

# Patent Owner's Demonstratives

Jumio Corp.,  
Petitioner

v.

FaceTec, Inc.,  
Patent Owner

IPR2025-00106 - Patent No. 10,776,471

IPR2025-00107 - Patent No. 11,157,606

IPR2025-00108 - Patent No. 11,693,938

IPR2025-00109 - Patent No. 11,874,910

# Numerous Reasons FaceTec Wins

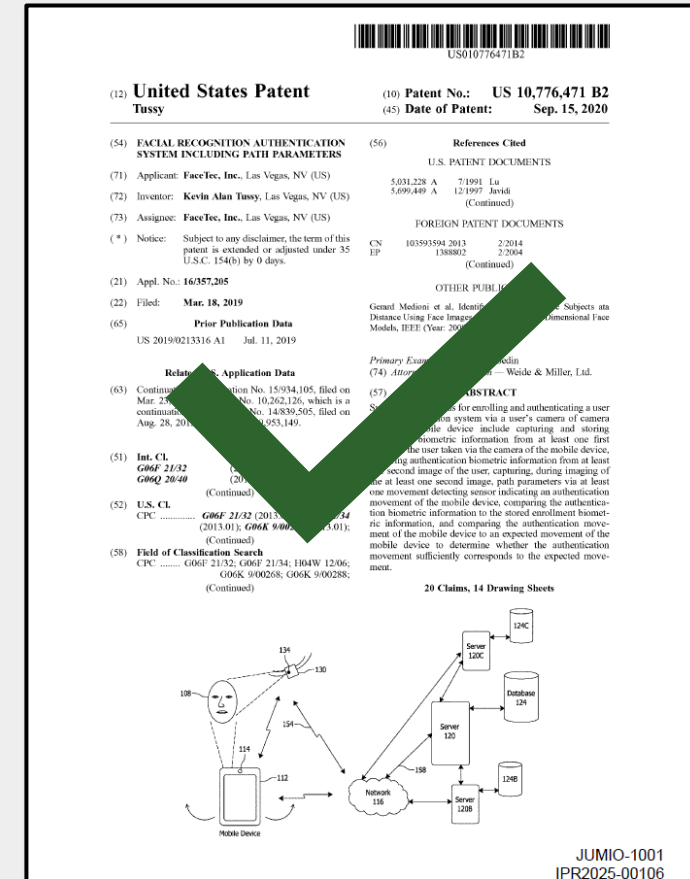
Jumio is time-barred and failed to name all real parties in interest

Objective evidence demonstrates nonobviousness

Dr. Daft's testimony must be excluded

Jumio's obviousness case does not reach the claims

Claims are **not** unpatentable



# **Jumio Is Time-Barred and Failed to Name All Real Parties in Interest**

# No Dispute that iProov Is Time-Barred for Two Patents

Complaint

Case No. 2024-ART-BNW Document 1 Filed 12/28/21 Page 1 of 17

Christopher Austin (NV Bar No. 6559)  
caustin@weidemiller.com  
WEIDENMILLER & MILLER, LTD.  
30655 Park Run Drive  
Suite 100  
Las Vegas, NV 89144  
Telephone: (702) 382-4804  
Facsimile: (702) 382-4805

Nathaniel L. Dilger (CA Bar No. 196203)  
Email: ndilger@oncllp.com  
Peter R. Afrasiabi (CA Bar No. 193336)  
Email: rafraziabi@oncllp.com  
ONE LLP  
23 Corporate Plaza  
Suite 150-105  
Newport Beach, CA 92660  
Telephone: (949) 502-2870  
Facsimile: (949) 258-5081

William J. O'Brien (CA Bar No. 99526)  
Email: wobrien@oncllp.com  
ONE LLP  
9301 Wilshire Blvd  
Penthouse Suite  
Beverly Hills, CA 90210  
Telephone: (310) 866-5157  
Facsimile: (949) 943-2085

Attorneys for Plaintiff,  
FaceTec, Inc.

UNITED STATES DISTRICT COURT  
DISTRICT OF NEVADA

FACETEC, INC., a Delaware corporation,  
Plaintiff,  
v.  
iPROOV LTD, a United Kingdom limited  
liability company,  
Defendant.

Case No.  
COMPLAINT FOR:  
(1) PATENT INFRINGEMENT;  
(2) BREACH OF CONTRACT  
(3) INTENTIONAL INTERFERENCE  
WITH CONTRACTUAL RELATIONS  
JURY DEMAND

COMPLAINT

PAGE 1 OF 17

FACETEC EXHIBIT 2024  
JUMIO v. FACETEC  
IPR2025-00106

FaceTec served iProov with infringement complaints for the '471 and '606 patents in **early 2022** (see Exs. 2024-2026)

I, Jay J. Schutttert, Esq., of the law firm of Evans Fears & Schutttert LLP, hereby accept service of the Summons and Complaint for Defendant iProov Ltd, a United Kingdom limited liability company.

Dated: January 26, 2022.

EVANS FEARS & SCHUTTERT LLP

Ex. 2025

# No Dispute that iProov Is Time-Barred for Two Patents

**Petition**

UNITED STATES PATENT AND TRADEMARK OFFICE  
BEFORE THE PATENT TRIAL AND APPEAL BOARD

JUMIO CORPORATION,  
Petitioner  
v.  
FACETEC, INC.,  
Patent Owner.

IPR2025-00106  
U.S. Patent No. 10,776,471

PETITION FOR *INTER PARTES* REVIEW  
OF U.S. PATENT NO. 10,776,471

Mail Stop PATENT BOARD  
Patent Trial and Appeal Board  
U.S. Patent & Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450

- Jumio filed these IPRs **more than 1 year later**, in late 2024

## NOTICE OF FILING DATE ACCORDED TO PETITION AND TIME FOR FILING PATENT OWNER PRELIMINARY RESPONSE

The petition for *inter parte* review filed in the above proceeding has been accorded the filing date of **November 7, 2024**.

Paper 5

- If iProov is an **RPI or privy**, the '471 and '606 Petitions are **time-barred** under 35 U.S.C. § 315(b)

# Petitions that Fail to Name All RPis Cannot Be Considered

35 U.S.C. § 312(a)(2): “(a) **REQUIREMENTS OF PETITION.**—  
A petition filed under section 311 may be considered only if—  
...  
(2) the petition identifies all real parties in interest

- If iProov is an **RPI**, the Board may not consider the '938 and '910 Petitions
- Collectively, all four petitions must be rejected under § 315(b) and/or § 312(a)(2)

# Jumio Bears the Burden of Proving iProov Is Not an RPI/Privy



Jumio “**bears the ultimate burden of persuasion** to show that its petitions are not time-barred under § 315(b).”

*Worlds Inc. v. Bungie, Inc.*, 903 F.3d 1237, 1242 (Fed. Cir. 2018)



“When a patent owner provides sufficient evidence prior to institution that reasonably brings into question the accuracy of a petitioner’s identification of RPIs, the overall **burden remains with the petitioner** to establish that it has complied with the statutory requirement to identify all [real parties in interest].”

*Applications in Internet Time, LLC, v. RPX Corp.*, 897 F.3d 1336, 1343 (Fed. Cir. 2018)

# Exemplary Factors Supporting RPI Status



1. Whether a nonparty “desires review of the patent”
2. “Whether a petition has been filed at a nonparty’s ‘behest’”
3. “Who, from a ‘practical and equitable’ standpoint, will benefit from the redress that the chosen tribunal might provide”
4. “The extent to which [the nonparty] has an interest in and will benefit from [the petitioner’s] actions”
5. Whether the petitioner “can be said to be representing that interest after examining its relationship with” the nonparty

*Applications in Internet Time, LLC, v. RPX Corp.*, 897 F.3d 1336, 1349-1353 (Fed. Cir. 2018)

# Privity Extends Beyond Real Parties in Interest



“The notion of ‘privity’ is **more expansive**, encompassing parties that do not necessarily need to be identified in the petition as a ‘real party-in-interest.’”

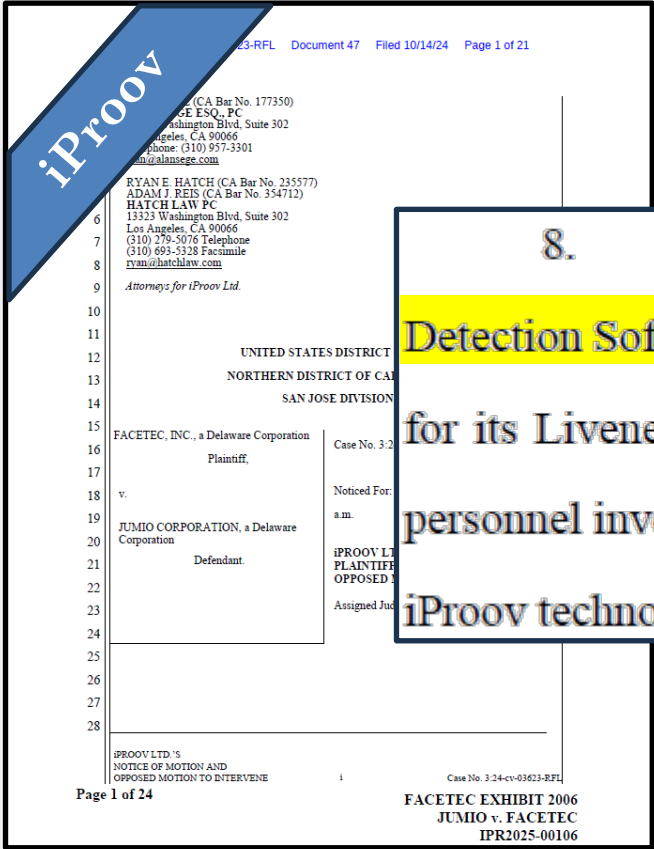
Consolidated Trial Practice Guide, 14



“[N]onparty preclusion may be based on a ‘**pre-existing substantive legal relationship**’ between the person to be bound and a party to the judgment . . . .”

