THE REPORTER: Hello and welcome to the ID Talk podcast. This week we've got part two of our deep dive into 3D face mapping with FaceTec's Senior Vice President of North American operations, Mr. Jay Meier. Uh - This is going to pick up right where we left off at the end of part one. So, if you haven't heard that yet, please go ahead and listen to that one first before continuing. Uh - Things get even more interesting this week, so it's especially important to make sure that you have the scientific and technological foundations that Jay laid out for us in the previous episode. And if you're up to speed now, here we go.

JAY: So, think about 3D for a second. This is why 3D is conceptually way better, right, because 3D doesn't struggle with the perspective distortions. You get - If it works well, you get the same relationships between geographic locations on your face from any image that – from image to image that you capture because it's the, you know - none of those factors change, right? And 3D, because it captures so much data and so much reliable data, that is not distorting with, you know – that does not suffer from perspective distortions, it doesn't have to look for other information like color and hue. So I'm not saying that our system doesn't look for color and hue, ok? It just doesn't

1 have to use that as a primary method of determining if
2 these faces match.
3 THE REPORTER: Due to a lack of data, it doesn't have
4 to rely on even more unreliable data to round everything
5 out.
6 JAY: Exactly, exactly. So 3D, in and of itself,
7 intrinsically, will work better than 2D. Everything else
8 constant. Ok, for those two reasons. Some 2D works better
9 than other 2D, right? But everything else constant, 3D will
10 always perform better than 2D for those reasons.
11 THE REPORTER: Yeah, and I guess in the context of, uh,
12 matching, like if you're matching to a 2D photo, it doesn't
13 matter that the photo is 2D because your 3D image can be
14 like positioned like, you know, um, computationally to be
15 like "yeah at this distance, this matches this 2D photo."
16 Am I making any sense?
17 JAY: Yeah, so let's get into what our system does
18 because you're on – you're tracking.
19 THE REPORTER: Okay.
20 JAY: If you've ever used the FaceTec user interface,
21 there - you'll see that there are two ovals, you know.
22 You're going to log onto your bank account or long onto
23 your Tinder account, Alex, and oh, or what was it Tony, I
24 don't remember, one of you guys, okay whatever.
25 THE REPORTER: My girlfriend is listening to this

podcast so you can just pick either one.

JAY: The Christian dating app, I don't care which one. So, you're logging onto whatever service provider that you're trying to get access to and if they're using our interface, an oval shows up and you fill the oval with your face, right? And then, the oval gets bigger, and you fill the oval with your face again, right? Well, how do you do that? The only way to do that is by moving the camera closer to your face, ok? So, we are intentionally creating variability in the depth of field, only we are doing it in a consistent way across all faces, right? So then what? What our system does is capture video frames, right? Well you move that device roughly five, six inches closer to your face, our system is capturing over 100 video frames of your face, okay. It's like 100 selfies from different - 100 different distances from the camera, right? As you're moving it closer, you're - it's 100 selfies and 100 different distances from the face to the camera, right? So think of it that way. More data is better than less data.

We have—if they're using one image against one image, and we're using 100 images against one image what's the likelihood that ours is going to have a higher confidence? It's going to have a higher confidence, you know? That's just because it's just that much more opportunities to measure and create assurances. But that's

1 not all that our system does, you know? Our system, the AI—
2 and this is where the super geek part comes in—I learn – I
3 figured this out in 2016 when I was first introduced to the
4 company, and I still get freaked out about it, okay. What
5 the system, the AI, is actually doing when it moves – when
6 it prompts you to move the camera closer to your face, it's
7 capturing those video frames, what is it measuring? It's
8 measuring the change in the perspective distortions. Think
9 about that.
10 It's measuring the changes in the perspective
11 distortions as you move the camera, as you take 100 selfies
12 between 6 inches and 1 – or you know – between 12 inches
13 and six inches away from your face, right? Do you
14 understand? So the AI then is able to determine curvatures
15 of the face and three dimensionality from those - the delta
16 of the perspective distortions. That's what our system
17 does. It doesn't actually measure a face like you'd
18 normally think of a face. Our system measures the changes
19 in the perspective distortions because guess what? The
20 cameras always distort the same way. It's a function of
21 depth of field and the two dimensionality of the sensor,
22 right? That's consistent. What's not consistent is the
23 depth of field, right? But your face creates perspective
24 distortions that are unique to your face. Because it's
25 unique! Do you understand? Your face generates perspective

