medical device regulations, there is a very robust procedure for proposing a ban and then creating a ban. Those procedures have not largely been followed in the United States. So some of the bands are really kind of very political is what I would say. But that doesn't mean that there should never be a ban. I do think that there are certain use cases in face recognition systems that need to be considered for for bands, particularly when the cameras are very low quality, such as, for example, face recognition on body cams used live. And I think we have to be very careful to not throw the baby out with the bathwater on either side.

2:08:25
Okay, thank you, Maxine. Thank you very much. I want to say thanks, Joseph. Thank you. Well, can you operate it? Could you elevate Paul from the community voices? And then we'll come back to the panel with the closing remarks. Do we have Paul? Oh, please.

2:08:49
Can you hear me?

2:08:50

Yes, we can hear you, Paul, please introduce yourself. What are the for Africa?

2:08:54
Okay, my name is Paul Damali. Originally based in Ghana, co founder and CEO of a proof of proof basically as ekyc infrastructure across African countries. We train our garden specifically to analyze, you know, Id documents of Africans, and we are across about six African countries currently.

2:09:22
Excellent. And so this is an African company that is specialized and focused in KYC. Do you access face data do you use face as an element in the KYC process?

2:09:37
Yes,

2:09:37
we do access these databases. Typically what has to happen first is us understanding the regulatory regime in each country. So for example, there are about 16 data protection laws all across Africa. And as it stands now, we are in about six of these countries. And that's Ghana, Nigeria. Kenya, South Africa, you need to sort of like really be locally informed and understand the local context and what the data protection and other adjoining regulations say about how to access these kind of biometric data, what to use them for. Most importantly, also thinking about how you enable consent based systems. One thing I want to point out, we've been using technologies in the industry not properly. So what we do at approved, we call it facial comparison, because it is enabled by consent by the customer. The visual recognition, however, means that I own which is typically what the security agents do, because they already have access to the database, and they don't enable the customer consent. If a security cameras have like fix your face, they don't need your permission to do. So there's a difference between those two, and we need to be able to recognize it. And so when it comes to application in industrial, like financial services out more of what is done is the consent of face comparison, which is concerns based.

2:11:13
Yes, so So what Paul is saying that, in thinking about how to protect against the misuse of face, we should distinguish between face authentication, and face recognition, those two animals might require different types of legislation or different types of handling. Thank you all for being with us. Thanks for joining that Africa family. I'm going to ask analysts to close on the thought back to you and then Teki Where do we go from here? I mean, obviously, we've just only begun, we've only opened the subject. I mean, we could go on to the whole evening discussing the subject, what should be the next steps for the international community, and then Teki, what should be the next steps for the African community.

2:11:59
The next steps for the international community is to have a non adversarial discussion between all the stakeholders that are in this debate. And to determine all of the regulatory tools that we need to be addressing this, we have to use more regular regulatory tools. We're not using all of them, we're not using certifications, we're not using codes of conduct, etc. So we've got to add those in. We've got to learn how to talk to each other, we've got to learn that we're going to have to work together to set

appropriate limits in context. And this is a joint operation, it can't be done unilaterally by any stakeholder.

2:12:47
Okay, thanks, Pam. So dialogue, not an adversarial, there's no, for or against, we got to get together. And we gotta develop the new types of of tools that actually allow us to assess

2:13:04
these tools are well understood. So we don't need to reinvent the wheel. But we do need to get on the road, we do need to take steps forward, we cannot just let the situation stay as it is because this is not productive.

2:13:19
Okay, so Teki, please guide us through this. Yes, for

2:13:24
for Africa, I think that we have to be more transparent, especially at the governmental level around how we are adopting and using these technologies. And I believe that for industry and vendors, they also need to come around the table and build this transparency into this whole area. And I would echo what Pam also said about bringing all the stakeholders to a dialogue. And clearly because of some of the key issues involved, I would call on all the regulatory agencies and regulating it and technologies, generally, regulators looking at data protection, and other human rights regulators and CSOs to sit around the table to really come up with some level of guidance on what is appropriate, what should be acceptable, and what should not

2:14:29
be the case, Africa digital rights have doing any of that right now.

2:14:33
We are currently conducting a number of research around facial technologies and how they are being deployed. And based on what we find out we will probably propose like we did with the ID some code of conduct on what should go in and what should be taken out like we did with the ID systems for Africa. Okay.

2:15:00
Well, as I said, this is not the end, this is the beginning, I think we will be bringing it the subject again throughout the year to see how it progressing in our thinking, we need actionable steps, we're identifying problems, but we're not identifying the steps to how we should solve them. I think we've exceeded our time, I knew this would be a very intense session. It's okay, we still have a lot of people with us. But I need to respect strictly the time now and end the session by thanking Pam and Teki. And also all of the community voices and all the other panelists. Special thanks, go to Patrick for a wonderful presentation, and to the four case studies that help prove our awareness of where face recognition is being used. So we bring back to the panel, whoever is still there. And just to wave goodbye, and to say, we'll see you again on the 16th. Please remember the 16th say that international

identity day, that's the day we're going to focus on the subject of inclusion by celebrating the recognition of September 16, international entity day, there's a whole programme of activities. So please stick around, come back on the 16th and let us hear from you within the community voices. So thank you all for enriching our knowledge this afternoon. And I just wish you all safe and and productive continuation of your day. Thank you.

2:16:39
Thank you.

2:16:40
Thank you.

2:16:40
Bye,