*Taylor v. Sturgell*, 553 U.S. 880, 894-95 (2008)

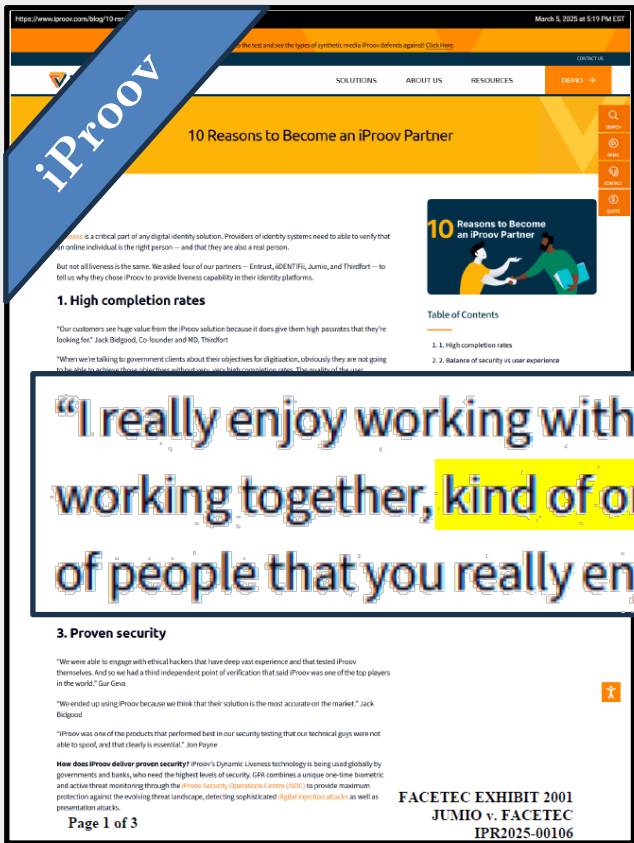
# iProov Supplies the Accused Technology to Jumio



8. Under the terms of the iProov-Jumio Agreement, iProov provides its Liveness Detection Software to Jumio for use in Jumio's own products. iProov maintains the source code for its Liveness Detection Software, as well as the technical documentation and employs the personnel involved in its development. iProov provides binary files to Jumio, who then embeds iProov technology into its products.

Ex. 2006, 23

# Jumio and iProov Collaborated re Accused Products

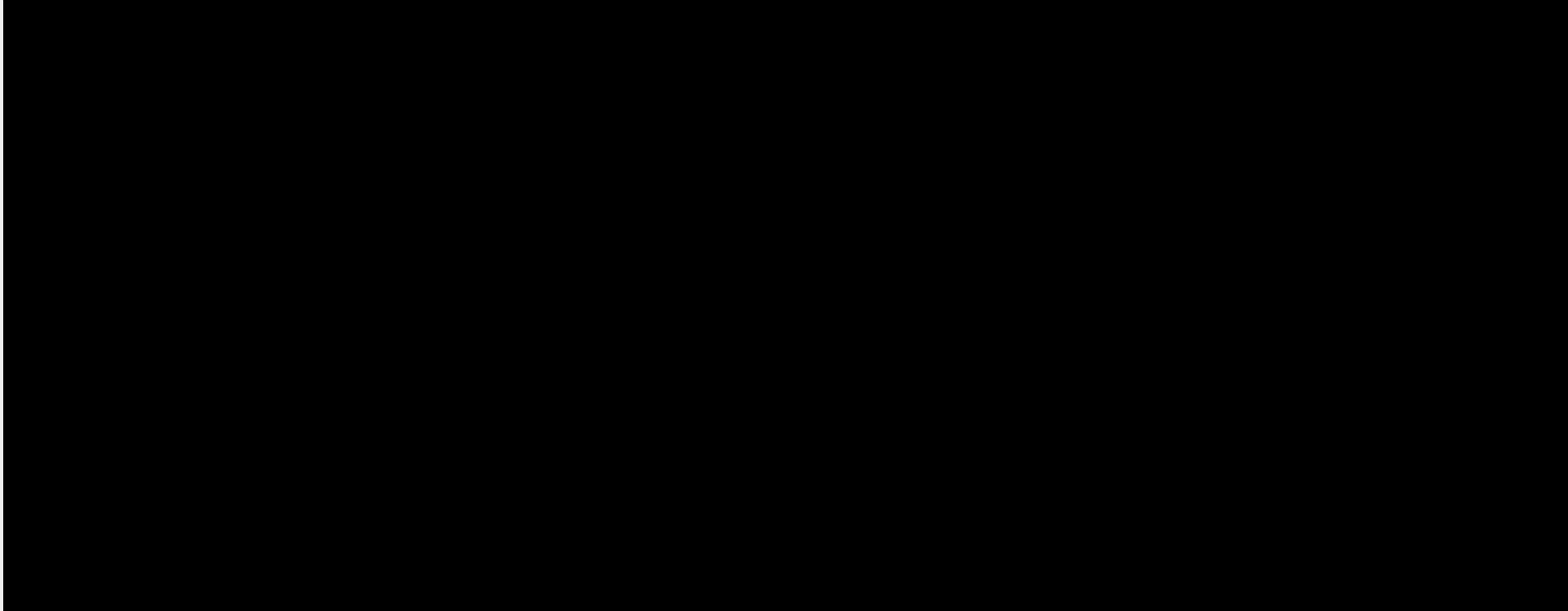


According to Jumio’s Chief Revenue Officer:

“I really enjoy working with the iProov team. So far everyone has proven to be really good to deal with. We’re working together, kind of one team, and I just can’t emphasize it enough: it’s great to be working with a bunch of people that you really enjoy spending time with.” Dean Hickman-Smith

Ex. 2001, 2

# Indemnification Supports Both RPI and Privity



# Indemnification Supports Both RPI and Privity

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Document 47 Filed 10/14/24 Page 1 of 21

**iProov**

RYAN E. HATCH (CA Bar No. 177350)  
ADAM J. FEIS (CA Bar No. 354712)  
HATCH LAW PC  
13323 Washington Blvd, Suite 302  
Los Angeles, CA 90066  
(310) 957-3301  
ryan@hatchlaw.com

Attorneys for iProov Ltd.

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN JOSE DIVISION

FACETEC, INC., a Delaware Corporation  
Plaintiff,

v.

JUMIO CORPORATION, a Delaware Corporation  
Defendant.

Case No. 3:23-cv-00100  
Noticed For Filing  
a.m.  
iPROOV LTD.'S  
PLAINTIFF  
OPPOSED MOTION  
Assigned Judge

Page 1 of 24

customers from infringement allegations.”). Second, iProov does in fact have an indemnification agreement with Jumio. Declaration of Ryan E. Hatch (“Hatch Decl.”), ¶ 7. And FaceTec already iProov also demonstrated that it has an economic interest in defending its customers. FaceTec finally argues iProov should only be granted limited intervention limited to the purposes expressly identified by iProov in its Motion. FaceTec cites no precedent granting such a request against the manufacturer of a product accused of infringement. In such cases, manufacturers routinely intervene as full parties to the suit, and iProov must not be hamstrung in its efforts to defend its customer from FaceTec’s claims of infringement.

Ex. 2006, 7, 10

106POR, 66, 67, 70; 106Sur-Reply, 30; 107POR, 64-66, 70;  
107Sur-Reply, 28; 108POR, 64-66, 70; 108Sur-Reply, 30;  
109POR, 67, 69, 72; 109Sur-Reply, 31

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

# Indemnification Supports Both RPI and Privity

Document 52 Filed 11/01/24 Page 1 of 6

**Judge Lin**

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

FACETEC, INC.,  
Plaintiff,  
v.  
JUMIO CORPORATION,  
Defendant.

Case No. 24-cv-00106  
ORDER  
VOLUNTARY  
PREJUDICIAL  
DISMISSAL  
MOTION  
Re: Dkt. No. 45

On June 14, 2024, FaceTec, Inc. brought this patent infringement action against Jumio Corporation concerning liveness detection, which helps face authentication by presenting a live human face. (Dkt. No. 1.) Jumio has represented that the allegedly infringing liveness detection applications was provided entirely by iProov Ltd. On September 10, 2024, FaceTec filed a notice of voluntary dismissal without prejudice. (Dkt. No. 45.) Because Jumio has answered the Complaint, Federal Rule of Civil Procedure 41(a)(2) prohibits voluntary dismissal without court approval. The Court finds both iProov's motion to intervene and FaceTec's motion for determination without oral argument pursuant to the reasons stated below, FaceTec's motion for voluntary dismissal and iProov's motion to intervene is **GRANTED**. This order is based on the facts, the applicable legal standards, and the arguments made by the parties. *FaceTec's Motion for Voluntary Dismissal Without Prejudice*

Page 1 of 6

1

JUMIO v. FACETEC  
IPR2025-00106

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.)

The disposition of this action may impair iProov’s ability to protect its interest. A finding of infringement based on accused technology owned by iProov would effectively be a finding of infringement by iProov. That would plainly affect iProov’s interest in that technology and its ability to market the accused technology to Jumio and other customers. FaceTec does not

Ex. 2010, 4

# Jumio and iProov Collaborated re Invalidity

Judge Lin

ReportsUtilitiesHelpLog Out

ADRMOP, AO279, PRVADR, STAYED

U.S. District Court  
California Northern District (San Francisco)  
CIVIL DOCKET FOR CASE #: 3:24-cv-03623-RFL

Case v. Jumio Corporation  
To: Judge Rita F. Lin  
35:271 Patent Infringement

Date Filed: 06/14/2024  
Jury Demand: Both  
Nature of Suit: 830 Patent  
Jurisdiction: Federal Question

Plaintiff

FaceTec, Inc.  
a Delaware corporation

represented by Nathaniel Luke Dilger  
One LLP  
23 Corporate Plaza  
Suite 150-105

01/08/2025

74

**ORDER** by Judge Rita F. Lin granting [69](#) Motion for Extension of Time to File. There is good cause to continue the requested deadlines for one week based on the need for iProov to coordinate finalizing invalidity contentions with Jumio, in light of the holidays. Disclosure of Invalidity Contentions under Patent Local Rules 3-3 and 3-4, and Exchange of Proposed Terms for Construction under Patent Local Rule 4-1, are due January 17, 2025. If the parties belief a further extension of other case deadlines is needed as a result, they may submit a further stipulation and proposed order, or if necessary, a motion. *(This is a text-only entry generated by the court. There is no document associated with this entry.)* (rflc1, COURT STAFF) (Filed on 1/8/2025) (Entered: 01/08/2025)

Page 1 of 15

IPR2025-00106

Ex. 2008, 12-13

15

106POR, 66, 67, 71; 107POR, 65, 67, 70  
108POR, 65, 67,70; 109POR, 67, 69, 73

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

# Jumio and iProov Collaborated re Invalidity

Ms. Kaiser

UNITED STATES PATENT AND TRADEMARK OFFICE  
BEFORE THE PATENT TRIAL AND APPEAL BOARD  
  
JUMIO CORPORATION,  
Petitioner  
  
FAC  
P  
  
Patent  
  
Inter Partes Re  
  
DECLARATION







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

Jumio Exhibit 1049 Page 1  
Jumio v. FaceTec IPR2025-00106

Ex. 1049, ¶6

# iProov's Invalidity Contentions Rely on IPR References

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**iProov**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Case No. 3:24-3623-RFL  
INTERVENOR IPROOV LTD'S PRELIMINARY

FACETEC, INC., a Delaware corporation,  
Plaintiff,  
v.  
JUMIO CORPORATION, a Delaware  
corporation,  
Defendant,  
and  
IPROOV, LTD, a United Kingdom limited  
company,  
Intervenor.