1 distortions over those 100 frames that are different than
2 my face generates over those 100 frames because the
3 variable is the shape of the face. It's no longer the
4 distance between the face and the camera. You understand
5 what I'm saying?
6 THE REPORTER: Yeah.
7 JAY: So my - It turns out that the perspective
8 distortions are basically a biometric. It's a new
9 biometric. And that's why they can't really measure our
10 stuff—is because we have to have live captures so that we
11 can force them to move the camera five or six inches closer
12 to their face so we can capture all those video frames so
13 we can measure the perspective distortions. From those
14 perspective distortions, our AI is able to generate—it's
15 not literally a 3D composite—but it generates consistent
16 and reliable three-dimensional data about the face, okay.
17 It's not – It's not creating a, uh, uh, three-dimensional
18 mask of your face or like the pin, you know, thing or
19 whatever. It doesn't do that. But it generates consistent
20 and extraordinarily reliable data about the three
21 dimensionality of your face. Follow?
22 THE REPORTER: Yeah,
23 JAY: So –
24 THE REPORTER: That's still usable when you're
25 comparing to a 2D image. Like it's not –

JAY: Yeah!

THE REPORTER: You say it's like a different biometric but it's still one that can be equivalenced to the 2D data.

JAY: The AI is so good that it can kind of predict what the face should look like, what the perspective distortion should be at a particular distance, okay? So, it's - It may not be perfectly interchangeable with two dimensionality but we're capturing so much more data and so much more reliable data with the 3D face scan and then ultimately the face map that we still are measuring more data, right? The potential match accuracy is much higher with 3D to 2D than 2D to 2D. So intrinsically 3 - that's why 3D is superior. We have two eyes in our head so our brain can triangulate three dimensionality, right? So we don't bump into stuff, right? That's - We have to be able to interpret 3D data accurately. That's what our system does, and it does it in a very, very unique way. So we have a lot of intellectual property around the user interface, two ovals, right? Because that is the only way we can figure out to capture 100 different video frames in a very controlled environment. Make sense?

THE REPORTER: Is that the - also the liveness check that is the movement? Or is that a separate—

JAY: No, it's both. It's all of the above, okay. So there's only two vendors that I'm aware of that have any -

1 a real viable, market capable, three-dimensional face
2 system. And that's the Face ID in Apple's iPhones, right?
3 What that does is it has a special sensor in the phone that
4 projects 60,000 beams of infrared light on your face. You
5 can't see it, but the other special sensor — er, they have
6 a special projector that projects 60,000 beams of infrared
7 light on your face—and then they have a special sensor that
8 can see the infrared light and it - including the distances
9 of the light beams, okay. So it literally is like when you
10 put your face in a, you know, a screen of pins or whatever
11 and your creepy face image emerges on the other side, you
12 know. Mine's creepy.
13 THE REPORTER: They're all creepy.
14 JAY: Okay, but that's effectively what Apple's system
15 does. Our system—and you have to have the Apple iPhone with
16 those two pieces of technology built in, in order to do
17 Face ID, right? Well guess what? That costs a lot more
18 money. It works really good. It works really, really well,
19 okay, but you pay for it. That's why an iPhone costs $1500
20 today and an almost equivalent Samsung is $750, you know.
21 Part of that is this technology. You can't ask the world to
22 standardize on patented technology that Apple owns, right?
23 So that's a problem. What we really need is a biometric
24 face matcher that is capable of using the two-dimensional
25 sensors that are in any phone. And that's what ours does.

1 We – we capture so much information with our 3D system that
2 our software, our system will work on almost any device. I
3 think we estimated one time that if you go measure any, we
4 —let me put it a different way. The resolution of the
5 cameras have changed a lot over time, right? Well a lot of
6 these, you know, a lot of guys when they go to get their
7 face matching system tested, you know, they kind of hope
8 you don't notice, but they only use the most modern iPhone,
9 right, because it has this super incredible camera in it,
10 right? Is that realistic? No, because only about 30% of the
11 global population uses an iPhone at all. And half of those
12 don't have the face matching thing, right? Our system only
13 needs 0.3 megapixels. That's the resolution of the camera,
14 the minimum resolution that our system needs in order to
15 capture enough data to be accurate enough, okay? And when I
16 say accurate enough, I mean 1 in 2 million false accept
17 rate not 1 in 10,000 which is the benchmark in all the NIST
18 tests. You want to know why the benchmark is so low? They
19 had false acceptance - a false reject of 1% you've got to
20 have a 1 in 10,000 false accept rate? That's written into
21 the new draft of 800-63.
22 That's a low false- That's a very high false
23 accept rate compared to ours, which is , you know, in a
24 similar circumstance more like 1 in 2 million, right? So -
25 That's because of three dimensionality. And that includes

