IPR2025-00106 (U.S. Patent No. 10,776,471)
IPR2025-00107 (U.S. Patent No. 11,157,606)
IPR2025-00108 (U.S. Patent No. 11,693,938)
IPR2025-00108 (U.S. Patent No. 11,874,910)

Jumio Corporation (Petitioner)

v.

FaceTec, Inc. (Patent Owner)

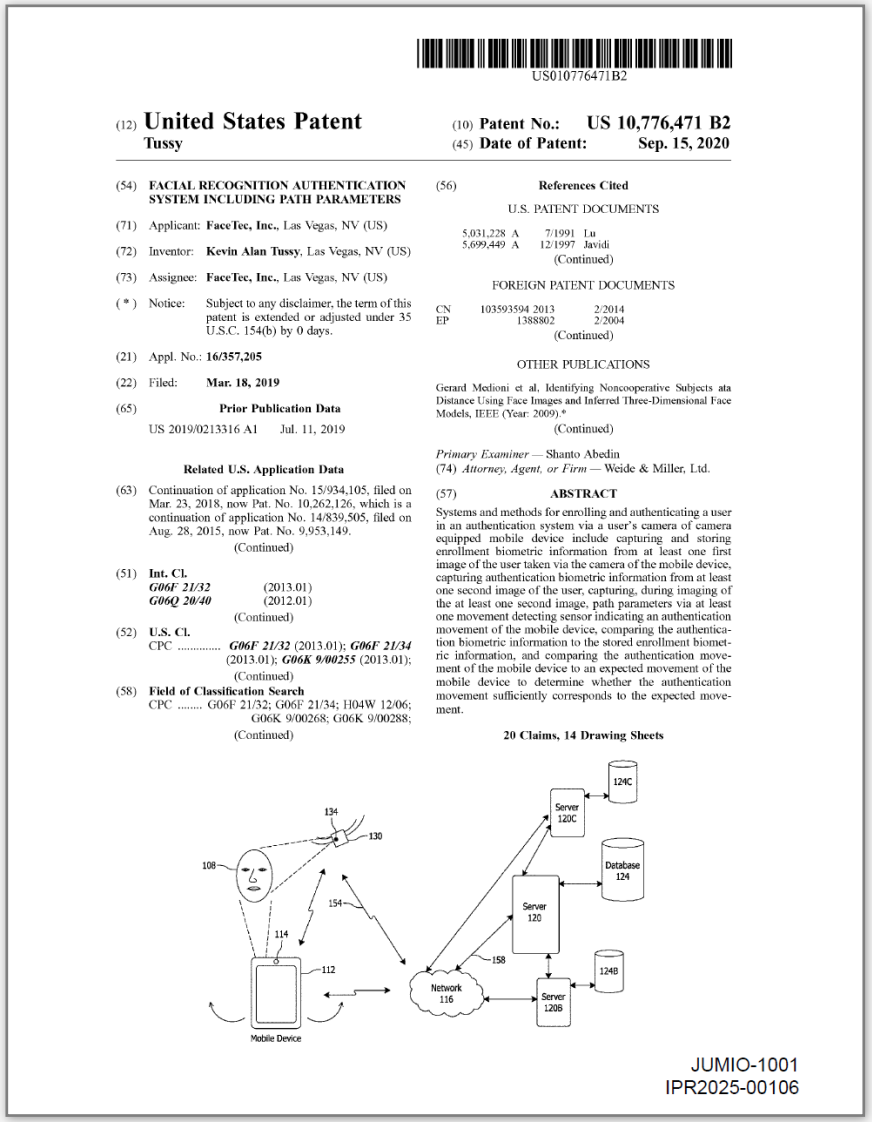
March 17, 2026

Roadmap

1. The FaceTec Patents
2. Instituted Grounds and Prior Art
3. POSITA Level and Dr. Daft
4. RPI / Privity
5. Secondary Considerations

The FaceTec Patents

The FaceTec Patents



US010776471B2

(12) **United States Patent**
Tussy

(10) **Patent No.: US 10,776,471 B2**
(45) **Date of Patent: Sep. 15, 2020**

(54) **FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS**

(71) Applicant: **FaceTec, Inc.**, Las Vegas, NV (US)

(72) Inventor: **Kevin Alan Tussy**, Las Vegas, NV (US)

(73) Assignee: **FaceTec, Inc.**, Las Vegas, NV (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **16/357,205**

(22) Filed: **Mar. 18, 2019**

(65) **Prior Publication Data**

US 2019/0213316 A1 Jul. 11, 2019

Related U.S. Application Data

(63) Continuation of application No. 15/934,105, filed on Mar. 23, 2018, now Pat. No. 10,262,126, which is a continuation of application No. 14/839,505, filed on Aug. 28, 2015, now Pat. No. 9,953,149.
(Continued)

(51) **Int. Cl.**
G06F 21/32 (2013.01)
G06Q 20/40 (2012.01)
(Continued)

(52) **U.S. Cl.**
CPC ***G06F 21/32*** (2013.01); ***G06F 21/34*** (2013.01); ***G06K 9/00255*** (2013.01);
(Continued)

(58) **Field of Classification Search**
CPC G06F 21/32; G06F 21/34; H04W 12/06; G06K 9/00268; G06K 9/00288;
(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,031,228 A 7/1991 Lu
5,699,449 A 12/1997 Javidi
(Continued)

FOREIGN PATENT DOCUMENTS

CN 103593594 2013 2/2014
EP 1388802 2/2004
(Continued)

OTHER PUBLICATIONS

Gerard Medioni et al, Identifying Noncooperative Subjects ata Distance Using Face Images and Inferred Three-Dimensional Face Models, IEEE (Year: 2009).*
(Continued)

Primary Examiner — Shanto Abedin
(74) *Attorney, Agent, or Firm* — Weide & Miller, Ltd.

(57) **ABSTRACT**

Systems and methods for enrolling and authenticating a user in an authentication system via a user's camera of camera equipped mobile device include capturing and storing enrollment biometric information from at least one first image of the user taken via the camera of the mobile device, capturing authentication biometric information from at least one second image of the user, capturing, during imaging of the at least one second image, path parameters via at least one movement detecting sensor indicating an authentication movement of the mobile device, comparing the authentication biometric information to the stored enrollment biometric information, and comparing the authentication movement of the mobile device to an expected movement of the mobile device to determine whether the authentication movement sufficiently corresponds to the expected movement.

20 Claims, 14 Drawing Sheets

JUMIO-1001
IPR2025-00106

13A and 13B. Typical cameras on a mobile device or any other device include a curved lens. This results in a "fish-eye" effect in the resulting images taken by the camera. In

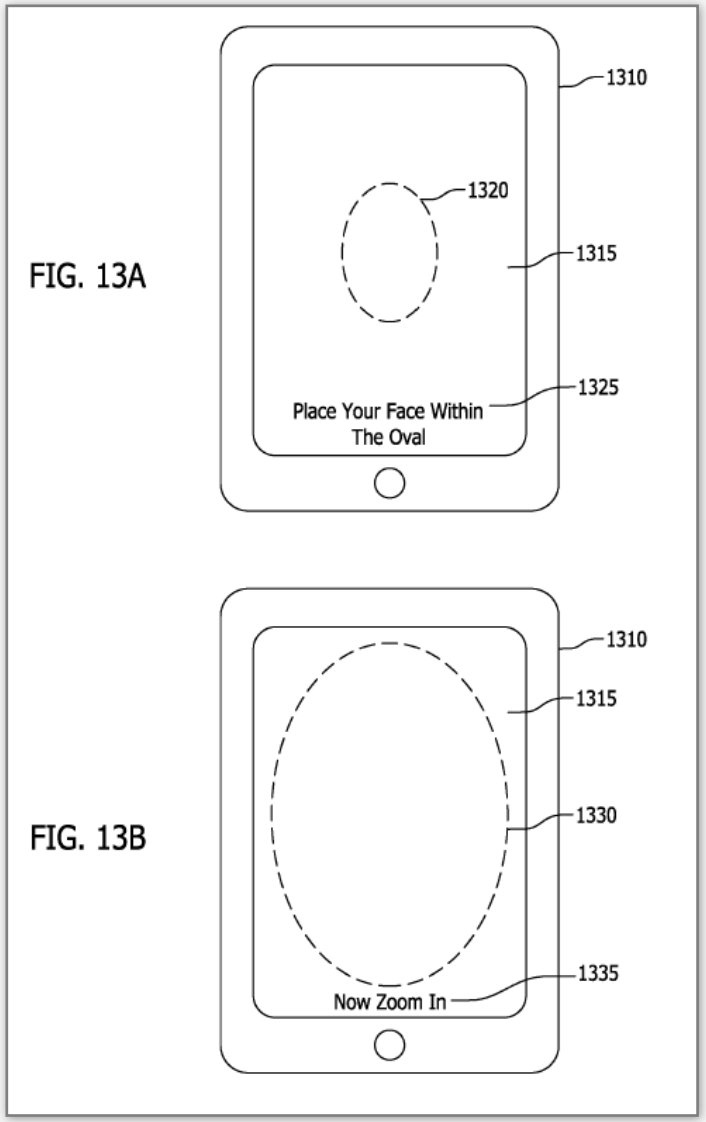
'471 Patent (EX1001), 28:36-37

ment images. Further, because the fish-eye effect is expected when an actual, three-dimensional person is present, an absence of the relative change in the dimensions of the facial features alerts the system to a fraudulent attempt at authentication. This effect could not easily be re-created with a two dimensional picture (printed photograph or screen) and thus, this step can serve as a secure test to prevent a two dimensional picture (in place of a live face) from being used for authentication.

'471 Patent (EX1001), 29:11-19

'471 Petition (Paper 1), 4-5; Daft Decl. (EX1003), ¶55

The FaceTec Patents



'471 Patent (EX1001), Fig. 13A, Fig.13B

authentication system. For example, during enrollment, enrollment images may be provided by the user at both the close and far proximity from the lens, in addition to other positions through the movement. Later, during authentica-

'471 Patent (EX1001), 29:4-7

positions of the screen. When an actual, three-dimensional person images himself or herself close up and far away, it has been found that the biometric results are different due to the fish-eye effect of the lens. Thus, a three-dimensional person may be validated when biometric results are different in the close-up and far away images. This also allows the user to have multiple biometric profiles for each of the distances.

'471 Patent (EX1001), 3:52-59

'471 Petition (Paper 1), 4-5

The ’471 Patent, Claim 1

1. A system for authenticating three-dimensionality of a user via a user’s camera equipped computing device, the computing device comprising:

a processor configured to execute machine executable code;

a screen configured to provide a user interface to the user;

a camera configured to capture images;

one or more memories configured to store machine readable instructions that are stored on the memory of the authentication server which when executed by the processor, cause the computing device to:

capturing at least one first image of the user taken with the camera of the computing device at a first location which is a first distance from the user;

processing the at least one first image or a portion to create first data;

moving the camera from the first location to a second location, the second location being a second distance from the user, or the user moving from the first location to the second location to change the distance between the user and the camera from the first distance to a second distance;

capturing at least one second image of the user taken with the camera of the computing device at the second distance from the user, the second distance being different than the first distance;

processing the at least one second image or a portion thereof to create second data;

comparing the first data to the second data to determine whether expected differences exist between the first data and the second data which indicated three-dimensionality of the user;

authenticating the user when differences between the first data and the second data have expected distortion resulting from movement of the camera from the first location to the second location or movement of the user from the first location to the second location, which causes the change in distance between the user and the camera.

1. A system for authenticating three-dimensionality of a user via a user’s camera equipped computing device, the computing device comprising:

authenticating the user when differences between the first data and the second data have expected distortion resulting from movement of the camera from the first location to the second location or movement of the user from the first location to the second location, which causes the change in distance between the user and the camera.

The ’606 Patent, Claim 1

1. A method for verifying three-dimensionality of a user’s face using images of the user’s face captured using a camera equipped computing device, the method comprising:

capturing at least one first image of the user taken camera of the computing device at a first distan the user;

processing the at least one first image to obt biometric data from the at least one first imag

capturing at least one second image of the user tak the camera of the computing device at a second dis- tance from the user, the second distance being different than the first distance;

processing the at least one second image to obtain biometric data based on the at least one second

comparing the first biometric data with the seco metric data to determine whether the first b data matches the second biometric data;

comparing the first biometric data to second b data to determine whether differences betwee least one first image and the at least one secon match expected differences resulting from mo of the camera or the user which changed the between the user and camera from the first dis the second distance;

determining that the user’s face is three-dim when:

the first biometric data does not match the seco metric data; and

the second biometric data has the expected differ compared to the first biometric data resulting from the change in distance between the user and the camera when capturing the at least one first image and the at least one second image.

comparing the first biometric data to second biometric data to determine whether differences between the at least one first image and the at least one second image match expected differences resulting from movement of the camera or the user which changed the distance between the user and camera from the first distance to the second distance;

The ’938 Patent, Claim 1

1. A non-transient computer readable medium containing non-transitory machine executable code configured to determine if the three-dimensional shape is consistent with that of a human face, the non-transitory machine executable code configured to:

receive or derive first biometric data from at least one first image of a user taken with a computing device camera located at a first distance from the user;

receive or derive second biometric data from at least one second image of the user taken with the computing device camera located at a second distance from the user, the second distance being different than the first distance;

compare the first biometric data with second biometric data for expected differences that result from characteristics of a human face and the at least one first image and the at least one second image being captured at different distances from the user;

determine that the three-dimensional shape is consistent with that of a human face when the second biometric data does not match the first biometric data for expected differences compared to the first biometric data, the expected differences comprising at least differences due to the change in the relative orientation between the user’s facial features and the camera when the at least one first image was captured at the first distance and the at least one second image was captured at the second distance, wherein the expected differences result from fish-eye type distortion in at least one of the at least one first image and the at least one second image and due to the three-dimensional nature of the human face and the change in distance between the camera and the user.

The ’910 Patent, Claim 1

1. A computing device for verifying three-dimensionality of a user via a user’s camera equipped computing device, the computing device comprising:

a processor configured to execute machine executable code;

a screen configured to provide a user interface to the user;

a camera configured to capture images;

one or more memories configured to store machine readable instructions that are stored on the memory of the authentication server which when executed by the processor, cause the computing device to:

capturing at least one first image of the user taken with the camera of the computing device at a first location which is a first distance from the user;

processing the at least one first image or a portion thereof to create first data;

capturing at least one second image of the user taken with the camera of the computing device is at a second distance from the user, the second distance being different than the first distance, the capturing at least one second image of the user occurring after movement of the camera or the user to establish the camera at the second distance from the user;

processing the at least one second image or a portion thereof to create second data;

comparing the first data to the second data to determine whether expected differences exist between the first data and the second data which indicates three-dimensionality of the user;

verifying the images of the user exhibit three dimensional traits when the expected differences exist between the first data and the second data as a result of capturing the at least one first image and the at least one second image at different distances from the user.

1. A computing device for verifying three-dimensionality of a user via a user’s camera equipped computing device, the computing device comprising:

compare the first biometric data with second biometric data for expected differences that result from characteristics of a human face and the at least one first image and the at least one second image being captured at different distances from the user;

Roadmap

1. The FaceTec Patents
2. **Instituted Grounds and Prior Art**
3. POSITA Level and Dr. Daft
4. RPI / Privity
5. Secondary Considerations

Instituted Grounds

Instituted Grounds For The ’471 Patent

Ground	Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1A	1–13, 15–17, 19, 20	103	Derakhshani, Tanii
1B	14	103	Derakhshani, Tanii, Tahk
1C	18	103	Derakhshani, Tanii, Hoyos
2A	1–3, 5, 7–12, 16, 17, 19, 20	103	Zhang, Tanii
2B	4, 6, 13–15	103	Zhang, Tanii, Tahk
2C	18	103	Zhang, Tanii, Hoyos

IPR2025-00106 Decision on Institution (DI) (Paper 17), 6

Instituted Grounds For The ’606 Patent

Claim(s) Challenged	35 U.S.C. §	References/Basis
1–4, 6–7, 9–16, 18–20	103[1]	Derakhshani, Tanii
5, 8, 17	103	Derakhshani, Tanii, Tahk
1–3, 9–12, 14, 16, 18–20	103	Zhang, Tanii
4–8, 13, 15, 17	103	Zhang, Tanii, Tahk

IPR2025-00107 Decision on Institution (Paper 17), 6

Instituted Grounds For The ’938 Patent

Ground	Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1A	1–10, 12–24	103	Derakhshani, Tanii
1B	11	103	Derakhshani, Tanii, Tahk
2A	1–3, 5–9, 12–14, 16–20, 22–24	103	Zhang, Tanii
2B	4, 10–11, 21	103	Zhang, Tanii, Tahk
2C	15	103	Zhang, Tanii, Suzuki

IPR2025-00108 Decision on Institution (Paper 17), 6

Instituted Grounds For The ’910 Patent

Claim(s) Challenged	35 U.S.C. [1] §	References
1–13, 15–24	103	Derakhshani, Tanii
14	103	Derakhshani, Tanii, Tahk
1–3, 5–12, 15–17, 19–24	103	Zhang, Tanii
4, 13, 14	103	Zhang, Tanii, Tahk
18	103	Zhang, Tanii, Hoyos

IPR2025-00109 Decision on Institution (Paper 17), 5-6

Disputed Challenged Claims

Prior Art	’471 Patent	’606 Patent	’938 Patent	’910 Patent
Derakhshani-Tanii	1, 3, 5, 7, 8, 10, 12, 16, 17	1, 3, 10, 12, 19	1, 5, 7, 8, 17, 20, 24	1, 3, 5, 7, 10, 12, 16, 22
Derakhshani-Tanii-Hoyos	18			18
Zhang-Tanii	1, 3, 7, 10, 12, 16	1, 3, 10, 12, 19	1, 8, 17, 20	1, 3, 7, 10, 12, 16, 22
Zhang-Tanii-Hoyos	18			18

Undisputed Challenged Claims

Prior Art	'471 Patent	'606 Patent	'938 Patent	'910 Patent
Derakhshani-Tanii	2, 4, 6, 9, 11, 13, 15, 19, 20	2, 4, 6, 7, 9, 11, 13-16, 18, 20	2-4, 6, 9, 10, 12-16, 18, 19, 21-23	2, 4, 6, 8, 9, 11, 13, 15, 17-21, 23, 24
Derakhshani-Tanii-Tahk	14	5, 8, 17	11	14
Derakhshani-Tanii-Hoyos				
Zhang-Tanii	2, 5, 8, 9, 11, 17, 19, 20	2, 9, 11, 14, 16, 18, 20	2, 3, 5-9, 12-14, 16, 18, 19, 22-24	2, 5, 6, 8, 9, 11, 15, 17, 19, 20, 21, 23, 24
Zhang-Tanii-Tahk	4, 6, 13-15	4-8, 13, 15, 17	4, 10, 11, 21	4, 13, 14
Zhang-Tanii-Hoyos				
Zhang-Tanii-Suzuki			15	

Roadmap

1. The FaceTec Patents

2. Instituted Grounds and Prior Art
   a. **Derakhshani-Tanii**
   b. Zhang-Tanii
   c. Hoyos
   d. Tanii is analogous art

Derakhshani

Derakhshani

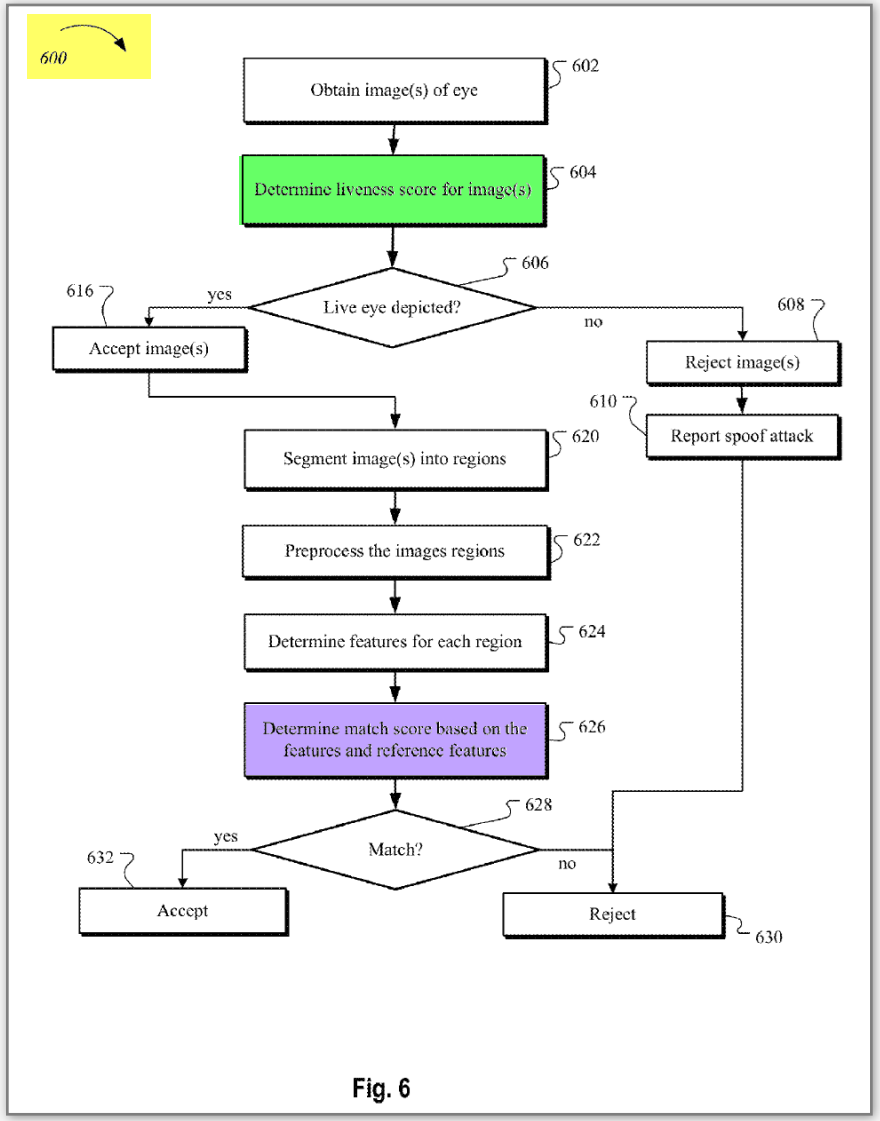


Fig. 6

FIG. **6** is a flow chart of an example process **600** for authenticating an individual based on one or more images of the white of an eye. A liveness score is determined for the obtained images and used to accept or reject the images. When an image of a live eye is detected and accepted, the image is further analyzed to determine a match score by extracting features from the image and comparing the features to a reference record. The user is then accepted or rejected based on the match score.

Derakhshani (EX1005), 9:59-67

Derakhshani (EX1005), Fig. 6

'471 Petition (Paper 1), 27; '471 Reply (Paper 52), 9

Derakhshani

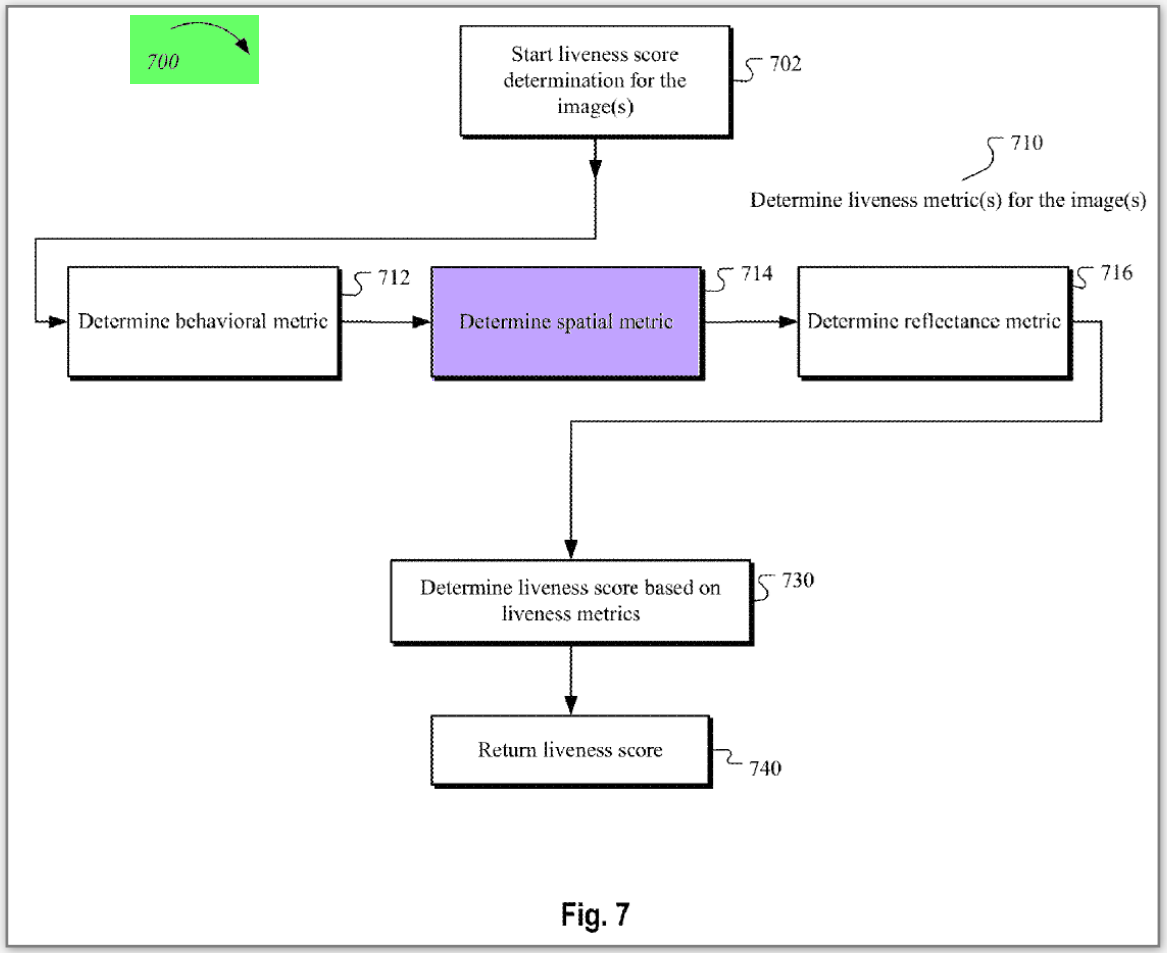


Fig. 7

Derakhshani (EX1005), Fig. 7

Focus Distance Approach

In this example, a spatial metric is determined **714** based on a distance from a sensor to a landmark that appears in a plurality of the images each having a different respective focus distance. Focus distance is the distance from a sensor to a point in its field of view that is perfectly in focus. For some

Derakhshani (EX1005), 16:44-48

Parallax Approach

In some implementations, determining **714** the spatial metric comprises determining parallax of two or more landmarks that appear in a plurality of the images. Parallax is the apparent displacement of an observed object due to a change in the position of the observer. A plurality of images taken from different perspectives on the subject may result in landmarks within the images appearing to move by different amounts because of differences in their distance from the sensor. This

Derakhshani (EX1005), 17:45-52

'471 Petition (Paper 1), 7-8, 45

Derakhshani's Landmarks

sensor. For example, a landmark (e.g., an iris, an eye corner, a nose, an ear, or a background object) may be identified and located in the plurality of images with different focus distances. A landmark's representation in a particular image has

Derakhshani (EX1005), 16:51-54

the sensor. However the locations of landmarks (e.g., an eye, nose, mouth, and ear) in the two dimensional image will occur in a two dimensional plane, unlike landmarks in and around a real live eye. For example, the locations of multiple landmarks may be fit to the closest two dimensional plane and the average distance of the landmarks from this fit plane can be determined as the spatial metric. A high value for this spatial

Derakhshani (EX1005), 17:16-22

dimensional shape. Determining the spatial metric may include determining parallax of two or more landmarks that appear in a plurality of the images. Half-tones may be

Derakhshani (EX1005), 3:5-7

'471 Petition (Paper 1), 7-8; '471 Reply (Paper 52), 1

Derakhshani's Focus Distance Approach

frequency components are expected. By comparing the degree of focus for a landmark in images with different focus distances, the distance from the sensor to the landmark may be estimated. In some implementations, distances from the

Derakhshani (EX1005), 16:66-17:2

sensor. The positions of these landmarks in the space viewed by the camera may be compared to a model by determining a spatial metric (e.g., the mean square difference between the detected location of one or more landmarks and the corresponding modeled locations of the one or more landmarks) that reflects deviation from the model.

Derakhshani (EX1005), 17:6-11

determined as the spatial metric. A high value for this spatial metric may indicate a three-dimensional subject and a higher likelihood that the subject is a live eye, while a low value may indicate a higher likelihood that the subject is a two-dimensional spoof attack.

Derakhshani (EX1005), 17:22-26

'471 Petition (Paper 1), 7-8, 10, 21

Derakhshani's Match Score

If the liveness score indicates a high likelihood that live eye is depicted in the images, the one or more images are accepted **616** and subjected to further analysis to complete the authentication process.