Page 1 of 193

1 FACETEC EXHIBIT 2011  
JUMIO v. FACETEC  
IPR2025-00106

3. U.S. PATENT PUB. NO. 2011/0299741 ("ZHANG")

31. U.S. PATENT PUB. NO. US 2002/0113884 ("TANII")

32. U.S. PATENT NO. US 8,437,513 ("DERAKHSHANI")

33. U.S. PATENT PUB. NO. 2010/0014720 ("HOYOS")

Ex. 2011, 15, 127, 128, 133

iProov is pursuing invalidity in two separate  
litigations for the '471 and '606 patents, and one  
litigation for the '938 and '910 patents

106POR, 68; 107POR, 67-68  
108POR, 67-68; 109POR, 70

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

17

# Jumio's Presents No Credible Evidence in Response



- Despite bearing the burden of persuasion, Jumio presents **no new post-institution evidence** to support that iProov is not an RPI or privy
- Relies only on attorney argument and Ms. Kaiser's pre-institution testimony, which did not withstand cross-examination

# Jumio's Attorney Argument Is Not Evidence

## Jumio's Attorney Argument

(1) Contrary to what iProov told the district court, the indemnification provisions have not been triggered

Jumio's counsel refused to respond to FaceTec's questions attempting to verify the truth and scope of their assertions:

**We will not continue this deposition via email.**

Ex. 1055, 3

## Jumio's Attorney Argument Is Not Evidence

- Jumio had the opportunity to provide a fact witness declaration, but chose not to
- Only attorney argument remains



“Statements of counsel . . . are not evidence.”

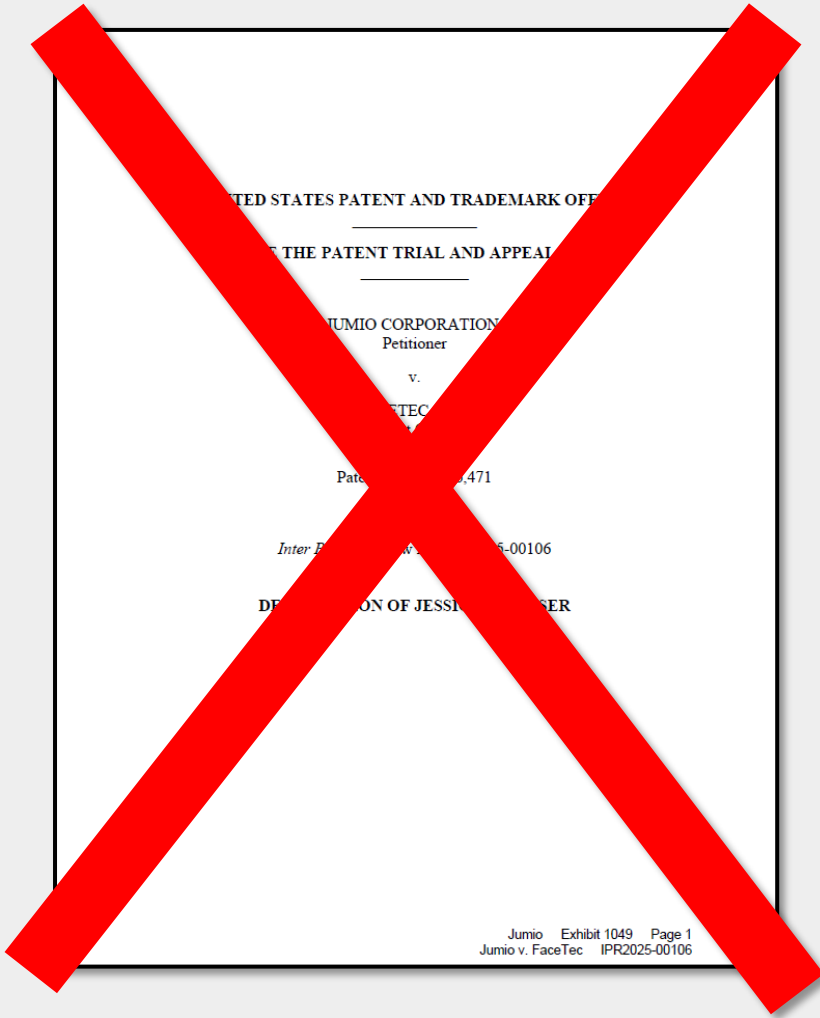
*NexStep, Inc. v. Comcast Cable Commc'ns, LLC*, 119 F.4th 1355, 1376 n.6 (Fed. Cir. 2024)



“Attorney argument . . . is not evidence” and cannot rebut evidence of record

*Gemtron Corp. v. Saint-Gobain Corp.*, 572 F.3d 1371, 1380 (Fed. Cir. 2009)

# Ms. Kaiser's Declaration Cannot Be Credited



Three categories of problems with Ms. Kaiser's testimony:

- (1) Admitted deficiencies
- (2) Refusals to answer based on overly broad privilege and work product objections
- (3) Inability to recall key information

106POR, 73-77; 106Sur-Reply, 32-34; 107POR, 73-76  
107Sur-Reply, 30-32; 108POR, 73-76; 108Sur-Reply, 32-33  
109POR, 75-79; 109 Sur-Reply, 33-34

# Admitted Deficiencies in Ms. Kaiser's Testimony

**Ms. Kaiser's declaration:**

1. I am an attorney with Perkins Coie LLP. I have personal knowledge of the facts set forth below, and if called as a witness, could and would competently testify thereto.

**But at her deposition,  
she admitted:**

9           A. I believe in Exhibit 1049 there  
10           are statements about what the petitioner  
11           knew or didn't know, and in making those,  
12           I made an investigation to make sure that  
13           that was true. Part of that investigation  
14           involved talking to people at the law firm  
15           who would have had knowledge about that,  
16           about those statements.

Ex. 1049, ¶1; Ex. 2086, 12:9-16

# Admitted Deficiencies in Ms. Kaiser's Testimony

**Ms. Kaiser's declaration:**

1. I am an attorney with Perkins Coie LLP. I have personal knowledge of the facts set forth below, and if called as a witness, could and would competently testify thereto.

**But at her deposition,  
she admitted:**

14 Q. What's your understanding of the  
15 nature of the coordination between Jumeo  
16 and IProov in relation to the invalidity  
17 contentions?

18 A. I don't have any personal  
19 knowledge. As I testified earlier, I  
20 didn't work on the invalidity contentions.  
21 But, I guess, I do know consistent with  
22 what's in my declaration, that there was  
23 no coordination prior to the IPR petitions  
24 being filed between Jumeo and IProov.

Ex. 1049, ¶1; Ex. 2086, 68:14-24

# Ms. Kaiser Did Not Speak to Jumio During Her Investigation

**Ms. Kaiser's declaration:**

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 or their substance with iProov.

**But at her deposition,  
she admitted:**

13 Q. Did you also speak with anyone  
14 at Jumio about this issue?  
15 MR. MOONEY: Objection. Form.  
16 THE WITNESS: I did not  
17 personally. I don't recall whether people  
18 on the team may have, but I did not  
19 personally.

Ex. 1049, ¶4; Ex. 2086, 13:13-19

# Ms. Kaiser Does Not Know if Jumio Sent Draft IPR Petitions to iProov

**Ms. Kaiser's declaration:**

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 or their substance with iProov.

**But at her deposition,  
she admitted:**

6 Q. Do you know if they shared them  
7 with other members of their team within  
8 Jumio?  
9 A. I do not.  
10 Q. Do you know if they shared them  
11 with anyone outside of Jumio besides  
12 Perkins Coie?  
13 A. I do not.

Ex. 1049, ¶4; Ex. 2086, 41:6-13

# Ms. Kaiser Does Not Know if Jumio Spoke with iProov After Filing

**Ms. Kaiser's declaration:**

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 or their substance with iProov.

**But at her deposition,  
she admitted:**

8 Q. Are you aware of anyone at Jumio  
9 who spoke with iProov about the IPR  
10 petitions after they were filed?  
11 A. I don't know.

Ex. 1049, ¶4; Ex. 2086, 74:8-11

# Ms. Kaiser Does Not Know if iProov Gave Jumio Prior Art

**Ms. Kaiser's declaration:**

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

**But at her deposition,  
she admitted:**

17 Q. Did IProov provide any prior art  
18 to Jumio before the IPR petitions were  
19 filed?

3 THE WITNESS: I'm not aware of  
4 conversations between IProov -- any  
5 conversations between IProov and Jumio  
6 directly, so I don't think I have  
7 knowledge to answer the question as you  
8 phrased it.

Ex. 1049, ¶5; Ex. 2086, 44:17-45:8 (intervening objections omitted)

# Ms. Kaiser's Refusal to Answer Questions

8                   What did you do to prepare the  
9                   declaration -- the four declarations that  
10                  you submitted in the IPRs?

11                 MR. MOONEY: Caution the witness  
12                 not to reveal any attorney-client  
13                 privileged information or work product in  
14                 responding to that question, but you can  
15                 respond.

16                 THE WITNESS: I don't know that  
17                 I can respond to the question without  
18                 revealing privileged information or work  
19                 product.

Ex. 2086, 10:8-19

# Ms. Kaiser's Refusal to Answer Questions

3           Q.    Has Jumeo requested a refund of  
4           any of the fees that have been billed to  
5           Jumeo?

6           MR. MOONEY:   Just a second,  
7           Ms. Kaiser.

11           And I would caution the witness  
12           not to reveal any attorney-client  
13           privileged communication in responding the  
14           question.

15           MS. JONES:   And I would repeat  
16           that from the perspective of a Perkins  
17           Coie privilege or work product protection.

18           THE WITNESS:   I don't think I  
19           can answer the question in light of the  
20           instructions.

Ex. 2086, 80:3-20 (some intervening objections omitted)

7           THE WITNESS:   I am going to  
8           follow my counsel's instruction and not  
9           respond to the question.

Ex. 2086, 81:7-9

17           THE WITNESS:   I am taking my  
18           counsel's instruction and declining to  
19           answer the question.