1 3D to 2D images. So that when Service New South Wales
2 doesn't save biometric data—they, it's against the law for
3 them to save the biometric data—they already have images of
4 your face in a driver's license database, right? Like
5 that's not biometric data, but it's just old biometric
6 data. So, what they do is they capture the three-
7 dimensional face scan that our system captures, which is
8 liveness data and matching data captured concurrently from
9 the same sensor, okay? So if its - And then it transmits
10 that to behind their firewall to where liveness is checked
11 and if the person – if this is a deemed to be a live
12 person, they match our 3D face map, which doesn't include
13 the liveness data against the 2D image that's there. And it
14 either matches or it doesn't, right? Either way, they
15 delete the biometric - 3D face map. They don't save any of
16 that information. So they get the benefit of our liveness
17 and the benefit of our matching without having to
18 compromise their laws and regulations about face matching
19 data and saving it in a database, okay?
20 THE REPORTER: I think you had mentioned last week too
21 that the data that is left over after they delete the face
22 map is useless. It can't be resubmitted. So-
23 JAY: Yeah.
24 THE REPORTER: Even if they lost everything or it was
25 stolen, uh -

1 JAY: Right.
2 THE REPORTER: - there would be no use for it.
3 JAY: Well, and that's a critical selling feature in
4 our view, you know. What you're talking – what you're –
5 what that regards is what's called honeypot risk, right?
6 What New – What Service New South Wales was trying to
7 mitigate was the potential for a hacker to get into that
8 database and steal biometric template data, alright? And
9 presumably if you listen to the guys at Fido and you listen
10 to the guys at Apple and all those other places, they'll
11 tell you that if anybody gets ahold of biometric template
12 data that is something having to do with your face, your
13 life is over. You can't do anything ever again. That's -
14 and that's why they say, "Well that's why we do the face
15 matching on the device only, and that's why we don't bind
16 identity data to the face matching biometric because even
17 if they steal it, they won't know whose it is." You know, I
18 mean. It's nonsense. Cryptography works really well, okay.
19 So we send biometric data through the internet, we encrypt
20 it six ways from Sunday, we send it from the device to the
21 server behind Service New South Wales's firewall, which is
22 the safest place in the network you could put something
23 like that, right?
24 Liveness is tested, and if liveness is - is
25 affirmed, the system deletes a bunch of liveness data,

1 okay. So remember that our system, first thing it does -
2 the SDK - is take control of the sensor, the camera and the
3 data feed from it, right? That's so we can mitigate against
4 deepfake injection attacks, right? It's - it's pretty
5 rudimentary and simple if you can show that the only data
6 you are using came from this particular camera, then you
7 know that's something that can't show that it came from
8 that camera might have been injected into the flow. And you
9 can delete the whole – the whole transaction. That's the
10 primary method of, uh, mitigating deepfake injection
11 attacks, is to get control of the biometric sensor and the
12 data flow from it so you know exactly what data you should
13 have and exactly how that data should exist, right?
14 And if any - if the characteristics aren't there
15 or there's other characteristics that wouldn't normally be
16 there, you know data has been injected. So, you can shut
17 the whole thing down, okay. So the first - that's what you
18 do first. Because it's captured - it's one camera, and
19 because of the three dimensionality, we can capture
20 liveness data and matching data at the same time. It's
21 basically the same data, you know? It's one data file that
22 we call a face scan. It's all this three-dimensional data
23 and some other data that's collected about liveness, right,
24 that is interwound with all the matching data. It's one
25 file we call a face scan, okay. And there's other stuff -