Derakhshani (EX1005), 11:43-45

The one or more images may be segmented **620** to identify regions of interest that include the best views of vasculature in the white of an eye. In some implementations, anatomical

Derakhshani (EX1005), 11:46-48

Features are determined **624** for each image region that reflect structure or properties of the vasculature visible in that region of the user's eye. In some implementations, minutia

Derakhshani (EX1005), 13:9-11

'471 Petition (Paper 1), 27; '471 POR (Paper 43), 33; Daft Decl. (EX1003), ¶ 185; Daft Reply Decl. (EX1060), ¶16

Derakhshani

Dr. Daft

13. Spatial metric: The spatial metric measures three-dimensionality based differences in landmarks that appear in a plurality of captured images due to differences in the distance from the sensor to a landmark. (EX1005, 16:44-47, 17:22-26.) One image of the plurality of captured images may be a close-up image, and another image of the plurality of captured images may be captured at a different distance further away from the user. The close-up image may capture the eye vasculature (with enough precision), and the further-away image may capture the landmark(s) (with enough precision). Derakhshani names examples landmarks including "a nose, an ear," or a "mouth." (EX1005, 16:51-54, 17:16-17.) It also discusses "landmarks on a particular user's face," and a "landmark may be a portion of a face depicted in the images." (EX1005, 3:13-15, 17:29-36.)

Daft Repl. Decl. (EX1060), ¶13

'471 Reply (Paper 52), 1-2

Derakhshani's Focus Distance Approach

Dr. Turk

Q Okay. So Derakhshani's focus distance approach captures a plurality of images with different distances, right? We talked about that earlier.

A Yes.

Q Okay. And in that, would Derakhshani be capturing one image where a given landmark is in focus, and in another image, that same landmark is then blurry?

A That is my understanding of how he's describing that process.

Q Okay.

A And this is a process well known in the literature as depth from defocus --

Q Depth from --

A -- or depth from focus.

Turk Depo Tr. (EX1059), 144:11-21

'471 Reply (Paper 52), 4, 8

Derakhshani's Parallax Approach

that appear in a plurality of the images. Parallax is the apparent displacement of an observed object due to a change in the position of the observer. A plurality of images taken from different perspectives on the subject may result in landmarks within the images appearing to move by different amounts because of differences in their distance from the sensor. This

Derakhshani (EX1005), 17:47-52

because of differences in their distance from the sensor. This parallax effect may be measured and used as a spatial metric that reflects the three-dimensional nature of a subject in the view of the sensor. If all the landmarks in the images undergo

Derakhshani (EX1005), 17:52-55

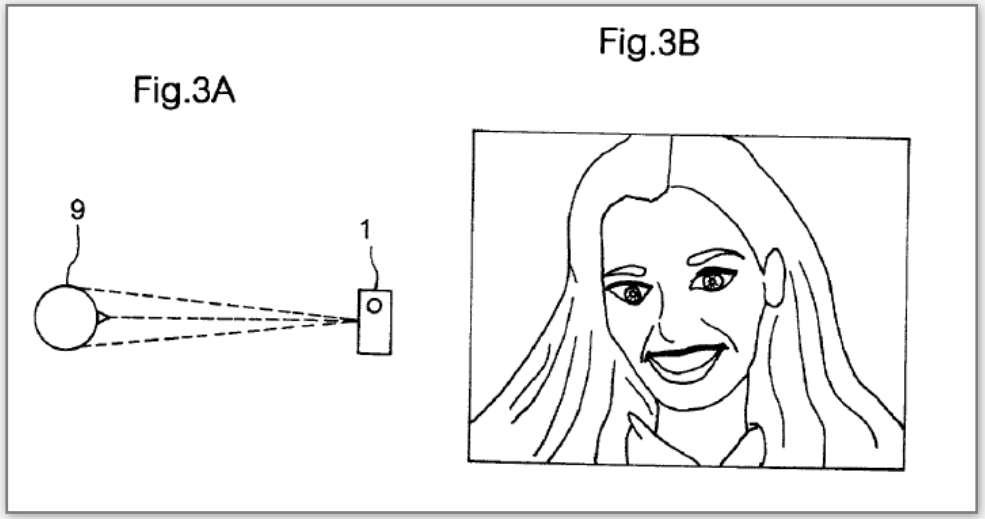
view of the sensor. If all the landmarks in the images undergo the same apparent displacement due to relative motion of the sensor, i.e., the difference in the parallax effect for the landmarks is small, then the subject viewed by the camera has higher likelihood of being a two-dimensional spoof attack. In

Derakhshani (EX1005), 17:55-59

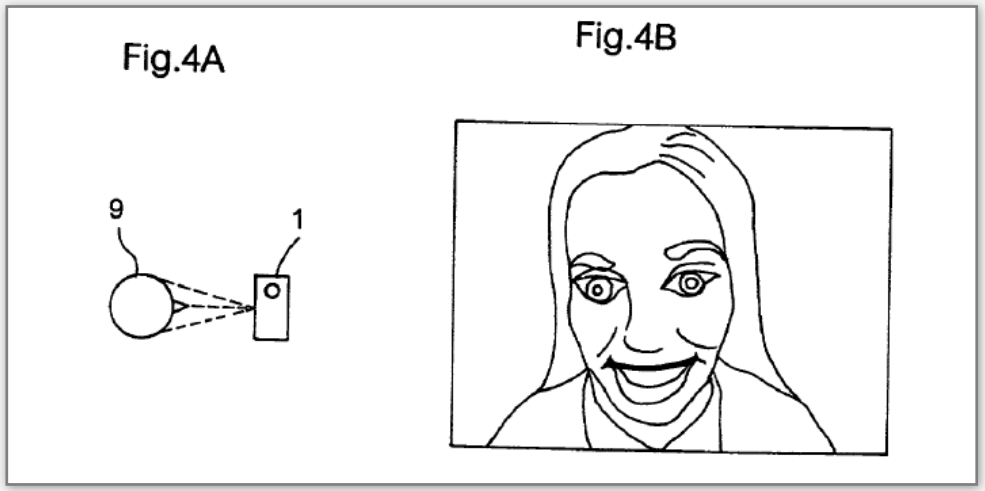
'471 Petition (Paper 1), 7-9, 21-23

Tanii

Tanii



Tanii (EX1007), Figs. 3A-3B,



Tanii (EX1007), Figs. 4A-4B

while he is talking through the phone. With a cellular phone containing a camera, the lens is adjusted to have a wide-angle focal length such that the face of the user captured in the image is appropriately sized. When the user's face is close to the camera when such an optical system is used, the exaggeration warp becomes more noticeable.

Tanii (EX1007), [0007]

[0047] Where the main object **9** and the cellular phone **1** are located at a sufficient distance from each other when image capture is performed, as shown in **FIG. 3A**, a natural image can be obtained, as in the image shown in **FIG. 3B**.

Tanii (EX1007), [0047]

However, where the main object **9** and the cellular phone **1** are close together, as shown in **FIG. 4A**, an unnatural image results in which the perspective is exaggerated, as in the image shown in **FIG. 4B**.

Tanii (EX1007), [0047]

Derakhshani-Tanii: Disputed Recitations

Disputed Recitation	'471 Claim(s) Or Element	'606 Claim(s) Or Element	'938 Claim(s) Or Element	'910 Claim(s) Or Element
"user"	1[pre], 10[pre]			1, 10, 22
"face"		1, 10, 19	1, 8, 17, 20	
"verifying . . . the user's ears[/features on a side of a user's head]"	3/12	3/12		3/12
"first [] data," "second [] data"	5[a]		5[a]	5[a]
"biometric data"	7/16	1[b], 10[c], 19[a]	1[a], 17[d]	7/16
"mapping of facial features"	8/17		7/24	

’471 Patent, Element 1[pre] And Claim 9

’471 Patent, Element 1[pre]

1. A system for authenticating three-dimensionality of a user via a user’s camera equipped computing device, the computing device comprising:

’471 Patent, Claim 9

9. The method according to claim 1, wherein the first image and the second image is of the user’s face and the user’s face is held steady and without movement during capture of the first image and the second image.

’910 Patent, Element 1[pre] And Claim 9

’910 Patent, Element 1[pre]

1. A computing device for verifying three-dimensionality of a user via a user’s camera equipped computing device, the computing device comprising:

’910 Patent, Claim 9

9. The method according to claim 1, wherein the first image and the second image is of the user’s face and the user’s head and facial features are held steady and without movement during capture of the first image and the second image.

Derakhshani-Tanii: Disputed Recitations

Disputed Recitation	'471 Claim(s) Or Element	'606 Claim(s) Or Element	'938 Claim(s) Or Element	'910 Claim(s) Or Element
"user"	1[pre], 10[pre]			1, 10, 22
"face"		1, 10, 19	1, 8, 17, 20	
"verifying . . . the user's ears[/features on a side of a user's head]"	3/12	3/12		3/12
"first [] data," "second [] data"	5[a]		5[a]	5[a]
"biometric data"	7/16	1[b], 10[c], 19[a]	1[a], 17[d]	7/16
"mapping of facial features"	8/17		7/24	

Derakhshani Teaches Capturing An Image Of A Face

Derakhshani

sensor. For example, a landmark (e.g., an iris, an eye corner, a nose, an ear, or a background object) may be identified and located in the plurality of images with different focus distances. A landmark's representation in a particular image has

Derakhshani (EX1005), 16:51-54

Dr. Daft

395. Derakhshani discloses that, as part of the process to verify that the face is in fact three-dimensional, "a landmark (e.g., an iris, an eye corner, a nose, an ear, or a background object) may be identified and located in the plurality of images." *Derakhshani*, 16:44-54 (focus-distance approach), 17:45-64 (parallax approach).

Daft Decl. (EX1003), ¶395

'606 Petition (Paper 1), 7, 16-17

Derakhshani Teaches Capturing An Image Of A Face

In some implementations, the spatial metric is a measure of the deviation of the subject from a two-dimensional plane. One possible spoofing strategy is to present a two dimensional image (e.g., a photograph) of a registered user's eye to the sensor. However the locations of landmarks (e.g., an eye, nose, mouth, and ear) in the two dimensional image will occur in a two dimensional plane, unlike landmarks in and around a real live eye. For example, the locations of multiple landmarks may be fit to the closest two dimensional plane and the average distance of the landmarks from this fit plane can be determined as the spatial metric. A high value for this spatial metric may indicate a three-dimensional subject and a higher likelihood that the subject is a live eye, while a low value may indicate a higher likelihood that the subject is a two-dimensional spoof attack.

Derakhshani (EX1005), 17:12-26

'471 Petition (Paper 1), 10, 28, 32;
'606 Petition (Paper 1), 7, 16; '471 Reply (Paper 52), 1-3, 9;
Daft Reply Decl. (EX1060), ¶¶28, 38, 40, 43, 46, 48, 50;

Derakhshani Teaches Capturing An Image Of A Face

Dr. Daft

a portion of a face depicted in the images." (EX1005, 3:13-15.) Derakhshani also states that an image may comprise multiple "landmarks (e.g., an eye, nose, mouth, and ear." (EX1005, 17:16-19; *see also* 3:5-7 ("two or more landmarks that appear in a plurality of the images"), 17:2-6 ("multiple landmarks").) Dr. Turk also agreed that Derakhshani captures an image having multiple landmarks. (EX1059, 136:25-137:3.) It would have been obvious for an image comprising an eye, nose, mouth, and ear, as Derakhshani discloses, to be an image of a face because these are facial features that when they are all included in an image, it would be an image of a user's face. (EX1005, 17:16-20.)

Daft Reply Decl. (EX1060), ¶20

Dr. Turk

Q Okay. So if Derakhshani is capturing an image that has an ear, nose, mouth and eye, what type of image is it capturing?

A Well, I don't think Derakhshani ever says that it will capture images that include all of those.

Q Uh-huh.

A So they may well just be individual examples that would never be in the same image.

If Derakhshani were to capture something with all of those, it would be an image that is generally different than the images that are shown in Derakhshani, because those images generally don't cover larger parts of the face that would include such features.

Turk Depo Tr. (EX1059), 137:4-17

Derakhshani Teaches Capturing An Image Of A Face

sensor. For example, a landmark (e.g., an iris, an eye corner, a nose, an ear, or a background object) may be identified and located in the plurality of images with different focus distances. A landmark's representation in a particular image has

Derakhshani (EX1005), 16:51-54

Derakhshani Teaches Capturing An Image Of A Face

Dr. Turk

Q And if Derakhshani captures images that have a nose, ear, mouth or background object, then it must be capturing images that includes more than the user's eye; is that right?

A It can capture images that include things that are not part of the user's eye --

Q Okay.

A -- for example, the background, parts of the background.

Turk Depo Tr. (EX1059), 136:16-24

Q Okay. Now, Derakhshani, as we talked about earlier, talks about the landmark being a background object, right?

A That that's one example of what a landmark could be, yes.

Q Okay. What is a background object?

A I would say it's anything that's not part of the main object being imaged, which in this case is the eye.

Q Okay. So it would be -- would it be attached to the human?

A Derakhshani doesn't define it, but I think typically, in this context, it probably is referring to something not attached to a human.

Q Okay. For example, a painting behind you?

A I think that's a good example.

Turk Depo Tr. (EX1059), 148:11-149:1

'471 Reply (Paper 52), 1-2, 3-4

Derakhshani Teaches Capturing An Image Of A Face

Dr. Daft

21. Derakhshani also names a "background object" as an example landmark. (EX1005, 16:51-54.) It would have been obvious for an image comprising an eye and a background object (landmark) to be an image of a user's face. For example, the background object may be a painting on a wall located behind the user. In order to capture the user's eye and the painting in the image, the sensor would have to be back far enough from the user such that the user's face would be captured. Thus, Dr. Turk's suggestion (at, *e.g.*, ¶¶85 and 89 of his declaration (EX2061)) that Derakhshani captures images of the user's eyes only is wrong. I also note that Derakhshani does not disclose capturing the user's eye vasculature as its primary purpose, as Dr. Turk argues at ¶¶87 and 92 of his declaration.

Daft Reply Decl. (EX1060), ¶21

'471 Reply (Paper 52), 1-2

Derakhshani Teaches Capturing An Image Of A Face

Dr. Daft

26. Dr. Turk argues that Derakhshani's system is not adapted to capture the user's face or head. (EX2061, ¶¶87, 89.) I disagree. To make an accurate determination of the spatial metric, a POSITA would have understood that there mean there must be a discernable difference in distance between the user and the sensor. This would mean at least one captured image would be taken such that the sensor is far enough away from the user, thereby including more than just the user's eye in the image. Derakhshani discusses this at 17:55-59: "[i]f all the landmarks in the image undergo the ***same apparent displacement*** due to relative motion of the sensor, ***i.e., the difference in the parallax effect for the landmarks is small***, then the subject viewed by the camera has [a] higher likelihood of being a two-dimensional spoof attack." (EX1005, 17:55-59.) A POSITA would have understood from this passage that a large difference in the parallax effect for the landmarks would be needed when the object is three-dimensional in order to avoid a false determination of a two-dimensional spoof attack.

Daft Reply Decl. (EX1060), ¶26

'471 Reply (Paper 52), 3

Derakhshani Teaches Capturing An Image Of A Face

Petition

4. Independent Claim 1

a. 1[pre]

If limiting, Derakhshani discloses or suggests 1[pre]. *Daft*, ¶¶389-90.

Derakhshani discloses "biometric authentication" systems and methods using a camera-equipped computing device. *See Derakhshani*, 1:11-25, 5:22-27, 6:3-5, 9:10-22, 18:1-3. As part of the authentication process, a device implementing Derakhshani's approach verifies the user's face is three-dimensional by capturing multiple images of the user's face to calculate a "spatial metric" representing the face's three-dimensionality. *Id.*, 1:11-25, 3:14-15, 16:44-18:4; *Daft*, ¶390.

'606 Petition (Paper 1), 16

Tanii Teaches Detecting A Face

nents. The construction shown in **FIG. 16** is identical to that shown in **FIG. 6**, except that a size detector **204** that detects the size of the image of the main object and a correction level selector **205** that selects the correction level are added.

Tanii (EX1007), [0074]

[0061] As described above, with regard to the cellular phone **1**, when the image of the main object, particularly the image of the face of the user who is holding the cellular phone **1**, is captured, the exaggeration warp may be corrected, allowing an image close to a natural image to be obtained. In addition, the setting as to whether or not

Tanii (EX1007), [0061]

'471 Reply (Paper 52), 4

Tanii Teaches Detecting A Face

Dr. Turk

Q Okay. And so in order for Tanii to detect the size of the user's object, would it need to be able to detect the face?

A Not necessarily. It would need to be able to detect an object. That object may happen to be a face, but it may not be detecting a face specifically.

Q Okay. But it needs to detect the object in order to determine the size of the object. Is that fair?

A Yeah, I think so.

Turk Depo Tr. (EX1059), 175:5-14

Tanii Teaches Detecting A Face

[0069] The shape of the sections may be changed depending on the configuration of the main object. For example, the shapes of the borders between the sections **811** through **814** may be determined in response to the contours of the main object by extracting the contours of the main object using image processing. Appropriate warp correction may be

Tanii (EX1007), [0069]

overall image (step S212). The size detector **204** (i) identifies the region of the image of the main object based on the location of clear edges in the image as well as on the color distribution in the image, and (ii) detects the size of the main object image by comparing the region occupied by the main object image with the sections **821** and **822** shown in **FIG. 13**.

Tanii (EX1007), [0076]

'471 Reply (Paper 52), 4

Tanii Teaches Detecting A Face

Dr. Daft

face. Further, Tanii describes different ways to detect the user's face, such as "extracting the contours of the main object using image processing." (EX1007, [0069].) Tanii also describes "identif[ying] the region of the image of the main object based on the location of clear edges in the image as well as on the color distribution in the image." (EX1007, [0076].)

Daft Reply Decl. (EX1060), ¶30

'471 Reply (Paper 52), 4

Derakhshani-Tanii: Disputed Recitations

Disputed Recitation	'471 Claim(s) Or Element	'606 Claim(s) Or Element	'938 Claim(s) Or Element	'910 Claim(s) Or Element
"user"	1[pre], 10[pre]			1, 10, 22
"face"		1, 10, 19	1, 8, 17, 20	
"verifying . . . the user's ears[/features on a side of a user's head]"	3/12	3/12		3/12
"first [] data," "second [] data"	5[a]		5[a]	5[a]
"biometric data"	7/16	1[b], 10[c], 19[a]	1[a], 17[d]	7/16
"mapping of facial features"	8/17		7/24	

’471 Patent, Claims 3/12 And ’606 Patent, Claims 3/12

’471 Patent, Claim 3

3. The system according to claim **1**, further comprising verifying the presence of the user’s ears in the at least one first image, and verifying the absence or reduced visibility of the user’s ears in the at least one second image, wherein the first distance is larger than the second distance.

’606 Patent, Claim 3

3. The method according to claim **1**, further comprising verifying the presence of the user’s ears in the at least one first image, and verifying the absence or reduced visibility of the user’s ears in the at least one second image, wherein the first distance is larger than the second distance.

’910 Patent, Claims 3/12

’910 Patent, Claim 3

3. The system according to claim 1, further comprising verifying the presence of one or more features on a side of a user’s head in the at least one first image, and verifying the absence or reduced visibility of the one or more features on the side of the user’s head in the at least one second image due to image capture at different distances from the user’s head, wherein the first distance is larger than the second distance.

Derakhshani Teaches Verifying The User's Ears/Features On The Side Of The User's Head

Derakhshani

sensor. For example, a landmark (e.g., an iris, an eye corner, a nose, an ear, or a background object) may be identified and located in the plurality of images with different focus distances. A landmark's representation in a particular image has

Derakhshani (EX1005), 16:51-54

Dr. Turk

Q Okay. And so since the landmarks are identified in the image, that means the landmarks are present in the image, right?

A Image values are determined to be a landmark. So those image values are present in the image --

Q Okay.

A -- and assigned with a particular landmark's identity, I guess.

Turk Depo Tr. (EX1059), 141:18-25

'471 Petition (Paper 1), 16, 32; '471 Reply (Paper 52), 7

Derakhshani Teaches Verifying The User's Ears/Features On The Side Of The User's Head

Derakhshani

of view of the sensor. Degree of focus is a measure of the extent to the image of the landmark is blurred by optical effects in the light sensor (e.g., due to diffraction and convolution with the aperture shape). The degree of focus for a landmark in a particular image may be estimated by determining the high frequency components of the image signal in the vicinity of the landmark. When the landmark is in focus, more high frequency components in its vicinity are expected. When the degree of focus is low for a landmark, smaller high frequency components are expected. By comparing the

Derakhshani (EX1005), 16:57-66

Dr. Turk

Q What does it mean for a landmark to be blurred?

A To be displayed in the image of that landmark in a way that is not as sharp in the image as it could be.

Q Okay. So if it's not as sharp, it's harder to see; is that right?

A It's not harder to see the presence of --

Q Okay.

A -- but it might be hard to determine certain things about it.

Turk Depo Tr. (EX1059), 142:12-25

'471 Petition (Paper 1), 7, 22; '471 Reply (Paper 52), 8

Derakhshani-Tanii: Disputed Recitations

Disputed Recitation	'471 Claim(s) Or Element	'606 Claim(s) Or Element	'938 Claim(s) Or Element	'910 Claim(s) Or Element
"user"	1[pre], 10[pre]			1, 10, 22
"face"		1, 10, 19	1, 8, 17, 20	
"verifying . . . the user's ears[/features on a side of a user's head]"	3/12	3/12		3/12
"first [] data," "second [] data"	5[a]		5[a]	5[a]
"biometric data"	7/16	1[b], 10[c], 19[a]	1[a], 17[d]	7/16
"mapping of facial features"	8/17		7/24	

’471 Patent, Elements 1[d2], 1[d5], And 5[a]

’471 Patent, Element 1[d2]

processing the at least one first image or a portion to create first data;

’471 Patent, Element 1[d5]

processing the at least one second image or a portion thereof to create second data;

’471 Patent, Element 5[a]

5. The system according to claim **1**, further comprising comparing the first data, second data, or both to enrollment data derived from an enrollment image, the enrollment image captured and stored prior to an authenticating; and

’938 Patent, Elements 1[a], 1[b], And 5[a]

’938 Patent, Element 1[a]

receive or derive first biometric data from at least one first image of a user taken with a computing device camera located at a first distance from the user;

’938 Patent, Element 1[b]

receive or derive second biometric data from at least one second image of the user taken with the computing device camera located at a second distance from the user, the second distance being different than the first distance;

’938 Patent, Element 5[a]

5. The non-transient computer readable medium of claim **1** wherein the machine executable code is further configured to compare at least portions of the first data, second data, or both to enrollment data derived from an enrollment image, the enrollment image captured and stored prior to an authentication session; and

’910 Patent, Elements 1[d2], 1[d4], And 5[a]

’910 Patent, Element 1[d2]

processing the at least one first image or a portion thereof to create first data;

’910 Patent, Element 1[d4]

processing the at least one second image or a portion thereof to create second data;

’910 Patent, Element 5[a]

5. The system according to claim **1**, further comprising comparing the first data, second data, or both to enrollment data derived from an enrollment image, the enrollment image captured and stored prior to an authenticating; and

Derakhshani's "landmarks" And "features"

users 522, 524, 526, 528, 530). The authentication module may then process the image data to authenticate the user by determining if the image data matches a reference record for a recognized user identity that has been previously created based on image data collected during an enrollment session.

Derakhshani (EX1005), 16:57-66

sional shape. A three-dimensional model including locations of landmarks corresponding to an expected shape for a subject including the live eye of a user may be used for comparison to the detected landmark locations. In some implementations, the relative positions of landmarks on a particular user's face may be determined during an enrollment session and used generate a three-dimensional model that is stored as part of a reference record. In some implementations, three-dimen-

Derakhshani (EX1005), 17:29-36

cate the individual. For example, images of the white of a user's eye can be obtained and analyzed to compare features of the eye to reference record in order to authenticate the user and grant or deny the user access to a resource. Adversaries or

Derakhshani (EX1005), 4:21-24

'471 Petition (Paper 1), 7-8, 36; '471 Reply (Paper 52), 9; Daft Decl. (EX1003), ¶214; Daft Reply Decl. (EX1060), ¶173

Decision On Institution

Patent Owner's argument that Petitioner contradictorily relies on "landmarks" to teach "first data" and "second data" in claim 1 and "features" to teach "first data" and "second data" in claim 5 splits hairs. Prelim. Resp. 48–50. We understand Petitioner to use the terms "landmarks" and "features" synonymously. For example, Petitioner asserts that, in Derakhshani, a "landmark" may be a "user's eyes, nose, ears, and *other features*." Pet. 22 (emphasis added) (citations omitted). Similarly, Petitioner synonymously uses the terms "landmarks" and "features" when describing "processing the images to identify *feature landmarks*." Pet. 31 (emphasis added). Accordingly, we determine Petitioner does not contradict itself or inconsistently map Derakhshani to the claims.

IPR2025-00106 DI (Paper 17), 50

'471 Patent DI (Paper 17), 50

Derakhshani-Tanii: Disputed Recitations

Disputed Recitation	'471 Claim(s) Or Element	'606 Claim(s) Or Element	'938 Claim(s) Or Element	'910 Claim(s) Or Element
"user"	1[pre], 10[pre]			1, 10, 22
"face"		1, 10, 19	1, 8, 17, 20	
"verifying . . . the user's ears[/features on a side of a user's head]"	3/12	3/12		3/12
"first [] data," "second [] data"	5[a]		5[a]	5[a]
"biometric data"	7/16	1[b], 10[c], 19[a]	1[a], 17[d]	7/16
"mapping of facial features"	8/17		7/24	

’471 Patent, Claims 7/16 And ’606 Patent, Elements 1[b]/10[c]/19[a]

’471 Patent, Claim 7

7. The system according to claim 1, wherein the first data and the second data comprise biometric data.

’606 Patent, Element 1[b]

processing the at least one first image to obtain first biometric data from the at least one first image;

’938 Patent, Elements 1[a]/17[d] And ’910 Patent, Claims 7/16

’938 Patent, Element 1[a]

receive or derive first biometric data from at least one first image of a user taken with a computing device camera located at a first distance from the user;

’910 Patent, Claim 7

7. The system according to claim 1, wherein the first data and the second data comprise biometric data.

Derakhshani's Teaches "biometric data"

In some implementations, the spatial metric is a measure of the deviation of the subject from a two-dimensional plane. One possible spoofing strategy is to present a two dimensional image (e.g., a photograph) of a registered user's eye to the sensor. However the locations of landmarks (e.g., an eye, nose, mouth, and ear) in the two dimensional image will occur in a two dimensional plane, unlike landmarks in and around a real live eye. For example, the locations of multiple landmarks may be fit to the closest two dimensional plane and the average distance of the landmarks from this fit plane can be determined as the spatial metric. A high value for this spatial metric may indicate a three-dimensional subject and a higher likelihood that the subject is a live eye, while a low value may indicate a higher likelihood that the subject is a two-dimensional spoof attack.

Derakhshani (EX1005), 17:12-26

'471 Petition (Paper 1), 10, 28; '471 Reply (Paper 52), 10; Daft Reply Decl. (EX1060), ¶¶ 48, 50;

Derakhshani's Teaches "biometric data"

Dr. Turk

Q Okay. And what is the meaning of the term "biometric data" in your opinion?

A Again, I don't have a precise definition at the top of my -- tip of my tongue right now, but in general, it means -- very broadly, it means data about a human, human biology or body or something.

In the context of biometrics, and especially biometric security, it means data about a human or derived from a human that can be used for identity -- to determine identity.

Turk Depo Tr. (EX1059), 44:4-13

'471 Petition (Paper 1), 10, 28; '471 Reply (Paper 52), 10; Daft Reply Decl. (EX1060), ¶47

Derakhshani-Tanii: Disputed Recitations

Disputed Recitation	'471 Claim(s) Or Element	'606 Claim(s) Or Element	'938 Claim(s) Or Element	'910 Claim(s) Or Element
"user"	1[pre], 10[pre]			1, 10, 22
"face"		1, 10, 19	1, 8, 17, 20	
"verifying . . . the user's ears[/features on a side of a user's head]"	3/12	3/12		3/12
"first [] data," "second [] data"	5[a]		5[a]	5[a]
"biometric data"	7/16	1[b], 10[c], 19[a]	1[a], 17[d]	7/16
"facial features"	8/17		7/24	

’471 Patent, Claims 8/17 And ’938 Patent, Claims 7/24

’471 Patent, Claim 8

8. The system according to claim **1**, wherein the first data and the second data comprise a mapping of facial features.

’938 Patent, Claim 7

7. The non-transient computer readable medium of claim **1** wherein the first biometric data and the second biometric data comprise image data of facial features.

Derakhshani's Teaches "facial features"

the sensor. However the locations of landmarks (e.g., an eye, nose, mouth, and ear) in the two dimensional image will occur in a two dimensional plane, unlike landmarks in and around a real live eye. For example, the locations of multiple land-marks may be fit to the closest two dimensional plane and the average distance of the landmarks from this fit plane can be determined as the spatial metric. A high value for this spatial

Derakhshani (EX1005), 17:16-19

'471 Petition (Paper 1), 10, 32; '471 Reply (Paper 52), 10; Daft Reply Decl. (EX1060), ¶¶20, 47, 50

Derakhshani's Teaches "facial features"

Derakhshani

the sensor. However the locations of landmarks (e.g., an eye, nose, mouth, and ear) in the two dimensional image will occur in a two dimensional plane, unlike landmarks in and around a real live eye. For example, the locations of multiple land-

Derakhshani (EX1005), 17:16-19

Dr. Turk

Q Okay. How would you describe what the term "face" means?

A Generally, I would describe it as the part of -- assuming we're talking about humans here, the part of the human's head that is on the front side of the head, in general, and includes what people tend to refer to as features, such as eyes, nose, mouth, eyebrows, forehead and such, but I don't have an exact definition in mind at the moment.