Ex. 2086, 81:17-19

13           THE WITNESS:   I'll take my  
14           counsel's advice and not answer that  
15           question.

Ex. 2086, 82:13-15

# Ms. Kaiser's Inability to Recall Who She Spoke With

8           Q.    Did you speak with every team  
9           member that you believe worked on the  
10          invalidity contentions as part of your  
11          investigation?

12          A.    I don't recall.

Ex. 2086, 66:8-66:12

22           THE WITNESS:   So I submitted  
23          this declaration over five months ago.  My  
24          recollection is I conducted an  
25          investigation, as I mentioned to you  
1          earlier.  As part of that investigation, I  
2          spoke to team members who worked on the  
3          invalidity contentions.  I believe that  
4          included Mr. Kinsel and Jessie, and it may  
5          have included other people.  I just don't  
6          recall specific names.

Ex. 2086, 65:22-66:6

# Objective Evidence Demonstrates Nonobviousness

# *Presumption of Nexus*

# FaceTec's Software Embodies the Claims (Undisputed)

## US 10,776,471

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.



Ex. 1001, claim 1

# FaceTec's Software Embodies the Claims (Undisputed)

## US 11,157,606

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 with the camera of the computing device at a **first distance** from the user;
- processing the at least one first image to obtain **first biometric data** from the at least one first image;
- capturing at least one **second image** of the user taken with the camera of the computing device at a **second distance** from the user, the second distance being different than the first distance;
- processing the at least one second image to obtain **second biometric data** based on the at least one second image;
- comparing the first biometric data with the second biometric data to determine whether the first biometric data matches the second biometric data;

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;

**determining that the user's face is three-dimensional** when:

- the first biometric data does not match the second biometric data; and
- the second biometric data has the expected differences as 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.

Ex. 1001, claim 1



# FaceTec's Software Embodies the Claims (Undisputed)

## US 11,693,938

8. A method for determining when a user, based on images of the user's face, does not exhibit three-dimensionality, the method comprising:

capturing at least one **first image** of the user's face taken with a camera located at a **first distance** from the user's face, the camera associated with a computing device; processing the at least one first image or a portion thereof to create **first data**;

moving the camera to a second distance from the user's face, where the second distance is different from the first distance;

capturing, at the **second distance**, at least one **second image** of the user's face taken with the camera associated with the computing device;

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

**examining the first data and the second data to determine whether differences between the first data and the second data indicate an expected type of distorting change in at least one image that is consistent with a real person being imaged and which is indicative of three-dimensionality;**

**determining the user's face is not three-dimensional when the first data and the second data do not have expected differences indicating the user exhibits three-dimensionality.**

Ex. 1001, claim 8



# FaceTec's Software Embodies the Claims (Undisputed)

## US 11,874,910

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.



Ex. 1001, claim 1

# FaceTec's Software Is Coextensive with the Claims

Integrated into this library is a piece of functionality called 3D Liveness Detection, which is our core foundational part of the product that opens up an interface for users to perform what we call a face scan.

Ex. 1082, 20:1-5

I do know that the primary aspect about the 3D Liveness Detection is the two-distance capture, the analysis of the signals that are apparent in the image data from the far distance to the close distance, extraction of perspective distortion signals, 3D signals. I do recall that we've looked at it before,

Ex. 1082, 52:18-23

And through that process, we developed what we initially called ZoOm. So for quite some time in the very early days of the company, we were developing the foundations of what would become ZoOm. And that is the -- the essential component to that is the two-distance capture of faces of users to identify, process, analyze, and extract the signal that occurs in the difference between the far-distance capture and the close-distance capture.

Ex. 1082, 25:17-25

A I'm not entirely sure if it was in 2013. I know that we've been focusing on it since basically the very beginning, and this two-distance capture and the extraction of those signals has been present in all of the versions of ZoOm or the FaceTec SDKs that we've ever put out.

Ex. 1082, 27:11-16

# FaceTec's Software Is Coextensive with the Claims

A Not entirely sure. It was in the very, very early days because, for the vast majority of the history of our company, we've been focusing on extracting the signal that occurs when doing this two-distance capture. So it was -- it was in the very, very early days of FaceTec.

Ex. 1082, 27:4-9

And the core primarily thing that we do as a part of 3D Liveness Detection and 3D Liveness Checks, that's essentially the core to our business. It's pretty much the only thing we get paid for. Customers come to us for this 3D Liveness Detection. It is analyzing signals that are apparent when we compare the far-distance images and signals to the close-distance images and signals. That's where the most significant signal for us to make a 3D liveness determination comes from. It's what sets us apart from all other solutions, is the 3D nature of this signal extraction and detection of expected differences comes from.

Ex. 1082, 40:19-41:5

## PROTECTIVE ORDER MATERIAL - ATTORNEYS' EYES ONLY

### CONFIDENTIAL - ATTORNEYS' EYES ONLY

UNITED STATES PATENT AND TRADEMARK OFFICE  
BEFORE THE PATENT TRIAL AND APPEAL BOARD

JUMIO CORPORATION,  
Petitioner,  
v.

FACETEC, INC.,  
Patent Owner.

Patent Nos.: 10,776,471  
11,157,606  
11,693,938  
11,874,910

Inter Partes Review Nos.: IPR2025-00106  
IPR2025-00107  
IPR2025-00108  
IPR2025-00109

\*\* CONFIDENTIAL - ATTORNEYS' EYES ONLY \*\*

DEPOSITION OF JOSHUA ROSE, Volume 1  
San Diego, California  
Thursday, January 15, 2026

Reported by:  
LESLIE JOHNSON, RPR, CCRR, CSR No. 11451  
Job No.: 7811282

PAGES 1 - 164

Page 1

Veritext Legal Solutions  
Calendar-CA@veritext.com 866-299-5127

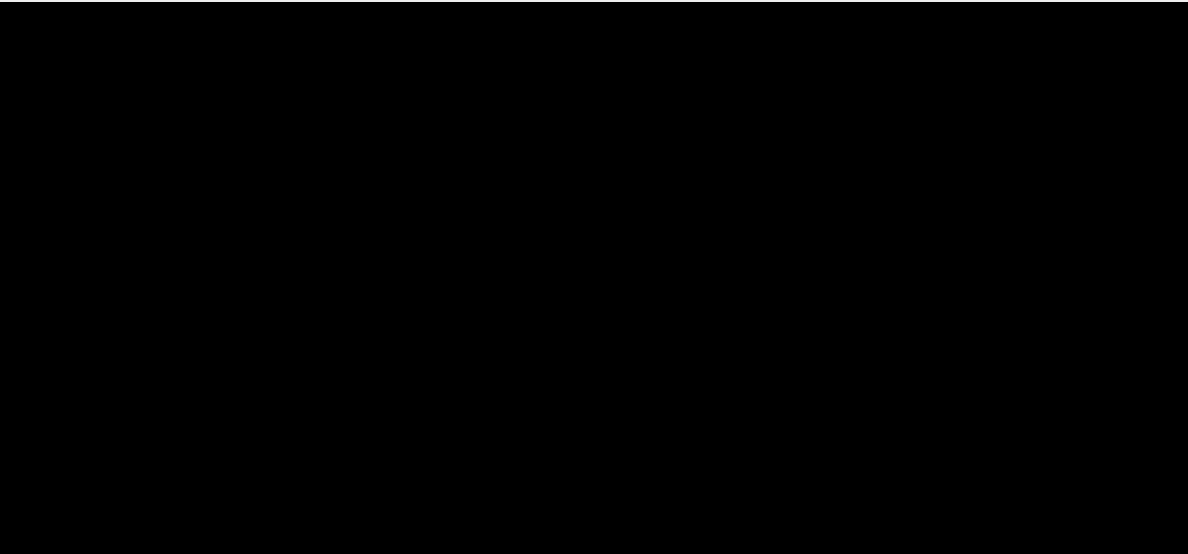
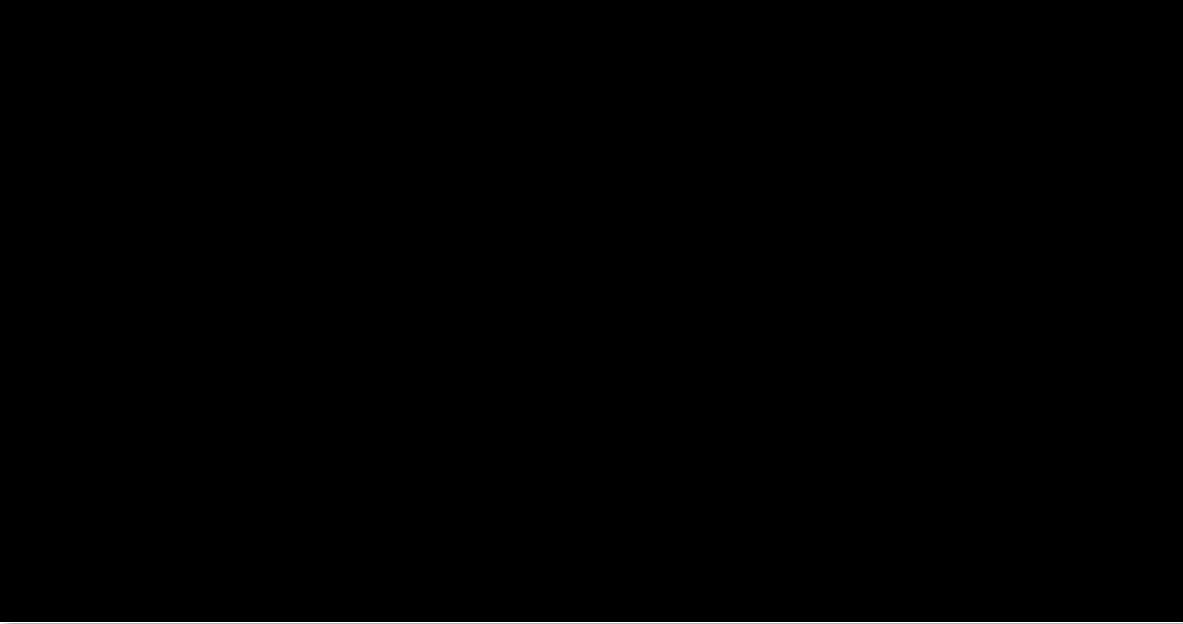
Jumio EX1082 Page 1  
Jumio v. FaceTec IPR2025-00108

THE WITNESS: So FaceTec's -- nearly all of FaceTec's entire business is customers and partners paying us for the 3D Liveness Check, the strength of that check, the security of it, the methods and approach that we take to doing it, the primary foundation of that being the capture and analysis of data from the user at the far distance and then the close distance, extracting a signal from that -- extracting many signals from that, including perspective distortion, other distortions and other signals.