1 if you think about three dimensionality—here's another
2 reason 3D is better than 2D, and a lot of the 2D guys are
3 trying to show that they can do 3D now in some way for the
4 liveness, but they can't, you know; NIST tests show that
5 none of them do it very well. Um, a human face must be
6 three-dimensional to be a human face. If it's not 3D, it's
7 not a human face. So we're not really testing in the
8 liveness sense – we're not testing for three
9 dimensionality, we're testing for something that's not
10 three-dimensional, right?
11 If it's 3D it's not 2D. Well, conversely if it's
12 2D, you know it cannot be a human face, right? So think
13 about all the presentation attacks that you – that people
14 have been worried about. They put a – they put a picture up
15 to the camera, right. They hold a, a high def screen up the
16 camera, right. If it's not a mask—if it's not a physically
17 three-dimensional presentation attack, our system will veto
18 it immediately because we'll know it's 2D and therefore
19 can't be a living human being, right. So then you get into
20 other things about, you know, like a mask. And there's
21 another - there's another company out there that keeps
22 posting stuff about super, super masks, you know, that
23 costs $5000 or whatever and it dupes all of these, these
24 things. Well, only if you're measuring three - If the only
25 thing you measure is three dimensionality, then those masks

1 will work. They'll get through the liveness. But if you so
2 – if you measure what we call passive liveness
3 characteristics—and what we call passive is different than
4 what NIST calls passive, okay, I can explain that if you
5 want. But what we call passive liveness characteristics are
6 involuntary human cues.
7 And the perfect example is how your pupils dilate
8 under different conditions, right. You have no control over
9 that. You can't make your pupil dilate. The only way your
10 pupils dilate is if more or less light, you know, is
11 hitting your retina or whatever. And that's a control to
12 control how much light gets into your eye, right. It's
13 involuntary. Your body does it and you don't even know it.
14 And there's a bunch of other involuntary human cues, you
15 know. A really poor one, which AI could probably spoof—so
16 I'm just throwing it out there guys—you know when you move
17 your camera closer to your face, your eyes have a tendency
18 to focus on something that's closer and so they go a little
19 bit more cross-eyed, you know. That's an easy one, right.
20 So don't worry about that one. But we have 70 or more of
21 these involuntary human cues that our system watches in
22 addition to the three dimensionality, right.
23 And we don't tell anybody what they are. I don't
24 even know what they are. It's under lock and key. And
25 that's so, you know, if I told everybody that all you have

1 to do is show the eyes focusing on something closer then,
2 that's what they'd attack like okay our AI is going to do
3 that, you know. The thing is they have to have the same 70
4 measurements, and the same 70 measurements have to be in
5 the same order. The resolutions have to be the same. And
6 guess what? When you're in control of the sensor you can
7 change the resolution of the data that it captures, right?
8 There's so much randomness there that attackers don't know
9 what to attack to defeat our liveness. That's why our
10 liveness is so much better than anything out there. It's
11 3D, which means it's not 2D, which is an - a layup.
12 Presentation attacks largely are gone, and we use 70 or
13 more involuntary human cues that no one knows what they
14 are, so you don't know what to attack. How would you
15 concoct a liveness attack on our system even if you knew
16 what the 70 measurements were? What order would you put
17 them in? What would the resolution be? Anything that's not
18 what we expect is a spoof attack, remember.
19 THE REPORTER: This is why Tony and I are having so
20 much trouble, uh, getting your spoof bounty. Like we've
21 been trying and we can't figure out, first of all, how to
22 make a mask.
23 TONY: Uh, you can buy them. I couldn't - I couldn't
24 find the website for the spoof bounty at first, so that was
25 - that was a bit of a hurdle.

JAY: Let me help you. It's wwwspoofbounty.com.

TONY: Thank you, Jay.

JAY: s p o o f b o u n t y.com, that's the Spoof Bounty program.

THE REPORTER: Now we're cooking.

TONY: Now we're cooking. Now we're in business.

THE REPORTER: You're in trouble.

JAY: You and 150,000 other attacks have failed, okay. 150,000. We've had 150,000 distinct attacks on that. We paid out twice in two - when we started in 2019 as I understand it the payout was a partial payout because the attacker got part-way in. We don't give you 600,000 if you just get part-way in, you can get, you know, 30, 30, 30, 30, 30, or whatever it is, right. The total you could get is 600. No one's ever gotten more than the first layer. And of course, we could - part of the deal is that we make you sign a contract that says that we can use whatever information we gather to improve our stuff. So, it's great R&D, right. We haven't had a breach in the spoof bounty program since 2019 and it works pretty damn well. So anyway, um, you understand why 3D, and in addition some other types of involuntary human cues, passive liveness is far and away better than – than 2D stuff.