Turk Depo Tr. (EX1059), 42:22-43:5

'471 Petition (Paper 1), 10, 32; '471 Reply (Paper 52), 10

Derakhshani-Tanii Combination

Petitioner's Motivation To Combine

3. Motivation to Combine

A POSITA would have been motivated to combine Derakhshani and Tanii because both identify and account for the three-dimensionality of a face when capturing an image. *Daft*, ¶134. They differ, however, in what principles are used to account for that three-dimensionality: Derakhshani uses changes in focus distance and/or parallax effect (§VII.A.1-(Derakhshani)), whereas Tanii looks for distortions in a face caused by the interaction between the camera's lens and the distance from the imaged object (§VII.A.2-(Tanii); *Daft*, ¶134). A POSITA would have appreciated, however, that Tanii merely recognizes an obvious alternative to evaluating the depth of a face—consistent with Derakhshani's existing two approaches—and a POSITA would have been motivated to incorporate Tanii's evaluation into Derakhshani. *Id.*

'471 Petition (Paper 1), 12

'471 Petition (Paper 1), 12

Petitioner's Motivation To Combine

A POSITA would have also had particular motivation to substitute Derakhshani's existing approaches with Tanii's distance-induced distortion analysis. *Daft*, ¶139. Specifically, a POSITA would have understood that implementing Derakhshani's focus-distance approach requires a camera with the ability to set a focal plane at a distance with extreme sensitivity to selectively blur nearby objects at different distances. *See Derakhshani*, 16:48-51; *Daft*, ¶139 (citing Ex-1029). A POSITA would have also understood the cameras often found in mobile devices do not have this ability; mobile devices typically incorporate wide-angle lenses to capture a wide field of view with a large depth of field because of their small size. *Tanii*, [0007]; *Daft*, ¶140 (citing Ex-1017, Ex-1030). In other words, a POSITA would have known there is not enough room in mobile devices to incorporate large image sensors and optics to fine-tune the focus distance to induce blurring of out-of-plane objects. *Daft*, ¶140; Ex-1031.

'471 Petition (Paper 1), 14

'471 Petition (Paper 1), 14

Decision On Institution

> Petitioner notes that to implement Derakhshani's focus-distance approach requires a camera with the ability to set a focal plane with extreme sensitivity and that cameras in mobile phones often do not have this ability. Pet. 14 (citing Ex. 1003 ¶ 140; Ex. 1007 ¶ 7). Therefore, especially in the case of mobile phones, "a POSITA would have been motivated to modify Derakhshani . . . to capture at least two images at different *actual* distances and evaluate whether they exhibit different degrees of distance-induced (barrel/fish-eye) distortion, as Tanii suggests." *Id.* at 14–15 (citing Ex. 1003 ¶ 141). Petitioner argues that both techniques involve the application of

IPR2025-00106 DI (Paper 17), 31-32

> At this stage of the proceeding, we are persuaded that Petitioner has established a reasonable likelihood that a person of ordinary skill would have combined the teachings of Derakhshani and Tanii for the reasons provided by Petitioner and summarized above. Patent Owner's argument

IPR2025-00106 DI (Paper 17), 32

'471 Patent DI (Paper 17), 31-33

Decision On Institution

1981). As noted above, Petitioner proposes to modify "Derakhshani . . . to capture at least two images at different *actual* distances and evaluate whether they exhibit different degrees of distance-induced (barrel/fish-eye) distortion, as Tanii suggests." *Id.* at 14–15 (citing Ex. 1003 ¶ 141). Thus, Petitioner relies on Tanii for its teaching of evaluating distance induced distortions in a face caused by the camera's lens and the distance from the object. Pet. 12. Petitioner does not propose to modify Derakhshani by incorporating Tanii's teaching of correcting the distortion. At this stage of the proceeding, we do not agree with Patent Owner that combining Tanii with Derakhshani would destroy Derakhshani's basic objective. Further, at this stage, we also agree that improving Derakhshani's spoof detection and substituting techniques for spoof detection adequately supports the combination. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007).

IPR2025-00106 DI (Paper 17), 32-33

'471 Patent DI (Paper 17), 31-33

Roadmap

1. The FaceTec Patents

2. Instituted Grounds and Prior Art
   a. Derakhshani-Tanii
   b. **Zhang-Tanii**
   c. Hoyos
   d. Tanii is analogous art

Zhang

Zhang

(57) **ABSTRACT**

Multiple images including a face presented by a user are accessed. One or more determinations are made based on the multiple images, such as a determination of whether the face included in the multiple images is a 3-dimensional structure or a flat surface and/or a determination of whether motion is present in one or more face components (e.g., eyes or mouth). If it is determined that the face included in the multiple images is a 3-dimensional structure or that that motion is present in the one or more face components, then an indication is provided that the user can be authenticated. However, if it is determined that the face included in the multiple images is a flat surface or that motion is not present in the one or more face components, then an indication is provided that the user cannot be authenticated.

Zhang (EX1006), Abstract

Zhang

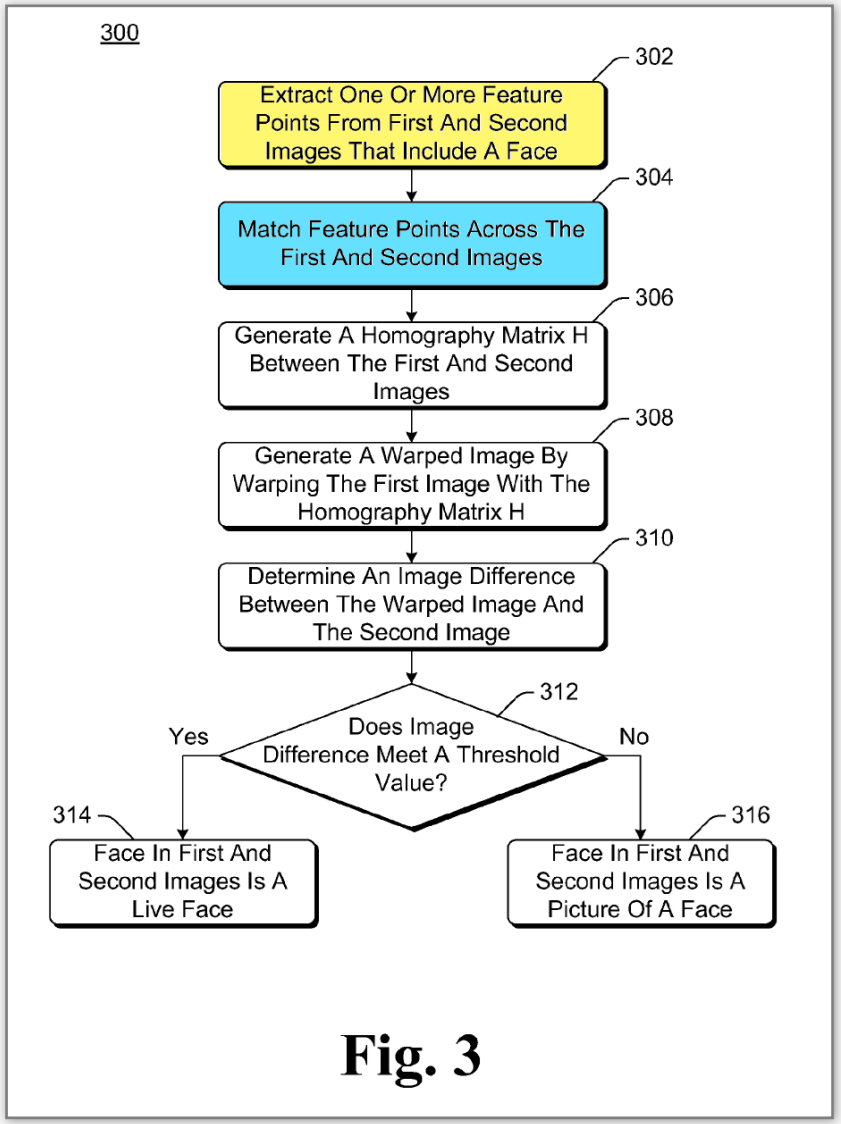


Fig. 3

Zhang (EX1006), Fig. 3

[0027] In process **300**, one or more feature points are extracted from two images, referred to in process **300** as the first and second images (act **302**). These first and second images each include a face of the same person, and can be, for example, images **106** of FIG. **1**. The one or more feature points are feature points of the face in the first and second images. A variety of different feature points can be extracted, such as a corner of an eye, a corner of a mouth, a tip of a nose, and so forth. Each feature point is a single pixel or a region of

Zhang (EX1006), [0027]

[0028] The feature points extracted in act **302** are matched across the first and second images (act **304**). This matching of the feature points across the first and second images refers to identifying the locations of the same feature points in each of the two images. For example, the locations of the same corner of the same eye in the face in the first and second images are identified. The matching of feature points across the first and

Zhang (EX1006), [0028]

Zhang

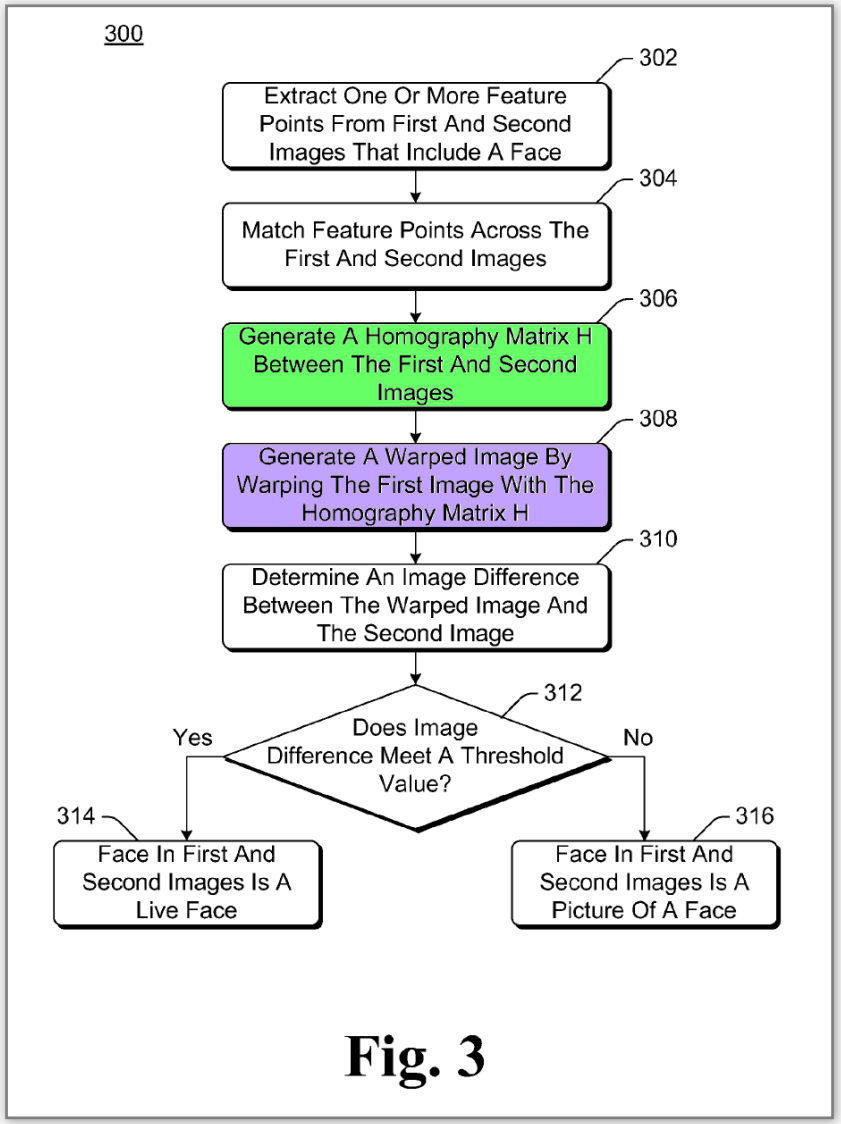


Fig. 3

Zhang (EX1006), Fig. 3

[0029] A homography matrix H between the first and second images is generated (act **306**). The first and second

Zhang (EX1006), [0029]

[0030] A warped image is then generated by warping the first image with the homography matrix H (act **308**). This homography matrix H is the homography matrix H generated in act **306**. The first image is warped based on the calculation

Zhang (EX1006), [0030]

'471 Petition (Paper 1), 49; Daft Reply Decl. (EX1060), 39

Zhang

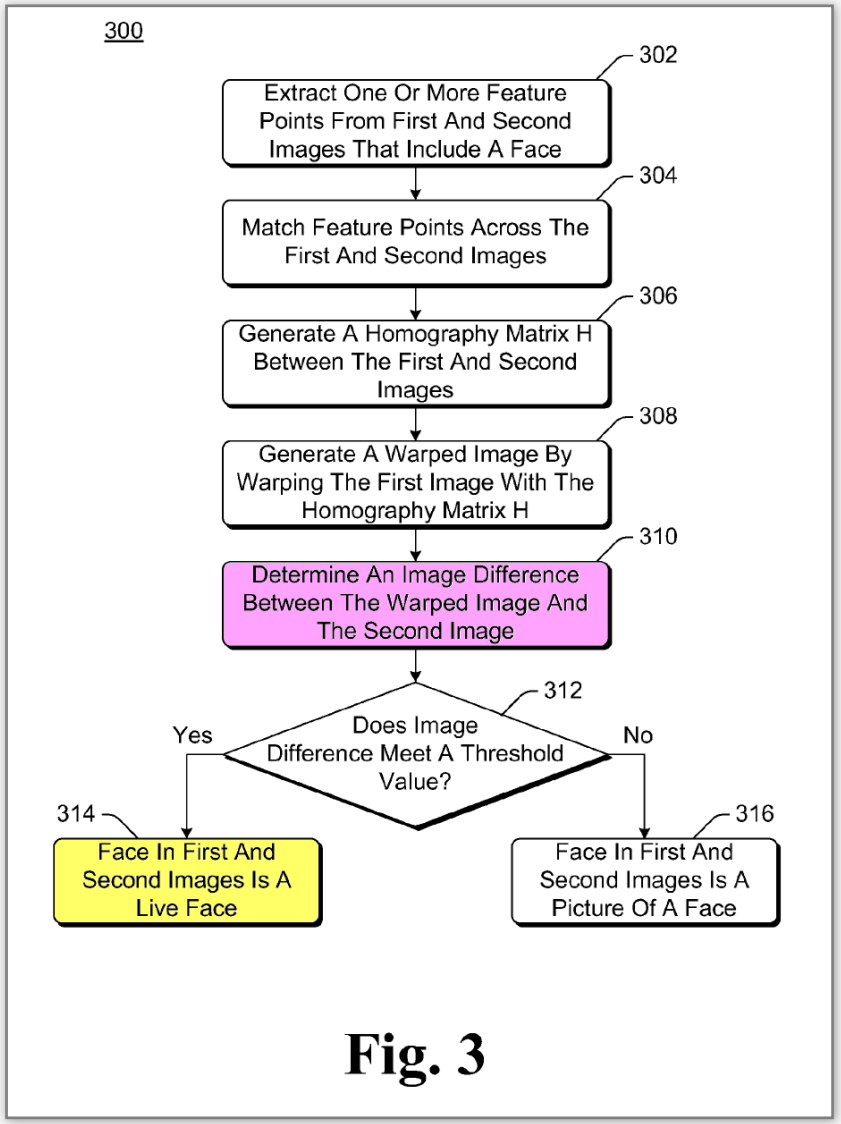


Fig. 3

Zhang (EX1006), Fig. 3

[0031] An image difference between the warped image (generated in act **308**) and the second image is determined (act **310**). The image difference can be computed in different manners. In one or more embodiments, the warped image and

Zhang (EX1006), [0031]

[0034] If the image difference meets the threshold value, then the face in the first and second images is determined to be a live face (act **314**). However, if the image difference does

Zhang (EX1006), [0034]

'471 Petition (Paper 1), 49, 62; Daft Reply Decl. (EX1060), 39

Zhang-Tanii: Disputed Recitations

Disputed Recitation	'471 Claim(s) Or Element	'606 Claim(s) Or Element	'938 Claim(s) Or Element	'910 Claim(s) Or Element
"[expected] differences" from movement/different distances	1[d7], 10[g]	1[f], 10[g], 19[d]	1[c], 8[c] & 8[f], 17[d] & 17[e], 20[f] & 20[g]	1[d5], 10[f], 22[d]
★ "verifying . . . the user's ears[/features on a side of a user's head]"	3/12	3/12		3/12
★ "biometric data"	7/16	1[b], 10[c], 19[a]	1[a], 17[d]	7/16

★ For the Zhang-Tanii Grounds, Patent Owner recycles the same arguments from the Derakhshani-Tanii Grounds

Zhang-Tanii: Disputed Recitations

Disputed Recitation	'471 Claim(s) Or Element	'606 Claim(s) Or Element	'938 Claim(s) Or Element	'910 Claim(s) Or Element
"[expected] differences" from movement/different distances	1[d7], 10[g]	1[f], 10[g], 19[d]	1[c], 8[c] & 8[f], 17[d] & 17[e], 20[f] & 20[g]	1[d5], 10[f], 22[d]
★ "verifying . . . the user's ears[/features on a side of a user's head]"	3/12	3/12		3/12
★ "biometric data"	7/16	1[b], 10[c], 19[a]	1[a], 17[d]	7/16

★ For the Zhang-Tanii Grounds, Patent Owner recycles the same arguments from the Derakhshani-Tanii Grounds

’471 Patent, Elements 1[d7]/10[g]

’471 Patent, Element 1[d7]

authenticating the user when differences between the first data and the second data have expected distortion resulting from movement of the camera from the first location to the second location or movement of the user from the first location to the second location, which causes the change in distance between the user and the camera.

’606 Patent, Elements 1[f]/10[g]/19[d]

’606 Patent, Element 1[f]

comparing the first biometric data to second biometric data to determine whether differences between the at least one first image and the at least one second image match expected differences resulting from movement of the camera or the user which changed the distance between the user and camera from the first distance to the second distance;

’938 Patent, Elements 1[c]/8[c] & 8[f]/ 17[d] & 17[e]/20[f] & 20[g]

’938 Patent, Element 1[c]

compare the first biometric data with second biometric data for expected differences that result from characteristics of a human face and the at least one first image and the at least one second image being captured at different distances from the user;

’910 Patent, Elements 1[d5]/10[f]/22[d]

’910 Patent, Element 1[d5]

compare the first biometric data with second biometric data for expected differences that result from characteristics of a human face and the at least one first image and the at least one second image being captured at different distances from the user;

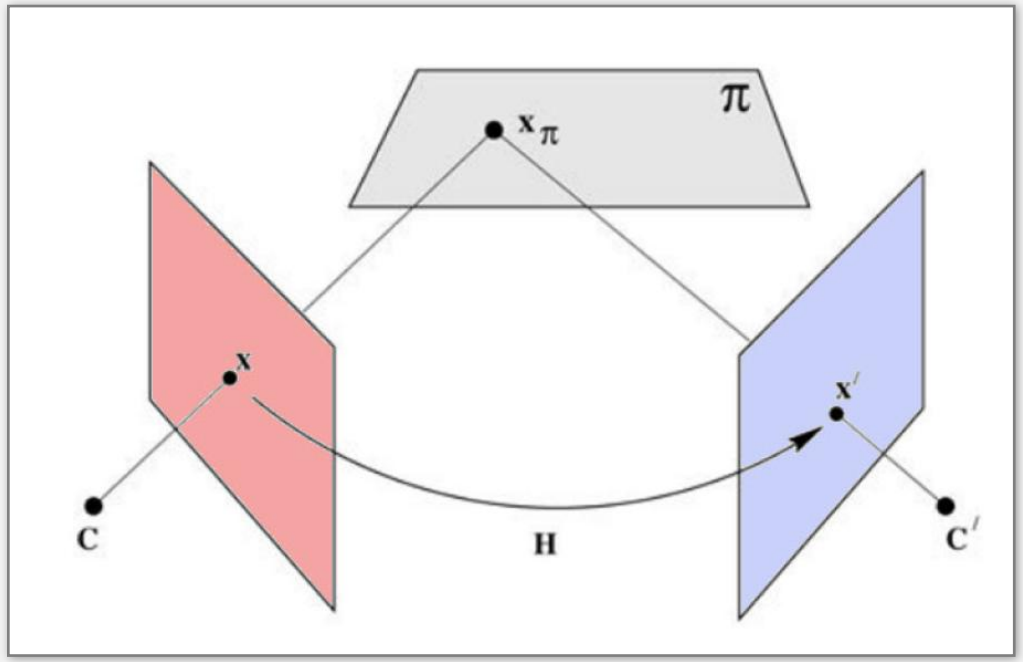
Zhang

Zhang

homography matrix, also referred to herein as matrix H. The homography based technique leverages the fact that two views of a flat (planar) surface are related based on a homography matrix H. Accordingly, in analyzing a first image and a

Zhang (EX1006), [0025]

Hartley Book



EX1023, 40 (annotated)

'471 Petition (Paper 1), 48, 61-62

Zhang Teaches "[expected] differences" From Movement/Different Distances

[0030] A warped image is then generated by warping the first image with the homography matrix H (act **308**). This homography matrix H is the homography matrix H generated in act **306**. The first image is warped based on the calculation

Zhang (EX1006), [0030]

[0031] An image difference between the warped image (generated in act **308**) and the second image is determined (act **310**). The image difference can be computed in different manners. In one or more embodiments, the warped image and

Zhang (EX1006), [0031]

'471 Petition (Paper 1), 49, 61-62

Zhang's Feature Points

[0028] The feature points extracted in act **302** are matched across the first and second images (act **304**). This matching of the feature points across the first and second images refers to identifying the locations of the same feature points in each of the two images. For example, the locations of the same corner of the same eye in the face in the first and second images are identified. The matching of feature points across the first and

Zhang (EX1006), [0028]

'471 Petition (Paper 1), 48, 60

Zhang's "selected locations"

[0032] In one or more embodiments, the image difference in act **310** is determined by obtaining the difference in color or intensity values between the warped and second images for each location in the warped and second images. In other embodiments, the image difference in act **310** is determined by obtaining the difference in color or intensity values between the warped and second images for selected locations in the warped and second images. The selected locations can be identified or selected in different manners. For example, any of a variety of conventional face detection algorithms or face recognition algorithms can be used to detect the face within each image, and the selected locations are the locations that are part of a face within at least one of the warped and second images. By way of another example, a conventional face detection algorithm can be used to detect various sets of sub-regions within a face (such as eyes, mouth, nose, and so forth), and the selected locations are the locations that are part of a sub-region in at least one of the warped and second images.

Zhang (EX1006), [0032]

'471 Petition (Paper 1), 61-63

Zhang's Feature Points And "selected locations"

Dr. Daft

feature points. Using Zhang's example of the corner of the eye as the "location," it would make sense for the comparison between the two images to be a comparison of the same feature point, such as the same corner of the same eye because otherwise a difference in color/intensity value may be due to different features points having different colors or intensity values due to, e.g., the user moving. For example, the color of the corner of an eye is likely to be different than the color of the corner of a mouth, thereby a comparison of the same pixel position having two different feature points (as Dr. Turk suggests) would not be indicative of whether the face is a 3D structure or a flat surface. Thus, Zhang's feature points are used for both generating the homography matrix H and the comparison of the images (part of authenticating the user).

Daft Reply Decl. (EX1060), ¶70

'471 Reply (Paper 52), 12-13; Daft Reply Decl. (EX1060), ¶70

Zhang-Tanii Combination

Petitioner's Motivation To Combine

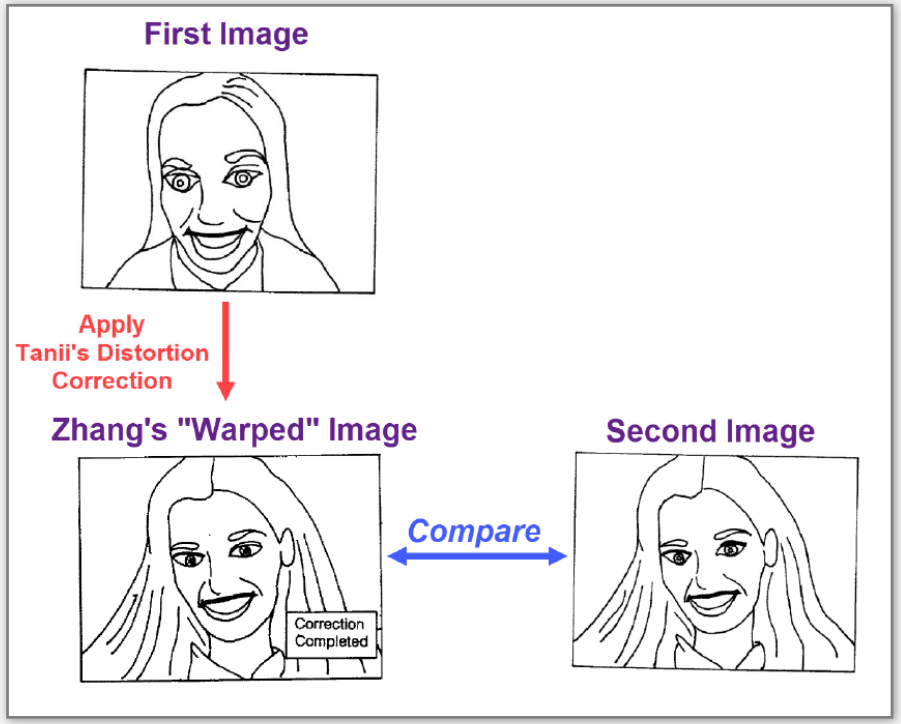
A POSITA would have therefore appreciated from Tanii that, even without modification, images captured by Zhang may exhibit distance-induced distortions, particularly when a wide-angle camera common in computers and mobile devices is used. *Id.*, ¶262. However, a POSITA would have also appreciated that any distance-induced distortions would *enhance* Zhang's process because a homography transformation would not correct for distance-induced distortions. *Id.* For instance,

* * *

Accordingly, a POSITA would have been motivated to use Zhang's existing process, but take advantage of the distance-induced distortions identified by Tanii by using a (wide-angle) camera that induces these distortions at different distances, and capturing two images of the face at different distances, because Zhang's procedure would identify the two images as different due to the differences in distance-induced distortion and verify three-dimensionality. *Id.*, ¶¶263-64.

'471 Petition (Paper 1), 50-51

Petitioner's Motivation To Combine



'471 Petition (Paper 1), 52

But a POSITA would have also been motivated to modify Zhang's process in view of Tanii in either of two additional ways.

First, a POSITA would have been motivated to perform Zhang's three-dimensional verification process, but rather than "warp" one image using a homography transform to compare it to the second image and evaluate the two for differences, a POSITA would "warp" (i.e., correct) the "close" image using Tanii's distortion-correction procedure to compare it to the "far" image and evaluate the two for differences.

'471 Petition (Paper 1), 52

Tanii

Dr. Daft

shows that he misunderstands Tanii. A POSITA would have understood that Tanii's figures are simplified line drawings that portray abstract representations of the distance-induced distortions caused by the optical effects. (EX1007, [0048], [0049], [0056].) An actual captured image, on the other hand, includes far more information. Thus, Tanii's figures do not depict the level of detail of a captured image. Tanii does not cause ears to "miraculously appear," as Dr. Turk asserts. Instead, barrel (aka perspective) distortion is portrayed: the magnification is changing based on the distance from the image center due to how the camera lens works. (EX1003, ¶¶46-51.) Given that Tanii's figures are simplified and abstract

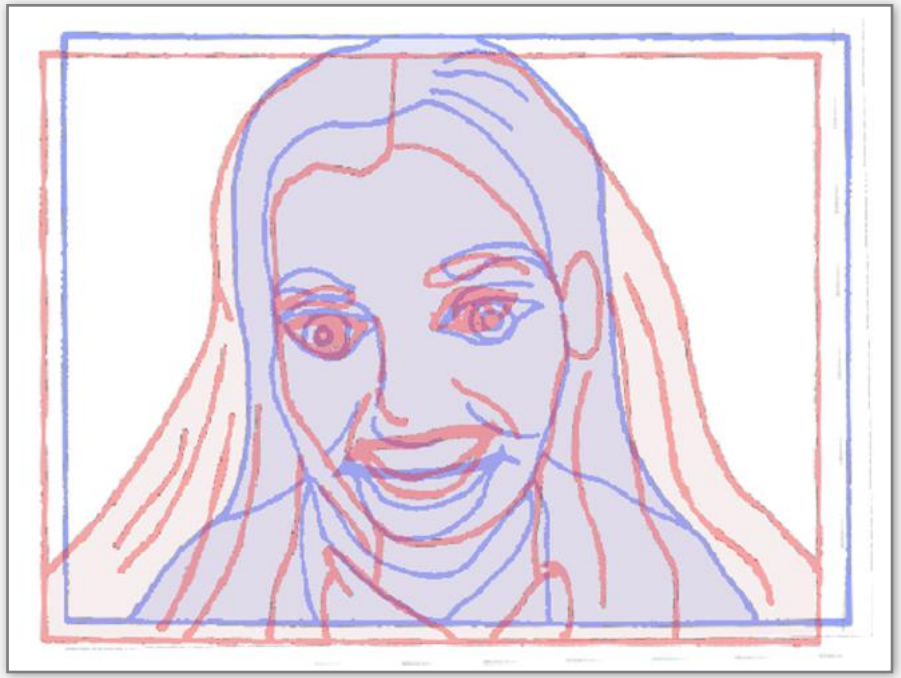
depictions, a POSITA would have understood that the ears are present in the actual captured image corresponding to Figure 4B, but because of the magnification, the ears are difficult to see. For example, the rightmost image (below) has ears that are present, but is difficult to see with the human eye due the distance-induced distortion. In those photographs, the user's ears appear increasingly distorted (reduced in lateral size compared with other facial features) as the distance between the sensor and the user is reduced. Also consistent with Tanii's figures, the user's nose exhibits distortion where it is relatively enlarged as this distance is reduced.