Our entire business is rooted in that being the single most important -- I'll say one of the most important things about putting -- about creating a secure remote solution that involves user accounts and identity verification and account creation and log-in and age verification, even ID scanning. Our entire business is rooted in the belief that that is one of the most important things.

Ex. 1082, 69:7-25

# Liveness Checks Are the Direct Result of the Claimed Inventions

| Jumio's Position                                                                                                                                                           |                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>“According to FaceTec, these liveness checks are critical to defend against, e.g., 3D masked attackers.”<br/>106Reply, 29; 107Reply, 28; 108Reply, 26; 109Reply, 28</p> |                                                                                                                                                                                                                       |
| Expected Differences Include Expected Differences in Human Traits                                                                                                          |  <p>106Sur-Reply, 6; 107Sur-Reply, 6; 108Sur-Reply, 6; 109Sur-Reply, 6<br/>Second Rose Decl., ¶14; <i>see also id.</i> ¶¶5-13</p> |
|                                                                                          |                                                                                                                                                                                                                       |

Ex. 1082, 120:12-20

# Liveness Checks Are the Direct Result of the Claimed Inventions



Affirming presumption of nexus and crediting “the Board’s explanation of how each alleged unclaimed feature results directly from claim limitations—such that Velodyne’s products are essentially the claimed invention—both adequate and reasonable”

*Quanergy Sys., Inc. v. Velodyne Lidar USA, Inc.*, 24 F.4th 1406, 1419 (Fed. Cir. 2022)

# Encryption and Camera Control Support the Performance of 3D Liveness Checks

## Jumio's Position

“[T]amper proofing with encryption is so ‘very important,’ according to FaceTec.”

106Reply, 28; 107Reply, 27; 108Reply, 25-26; 109Reply, 27

“FaceTec believes controlling the camera to be critical.”

106Reply, 24-25; 107Reply, 23-24; 108Reply, 22-23; 109Reply, 24

We've done this kind of foundational element of the two-distance capture and the analysis for expected differences in all of the versions of our product.

Ex. 1082, 41:6-18

# 3D Liveness Checks Prevent Level 4 and Level 5 Attacks

## Jumio's Position

“[T]he Bounty program has a bounty for decrypting the FaceScan file.”

106Reply, 28; 107Reply, 27; 108Reply, 25; 109Reply, 27

“FaceTec believes controlling the camera to be critical, so much so that it created a Level 5 threat in its Spoof Bounty Program based on camera feed integrity.”

106Reply, 24-25; 107Reply, 23-24; 108Reply, 22; 109Reply, 24

- That FaceTec continues to improve its technology to address a small subset of additional threats does not make those improvements critical
- Level 4 – Even if an attacker could successfully edit the contents of the 3D FaceScan, FaceTec's three-dimensional depth checks and three-dimensional liveness checks would still need to be spoofed in order for an attack to be successful
- Level 5 – Even if an attacker could successfully take over the camera feed and inject previously captured frames, FaceTec's three dimensional depth checks and three-dimensional liveness checks would still need to be spoofed in order for an attack to be successful

106Sur-Reply, 8; 107Sur-Reply, 8; 108Sur-Reply, 8; 109Sur-Reply, 8

Second Rose Decl., ¶¶37-50

# Deleting the 3D FaceScan Supports the Performance of 3D Liveness Checks by Derisking Storage of Biometric Data

## Jumio's Position

“FaceTec describes the removal of liveness data as a ‘critical selling feature in our view.’”

106Reply, 29-30; 107Reply, 28-29; 108Reply, 27; 109Reply, 28-29

3D to 2D images. So that when Service New South Wales doesn't save biometric data—they, it's against the law for them to save the biometric data—they already have images of

\*\*\*

either matches or it doesn't, right? Either way, they delete the biometric - 3D face map. They don't save any of that information. So they get the benefit of our liveness and the benefit of our matching without having to compromise their laws and regulations about face matching data and saving it in a database, okay?

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: 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?

Ex. 1073, 9:1-10:5

“Deleting the 3D FaceScan does not impact the ability of the software to determine 3D liveness.”

“[I]t occurs it after the user's liveness has been determined.”

106Sur-Reply, 9; 107Sur-Reply, 9; 108Sur-Reply, 9-10; 109Sur-Reply, 9  
Second Rose Decl., ¶¶30-31; *see also id.* ¶¶27-29

Enabling Compliance ≠ “Criticality” in Patent Law

# FaceTec's UI with Ovals Is Not Critical

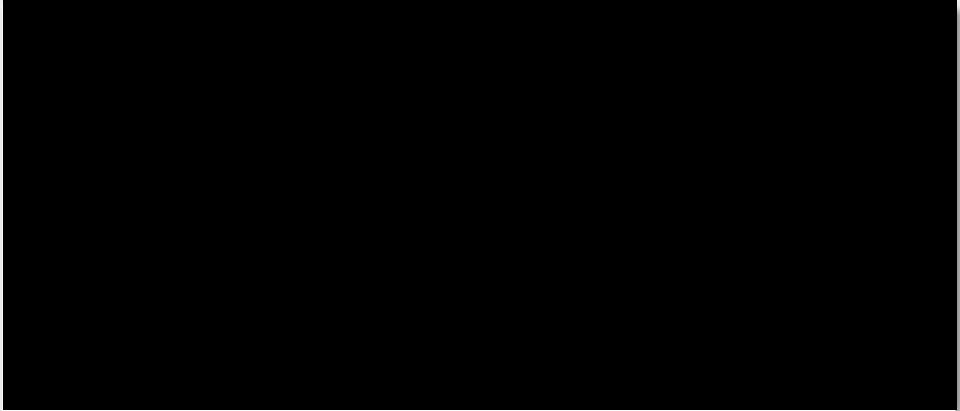
## Jumio's Position

while Rose viewed it as a 'security feature,' providing requisite 'guidance.'"

106Reply, 26; 107Reply, 25; 108Reply, 23-24; 109Reply, 25

Of course, in FIGS. 13A and 13B, shapes or guides other than ovals 1320 and 1330 may be used to guide the user to hold the mobile device 1310 at the appropriate distance from his or her face. For example, the mobile device 1310 may

106Ex. 1001, 29:43-46; 107Ex. 1001, 30:47-50; 108Ex. 1001, 29:46-49; 109Ex. 1001, 30:24-27  
Second Rose Decl., ¶¶32-36

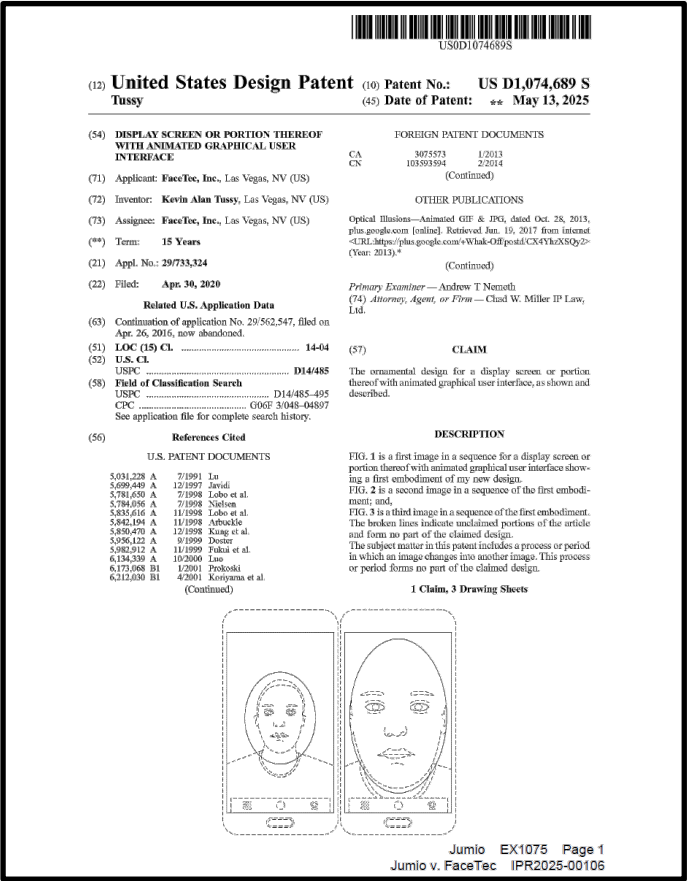


Ex. 1059, 112:7-13

46. iProov's technology includes at least two security features employed by FaceTec to enhance the security of its technology. The first is a user interface that requires users to provide images of their face from at least two different distances.

Ex. 2059, ¶46

# FaceTec’s UI with Ovals Is Not Critical



Ex. 1075



“Of course, a design patent cannot claim a purely functional design—a design patent is invalid if its overall appearance is ‘dictated by’ its function.”

*Sport Dimension, Inc. v. Coleman Co.*, 820 F.3d 1316, 1320 (Fed. Cir. 2016)

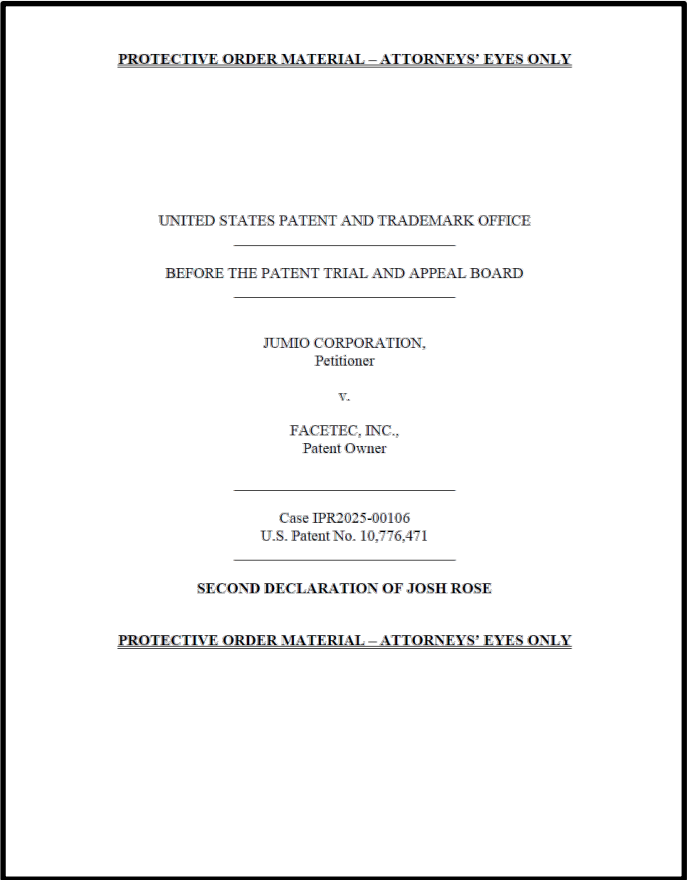
# Nexus Should Be Presumed Even Without Mr. Rose's Second Declaration



“[A] patent challenger cannot successfully rebut the presumption with argument alone—it must present evidence.”