They're trying to do 3D by turning your head, you know. "Oh, if you turn your head, we can show that it's—"

1 Well, it's because they're hoping that the AI thing shows
2 like no head, you know. I mean it's, it's not the—nice try,
3 alright. But it ain't going to work that well. So, anyway,
4 same sensor. We control the sensor, we control the data
5 flow from it, so we protect against deepfake injection
6 attacks, right. If - If data in the data flow is different
7 than what we can predict, what we know should be there, it
8 means there's something there that shouldn't be there,
9 which means we cut it off. It's done. No, the attack will
10 not be successful. We - Because it's one sensor, we capture
11 liveness data and matching data at the same time. It's
12 effectively the same data. It's all 3D. And we talked about
13 why 3D is better in matching. We talked about why 3D is
14 better in liveness, right. We then encrypt it.
15 And for all you guys that worship at the altar of
16 deterministic cryptography, I'm going to say it one more
17 time, I love cryptography. You have to use cryptography,
18 guys. Everybody needs to use a cryptography. If you don't,
19 you're going down in a hurry, okay. Just so we're clear,
20 crypto guys. We encrypt the 3D face scan. The face scan is
21 3D matching data and, and liveness data, I like to say, all
22 wound together into a single file, alright. We encrypted it
23 six ways from Sunday. We beam it behind the firewall where
24 the source data is, the verified identity profile is, where
25 the images or other biometric data that's already been

1 captured, right. The first thing we do is decrypt it once
2 it's behind the firewall. And if you think that, you know,
3 why is the firewall better? Because you have absolute
4 control of everything behind your firewall. You don't have
5 absolute control of everything that's in the cloud that you
6 rented part of, along with a million other companies that
7 rent part of the same cloud. And why the cloud is not
8 considered as secure. IDV vendors. If you're doing a SAS
9 model in the cloud, that's a problem. It's going to be a
10 bigger problem for you.
11 We move the data behind the firewall. We check for
12 liveness. We examine some of the liveness data, and if its
13 - if this is determined to be a living human being. Then we
14 delete the liveness data, okay. Remember, it was one file.
15 Think of it as one data packet, right? Liveness data and
16 matching data together. We've now deleted liveness data. We
17 have literally altered the file. We've changed it, okay. It
18 has completely different characteristics. It lacks a ton of
19 characteristics that the face scan has. We call what's left
20 the 3D face map. And the 3D face map is really just
21 matching data, which that is what is bound to the verified
22 identity profile. So, we have a 3D biometric representation
23 of your face, which then we can match against later because
24 we know it's the face that belongs to that identity,
25 because they're bound together. The face match - the face

1 map is bound to the identity profile, or it's measured –
2 it's matched against the 2D image.
3 So, if we're matching 3D against the 3D face map
4 that's already there that we collected when you enrolled—
5 more data. 3D versus 3D is way more data, right. Accuracy
6 level goes way up. Theoretically, at a 1% false reject
7 rate, we could have a false accept rate of 1 in 124
8 million. Notice I said theoretically. We've never been able
9 to prove that. There isn't a real-world example. So, all
10 you other vendors that say, "Oh, that's not real, it's just
11 in the lab." That's true. It's theoretical, right. But the
12 theoretical possibility of your 2D matcher isn't even close
13 to the theory – the possibility of ours, right. So, 3D to
14 3D is as good as you can get. 3D to 2D is still a lot more
15 data being compared than 2D to 2D, which we already talked
16 about, right. They can delete the biometric data or keep
17 it. That's a policy issue, right. So, what's the advantage
18 of collecting one data file, right? There's a number of
19 advantages. It gives you control of what that file should
20 be and the characteristics of that file. But remember, when
21 we delete the liveness data, we are literally altering the
22 data. We're altering the file, right. It's different.
23 This goes back to your honeypot thing that you
24 asked about. So, let's just – hypothetical example, right.
25 Let's say the file was originally written in English, okay.