Daft Reply Decl. (EX1060), ¶75

'471 Petition (Paper 1), 52

'471 Reply (Paper 52), 14-15; Daft Reply Decl. (EX1060), ¶75

Petitioner's Motivation To Combine



'471 Petition (Paper 1), 53

Alternatively, a POSITA would have appreciated the combination of Zhang and Tanii could be further simplified by eliminating the need to mathematically transform one image. *Daft*, ¶¶267-68. Instead, when evaluating two images for different degrees of distance-induced distortion, the two images (one "close", one "far") could be compared directly to determine whether they exhibit expected differences in degree of distance-induced distortions. *Id.*

'471 Petition (Paper 1), 53

Roadmap

1. The FaceTec Patents

2. Instituted Grounds and Prior Art
   a. Derakhshani-Tanii
   b. Zhang-Tanii
   c. **Hoyos**
   d. Tanii is analogous art

Hoyos

Hoyos

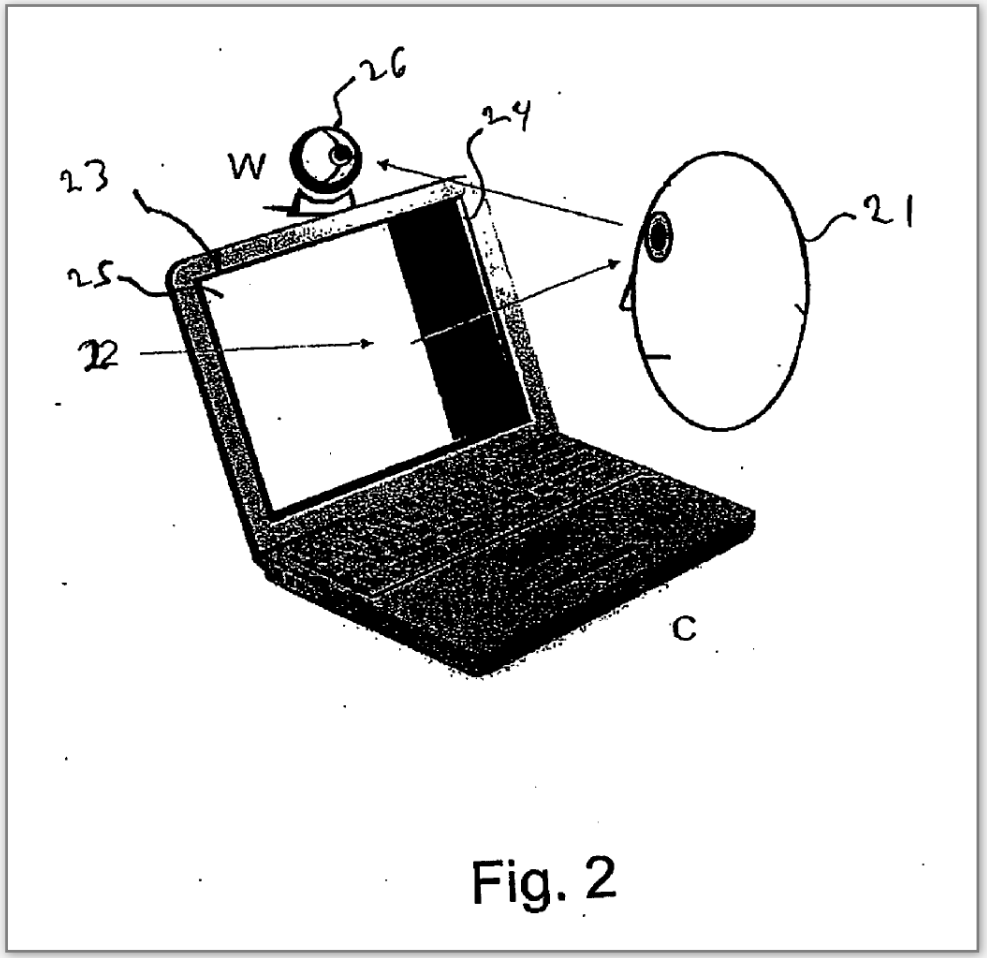


Fig. 2

Hoyos (EX1010), Fig. 2

of a live person **21** is shown. First, an image is displayed on a screen **23** with a black bar **24** on the right and a white area **25** on the left, and an image from a web-camera **26** that the person **21** looks at is recorded. A second image is displayed on the screen (not shown), but this time the black bar is on the left and the white area is on the right and a second image from the web-camera **26** is recorded.

Hoyos (EX1010), [0034]

[0035] The difference between the two images is recorded and the difference at each pixel is squared. The images are then blurred by convolving with a low-pass filter and then threshold the image. Areas above threshold are areas of change between the two images. The system expects to see a change primarily on the cornea, where a sharp image of the screen is reflected.

Hoyos (EX1010), [0035]

Hoyos: Disputed Recitations

Disputed Recitation	’471 Claim(s) Or Element	’606 Claim(s) Or Element	’938 Claim(s) Or Element	’910 Claim(s) Or Element
“reflection . . . off of the user’s face/[from a face of the user]”	18			18

’471 Patent, Claim 18

18. The method according to claim **10**, further comprising displaying an image on a screen of the computing device while capturing the at least one first image and/or the at least one second image, and processing the at least one first image and/or the at least one second image to detect a reflection of the displayed image off of the user’s face.

’910 Patent, Claim 18

18. The method according to claim **10**, further comprising illuminate a screen of a computing device while capturing the at least one first image and/or the at least one second image, and processing the at least one first image and/or the at least one second image to detect a reflection of the illumination from a face of the user.

Hoyos Teaches A "reflection . . . off of the user's face"

Hoyos

[0018] In some embodiments a first image is presented on a computer screen, wherein the computer screen is oriented to face a user; at least one camera is positioned proximate the computer screen, wherein the at least one camera is oriented to face the user so that light emitted by the computer screen as the first image is reflected by the user and captured by the at least one camera; obtaining a second image through the at least one camera; and determining whether at least a portion of the second image includes a representation of the first image on the computer screen reflected by a curved surface consistent with a human eye.

Hoyos (EX1010), [0018]

Dr. Turk

Q Sure. My question was, so the reflection of the curved surface of the eye is determined only for the second image in the embodiment of paragraph 18; is that right?

A That is my understanding, yes.

Turk Depo. Tr. (EX1059), 123:6-10

Roadmap

1. The FaceTec Patents

2. Instituted Grounds and Prior Art
   a. Derakhshani-Tanii
   b. Zhang-Tanii
   c. Hoyos
   d. **Tanii is analogous art**

Tanii Is Analogous Art

Same Field Of Endeavor

’471 Patent

based on known and trusted enrollment data. In addition or as an alternative, the known specifications of a mobile phone camera for a given model may be utilized to predict the expected distortion of the person’s facial features at different distances from the lens. Thus, the authentication may be

’471 Patent (EX1001), 30:1-5

Tanii

[0007] In particular, cellular phones in which a digital camera is mounted are already on the market, and it is foreseen that in the future cellular phones will be used as TV phones by which to capture the image of the user’s face while he is talking through the phone. With a cellular phone containing a camera, the lens is adjusted to have a wide-angle focal length such that the face of the user captured in the image is appropriately sized. When the user’s face is close to the camera when such an optical system is used, the exaggeration warp becomes more noticeable.

Tanii (EX1007), [0007]

’471 Petition (Paper 1), 10, 14, 37; ’471 POPR (Paper 6), 2; ’471 POR (Paper 43), 58

Reasonably Pertinent To The Same Problem

’471 Patent

13A and 13B. Typical cameras on a mobile device or any other device include a curved lens. This results in a “fish-eye” effect in the resulting images taken by the camera. In

’471 Patent (EX1001), 28:36-38

The fish-eye effect becomes more pronounced on an image of a person’s face when the person images his or her face close to the lens. The effect results in the relative dimensions of the person’s face appearing different than when the imaging is done with the person’s face farther away from the lens. For example, a person’s nose may

’471 Patent (EX1001), 28:45-50

Tanii

[0007] In particular, cellular phones in which a digital camera is mounted are already on the market, and it is foreseen that in the future cellular phones will be used as TV phones by which to capture the image of the user’s face while he is talking through the phone. With a cellular phone containing a camera, the lens is adjusted to have a wide-angle focal length such that the face of the user captured in the image is appropriately sized. When the user’s face is close to the camera when such an optical system is used, the exaggeration warp becomes more noticeable.

Tanii (EX1007), [0007]

Roadmap

1. The FaceTec Patents
2. Instituted Grounds and Prior Art
3. **POSITA Level and Dr. Daft**
4. RPI / Privity
5. Secondary Considerations

POSITA Level And Dr. Daft

Proposed POSITA Levels

Petitioner	Patent Owner
a Bachelor's degree in electrical engineering, computer engineering, computer science, physics, or a related field, and two years' work experience related to ***biometrics, facial authentication, computer vision, and/or optics***, such that they would have had significant academic and/or work experience in both ***software development and optics***. Formal education can substitute for work experience and relevant work experience could substitute for formal education.	a Bachelor's degree in electrical engineering, computer engineering, computer science, physics, or a related field, and two years' work experience related to ***biometric security, facial authentication, and three-dimensional computer vision*** such that they would have had significant academic and/or work experience in both ***facial biometrics and computer vision***.

'471 Petition (Paper 1), 5

'471 POR (Paper 43), 28-29

Petitioner's Proposed POSITA Level Is Proper

'471 Patent

(54) **FACIAL RECOGNITION AUTHENTICATION SYSTEM INCLUDING PATH PARAMETERS**

`471 Patent (EX1001), Title

Dr. Daft

41. Facial-recognition systems were a well-known type of biometric-security system. *Id.*, 32, 98-103. They typically incorporate the use of "computer vision"—programming a computer to identify distinguishing features (in this case, a face) in an image. *Id.*, 103 ("A typical face recognition system is composed of three

Daft Decl. (EX1003), ¶41

'471 Petition (Paper 1), 4; '471 Opp. to Mot. to Exclude (Paper 66), 5

Petitioner's Proposed POSITA Level Is Proper

(57) **ABSTRACT**

Systems and methods for enrolling and authenticating a user in an authentication system via a user's camera of camera equipped mobile device include capturing and storing enrollment biometric information from at least one first image of the user taken via the camera of the mobile device,

`471 Patent (EX1001), Abstract

One other such method may be through the use of biometrics. For example, an electronic device may have an optical reader that may scan a user's fingerprint to determine that the person requesting access to a device or an account is authorized. However, such fingerprint systems are often prohibitively expensive for use on a small electronic device or are often considered unreliable and unsecure.

`471 Patent (EX1001), 1:50-56

1. A system for authenticating three-dimensionality of a user via a user's camera equipped computing device, the computing device comprising:

`471 Patent (EX1001), 38:7-9

'471 Reply (Paper 52), 21; '471 Opp. to Mot. to Exclude (Paper 66), 6

Petitioner's Proposed POSITA Level Is Proper

One other such method may be through the use of biometrics. For example, an electronic device may have an optical reader that may scan a user's fingerprint to determine that the person requesting access to a device or an account is authorized. However, such fingerprint systems are often prohibitively expensive for use on a small electronic device or are often considered unreliable and unsecure.

`471 Patent (EX1001), 1:50-56

13A and 13B. Typical cameras on a mobile device or any other device include a curved lens. This results in a "fish-eye" effect in the resulting images taken by the camera. In some instances, this curvature may not be visible to the human eye, or may only be noticeable at certain focal lengths. The curvature or fish eye effect can vary with focal length or distance between the user and the lens. The degree of the fish-eye effect is dependent on the type of optics used in the camera's lens and other factors.

`471 Patent (EX1001), 28:36-44

'471 Petition (Paper 1), 4; '471 Opp. to Mot. to Exclude (Paper 66), 6

Petitioner's Proposed POSITA Level Is Proper

Derakhshani

TECHNICAL FIELD

The present disclosure relates to biometric authentication based on images of the eye.

Derakhshani (EX1005), 1:6-7

BACKGROUND

It is often desirable to restrict access to property or resources to particular individuals. Biometric systems may be used to authenticate the identity of an individual to either grant or deny access to a resource. For example, iris scanners may be used by a biometric security system to identify an individual based on unique structures in the individual's iris.

Derakhshani (EX1005), 1:11-16

of view of the sensor. Degree of focus is a measure of the extent to the image of the landmark is blurred by optical effects in the light sensor (e.g., due to diffraction and convolution with the aperture shape). The degree of focus for a

Derakhshani (EX1005), 16:57-60

'471 Opp. to Mot. to Exclude (Paper 66), 6-7

Dr. Daft

- Bachelor's and Master's degrees in Physics, Ph.D. in Materials Science
- 2+ years of experience in biometrics and user authentication (Qualcomm and General Electric)
- 2+ years of experience in computer vision and imaging systems (Siemens)
- 25+ years of experience in optics

Dr. Daft

Q. Did you have two years of work experience in the field of biometrics in August 2014?

A. I had done work in the biometric field, and I had worked for a good deal -- more than two years in related fields.

Q. Had you done two years of work experience in the field of biometrics in August 2014?

A. Putting together my experience at GE and my work at Qualcomm, that would be the two years work experience.

Daft Depo Tr. (EX2082), 68:8-17

Q. Can you please describe for me your experience in fields related to biometrics as of August of 2014?

A. Yes. The work experience that I had done involved a project, when I worked at General Electric, that was a biometric fingerprint recognition. And the -- that was for law enforcement and military applications.

As well as that, I had experience when I was a consultant to Qualcomm. And there the biometric work was on an improved way of having fingerprint authentication for cell phones.

Daft Depo Tr. (EX2082), 74:1-11

'471 Opp. to Mot. to Exclude (Paper 66), 7-8

Dr. Daft

Q. You testified also that you had more than two years' experience in computer vision as of August 2014.

Do you recall that?

A. Yes, I do.

Q. Can you please describe for me your experience in computer vision as of August 2014?

A. My computer vision experience, as of August 2014, involved interpreting medical images. This is very important because this can aid a physician in producing a better diagnosis.

So I would take the medical imaging data and apply computer vision technique to it in order that the -- in order to help the physician diagnose disease.

Daft Depo Tr. (EX2082), 73:8-20

'471 Opp. to Mot. to Exclude (Paper 66), 7-8

Dr. Daft

A. Because I have been working for more than 30 years in a field which has exactly the same physics as optics; and, therefore, I have a lot more work experience than someone with the bachelor's degree in electrical engineering and the two years work experience. So I think I am more qualified than the -- the bar for a POSITA here.

Daft Depo Tr. (EX2082), 71:10-16

Q. And you testified that you had, as of August 2014, more than two years experience in optics.

Do you recall that?

A. Yes.

Q. And could you please describe your experience in optics as of August 2014?

A. Yes. There's two types of experience involved there. The first is that the diagnostic ultrasound that I have spent -- I had spent the majority of my time from 1990 to 2014 -- involves exactly the same physics as optics.

And so, in my mind, that is optic experience. Also, I was involved in several projects that bridged ultrasound and optical systems and so those directly involved optical systems.

Daft Depo Tr. (EX2082), 72:22-73:7

Roadmap

1. The FaceTec Patents
2. Instituted Grounds and Prior Art
3. POSITA Level and Dr. Daft
4. **RPI / Privity**
5. Secondary Considerations

RPI / Privity

RPI / Privity

Decision on Institution

Patent Owner argues that iProov is a real party in interest because it challenged the validity of the '471 patent in both the Nevada and California litigations based primarily on the same references asserted in this Petition.

* * *

We disagree. The overlap in the prior art asserted in this proceeding and in the Nevada litigation is insufficient to demonstrate that iProov was directing Petitioner to file this Petition. Petitioner argues that it did not

IPR2025-00106 DI (Paper 17), 19

'471 Patent DI (Paper 17), 19

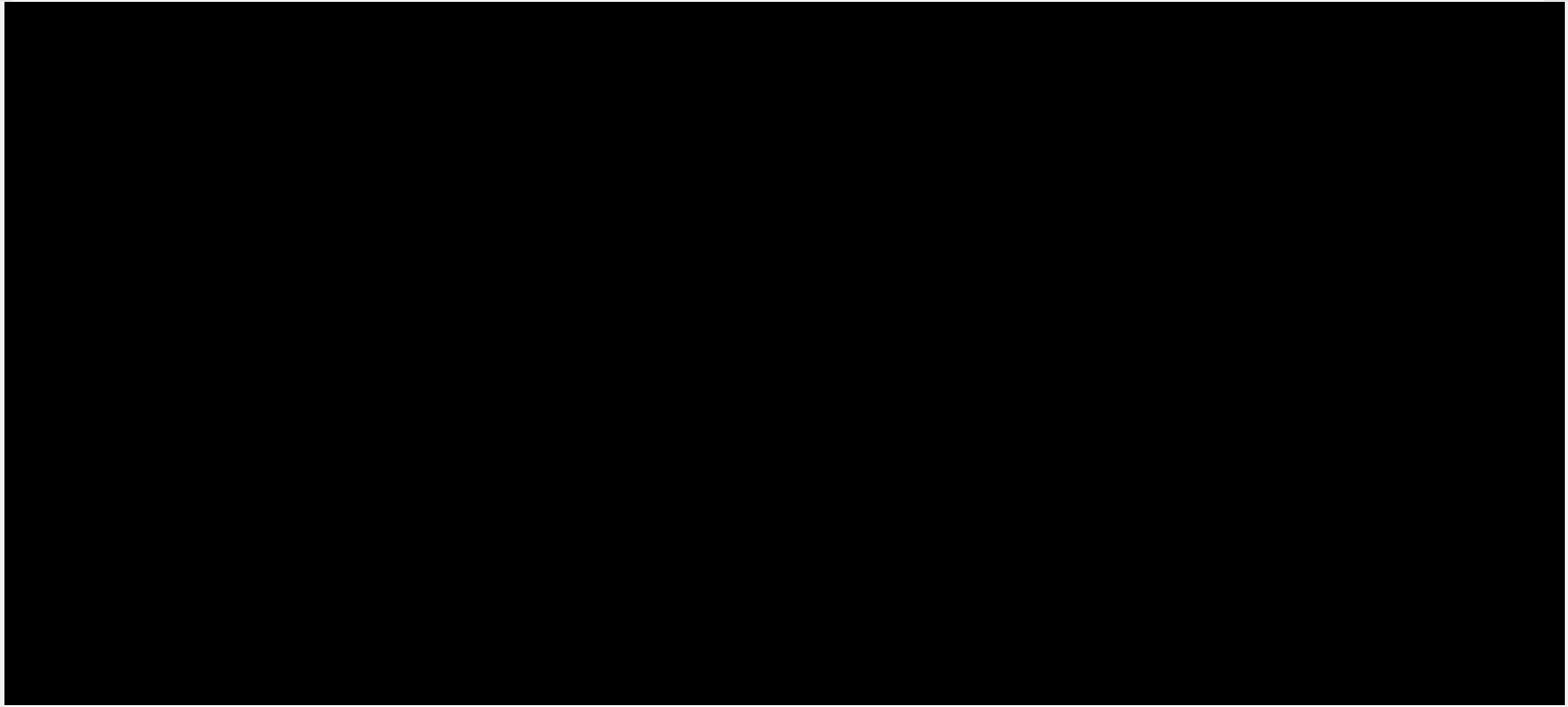
RPI / Privity

Decision on Institution

Finally, Patent Owner argues that iProov would stand to benefit from this Petition, perhaps even more than Petitioner, because it has customers beyond just Petitioner. Prelim. Resp. 17, 18. While it may be true that iProov would benefit if the challenged claims were held to be unpatentable, this fact alone does not demonstrate that Petitioner filed this Petition at the behest of iProov. *WesternGeco*, 889 F.3d at 1321 ("[A] common desire among multiple parties to see a patent invalidated, without more, does not establish privity.").

IPR2025-00106 DI (Paper 17), 21

iProov/Jumio Agreement



District Court

Order Granting Motion to Intervene

> iProov's interest is also "significantly protectable." This is a threshold inquiry, and "[n]o specific legal or equitable interest need be established. It is generally enough that the interest [asserted] is protectable under some law, and that there is a relationship between the legally protected interest and the claims at issue." *Sw. Ctr. for Biological Diversity*, 268 F.3d at 818. As FaceTec has recognized, Jumio "uses iProov liveness detection technology—not any new liveness detection technology proprietary to Jumio." (Dkt. No. 45 at 2.) iProov clearly has an interest in defending its proprietary technology against claims that it infringes Jumio's patents, and any finding of infringement by the accused iProov technology would necessarily affect iProov's interest. Moreover, iProov has an economic interest in the litigation because it has indemnified Jumio. (Dkt. No. 47-1, ¶ 7.)

EX2010, 4

iProov's Reply to FaceTec's Opposition

> 7. iProov and Jumio have entered into an agreement dated November 23, 2020, (the "iProov-Jumio Agreement"). The iProov-Jumio Agreement includes an indemnification obligation and was previously produced to FaceTec in the Nevada Action at Bates No. IP0255884–0255959.

EX2006 (Dkt. No. 47-1), ¶7

'471 Reply (Paper 52), 19; '471 POPR (Paper 6), 12; '471 POR (Paper 43), 66; '471 Sur-reply (Paper 59), 30-31

Jumio's Petitions

Ms. Kaiser

> 4. I personally worked on the Petitions and was the lead attorney on them. iProov did not direct, control, or fund the Petitions. iProov did not work on the Petitions nor was it involved with the Petitions in any way. Petitioner never provided drafts of the IPR Petitions to iProov, and Petitioner never discussed the IPR Petitions

EX1049, ¶4

'471 Reply (Paper 52), 20

Jumio's Petitions

Ms. Kaiser

5. I attest that iProov did not provide or suggest the prior art in the IPR Petitions to Petitioner, including Derakhshani and Zhang. Petitioner commissioned a prior art search independently to find prior art relevant to potential IPRs and the pending patent infringement action in the Northern District of California (*FaceTec, Inc. v. Jumio* Corp., C.A. No. 24-cv-03623). Petitioner knew about Derakhshani separate from that independent prior art search because it owns the Derakhshani patent. Petitioner did not have or look at the invalidity contentions in the Nevada action involving iProov (*FaceTec, Inc. v. iProov Ltd.*, C.A. No. 2:21-cv-02252) prior to filing the Petitions and the Petitions were not based on them.

EX1049, ¶5

'471 Reply (Paper 52), 20

Jumio's Petitions

Ms. Kaiser

6. With respect to Patent Owner's arguments that Petitioner and iProov coordinated on a joint set of invalidity contentions in the California action, any communications between Petitioner and iProov relating to those invalidity contentions occurred well *after* Petitioner filed the Petitions. Petitioner filed the Petitions on November 7, 2024. The invalidity contentions in the California case were initially due on December 27, 2024. On December 9, 2024, FaceTec, Jumio, and iProov submitted a stipulated request to extend the deadline to January 10, 2025, which the Court granted. The Court subsequently extended the deadline further to January 17, 2025, at iProov's request. Petitioner did not have any communications with iProov relating to the invalidity contentions in the California case before the Petitions were filed.

EX1049, ¶6

'471 Reply (Paper 52), 20

Roadmap

1. The FaceTec Patents
2. Instituted Grounds and Prior Art
3. POSITA Level and Dr. Daft
4. RPI / Privity
5. **Secondary Considerations**

Secondary Considerations

ZoOm

Dr. Turk

456. As set forth in the claim charts in Appendices A-H, FaceTec's software embodies and is coextensive with the challenged claims. Indeed, the core

Turk Decl. (EX2061), ¶456

Q Okay. So turning back to paragraph 456, Dr. Turk, you refer to FaceTec software. What do you mean by that?

A What I mean by that is what's in the citations. I believe the software is called ZoOm. I forget if there are other names or other versions but basically that.

Turk Depo Tr. (EX1059), 82:10-16

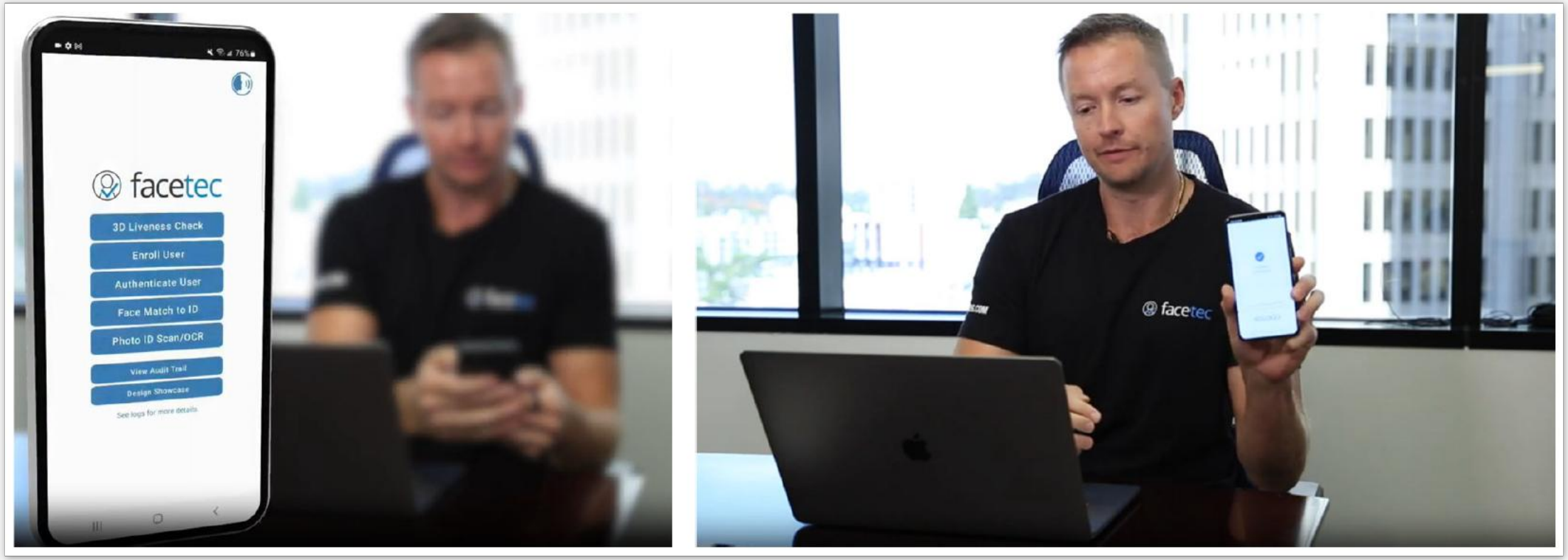
Liveness Decision

Mr. Rose

> At the end of the day, what we are providing back to the customer is essentially a true or false answer. So a successor -- when I say successfully prove 3D liveness, as we say, what we mean is that we received enough signal from the variety of checks and analyses and algorithms we're using such that we are extremely confident that what was presented was a real live human being in front of the camera and not some sort of spoof or attack.