*WBIP, LLC v. Kohler Co.*, 829 F.3d 1317, 1329 (Fed. Cir. 2016)

# Mr. Rose’s Second Declaration Should Be Admitted



Paper 64, Ex. A

“Mr. Rose is available for deposition March 10-13, 2026, and Petitioner has been provided an opposition to this motion to raise whatever issues it has with his testimony.”

Paper 64, 5

# *Direct Nexus*

# *Industry Praise*

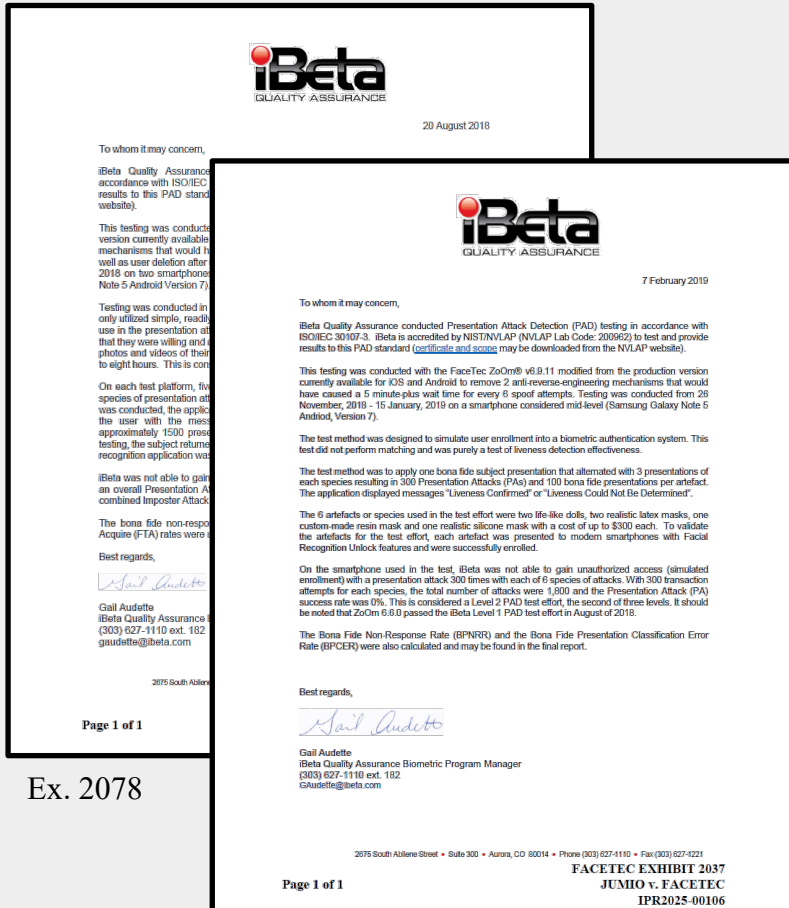
# Industry Praise



“Industry participants, especially competitors, are not likely to praise an obvious advance over the known art.”

*Apple Inc. v. Samsung Elecs. Co.*, 839 F.3d 1034, 1053 (Fed. Cir. 2016)

# Jumio Praised FaceTec's Software



“[W]e have partnered with a company called FaceTec out of the United States. They have built a *genius solution* that is easy to use and is *extremely strong and spoof proof*. They’re *pretty much the only company on the planet right now that has reached a level 2 certification against the Presentation Attack Detection ISO standard*, which means there are over 3000 standardised tests of paper prints out, screens, videos, masks, puppets that are used to test the [] spoof proofness of the authentication solution.”

Ex. 2057, 11:10; Ex. 2085, 8

Ex. 2037

# Jumio Praised FaceTec's Software

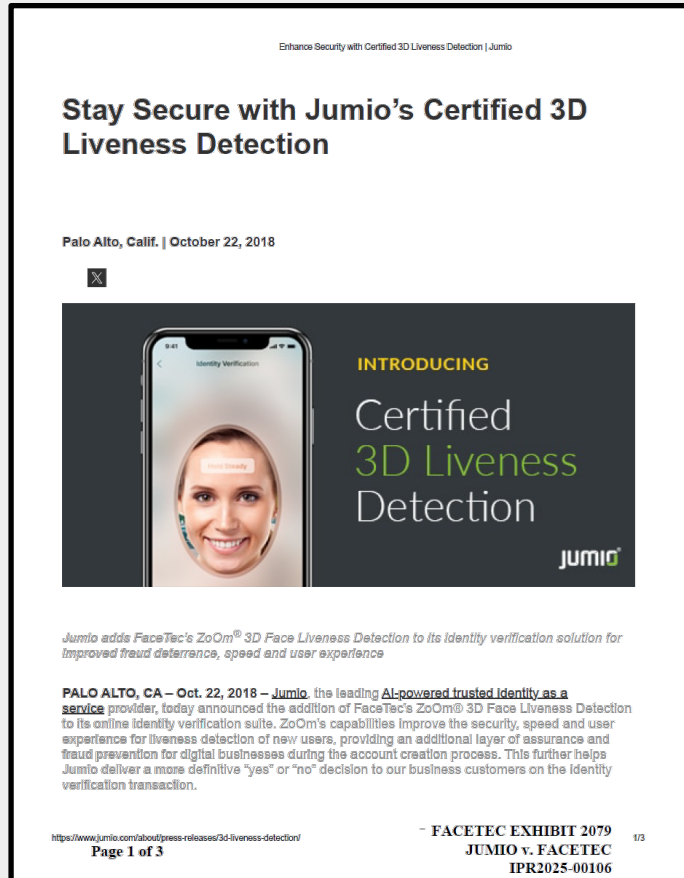


"In our tests, ZoOm quickly distinguished itself as the segment leader," said Philipp Pointner, Chief Product Officer of Jumio. "The interface is intuitive and the liveness detection AI is by far the strongest we have ever seen."

"In addition to its anti-spoofing detection capabilities, FaceTec's liveness detection offers some very tangible benefits in terms of a more streamlined user experience and omnichannel support," said Stephen Stuu, Chief Executive Officer of Jumio. "ZoOm-enhanced liveness detection will be integrated within the Netverify solution at no additional charge to our existing customers. This integration improves the quality of Jumio's identity verification process which, in turn, provides a better onboarding experience and dramatically reduces the number of manual reviews performed by our business customers."

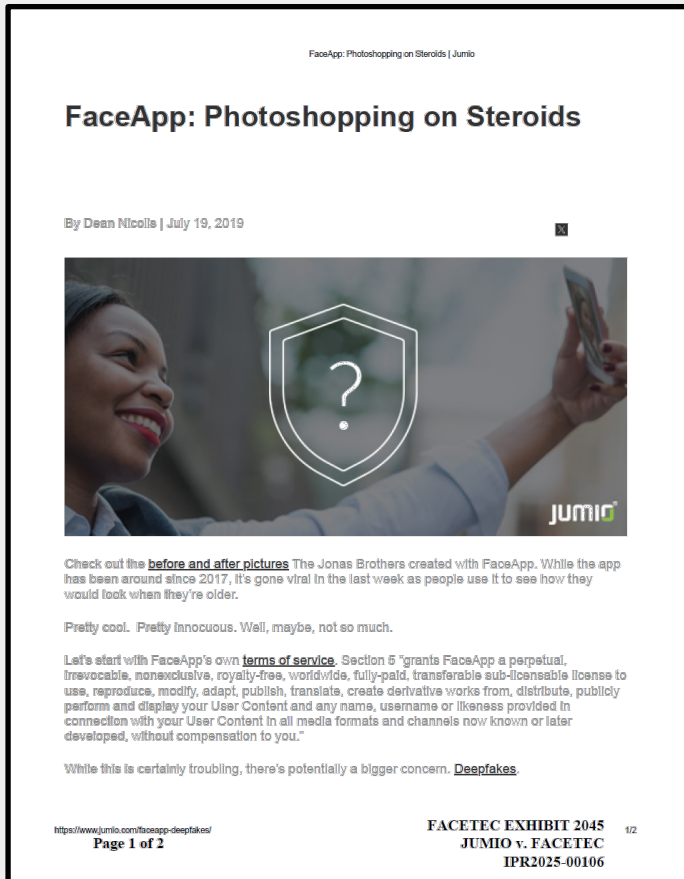
After rigorous testing of numerous liveness detection solutions in this quickly evolving space, ZoOm provided the most accurate and secure solution.

This new integration translates into a better and more accurate experience that helps digital companies increase their confidence that new users are who they claim to be during the crucial new customer onboarding process. The upgraded liveness detection functionality provides a more seamless experience that helps convert more legitimate customers and better flags suspicious accounts who attempt to spoof the liveness detection process. These advanced liveness detection technologies provide Jumio a significant competitive advantage in terms of speed, accuracy, and anti-spoofing capabilities.



Ex. 2079, 1-2

# Jumio Praised FaceTec's Software



With liveness detection, the online user is prompted to perform an action that cannot be easily replicated with a spoof. It might involve keystroke analysis, recording a series of random numbers, eyeball tracking or flashing lights on the user's face. At Jumio, we've embedded FaceTec's patented ZoOm technology into our identity verification and authentication workflows. Using this technology, users just fit their face into a small oval on the screen, and the oval gets larger and the user move closer to fit into the second oval. During the two-second process, we capture 30-60 frames of video per second and create an encrypted 3D face map, in which perspective distortion, or the fisheye effect, is measured. If it's not a three-dimensional object, FaceTec's algorithms will conclude it's a 2D image like a picture, rejecting the spoof attempt.

Ex. 2045, 2

# Jumio Was Not Using FaceTec's 3D:3D Face-Matching

## Jumio's Position

“The statements Petitioner made, which were made in the partnership announcement, discussed ZoOm, something more than just the check for three-dimensionality. Petitioner's license also included the *matching feature*, something separate from the 3D liveness checks but was discussed in tandem with the liveness check at the talk FaceTec cited.”