1 Uses the English language. And then when it's sent behind
2 the firewall, the file then changes to Japanese. So,
3 someone steals the Japanese document, and they try and
4 submit it to the system that's trying to read English. What
5 would happen? Error. That's what happens when you alter the
6 biometric file too. When you delete the liveness data, we
7 change the data that's in the file. We change the file
8 completely. But if somebody steals that and tries and
9 resubmit it, it doesn't have the proper characteristics. It
10 doesn't have the required characteristics, and our system
11 would just say error. This doesn't - does not compute,
12 right? So, it can't be used. So, why would anybody steal
13 it? So there is no - Let's say that we mitigate,
14 significantly mitigate the honeypot risk.
15 And there's other ways to do that, you know. There
16 are a couple other things. Encryption is a biggie, you
17 know. If you make the data unusable by encrypting it. We
18 made the data unusable by changing the file. You can make
19 the data unusable by encrypting it. Again, Cryptography is
20 essential. It's a good idea. So, we think our system is
21 fantastically productive compared to other systems, you
22 know. For all the reasons I've talked about over the last
23 half a dozen episodes. Start moving the biometric data,
24 right. It starts with – well, it starts with capturing the
25 sensor and protecting against deepfake injections. Then

capturing matching and face data, three-dimensional matching and, and liveness data concurrently, so it's one file, right. The advantages of 3D over 2D are pretty self-evident, okay. 3D liveness over other liveness is also self-evident, right. Send it behind the firewall so that it can be matched against the verified stored value that you already know belongs to the guy that's represented by the identity file behind the firewall, right. Other guys don't do that. It's a big deal. That's the basis of the PKI fallacy.

But here's one thing you got to know. If you don't move the biometric data to the database of identities, you can't match that biometric data against all of the other biometric data in the database. You can't do a one-to-many match. And what that - by moving the biometric data to the database and binding it to a verified identity profile, you have a complete description of this person now, and you can take that face data, and you can match it against all the other face data stored in the database, and you can do it anonymously so nobody has to get all upset, alright. If there's – if there's two accounts with the same face, the system will tell you if there's more than one account with the same face. Well, what does that mean? If there's more than one account with the same face. It could be the same name and address and phone number. It could be just a

1 duplicate account, right. And the bank or whoever doesn't
2 want to have two duplicate accounts. That creates
3 inefficiencies and problems for them down the road, right.
4 So, they can merge them or delete one or whatever it is and
5 really improve their system. But you also have - could have
6 two face - the same face on different files that are under
7 a different name. What if that happens?
8 TONY: That's fraud.
9 JAY: That's fraud, right. So, you delete both of them,
10 right. So now, think about that. You - I like to say you're
11 cleaning the database You can get rid of the duplicity; you
12 can get rid of the fraudulent files. And our customers are
13 using this to the max, okay. It's a big, big, big deal. I'm
14 not kidding. They love it because it's - they don't know
15 who's in their database. Jamie Dimon, chairman and CEO of
16 J.P. Morgan, said publicly on CNBC like a year and a half
17 ago, we have no idea who our account owners are. We have no
18 idea who's in control of these accounts. So, now you get a
19 sense of how you can clean that database of bad entries and
20 lower the risk profile of your business, right. Once it's
21 clean, you have a much higher quality identity verification
22 on the new entrants, right, which means you have more
23 confidence in the data you're collecting from a new
24 customer. And you - overall, you raise the integrity of the
25 quality of data in the database. The risk to the enterprise

1 goes way down.
2 So, if your guys aren't moving their biometric
3 data to the verified identity data somewhere, you need to
4 get a new vendor, because that is critically important in
5 today's world.
6 TONY: Well, I mean, just to bring it all back to the
7 UR code. The reason that you want to emphasize all these
8 unique things about FaceTec, I guess partly is that the UR
9 code is vendor agnostic. So, I mean, nobody has to use -
10 JAY: Liveness is vendor agnostic.
11 TONY: Yeah. So, like nobody needs to use FaceTec's
12 liveness technology. Um -
13 JAY: They want to.
14 TONY: But, you're making a good case.
15 JAY: Well, exactly. So, think about this. So, I - This
16 is the main point of the UR code, remember? We - We move
17 biometric data to the database. There's all these fake IDs.
18 There's all this - Your identity data is out there on the
19 dark web. We don't know who's in control of your identity
20 data, which means we don't know who's representing
21 themselves as you. We have no - almost no way to tell. So,
22 we move the biometric data to the database because there's
23 all this bad information, fake IDs and stolen, stolen
24 legitimate identity data out there, we can't trust that the
25 identity data that's presented anymore. And because of the