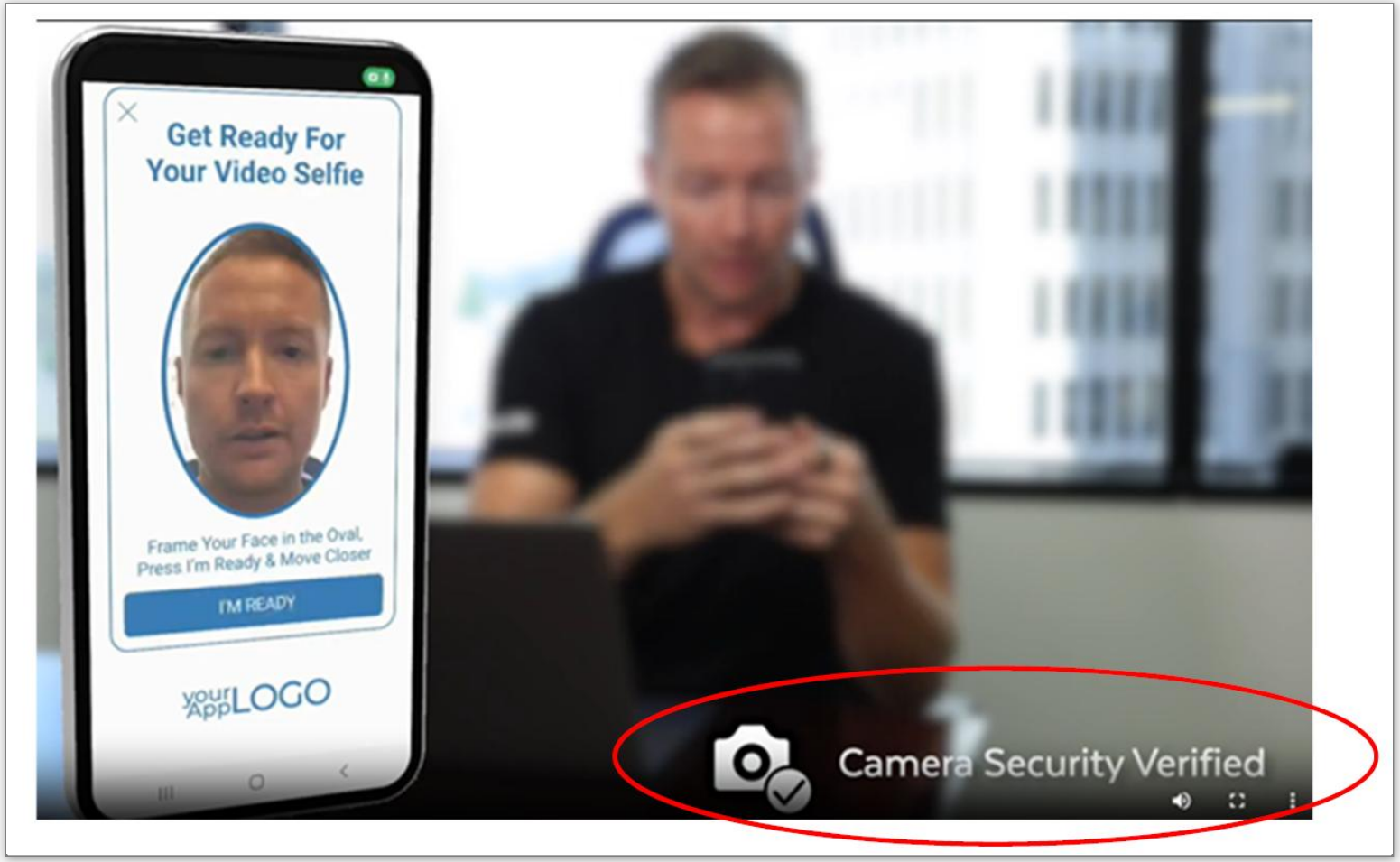
Rose Depo Tr. (EX1082), 75:13-21

Liveness Confirmed



EX2069, 00:20-00:45

Camera Control

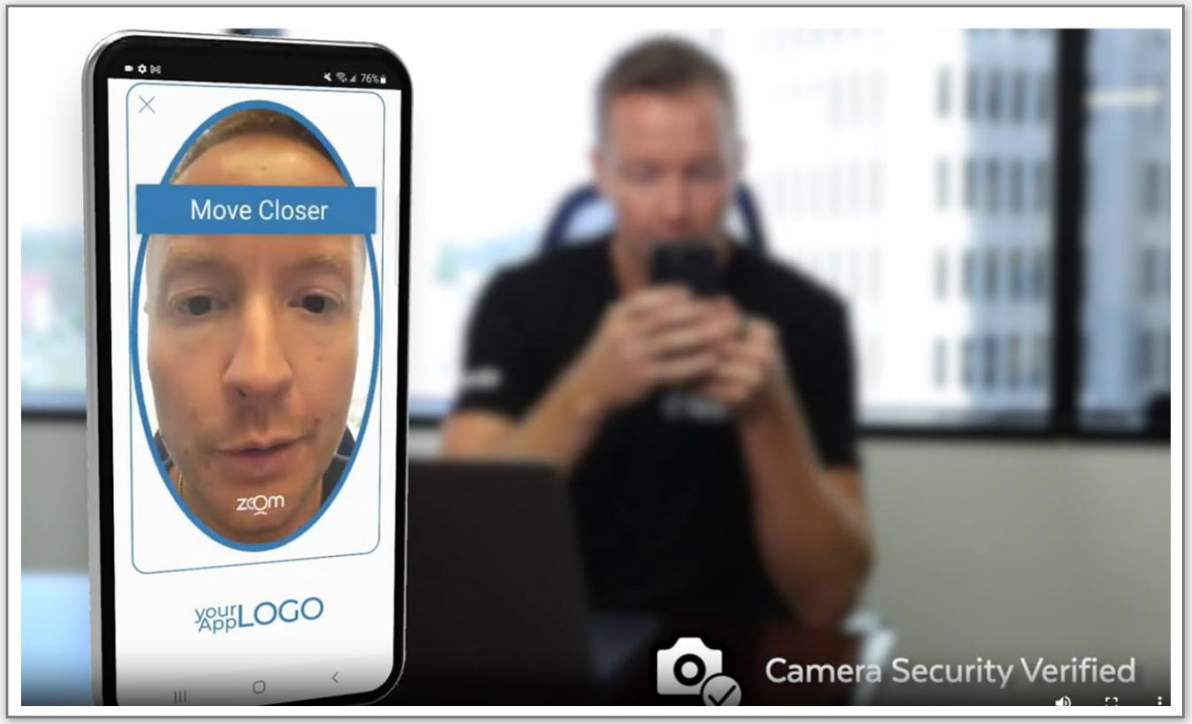


EX2069, 00:31 (annotated)

User Interface



EX2069, 00:31



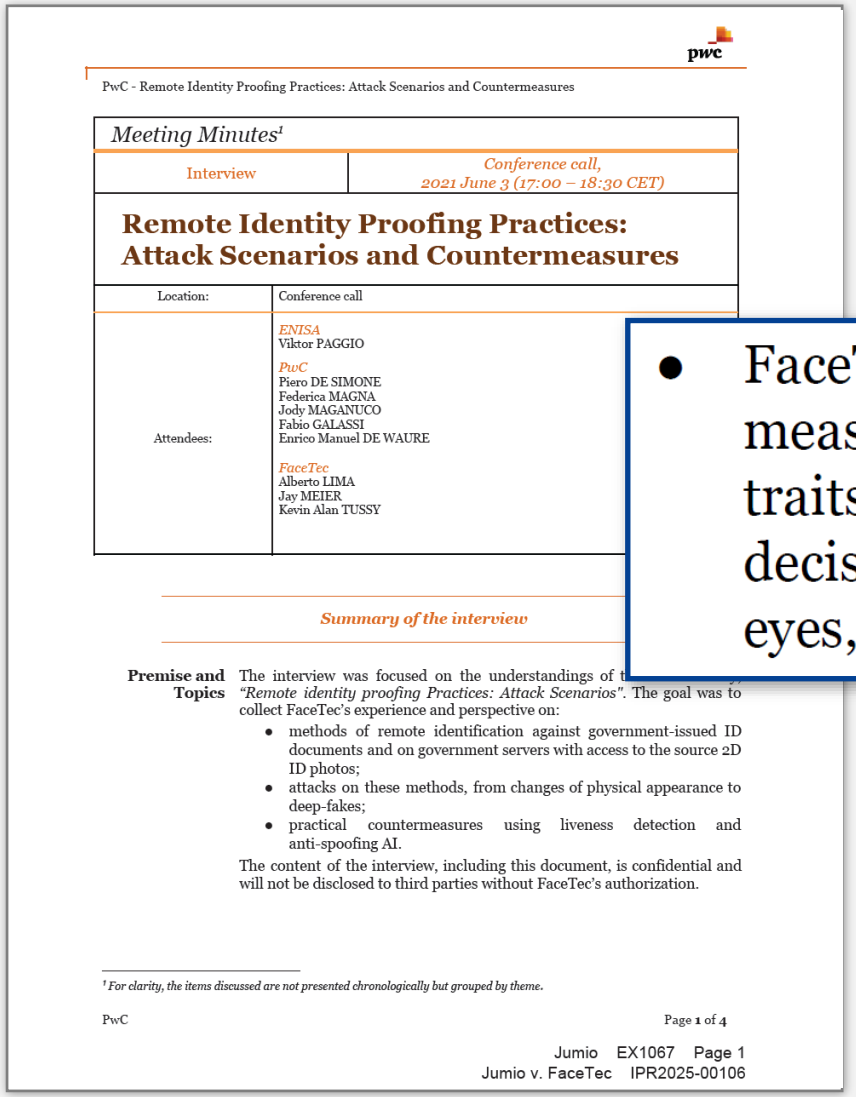
EX2069, 00:34

Data Encryption



EX2069, 00:37

Liveness Checks



pwc

PwC - Remote Identity Proofing Practices: Attack Scenarios and Countermeasures

Meeting Minutes[1]

Interview	*Conference call, 2021 June 3 (17:00 – 18:30 CET)*

Remote Identity Proofing Practices: Attack Scenarios and Countermeasures

Location:	Conference call
Attendees:	*ENISA* Viktor PAGGIO *PwC* Piero DE SIMONE Federica MAGNA Jody MAGANUCO Fabio GALASSI Enrico Manuel DE WAURE *FaceTec* Alberto LIMA Jay MEIER Kevin Alan TUSSY

Summary of the interview

Premise and Topics The interview was focused on the understandings of t… *"Remote identity proofing Practices: Attack Scenarios"*. The goal was to collect FaceTec's experience and perspective on:

- methods of remote identification against government-issued ID documents and on government servers with access to the source 2D ID photos;
- attacks on these methods, from changes of physical appearance to deep-fakes;
- practical countermeasures using liveness detection and anti-spoofing AI.

The content of the interview, including this document, is confidential and will not be disclosed to third parties without FaceTec's authorization.

[1] *For clarity, the items discussed are not presented chronologically but grouped by theme.*

PwC Page 1 of 4

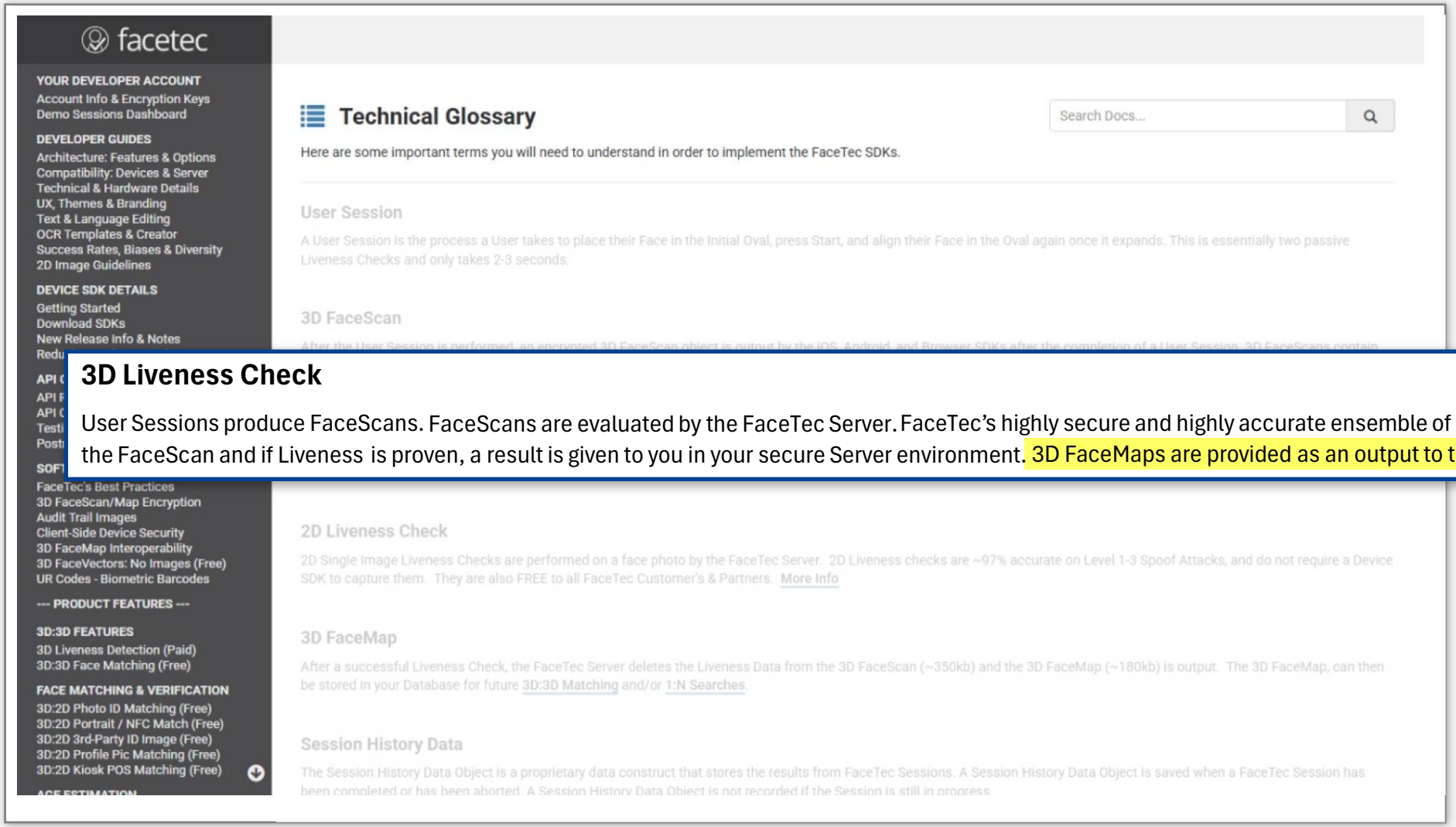
Jumio EX1067 Page 1
Jumio v. FaceTec IPR2025-00106

- FaceTec provides passive liveness via involuntary human signal measured by deep neural networks, which validate up to 60 human traits. All of the algorithms agree for a "Liveness Confirmed" decision to be rendered. Examples include, reflections in the user's eyes, reactions in the user's eye focus, and much more.

EX1067, 3

'471 Reply (Paper 52), 29

Removal Of Liveness Data



3D Liveness Check

User Sessions produce FaceScans. FaceScans are evaluated by the FaceTec Server. FaceTec's highly secure and highly accurate ensemble of 100+ Algorithms and heuristics evaluate the FaceScan and if Liveness is proven, a result is given to you in your secure Server environment. 3D FaceMaps are provided as an output to the Liveness Check API.

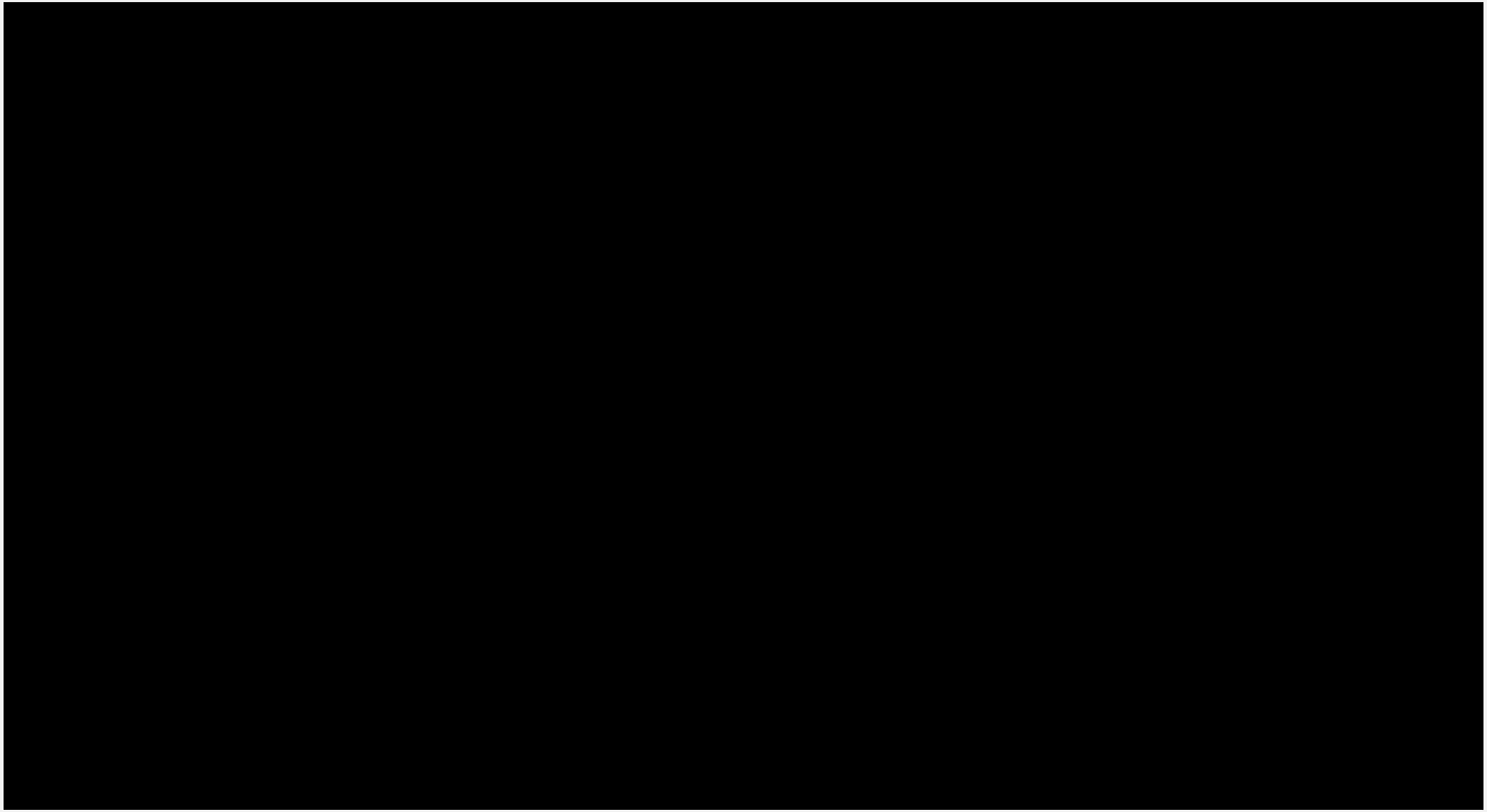
EX1083, 1

'471 Reply (Paper 52), 29

Three-Dimensionality



Three-Dimensionality



Claims Directed To Determining Three-Dimensionality

Dr. Daft

> 255. I understand that the challenged independent claims are directed to determining whether a user or user's face is three-dimensional.

Daft Reply Decl. (EX1060), ¶255

'471 Reply (Paper 52), 23-24

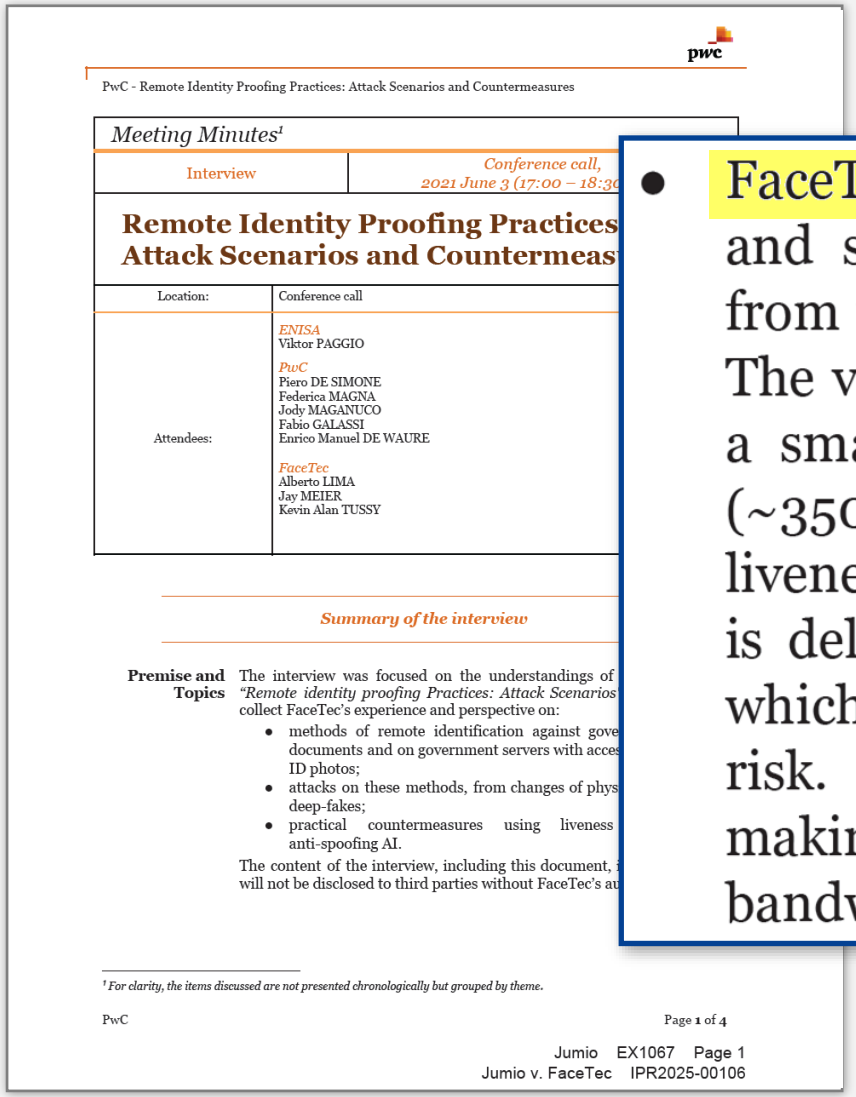
Fox Factory

the claimed invention and the product. As we explained, the purpose of the coextensiveness requirement is to ensure that nexus is only presumed when the product tied to the evidence of secondary considerations "*is* the invention disclosed and claimed." *Demaco*, 851 F.2d at 1392 (emphasis added). Thus, if the unclaimed features amount to nothing more than additional insignificant features, presuming nexus may nevertheless be appropriate.

Fox Factory, Inc. v. SRAM LLC, 944 F.3d 1366, 1374 (Fed. Cir. 2019)

'471 Reply (Paper 52), 24

Camera Integrity



pwc

PwC - Remote Identity Proofing Practices: Attack Scenarios and Countermeasures

Meeting Minutes[1]

Interview	*Conference call, 2021 June 3 (17:00 – 18:3*[illegible]

Remote Identity Proofing Practices
Attack Scenarios and Countermeas[illegible]

Location:	Conference call
Attendees:	*ENISA* Viktor PAGGIO *PwC* Piero DE SIMONE Federica MAGNA Jody MAGANUCO Fabio GALASSI Enrico Manuel DE WAURE *FaceTec* Alberto LIMA Jay MEIER Kevin Alan TUSSY

Summary of the interview

Premise and Topics The interview was focused on the understandings of [illegible] *"Remote identity proofing Practices: Attack Scenarios* collect FaceTec's experience and perspective on:

- methods of remote identification against gove[illegible] documents and on government servers with acces[illegible] ID photos;
- attacks on these methods, from changes of phys[illegible] deep-fakes;
- practical countermeasures using liveness [illegible] anti-spoofing AI.

The content of the interview, including this document, [illegible] will not be disclosed to third parties without FaceTec's au[illegible]

[1] *For clarity, the items discussed are not presented chronologically but grouped by theme.*

PwC Page 1 of 4

Jumio EX1067 Page 1
Jumio v. FaceTec IPR2025-00106

- FaceTec's technology works, first by ensuring camera feed integrity, and second, by acquiring the highest quality video data possible from the device at the maximum camera resolution and frame-rate. The video frames are then processed on the device itself, producing a small file containing 3D FaceScan data. This 3D FaceScan file (~350kb) is then encrypted and sent to the server for analysis. Once liveness is confirmed on the server, the one-time use liveness data is deleted, leaving only 3D matching data, called a 3D FaceMap, which cannot be resubmitted or reused, eliminating "Honeypot" risk. All remaining video data is deleted from the device itself, making the process secure as well as inclusive for clients on low bandwidth/data plans.

EX1067, 2

'471 Reply (Paper 52), 24; Daft Reply Decl. (EX1060), ¶267

Camera Integrity: Preventing Deepfake Injection Attacks

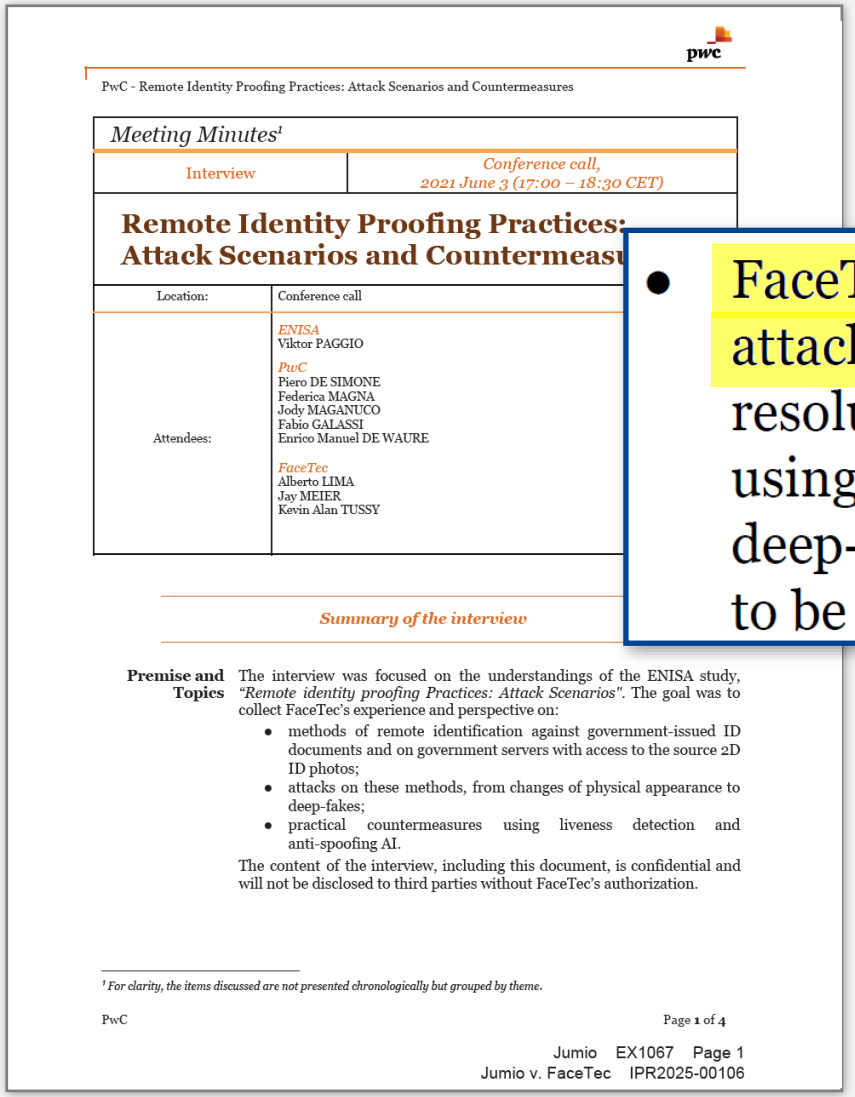
Mr. Meier

okay. So remember that our system, first thing it does - the SDK - is take control of the sensor, the camera and the data feed from it, right? That's so we can mitigate against deepfake injection attacks, right? It's - it's pretty

EX1073, 11:1-4

'471 Reply (Paper 52), 24-25; Daft Reply Decl. (EX1060), ¶268

Camera Integrity: Preventing Deepfake Injection Attacks



pwc

PwC - Remote Identity Proofing Practices: Attack Scenarios and Countermeasures

Meeting Minutes[1]

Interview	*Conference call, 2021 June 3 (17:00 – 18:30 CET)*

Remote Identity Proofing Practices: Attack Scenarios and Countermeasu

Location:	Conference call
Attendees:	*ENISA* Viktor PAGGIO *PwC* Piero DE SIMONE Federica MAGNA Jody MAGANUCO Fabio GALASSI Enrico Manuel DE WAURE *FaceTec* Alberto LIMA Jay MEIER Kevin Alan TUSSY

Summary of the interview

Premise and Topics The interview was focused on the understandings of the ENISA study, *"Remote identity proofing Practices: Attack Scenarios"*. The goal was to collect FaceTec's experience and perspective on:

- methods of remote identification against government-issued ID documents and on government servers with access to the source 2D ID photos;
- attacks on these methods, from changes of physical appearance to deep-fakes;
- practical countermeasures using liveness detection and anti-spoofing AI.

The content of the interview, including this document, is confidential and will not be disclosed to third parties without FaceTec's authorization.

[1] *For clarity, the items discussed are not presented chronologically but grouped by theme.*

PwC Page 1 of 4

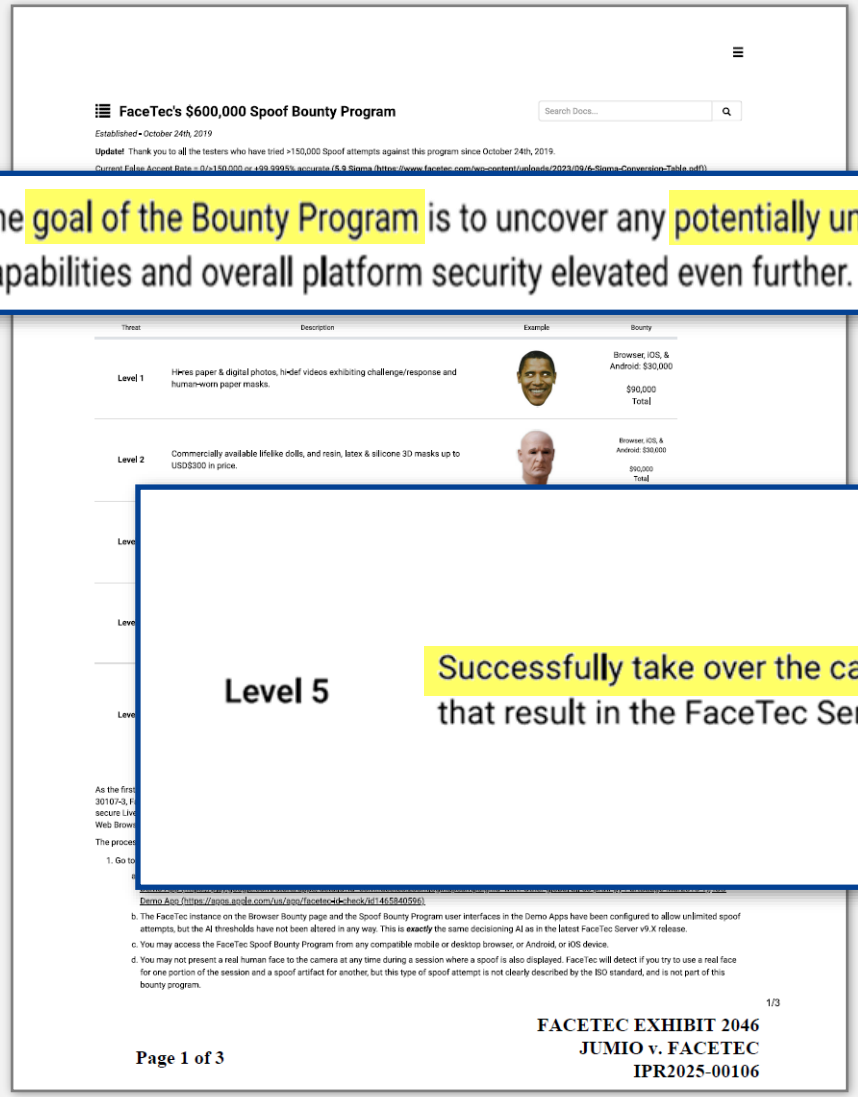
Jumio EX1067 Page 1
Jumio v. FaceTec IPR2025-00106

- FaceTec believes that the most difficult to defend attacks are video attacks utilizing video injection and virtual cameras, and lower resolution cameras pointed at higher resolution screens against using 2D face matching as the biometric modality, but considers deep-fake attacks (controllable real-time 3D puppets) the #1 threat to be concerned about in the future.