106Reply, 31; 107Reply, 30; 108Reply, 28; 109Reply, 30



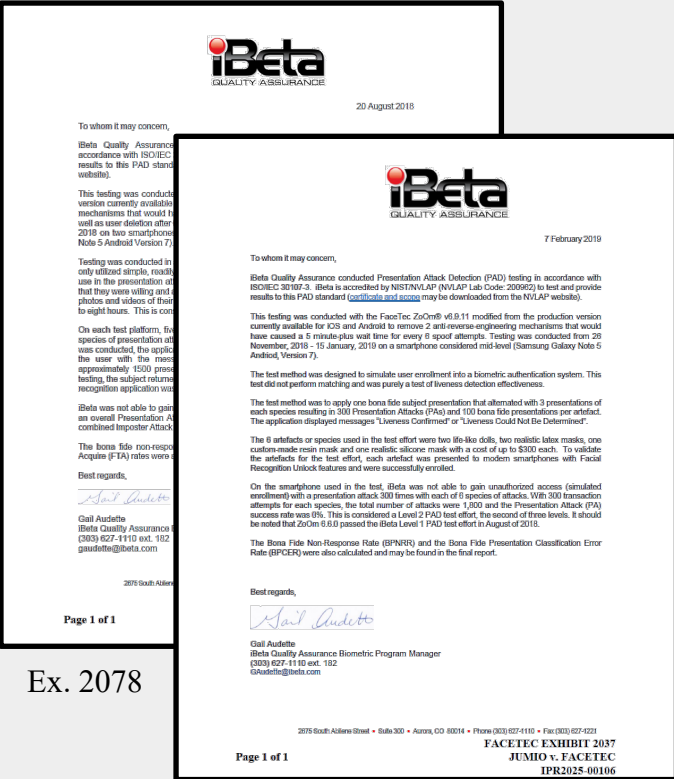
“It's a solution that is a marriage of two best in class solutions, *the identity proofing from Jumio* and the liveness and authentication from [FaceTec].”

Ex. 2057, 14:14; Ex. 2085, 10  
Second Rose Decl., ¶53

# Jumio Touted FaceTec's Certifications

## Jumio's Position

“FaceTec itself called ISO/IEC 30107-3 standard-based certifications (like iBeta and Bixelab) ‘outdated.’”  
106Reply, 30; 107Reply, 29; 108Reply, 27; 109Reply, 29



Ex. 2078

Ex. 2037



“[W]e have partnered with a company called FaceTec out of the United States. They have built a genius solution that is easy to use and is extremely strong and spoof proof. *They’re pretty much the only company on the planet right now that has reached a level 2 certification against the Presentation Attack Detection ISO standard*, which means there are over 3000 standardised tests of paper prints out, screens, videos, masks, puppets that are used to test the the spoof proofness of the authentication solution.”

Ex. 2057, 11:10; Ex. 2085, 8

# *Copying*

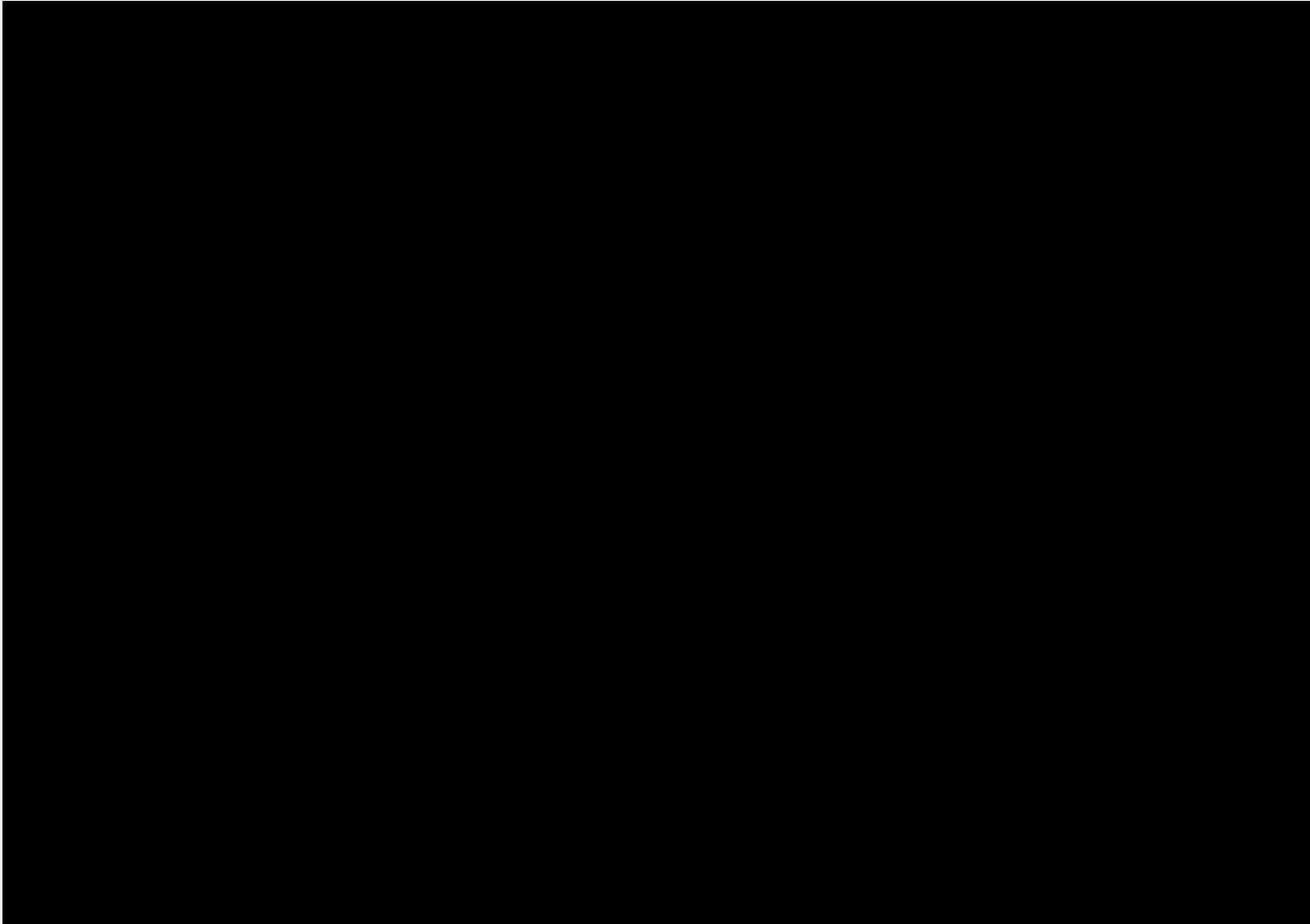
# Copying



“Evidence of access and substantial similarity *is* evidence of copying.”

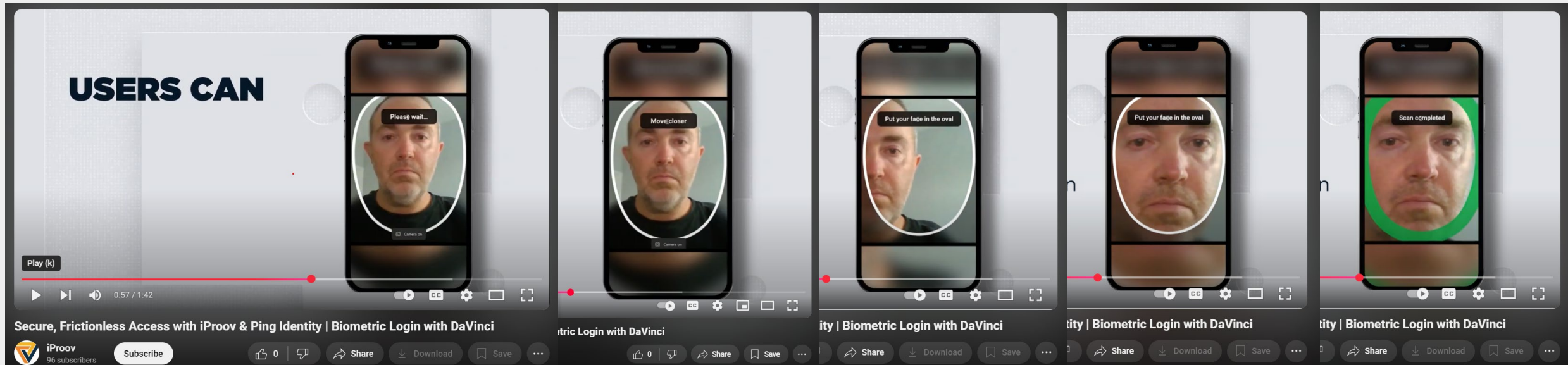
*Medtronic, Inc. v. Teleflex Innovations S.a.r.l.*, 70 F.4th 1331, 1340 (Fed. Cir. 2023)