1 PKI fallacy, we cannot trust that we know who's in control
2 of the device that the newfangled cryptographically secured
3 credentials are bound to, right. That's what verifiable
4 credentials and mobile driver's licenses, and that's the -
5 what they solve for is the integrity of the data, right.
6 It's a perfect representation of what's behind the
7 firewall at the DMV or at the State Department or whatever,
8 right, because that information is the only information we
9 can trust. But it's behind the firewall. In order to use
10 it, traditionally, you would have had to move biometric
11 data behind their firewall. You'd have to move biometric
12 data to a government resource who can then potentially
13 track you or find out that you're opening another account
14 at Tinder or whatever, right. So, the privacy people have a
15 big problem with that, you know. They do, and it's a
16 problem for us. It holds us back, right. Holds the whole
17 industry back. So, the mobile driver's license, for
18 example, takes all that driver's license data and moves it
19 into the control of the consumer. And it does it in a, a
20 pretty good way. Well, it's kind of a cumbersome way, but
21 it's pretty good, alright, for what it does. But what it
22 doesn't do is verify that the holder of the device that the
23 credential is bound to is the same person represented by
24 the mobile driver's license. There's virtually no way to do
25 that.

1 The only way it does it is it has a picture. So,
2 somebody can look at the picture and then look at your face
3 and say, "Oh, I guess that's pretty good." It's the same,
4 same strategy that we've been using for ages. And that's
5 how a lot of people learned how to buy beer underage,
6 right. Because that same vector. So, what the UR code does
7 is – its - the data is extracted from the issuing
8 authority, the DMV or whoever. It's the same data that's in
9 the mobile driver's license. Same data. Exact. It's not
10 changed. There's nothing changed. Same exact data, okay.
11 Same picture, same biometric data, same identity data, and,
12 but it's in a different type of container, okay. It's in a
13 2D barcode that is a lot easier to use, a lot less
14 expensive to use, and a lot less cumbersome. And we can
15 take that 2D barcode and digitally sign it. If you guys
16 remember the digital. That's cryptography.
17 THE REPORTER: Yeah.
18 JAY: Digital signatures guarantee the integrity of the
19 barcode and the data in it, and they also tell you who
20 issued it, so you know it's the right state. That's what a
21 digital key. That's what the asymmetric key pairs do. But
22 the UR code can't be adulterated that way, can't be changed
23 the same way that a mobile driver's license or a verifiable
24 credential cannot be altered. The UR Code can't be altered.
25 But it's so light and efficient, you can beam it around.

1 It’s free. We’re giving it to the issuing authorities so
2 they can give it to their citizens and their consumers and
3 their identity owners, and then it’s in the control of the
4 identity owner. You don’t have to ping the government
5 database in order to confirm that this guy is the guy
6 represented by the identity in the mobile driver’s license
7 or something else. So, it satisfies the privacy concerns,
8 you know. That’s why we’re pretty excited, you know.
9 There’s a lot. I mean, here’s an update. We actually have
10 paying customers now that are using the UR codes.
11 THE REPORTER: Oh, wow.
12 TONY: That was fast.
13 JAY: Yeah, pretty fast.
14 UM1: Yeah.
15 JAY: Works real good. Works real good. And we’re going
16 to have some more soon, you know. Some of these customers
17 are big customers. For me, resident economist and Wall
18 Street blood sucking analyst, the fact that we’re getting
19 paid as a result of the UR codes is meaningful.
20 THE REPORTER: Yeah.
21 JAY: The fact we’re getting paid as a result of UR
22 codes only three months after we released them is amazingly
23 meaningful, right. And it’s only going to get better from
24 here. It’s catching on. The fire is lit, you know. Not -
25 It’s not Jimmy John’s franchise restaurant tour in Toronto,

okay. This is international. So very, very exciting. We are going full throttle, full ahead. And, um, we think – we think that UR code, because we're not asking anybody, it's a protocol not a product, we think is going to revolutionize identity management on the Internet. It really is that disruptive. That's all I got to say about that.