EX1067, 3

'471 Reply (Paper 52), 25

Spoof Bounty Program



FaceTec's $600,000 Spoof Bounty Program

Established - October 24th, 2019

Update! Thank you to all the testers who have tried >150,000 Spoof attempts against this program since October 24th, 2019.

Current False Accept Rate = 0/>150,000 or >99.999% accurate (5.3 Sigma (https://www.facetec.com/wp-content/uploads/2023/09/6-Sigma-Conversion-Table.pdf))

Threat	Description	Example	Bounty
Level 1	Hi-res paper & digital photos, hi-def videos exhibiting challenge/response and human-worn paper masks.		Browser, iOS, & Android: $30,000 $90,000 Total
Level 2	Commercially available lifelike dolls, and resin, latex & silicone 3D masks up to USD$300 in price.		Browser, iOS, & Android: $30,000 $90,000 Total

As the first 30107-3, F secure Live Web Brows

The proces

1. Go to

Demo App (https://apps.apple.com/us/app/facetec-id-check/id1465840596)

b. The FaceTec instance on the Browser Bounty page and the Spoof Bounty Program user interfaces in the Demo Apps have been configured to allow unlimited spoof attempts, but the AI thresholds have not been altered in any way. This is **exactly** the same decisioning AI as in the latest FaceTec Server v9.X release.

c. You may access the FaceTec Spoof Bounty Program from any compatible mobile or desktop browser, or Android, or iOS device.

d. You may not present a real human face to the camera at any time during a session where a spoof is also displayed. FaceTec will detect if you try to use a real face for one portion of the session and a spoof artifact for another, but this type of spoof attempt is not clearly described by the ISO standard, and is not part of this bounty program.

1/3

FACETEC EXHIBIT 2046
JUMIO v. FACETEC
IPR2025-00106

Page 1 of 3

The goal of the Bounty Program is to uncover any potentially unknown vulnerabilities in the Liveness AI and security layers so any issues can be patched and the anti-spoofing capabilities and overall platform security elevated even further.

EX2046, 1

Level 5	Successfully take over the camera feed & inject previously captured frames that result in the FaceTec Server responding with Liveness Success.	ManyCam (https://manycam.com/) Vcam (https://www.e2esoft.com/vcam/) vlc2Cam (https://vlc2vcam.com/) FakeWebcam (https://www.fakewebcam.com/)	Browser, iOS, & Android: $40,000 $120,000 Total

EX2046, 1

'471 Reply (Paper 52), 25; Daft Reply Decl. (EX1060), ¶273

Evolving Threats

Dr. Turk

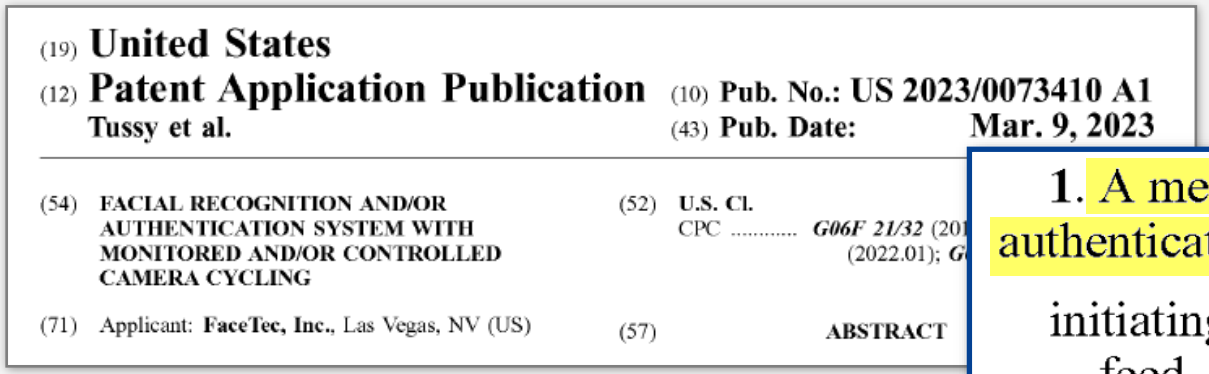
Q So would it be fair to say that FaceTec is seeking to ensure that its system is not spoofed by evolving types of attacks such as from utilizing 2D photos and videos to 3D dolls and masks?

MR. JOHNS: Objection; vague.

THE WITNESS: I think any company would want to be evolving their system to meet the latest kinds of attacks that they might be facing.

Turk Depo. Tr. (EX1059), 171:19-21

FaceTec Patent Portfolio



(19) **United States**

(12) **Patent Application Publication**

Tussy et al.

(10) **Pub. No.: US 2023/0073410 A1**

(43) **Pub. Date: Mar. 9, 2023**

(54) **FACIAL RECOGNITION AND/OR AUTHENTICATION SYSTEM WITH MONITORED AND/OR CONTROLLED CAMERA CYCLING**

(52) **U.S. Cl.**
CPC *G06F 21/32* (201
(2022.01); *G*

(71) Applicant: **FaceTec, Inc.**, Las Vegas, NV (US)

(57) **ABSTRACT**

1. A method for detecting video feed injection during an authentication session comprising:

initiating an authentication session which utilizes a video feed from a camera of a computing device used to capture video of a user during the authentication session;

requesting a video feed;

monitoring for receipt of the video feed;

receiving a received video feed;

detecting a time interval between requesting the video feed and receiving the received video feed;

comparing the time interval to an expected time interval;

if the time interval does not match an expected time interval, terminating the authentication session.

EX1074, Claim 1

'471 Reply (Paper 52), 25; Daft Reply Decl. (EX1060), ¶272

Fox Factory

J.A. 5284, 5289. A patent claim is not coextensive with a product that includes a "critical" unclaimed feature that is claimed by a different patent and that materially impacts the product's functionality by "lead[ing] to a chainring that will retain a chain in even the worst conditions." *See* J.A. 5282–84, 5289.

Fox Factory, Inc. v. SRAM LLC, 944 F.3d 1366, 1375 (Fed. Cir. 2019)

User Interface

Mr. Meier

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?

EX1073, 3:3-11

'471 Reply (Paper 52), 26; Daft Reply Decl. (EX1060), ¶275

User Interface

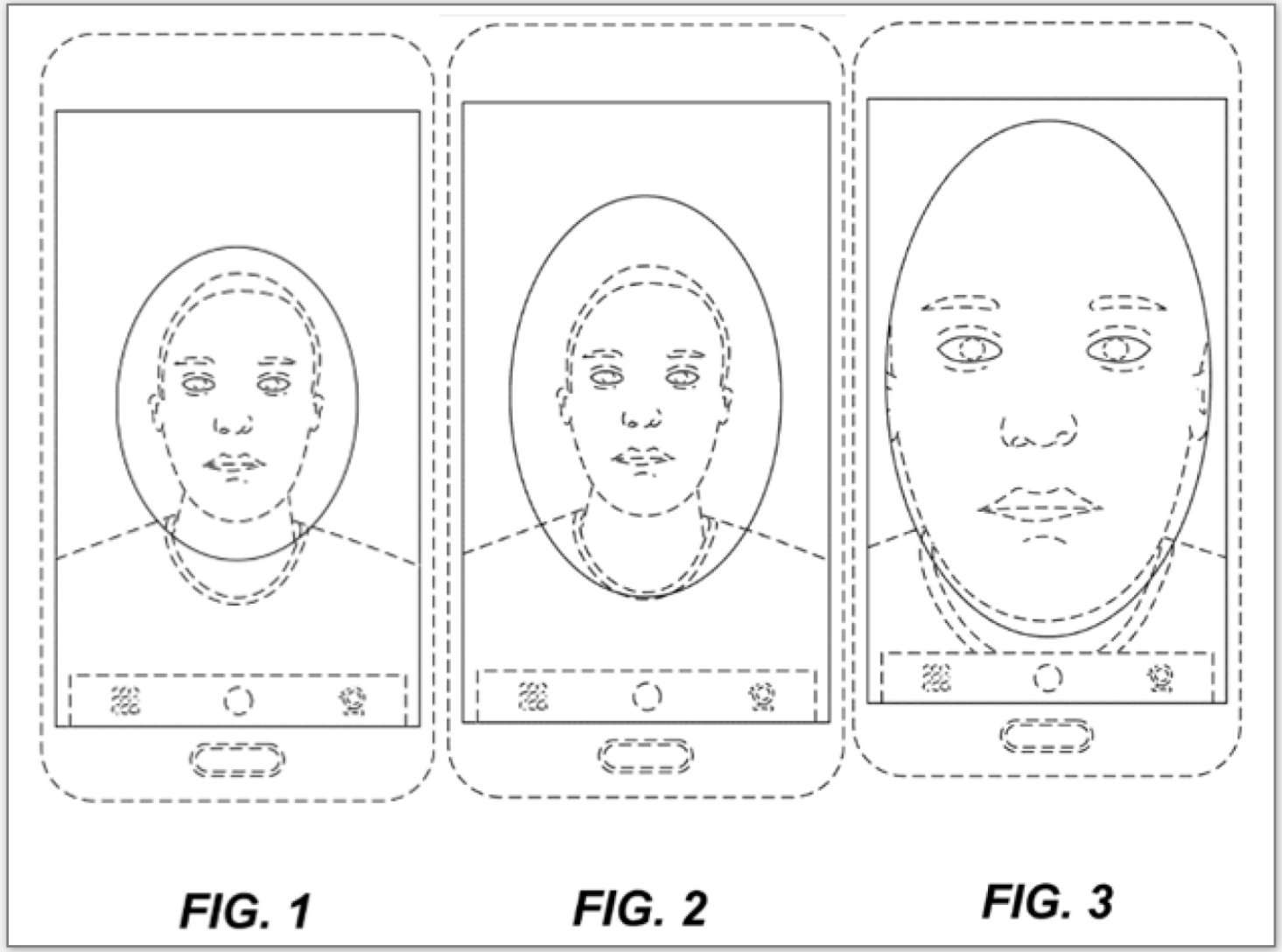
Mr. Meier

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?

EX1073, 6:17-21

'471 Reply (Paper 52), 26; Daft Reply Decl. (EX1060), ¶275

FaceTec's Patent Portfolio



EX1075, Figs. 1-3

'471 Reply (Paper 52), 27

FaceTec's 2025 Press Release



SUMMERLIN, Nev., June 4, 2025 /PRNewswire/ -- **FaceTec, Inc.**, a world leader in biometric cybersecurity and identity verification, is pleased to announce the recent allowance of a U.S. patent application and another newly issued patent, which both strengthen FaceTec's core IP protection of its 3D Liveness detection capability. FaceTec's software now performs over 3.5 billion 3D Liveness checks annually, and the company has recently released the ground-breaking **UR® Code** identity verification protocol.

EX1066, 1

In addition, FaceTec is proud to announce the USPTO has granted Design Patent D1,074,689, covering face-framing ovals as part of a graphical user interface. FaceTec pioneered this user interface over nine years ago. Since then, numerous less innovative companies have attempted to copy this design. This design patent expands the protection of FaceTec's customer-facing user interface.

EX1066, 1

'471 Reply (Paper 52), 26; Daft Reply Decl. (EX1060), ¶276

FaceTec's Patent Portfolio

1. A system for capturing images of a person's face and evaluating one or more characteristics of the person's face, the system comprising:
a processor configured to execute machine executable code;
a screen configured to provide a user interface to the user;
a camera configured to capture images;
one or more memories configured to store the machine executable code that is stored on the one or more memories of the authentication server which, when executed by the processor, cause the system to:
display a first face-framing prompt on the screen associated with the system;
responsive to the user positioning their face within the first face-framing prompt, capture at least one first image of the person's face taken with the camera of the system at a first location, which is a first distance from the person's face;
process the at least one first image or a portion thereof to create first data;
display a second face-framing prompt on the screen associated with the system, wherein the second face-framing prompt differs in size from the first face-framing prompt;
responsive to the user positioning their face within the second face-framing prompt, capture at least one second image of the person's face taken with the camera of the system at a second distance from the person's face, the second distance being different than the first distance, the capturing at least one second image of the person's face occurring after movement of the camera, the person's face, or both to establish the camera at the second distance from the person's face;
process the at least one second image or a portion thereof to create second data;
process the first data, the second data, or both to evaluate one or more characteristics of the person's face captured in the images and/or verify that the camera captured images of a real person.

1. A system for capturing images of a person's face and evaluating one or more characteristics of the person's face, the system comprising:

EX1077, Claim 1

display a first face-framing prompt on the screen associated with the system;

EX1077, Claim 1

'471 Reply (Paper 52), 26; Daft Reply Decl. (EX1060), ¶277

Encryption

Mr. Rose

Q Why are you encrypting the 3D face scan?

A To ensure the security of the system as a whole, it's important that the data that we process and analyze and inspect and pretty much anything that we do with the data hasn't been tampered with.

Rose Depo Tr. (EX1082), 35:21-25

Encryption

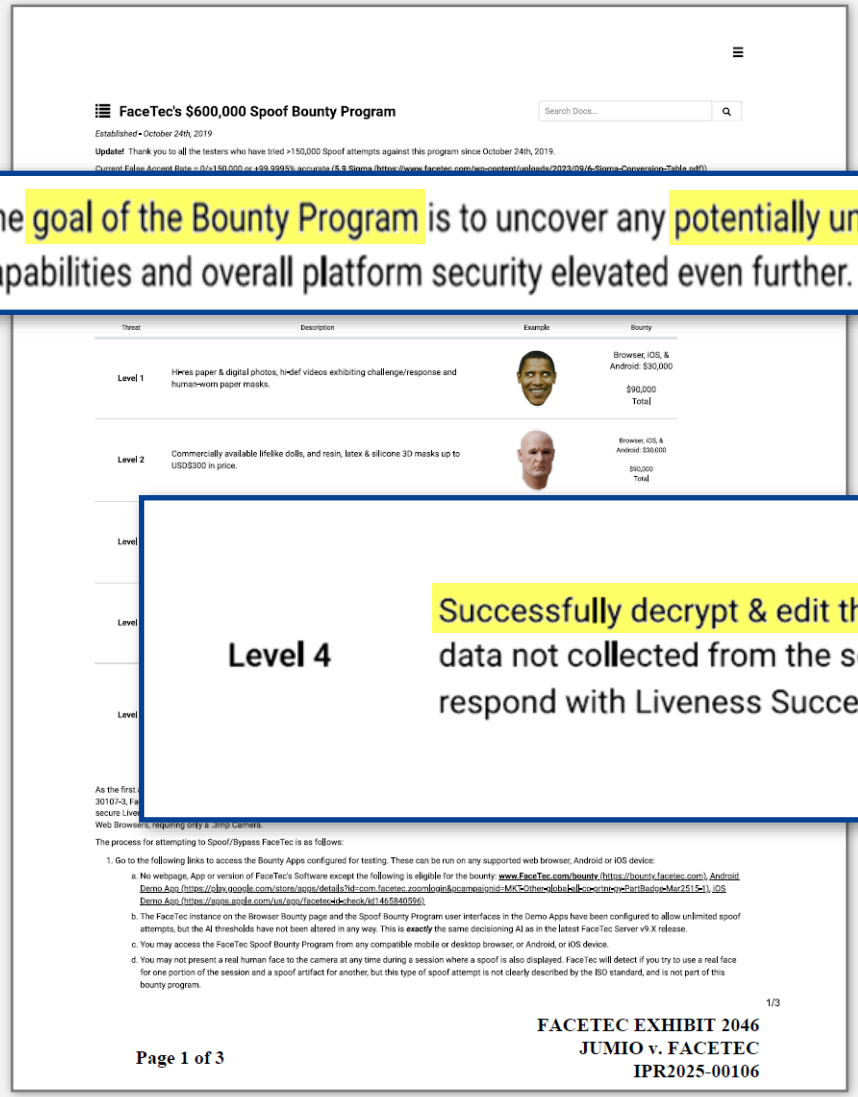
Mr. Rose

So another reason this encryption is important is also because, once the -- once we create this 3D face scan, which is an encrypted piece of data -- once that piece of data exists, we don't want a potential attacker to be able to decrypt that and be able to inspect or modify or tamper with that piece of data.

This also relates to level 4 of our Spoof Bounty program, which involves attack vectors that include being able to crack the decryption -- crack the encryption and be able to pull off some sort of bypass that would involve that.

Rose Depo Tr. (EX1082), 36:7-18

Spoof Bounty Program



FaceTec's $600,000 Spoof Bounty Program

Established - October 24th, 2019

Update! Thank you to all the testers who have tried >150,000 Spoof attempts against this program since October 24th, 2019.

Current False Accept Rate = 0/>150,000 or >99.999% accurate (5.3 Sigma (https://www.facetec.com/wp-content/uploads/2023/09/6-Sigma-Conversion-Table.pdf))

Threat	Description	Example	Bounty
Level 1	Hi-res paper & digital photos, hi-def videos exhibiting challenge/response and human-worn paper masks.		Browser, iOS, & Android: $30,000 $90,000 Total
Level 2	Commercially available lifelike dolls, and resin, latex & silicone 3D masks up to USD$300 in price.		Browser, iOS, & Android: $30,000 $90,000 Total
Level			
Level			
Level			

As the first
30107-3, Fa
secure Live
Web Browsers, requiring only a .5mp camera.

The process for attempting to Spoof/Bypass FaceTec is as follows:

1. Go to the following links to access the Bounty Apps configured for testing. These can be run on any supported web browser, Android or iOS device:
   a. No webpage, App or version of FaceTec's Software except the following is eligible for the bounty: **www.FaceTec.com/bounty** (https://bounty.facetec.com), Android Demo App (https://play.google.com/store/apps/details?id=com.facetec.zoomlogin&pcampaignid=MKT-Other-global-all-co-prtnr-py-PartBadge-Mar2515-1), iOS Demo App (https://apps.apple.com/us/app/facetec-id-check/id1465840596)
   b. The FaceTec instance on the Browser Bounty page and the Spoof Bounty Program user interfaces in the Demo Apps have been configured to allow unlimited spoof attempts, but the AI thresholds have not been altered in any way. This is ***exactly*** the same decisioning AI as in the latest FaceTec Server v9.X release.
   c. You may access the FaceTec Spoof Bounty Program from any compatible mobile or desktop browser, or Android, or iOS device.
   d. You may not present a real human face to the camera at any time during a session where a spoof is also displayed. FaceTec will detect if you try to use a real face for one portion of the session and a spoof artifact for another, but this type of spoof attempt is not clearly described by the ISO standard, and is not part of this bounty program.

1/3

Page 1 of 3

FACETEC EXHIBIT 2046
JUMIO v. FACETEC
IPR2025-00106

The goal of the Bounty Program is to uncover any potentially unknown vulnerabilities in the Liveness AI and security layers so any issues can be patched and the anti-spoofing capabilities and overall platform security elevated even further.

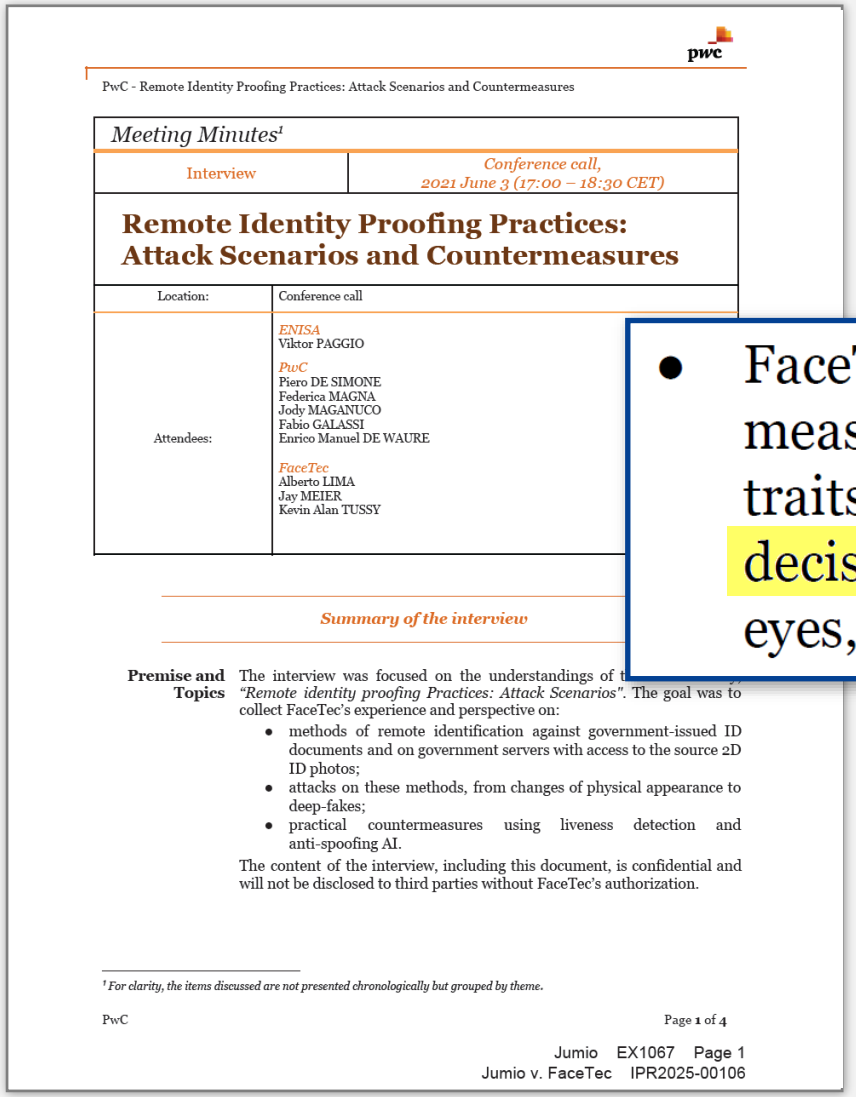
EX2046, 1

Level 4	Successfully decrypt & edit the contents of a 3D FaceScan to contain synthetic data not collected from the session, have the FaceTec Server process it and respond with Liveness Success.	3D FaceScan Tampering (https://dev.facetec.com/security-best-practices#facemap-tampering)	Browser, iOS, & Android: $60,000 $180,000 Total

EX2046, 1

'471 Reply (Paper 52), 28; Daft Reply Decl. (EX1060), ¶281

Liveness Checks



pwc

PwC - Remote Identity Proofing Practices: Attack Scenarios and Countermeasures

Meeting Minutes[1]

Interview	*Conference call, 2021 June 3 (17:00 – 18:30 CET)*

Remote Identity Proofing Practices: Attack Scenarios and Countermeasures

Location:	Conference call
Attendees:	*ENISA* Viktor PAGGIO *PwC* Piero DE SIMONE Federica MAGNA Jody MAGANUCO Fabio GALASSI Enrico Manuel DE WAURE *FaceTec* Alberto LIMA Jay MEIER Kevin Alan TUSSY

Summary of the interview

Premise and Topics The interview was focused on the understandings of t… *"Remote identity proofing Practices: Attack Scenarios"*. The goal was to collect FaceTec's experience and perspective on:

- methods of remote identification against government-issued ID documents and on government servers with access to the source 2D ID photos;
- attacks on these methods, from changes of physical appearance to deep-fakes;
- practical countermeasures using liveness detection and anti-spoofing AI.

The content of the interview, including this document, is confidential and will not be disclosed to third parties without FaceTec's authorization.

[1] *For clarity, the items discussed are not presented chronologically but grouped by theme.*

PwC Page 1 of 4

Jumio EX1067 Page 1
Jumio v. FaceTec IPR2025-00106

- FaceTec provides passive liveness via involuntary human signal measured by deep neural networks, which validate up to 60 human traits. All of the algorithms agree for a "Liveness Confirmed" decision to be rendered. Examples include, reflections in the user's eyes, reactions in the user's eye focus, and much more.

EX1067, 3

'471 Reply (Paper 52), 29

Liveness Checks

Mr. Meier

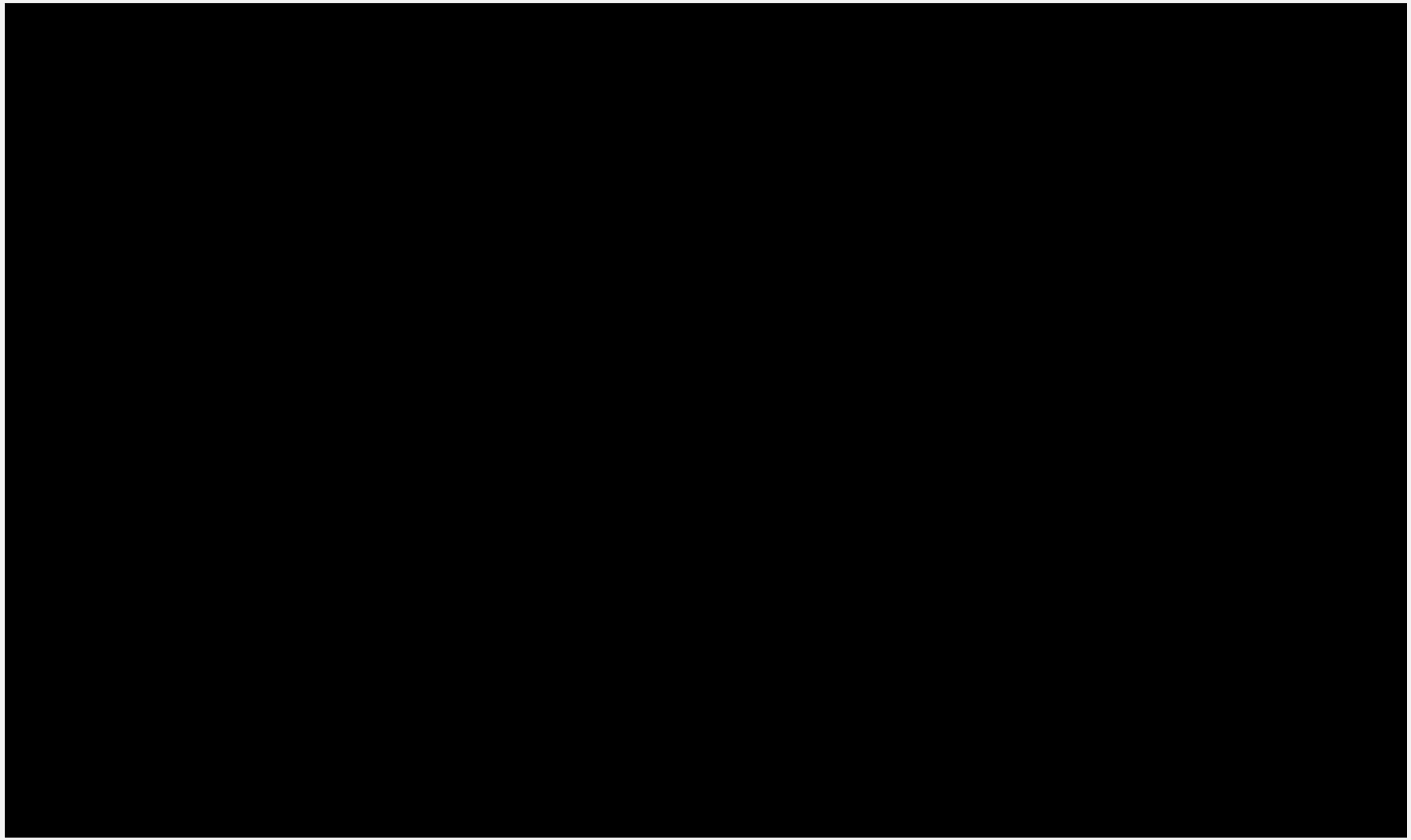
things. Well, only if you're measuring three - If the only thing you measure is three dimensionality, then those masks will work. They'll get through the liveness. But if you so

EX1073, 12:24-13:1

So don't worry about that one. But we have 70 or more of these involuntary human cues that our system watches in addition to the three dimensionality, right.

EX1073, 13:20-22

Liveness Checks



FaceTec's Patent Portfolio

17. A method, performed using a computing device, for providing authentication of a person during an authentication session, the method comprising:

capturing a first image of a head of the person with a camera at a first distance from the person, the camera associated with the computing device;

changing a distance between the person and the cam a second distance, which is different from th distance;

capturing a second image of the head of the perso the camera at the second distance from the pers

comparing one or more aspects of the head from th image or first biometric data derived from th image to one or more aspects of the head fro second image or second biometric data derive the second image to determine whether expect ferences are not present, wherein the expected ences:

would be present when the first image and second i of the head of the person being captured at di distances has three-dimensional characteristics t if the head did not have three-dimensional cha istics; and

the expected differences result from differences in relative dimensions of a person's face appearing different when capturing images is done close to the person's face and far from the persons face; and

if the expected differences are not present, denying authentication of the person and providing notice thereof to one or more of the person, a third party, or a software application, wherein the authentication is authentication of liveness, three-dimensionality, or both.

if the expected differences are not present, denying authentication of the person and providing notice thereof to one or more of the person, a third party, or a software application, wherein the authentication is authentication of liveness, three-dimensionality, or both.

'938 Patent (EX1001), Claim 17

'471 Reply (Paper 52), 29; Daft Reply Decl. (EX1060), ¶292

Removal Of Liveness Data

Mr. Meier

THE REPORTER: I think you had mentioned last week too that the data that is left over after they delete the face map is useless. It can't be resubmitted. So-

JAY: Yeah.

THE REPORTER: Even if they lost everything or it was stolen, uh -

JAY: Right.

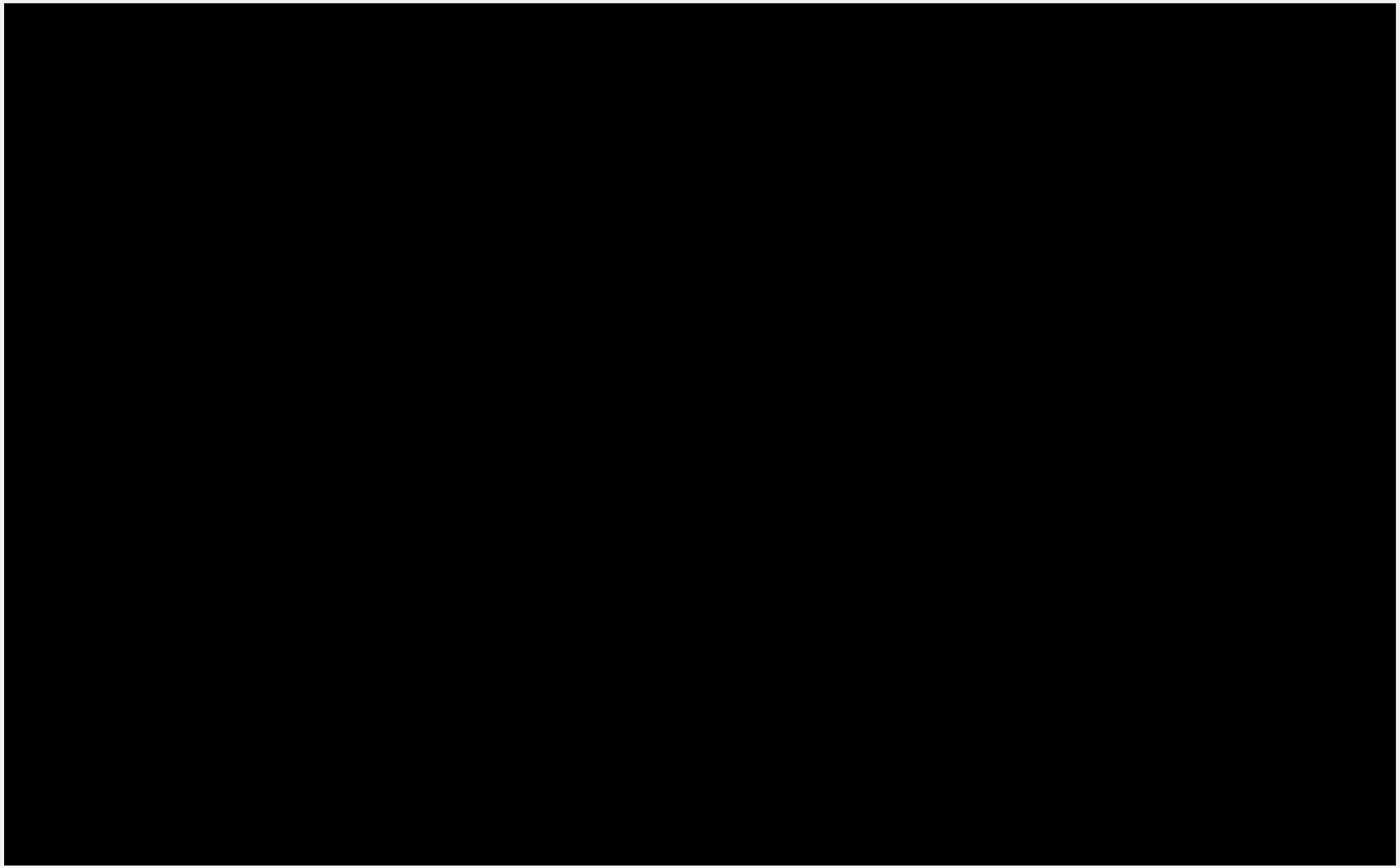
THE REPORTER: - there would be no use for it.

JAY: Well, and that's a critical selling feature in our view, you know. What you're talking - what you're - what that regards is what's called honeypot risk, right?

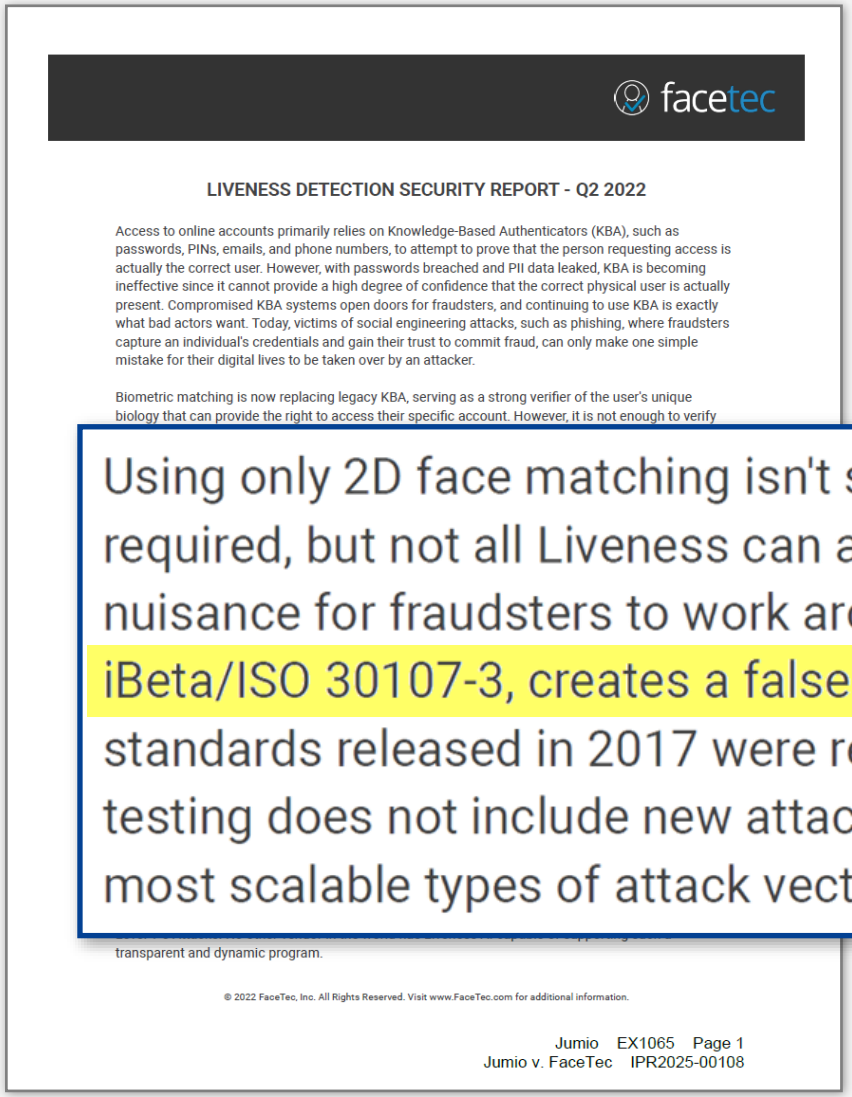
EX1073, 9:20-10:5

'471 Reply (Paper 52), 29-30; Daft Reply Decl. (EX1060), ¶296

Removal Of Liveness Data



FaceTec re: Standard-Based Certifications



facetec

LIVENESS DETECTION SECURITY REPORT - Q2 2022

Access to online accounts primarily relies on Knowledge-Based Authenticators (KBA), such as passwords, PINs, emails, and phone numbers, to attempt to prove that the person requesting access is actually the correct user. However, with passwords breached and PII data leaked, KBA is becoming ineffective since it cannot provide a high degree of confidence that the correct physical user is actually present. Compromised KBA systems open doors for fraudsters, and continuing to use KBA is exactly what bad actors want. Today, victims of social engineering attacks, such as phishing, where fraudsters capture an individual's credentials and gain their trust to commit fraud, can only make one simple mistake for their digital lives to be taken over by an attacker.

Biometric matching is now replacing legacy KBA, serving as a strong verifier of the user's unique biology that can provide the right to access their specific account. However, it is not enough to verify

transparent and dynamic program.

© 2022 FaceTec, Inc. All Rights Reserved. Visit www.FaceTec.com for additional information.

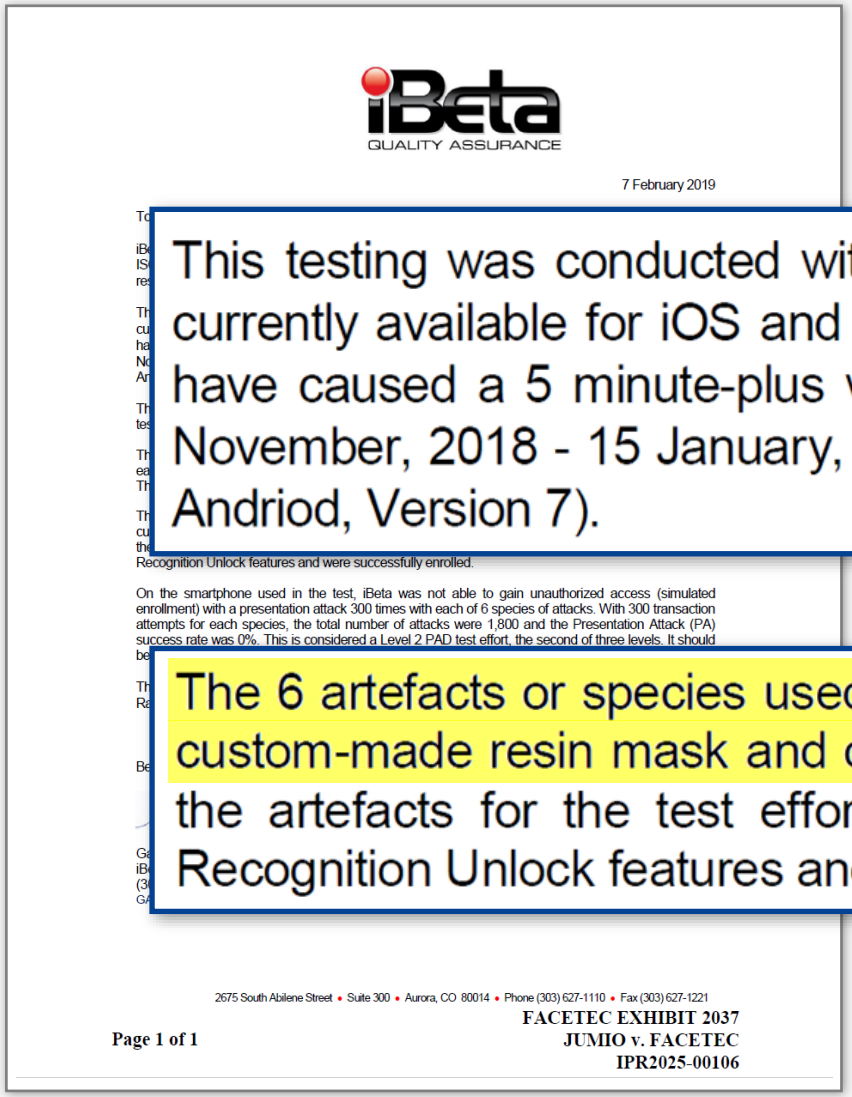
Jumio EX1065 Page 1
Jumio v. FaceTec IPR2025-00108

Using only 2D face matching isn't sufficient for remote identity verification. Liveness Detection is required, but not all Liveness can actually stop attackers. In fact, most cannot and have become a mere nuisance for fraudsters to work around. Relying on outdated standards and testing criteria, such as iBeta/ISO 30107-3, creates a false sense of security. Attack vectors have evolved so quickly that standards released in 2017 were rendered obsolete within just a few years. ISO 30107-3 and iBeta testing does not include new attack vectors such as digital deepfakes or video injection, two of the most scalable types of attack vectors with the potential to cause widespread damage.

EX1065, 1

'471 Reply (Paper 52), 30

iBeta Certification



iBeta QUALITY ASSURANCE

7 February 2019

Recognition Unlock features and were successfully enrolled.

On the smartphone used in the test, iBeta was not able to gain unauthorized access (simulated enrollment) with a presentation attack 300 times with each of 6 species of attacks. With 300 transaction attempts for each species, the total number of attacks were 1,800 and the Presentation Attack (PA) success rate was 0%. This is considered a Level 2 PAD test effort, the second of three levels. It should

2675 South Abilene Street • Suite 300 • Aurora, CO 80014 • Phone (303) 627-1110 • Fax (303) 627-1221

Page 1 of 1

FACETEC EXHIBIT 2037
JUMIO v. FACETEC
IPR2025-00106

This testing was conducted with the FaceTec ZoOm® v6.9.11 modified from the production version currently available for iOS and Android to remove 2 anti-reverse-engineering mechanisms that would have caused a 5 minute-plus wait time for every 6 spoof attempts. Testing was conducted from 26 November, 2018 - 15 January, 2019 on a smartphone considered mid-level (Samsung Galaxy Note 5 Andriod, Version 7).

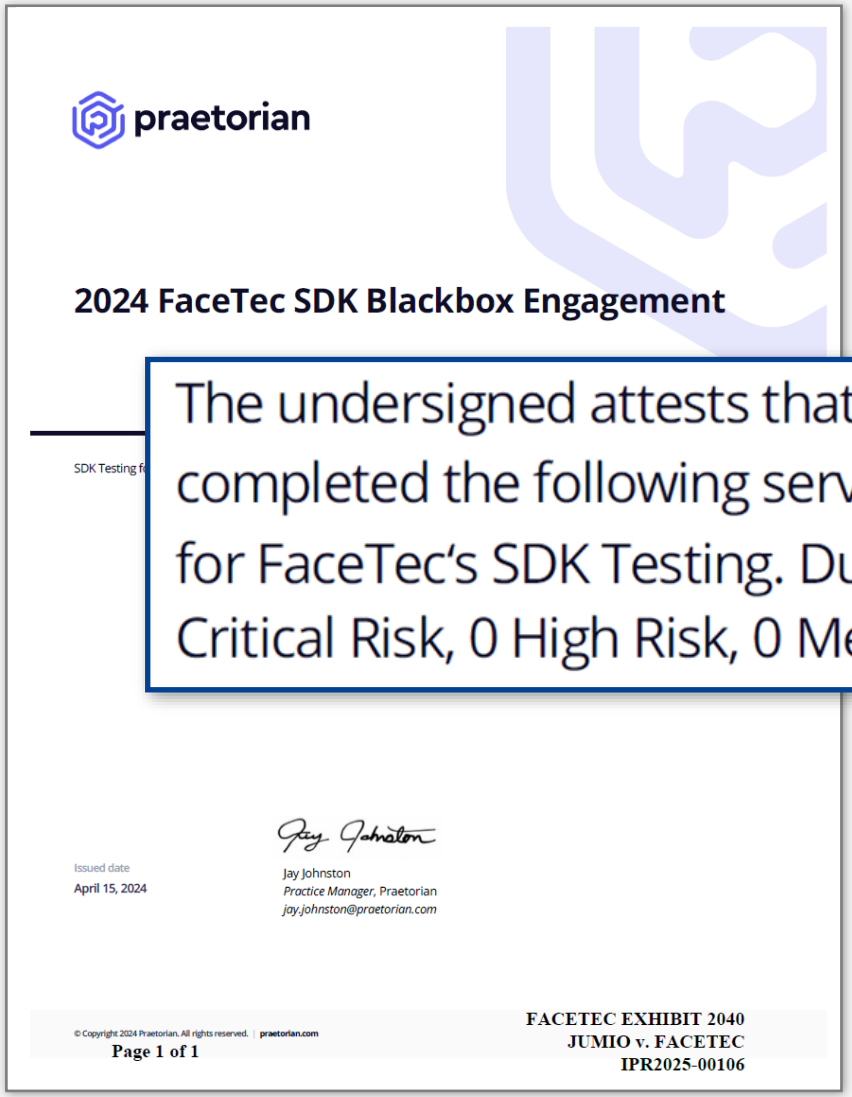
EX2037, 1

The 6 artefacts or species used in the test effort were two life-like dolls, two realistic latex masks, one custom-made resin mask and one realistic silicone mask with a cost of up to $300 each. To validate the artefacts for the test effort, each artefact was presented to modern smartphones with Facial Recognition Unlock features and were successfully enrolled.

EX2037, 1

'471 Reply (Paper 52), 30-31; Daft Reply Decl. (EX1060), ¶307

Praetorian Certification



praetorian

2024 FaceTec SDK Blackbox Engagement

SDK Testing f

Issued date
April 15, 2024

Jay Johnston
Practice Manager, Praetorian
jay.johnston@praetorian.com

© Copyright 2024 Praetorian. All rights reserved. | praetorian.com

FACETEC EXHIBIT 2040
JUMIO v. FACETEC
IPR2025-00106

The undersigned attests that between March 11, 2024 and March 27, 2024, Praetorian completed the following services: Application Penetration Test and Mobile Penetration Test for FaceTec's SDK Testing. During the assessment, Praetorian identified the following issues: 0 Critical Risk, 0 High Risk, 0 Medium Risk, 1 Low Risk, and 0 Informational.

EX2040, 1

'471 Reply (Paper 52), 30-31; Daft Reply Decl. (EX1060), ¶310

Praetorian Certification

praetorian

DATA SHEET

Application Penetration Testing

KEY BEN

Using a combination of manual and automated techniques, we can identify vulnerabilities ranging from classical web application vulnerabilities on the OWASP Top 10 to complex attack paths that chain together multiple weaknesses. Manual techniques, such as code review, log analysis, and analyzing memory in a debugger provide depth of coverage. They also give us the right opportunities to emulate attackers in order to find subtle vulnerabilities. Automated techniques, such as fuzzers and custom enumeration scripts, provide breadth of coverage and ensure we are finding as much as possible.

EX1069, 1

'471 Reply (Paper 52), 30-31; Daft Reply Decl. (EX1060), ¶310

Praetorian Certification

Mr. Rose

I think Praetorian would probably say that some of the testing that they do is cybersecurity. But this was an engagement with cybersecurity who -- with -- an engagement with -- sorry -- an engagement with Praetorian, who has many, many experts on their team, security experts, platform experts, you know, language experts, reverse engineering experts. And this engagement was related to them attempting to find vulnerabilities, attack vectors, and issues with obfuscation, other types of issues when testing our SDKs from a black box perspective.

Rose Depo Tr. (EX1082), 127:8-18

'471 Reply (Paper 52), 30-31

Certifications

Dr. Turk

Q And in citing all of these exhibits that we've been discussing with regard to FaceTec software, specifically Exhibit 2037, 2038, 2039, 2040 and 2078, did you ever go back and look to these companies' testing protocols?

A I don't believe I looked at their testing protocols.

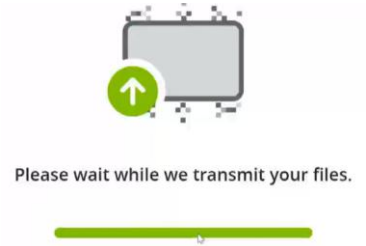
Turk Depo Tr. (EX1059), 171:23-172:4

'471 Reply (Paper 52), 30-31; Daft Reply Decl. (EX1060), ¶305

Jumio Presentation

Dr. Daft

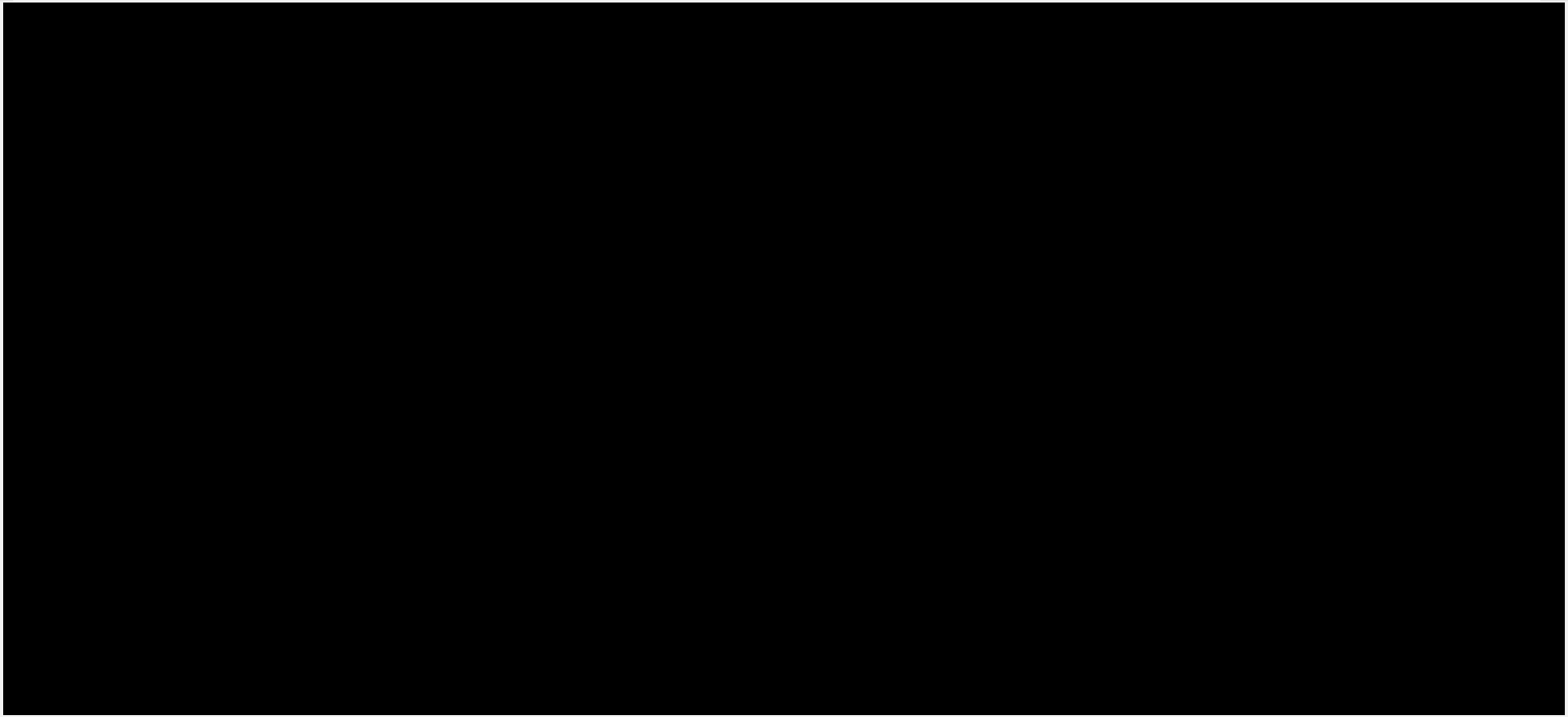
312. FaceTec also points to statements made by Jumio. I understand that, at the time the statements were made, Jumio was *not* a competitor of FaceTec. (*See* EX2057, 11:10.) Rather, as FaceTec pointed out, Jumio was a partner and licensee at the time. (POR, 16; EX2057, 11:10.) Additionally, the product and features that Jumio discusses lack a nexus to the purported invention of the challenged independent claims. For example, EX2057, a talk by Jumio, discusses their partnership with FaceTec and a demo of the product. The product shown and discussed is ZoOm, which, as I previously discussed, includes several other features beyond the three-dimensionality check, such as sending to a secure network shown below.



Daft Reply Decl. (EX1060), ¶312

'471 Reply (Paper 52), 31; Daft Reply Decl. (EX1060), ¶312

Jumio License Agreement



'471 Reply (Paper 52), 31; Daft Reply Decl. (EX1060), ¶312

Purported Copying By iProov

Dr. Turk

468. Following this extensive access, I understand that iProov released its "Liveness Assurance" software in late 2020. According to iProov's own materials, the software verifies that a user is a live human and not a spoof artifact. *See* Ex. 2059, ¶45; Ex. 2060. In my opinion, the software mimics FaceTec's patented approach by manipulating the interface to prompt user movement and capturing user images at different distances—resulting in substantially similar functionality. *See* Ex. 2059. Appendices A-D set forth a comparative analysis based on materials describing iProov's software service and FaceTec's patented software service.

Turk Decl. (EX2061), ¶468

'471 Reply (Paper 52), 32; Daft Reply Decl. (EX1060), ¶319

Purported Copying By iProov

Dr. Turk

Q Okay. Dr. Turk, did you create these eight appendices that are attached to your exhibit?

A No, I didn't. And I don't claim to have done that in the declaration. This was provided to me.

Turk Depo Tr. (EX1059), 181:5-8

Claim 1 Of The ’938 Patent

1. A non-transient computer readable medium containing non-transitory machine executable code configured to mine if the three-dimensional shape is consistent with a human face, the non-transitory machine executable configured to:

receive or derive first biometric data from at least or image of a user taken with a computing device c located at a first distance from the user;

receive or derive second biometric data from at lea second image of the user taken with the com device camera located at a second distance fro user, the second distance being different than th distance;

compare the first biometric data with second bio data for expected differences that result from c teristics of a human face and the at least one first and the at least one second image being captu different distances from the user;

determine that the three-dimensional shape is not ited when the second biometric data does not expected differences compared to the first bio data, the expected differences comprising at lea ferences due to the change in the relative di between the user’s facial features and the camera the at least one first image was captured at th distance and the at least one second image was ca at the second distance, wherein the expected ences result from fish-eye type distortion in at lea of the at least one first image and the at least one s image and due to the three-dimensional nature human face and the change in distance betwee camera and the user.

determine that the three-dimensional shape is not exhibited when the second biometric data does not have expected differences compared to the first biometric data, the expected differences comprising at least differences due to the change in the relative distance between the user’s facial features and the camera when the at least one first image was captured at the first distance and the at least one second image was captured at the second distance, wherein the expected differences result from fish-eye type distortion in at least one of the at least one first image and the at least one second image and due to the three-dimensional nature of the human face and the change in distance between the camera and the user.

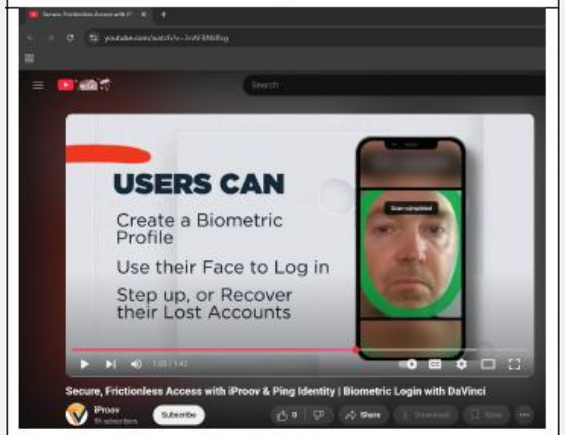
’938 Patent (EX1001), Claim 1

’471 Reply (Paper 52), 32; Daft Reply Decl. (EX1060), ¶321

Appendix C Of Dr. Turk's Declaration

iProov
The image below shows iProov's system allowing user to log in based on the biometric profile, which indicates that iProov authenticates using the biometric data obtained by processing the second image.

Turk Decl. (EX2061), 307

iProov
 Excerpt from Ex. 2071.

Turk Decl. (EX2061), 308

'471 Reply (Paper 52), 32; Daft Reply Decl. (EX1060), ¶321

Appendix C Of Dr. Turk's Declaration

Dr. Turk

Q But do you know if biometric information was actually compared?

A I don't know that for sure. I'd be interested to look more closely at iProov's system to determine that for sure --

Turk Depo Tr. (EX1059), 186:25-187:4

Claim 1 Of The '471 Patent

1. A system for authenticating three-dimensionality of a user via a user's camera equipped computing device, the computing device comprising:

a processor configured to execute machine executable code;

a screen configured to provide a user interface to the user;

a camera configured to capture images;

one or more memories configured to store machine readable instructions that are stored on the memory of the authentication server which when executed by the processor, cause the computing device to:

capturing at least one first image of the user taken with the camera of the computing device at a first location which is a first distance from the user;

processing the at least one first image or a portion to create first data;

moving the camera from the first location to a second location, the second location being a second distance from the user, or the user moving from the first location to the second location to change the distance between the user and the camera from the first distance to a second distance;

capturing at least one second image of the user taken with the camera of the computing device at the second distance from the user, the second distance being different than the first distance;

processing the at least one second image or a portion thereof to create second data;

comparing the first data to the second data to determine whether expected differences exist between the first data and the second data which indicated three-dimensionality of the user;

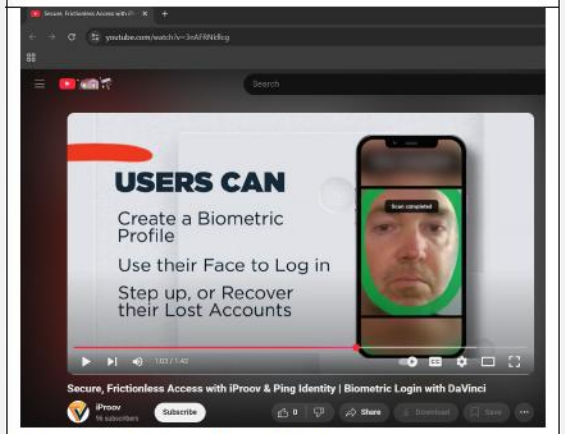
authenticating the user when differences between the first data and the second data have expected distortion resulting from movement of the camera from the first location to the second location or movement of the user from the first location to the second location, which causes the change in distance between the user and the camera.

comparing the first data to the second data to determine whether expected differences exist between the first data and the second data which indicated three-dimensionality of the user;

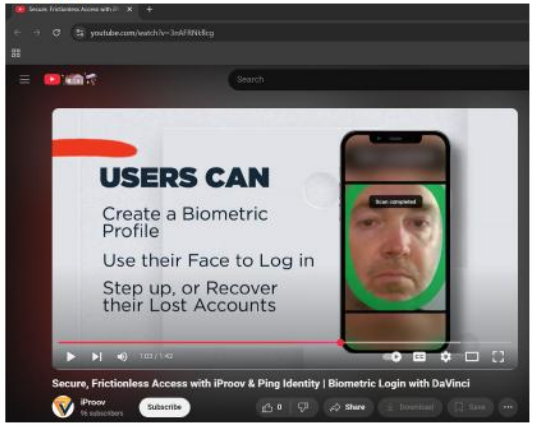
'471 Patent (EX1001), Claim 1

'471 Reply (Paper 52), 32; Daft Reply Decl. (EX1060), ¶322

Appendix A Of Turk's Declaration

iProov
 Excerpt from Ex. 2071.
iProov's system practices this element.

Turk Decl. (EX2061), 246

iProov
The image below shows iProov's system allowing log in based on the biometric profile, which indicates that iProov compares the biometric data obtained by processing the second image.  Excerpt from Ex. 2071.

Turk Decl. (EX2061), 247

'471 Reply (Paper 52), 32; Daft Reply Decl. (EX1060), ¶322

Appendix A Of Turk's Declaration

Dr. Turk

With respect to this limitation, does what you've cited in Exhibit 2071 show the actual comparing step?

A You're asking if the image there that is shown here shows the comparison step?

Q That's correct.

A I don't believe the image itself shows that step. I think the inference from this image and actually the whole video that this image comes from is that it seems to me that it's very likely that's what's happening.

Q What would you need to review to confirm that inference?

A Ultimately, iProov software.

Turk Depo Tr. (EX1059), 188:18-189:6

Purported Copying By Jumio

Dr. Turk

Q So does what you cited for this limitation with respect to Jumio actually show the determination step or element of 1[d] of the '938 patent?

A I believe the video, Exhibit 2072, provides good evidence that that's probably what's happening.

Q You say, "probably what's happening."

Is that, again, sort of what you previously testified as an inference?

A Yes, in the sense that I have not seen their software and been able to analyze exactly how their system works.

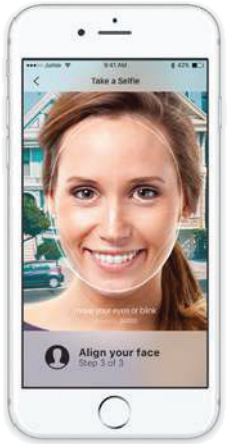
Turk Depo Tr. (EX1059), 189:17-190:2

'471 Reply (Paper 52), 32-33

Alleged Long Felt Need / Failure Of Others

Liveness Detection for Mobile

To ensure a real person is behind the mobile device during the transaction, Jumio requires users to follow a target on the screen with their eyes as it moves in a random pattern. The liveness detection workflow consists of two steps:



Selfie Capture for Similarity Check:

Does the photo printed on the ID match with the user´s selfie? The user is requested to align their face within a frame overlay. During the alignment, real time feedback is offered (e.g. move closer) to guide the user properly. After the user has aligned their face, a 'selfie' photo is taken and used to perform the similarity check.



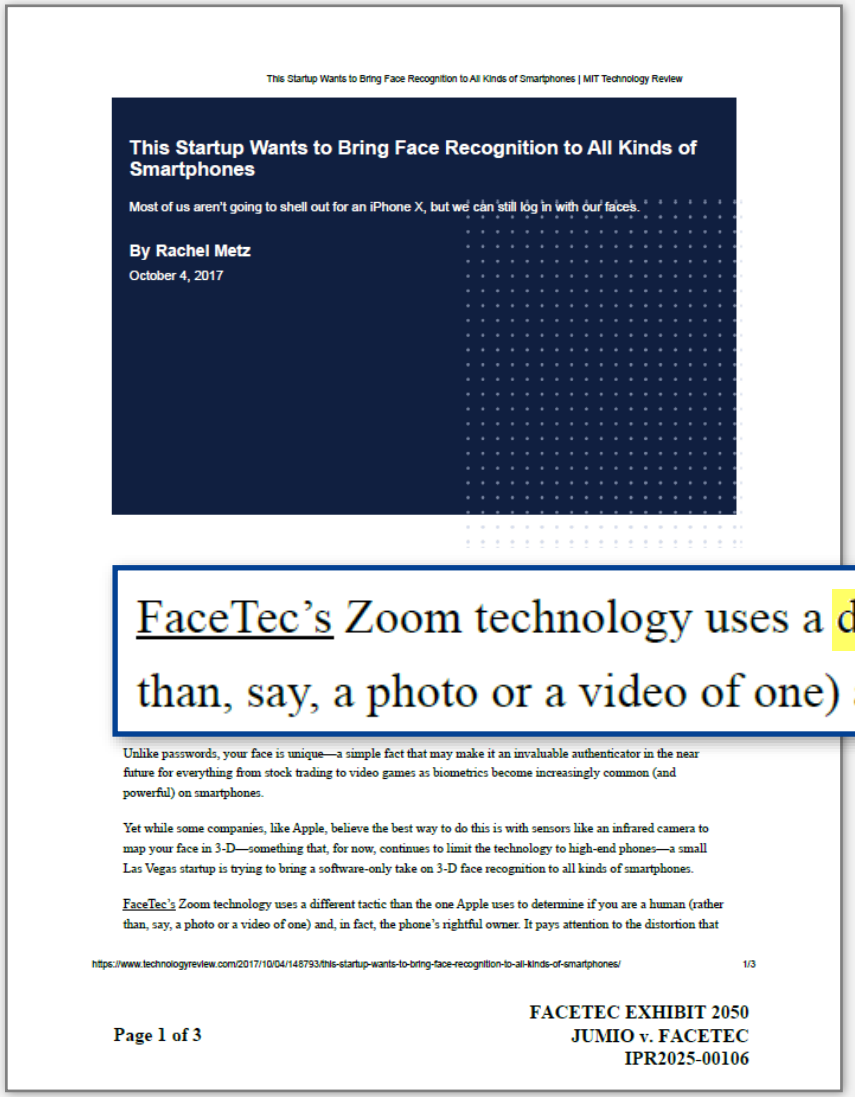
Eyeball Tracking for Liveness Check:

After the selfie is captured by the smartphone, a biometric-based technique known as eyeball tracking is employed to ensure the person is real and physically present during the transaction. A small circle is displayed and moves in random pattern around the screen while the user is instructed to follow the circle with their eyes. Since the dot moves randomly, we are easily able to disqualify photos, printouts, and pre-recorded videos from being substituted for a live camera capture.

JUMIO®

EX2049, 1

Purported Skepticism



This Startup Wants to Bring Face Recognition to All Kinds of Smartphones | MIT Technology Review

This Startup Wants to Bring Face Recognition to All Kinds of Smartphones

Most of us aren't going to shell out for an iPhone X, but we can still log in with our faces.

By Rachel Metz

October 4, 2017

Unlike passwords, your face is unique—a simple fact that may make it an invaluable authenticator in the near future for everything from stock trading to video games as biometrics become increasingly common (and powerful) on smartphones.

Yet while some companies, like Apple, believe the best way to do this is with sensors like an infrared camera to map your face in 3-D—something that, for now, continues to limit the technology to high-end phones—a small Las Vegas startup is trying to bring a software-only take on 3-D face recognition to all kinds of smartphones.

FaceTec's Zoom technology uses a different tactic than the one Apple uses to determine if you are a human (rather than, say, a photo or a video of one) and, in fact, the phone's rightful owner. It pays attention to the distortion that

https://www.technologyreview.com/2017/10/04/148793/this-startup-wants-to-bring-face-recognition-to-all-kinds-of-smartphones/ 1/3

Page 1 of 3

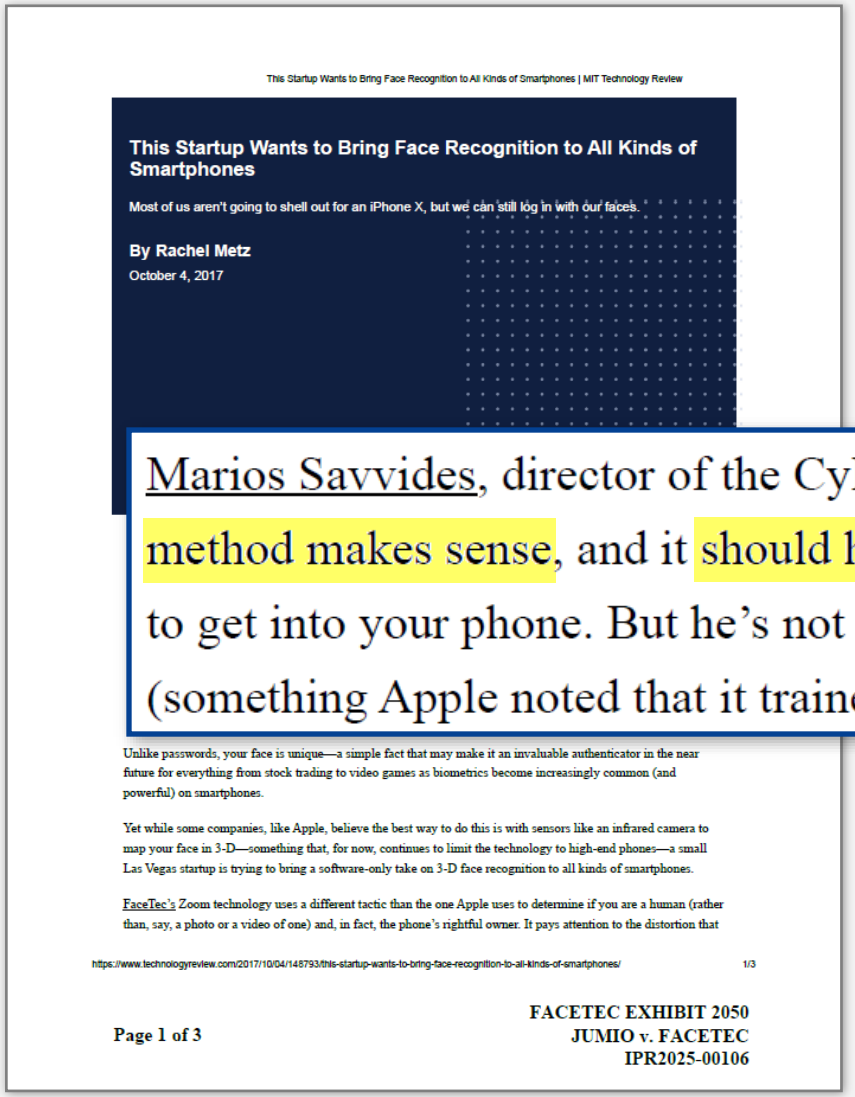
FACETEC EXHIBIT 2050
JUMIO v. FACETEC
IPR2025-00106

FaceTec's Zoom technology uses a different tactic than the one Apple uses to determine if you are a human (rather than, say, a photo or a video of one) and, in fact, the phone's rightful owner. It pays attention to the distortion that

EX2050, 1

'471 Reply (Paper 52), 34

Purported Skepticism



This Startup Wants to Bring Face Recognition to All Kinds of Smartphones | MIT Technology Review

This Startup Wants to Bring Face Recognition to All Kinds of Smartphones

Most of us aren't going to shell out for an iPhone X, but we can still log in with our faces.

By Rachel Metz
October 4, 2017

Unlike passwords, your face is unique—a simple fact that may make it an invaluable authenticator in the near future for everything from stock trading to video games as biometrics become increasingly common (and powerful) on smartphones.

Yet while some companies, like Apple, believe the best way to do this is with sensors like an infrared camera to map your face in 3-D—something that, for now, continues to limit the technology to high-end phones—a small Las Vegas startup is trying to bring a software-only take on 3-D face recognition to all kinds of smartphones.

FaceTec's Zoom technology uses a different tactic than the one Apple uses to determine if you are a human (rather than, say, a photo or a video of one) and, in fact, the phone's rightful owner. It pays attention to the distortion that

https://www.technologyreview.com/2017/10/04/148793/this-startup-wants-to-bring-face-recognition-to-all-kinds-of-smartphones/ 1/3

Page 1 of 3

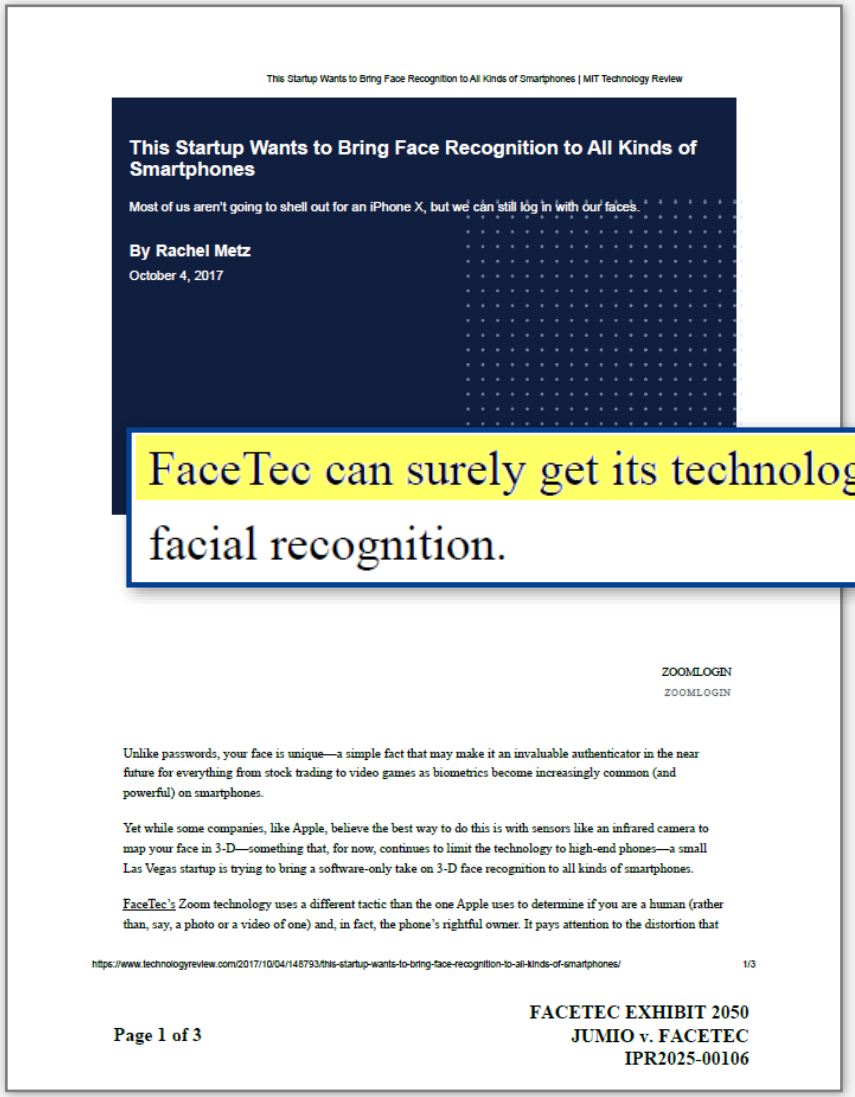
FACETEC EXHIBIT 2050
JUMIO v. FACETEC
IPR2025-00106

Marios Savvides, director of the CyLab Biometrics Center at Carnegie Mellon University, says that FaceTec's method makes sense, and it should help deflect some spoofing attacks like those using photographs in an attempt to get into your phone. But he's not sure if it could prevent someone with a 3-D mask from accessing the handset (something Apple noted that it trained Face ID to avoid).

EX2050, 2

'471 Reply (Paper 52), 34; Daft Reply Decl. (EX1060), ¶338

Purported Skepticism



This Startup Wants to Bring Face Recognition to All Kinds of Smartphones | MIT Technology Review

This Startup Wants to Bring Face Recognition to All Kinds of Smartphones

Most of us aren't going to shell out for an iPhone X, but we can still log in with our faces.

By Rachel Metz

October 4, 2017

ZOOMLOGIN

ZOOMLOGIN

Unlike passwords, your face is unique—a simple fact that may make it an invaluable authenticator in the near future for everything from stock trading to video games as biometrics become increasingly common (and powerful) on smartphones.

Yet while some companies, like Apple, believe the best way to do this is with sensors like an infrared camera to map your face in 3-D—something that, for now, continues to limit the technology to high-end phones—a small Las Vegas startup is trying to bring a software-only take on 3-D face recognition to all kinds of smartphones.

FaceTec's Zoom technology uses a different tactic than the one Apple uses to determine if you are a human (rather than, say, a photo or a video of one) and, in fact, the phone's rightful owner. It pays attention to the distortion that

https://www.technologyreview.com/2017/10/04/148793/this-startup-wants-to-bring-face-recognition-to-all-kinds-of-smartphones/ 1/3

Page 1 of 3

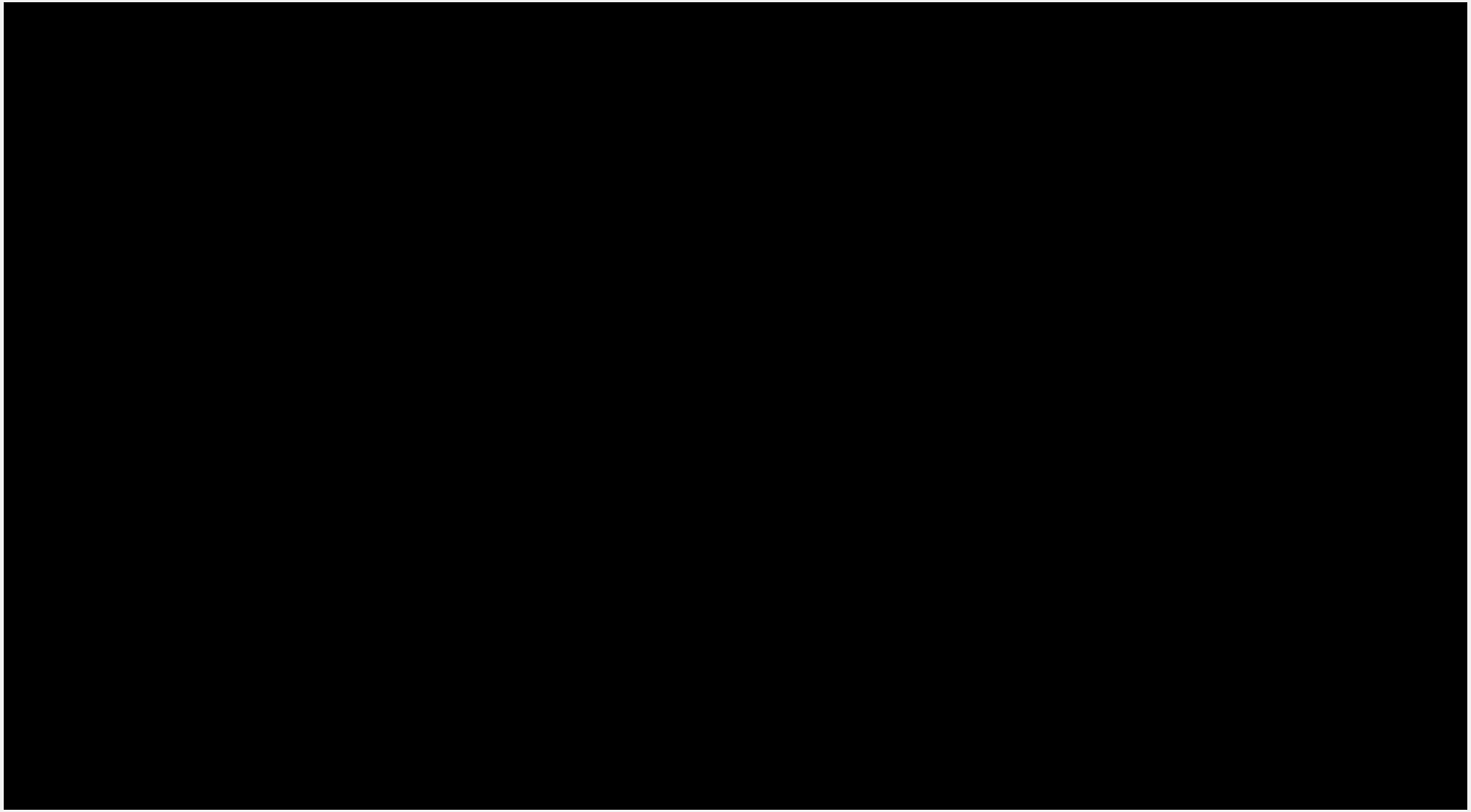
FACETEC EXHIBIT 2050
JUMIO v. FACETEC
IPR2025-00106

FaceTec can surely get its technology to work, he says, and it would be more secure than simple two-dimensional facial recognition.

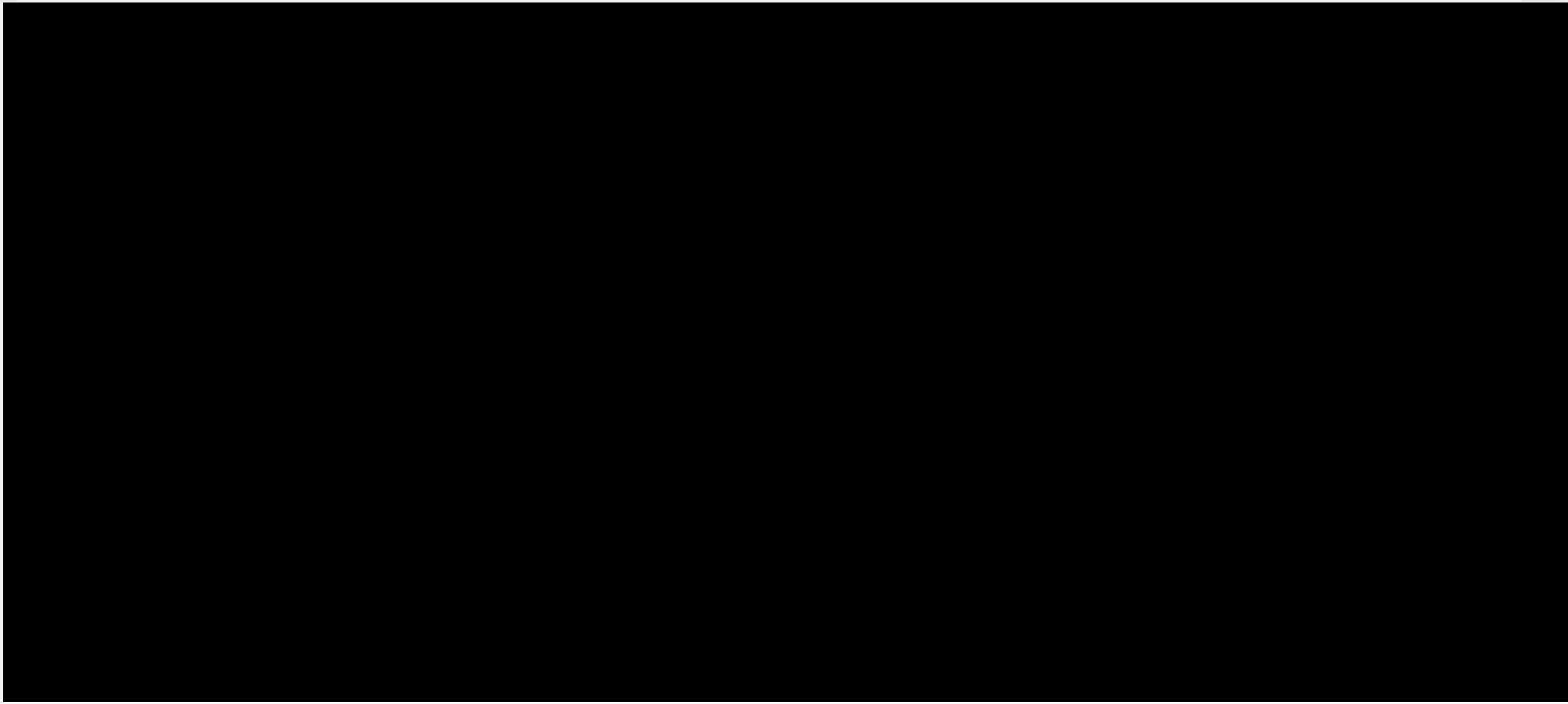
EX2050, 3

'471 Reply (Paper 52), 34; Daft Reply Decl. (EX1060), ¶339

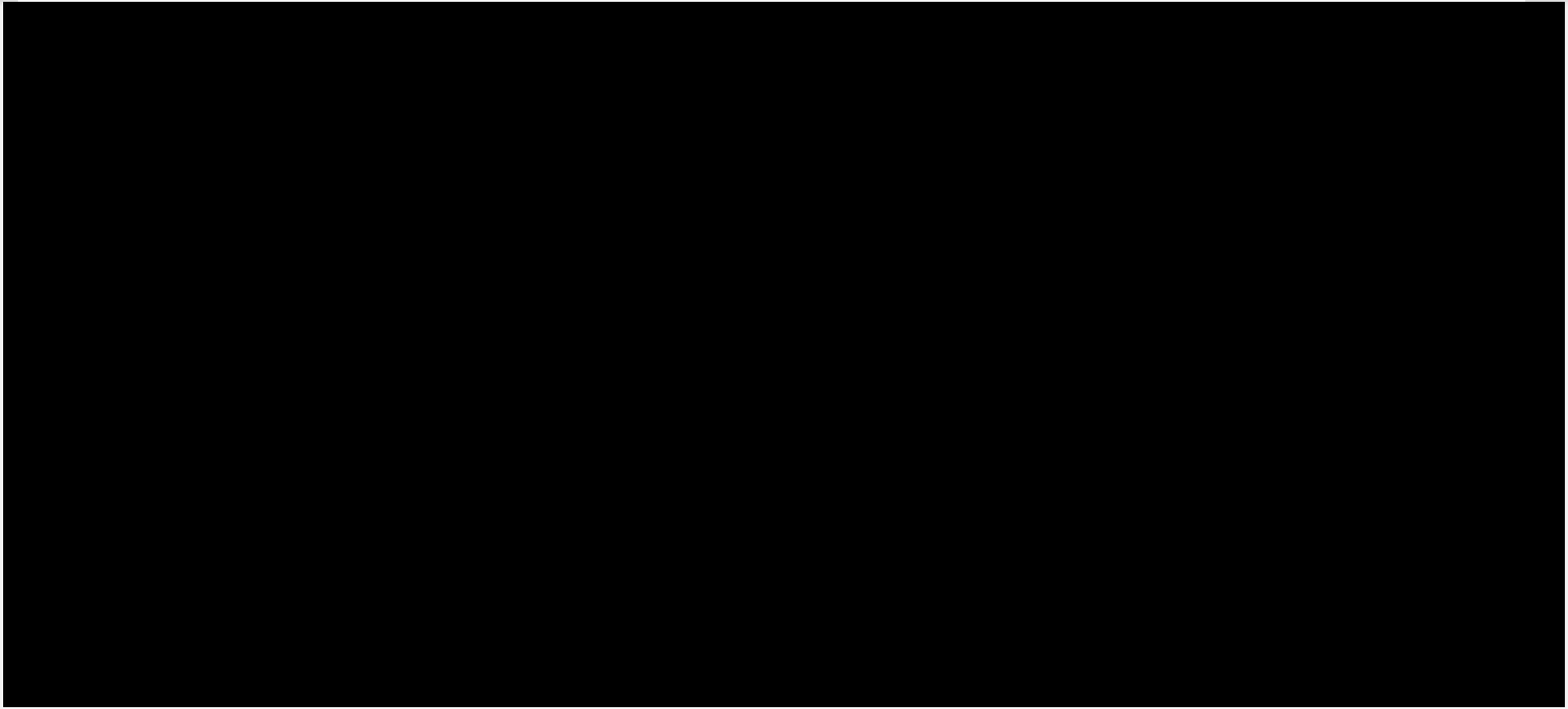
“Customer-Facing” Features



Jumio License Agreement



iProov Agreement



FaceTec's Contradictory Statements

Patent Owner

> FaceTec's 3D liveness detection technology was the first of its kind and effectively created the market for secure software-based 3D liveness detection, displacing 2D facial recognition technologies, particularly in high-risk industries.

'471 POR (Paper 43), 23

> The commercial success of FaceTec's software is not due to other factors. FaceTec was not the market incumbent, for example. In fact, FaceTec's software for 3D liveness detection was its first product, and thus, FaceTec had no brand recognition or goodwill. Ex. 2059, ¶54. Further, FaceTec engages in very few

'471 POR (Paper 43), 26

'471 Reply (Paper 52), 35; '471 POR (Paper 43), 23, 26

CERTIFICATE OF SERVICE (37 C.F.R. § 42.6(e)(4))

I hereby certify that the attached PETITIONER'S DEMONSTRATIVES were served as of the below date via email (by agreement) to the following counsel of record for Patent Owner:

Joshua L. Goldberg
Christopher C. Johns
Jason Stach
Chen Zang
Anthony Berlenbach
Kassandra M. Officer
Email: Joshua.Goldberg@finnegan.com
Email: Christopher.Johns@finnegan.com
Email: Jason.Stach@finnegan.com
Email: Chen.Zang@finnegan.com
Email: Anthony.Berlenbach@finnegan.com
Email: Kassandra.Officer@finnegan.com
Email: FaceTec-Jumio-IPRs@finnegan.com

Dated: March 12, 2026

/Jean Nguyen/
Jean Nguyen