# iProov Copied FaceTec's Software



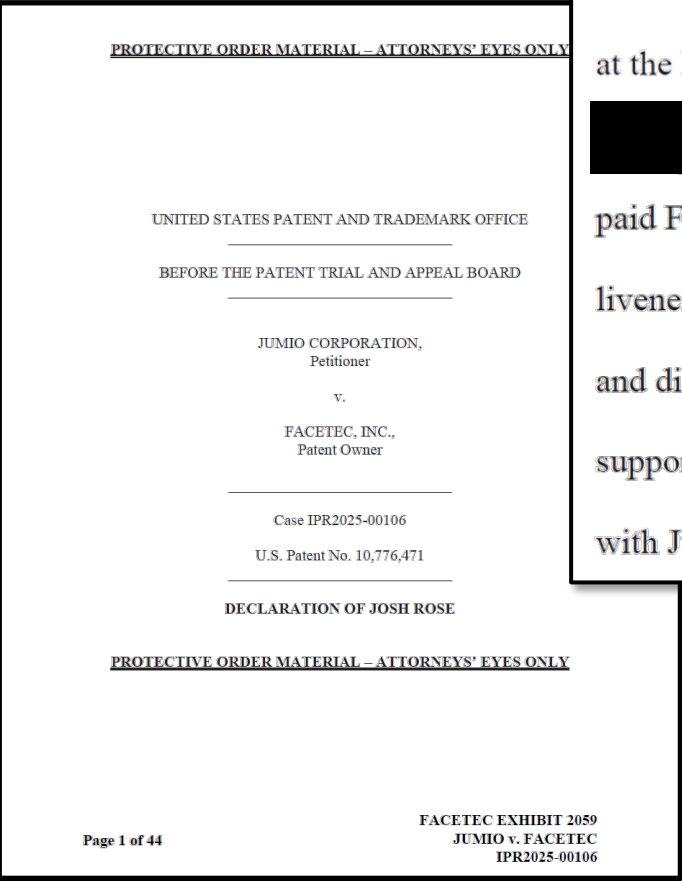
Exs. 2051-2056

# iProov Copied FaceTec's Software

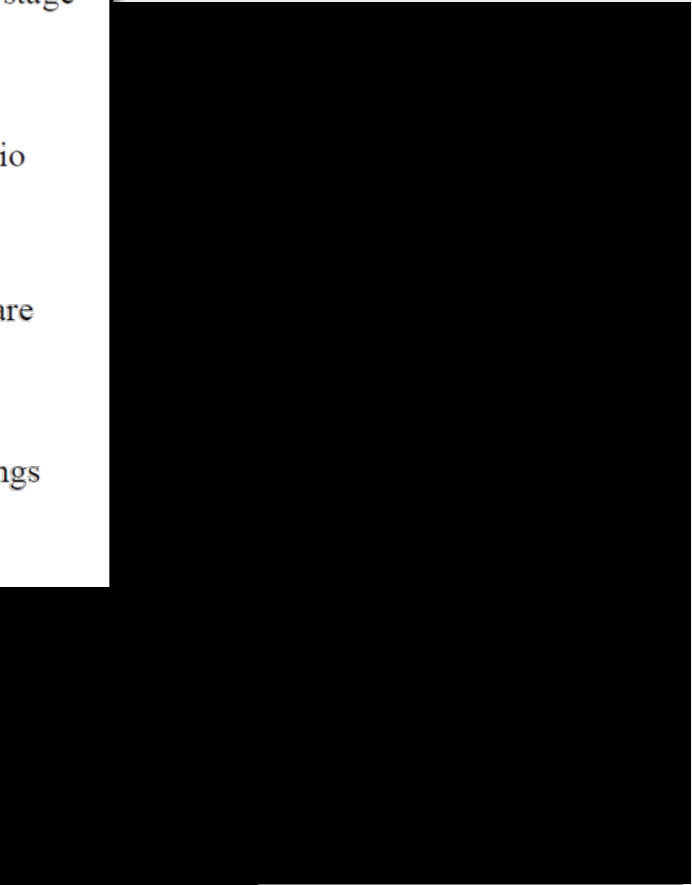


Ex. 2071; *see also* Turk, ¶¶466-69, App'x A-D

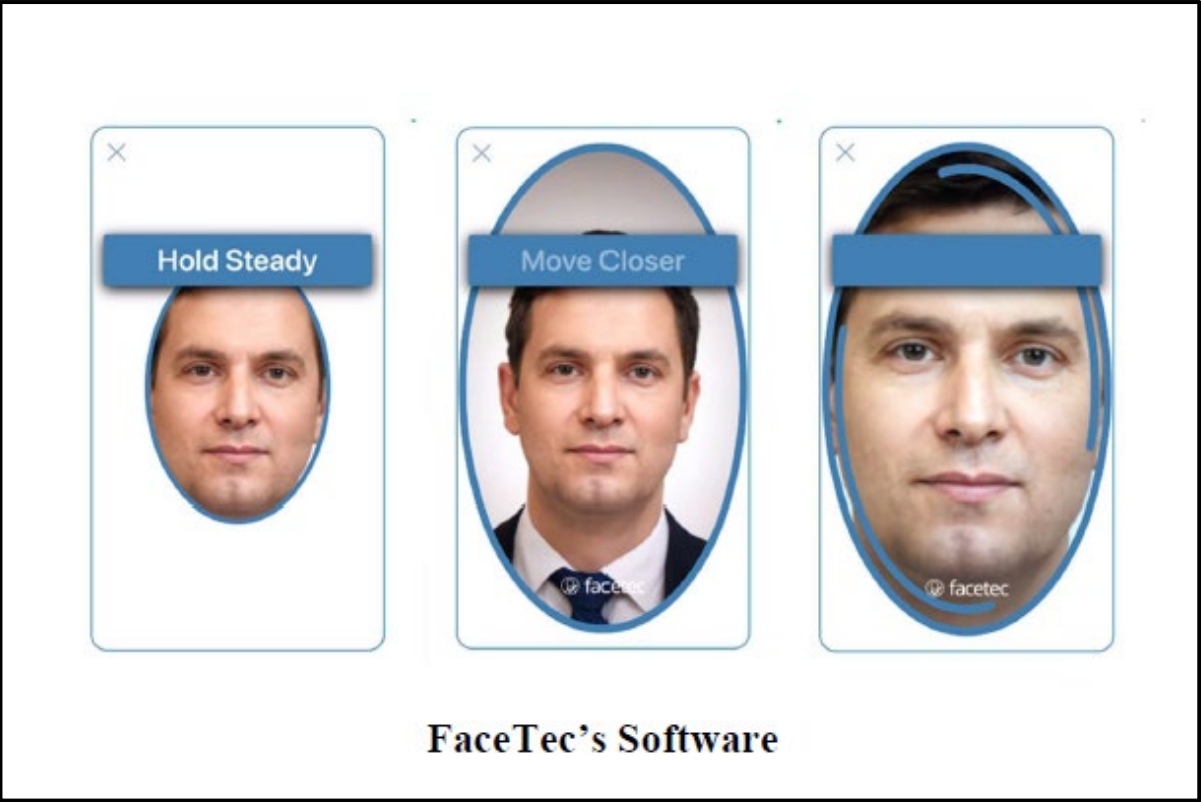
# Jumio Copied FaceTec's Software



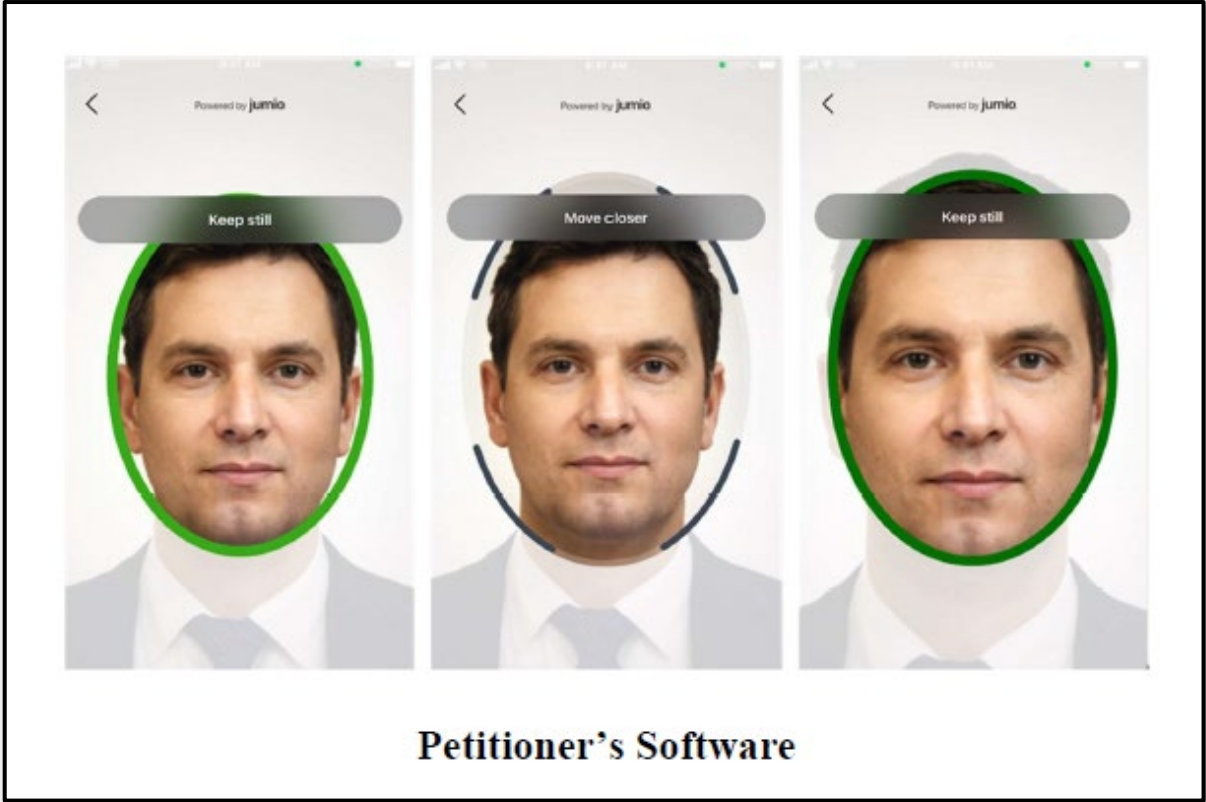
50. Jumio called FaceTec's software "a genius solution" publicly on stage at the Finovate EU 2019 conference and licensed FaceTec's software from [REDACTED] Ex. 2057 at 11:10. During that time, Jumio paid FaceTec over [REDACTED] for the performance of over [REDACTED] 3D liveness checks. *See* Ex. 2058. Jumio also had full access to FaceTec's software and digital documentation as well as deep access to FaceTec's developers for support. FaceTec had a multitude of emails, phone calls, and in-person meetings with Jumio and sent Jumio presentations, sales materials, and white papers.



# Jumio Copied FaceTec's Software



FaceTec's Software



Petitioner's Software

Ex. 2072; *see also* Turk, ¶¶470-73, App'x E-H

# Jumio's Response Lacks Credibility

## Jumio's Position

FaceTec fails to show “any kind of determination of three-dimensionality resulting from expected differences between images.”

106Reply, 32-33; 107Reply, 31-32; 108Reply, 29-30; 109Reply, 31-32

- Dr. Turk established access and substantial similarity
  - Dr. Turk does not have access to iProov's or Petitioner's source code
  - Petitioner does have access to its source code and is conspicuously silent
- Logical inference that iProov's or Petitioner's software is comparing the images for expected differences
  - Imposition on the user

# *Long-Felt Need, Failures of Others, and Licensing*

# FaceTec's Software Satisfied a Long-Felt Need

Received November 6, 2014, accepted November 20, 2014, date of publication December 18, 2014, date of current version January 7, 2015.

IEEE Access

Received November 6, 2014, accepted November 20, 2014, date of publication December 18, 2014, date of current version January 7, 2015.  
Digital Object Identifier 10.1109/ACCESS.2014.2381272

## Biometric Antispoofing Methods: A Survey in Face Recognition

JAVIER GALBALLY<sup>1</sup>, SÉBASTIEN MARCEL<sup>2</sup>, (Member, IEEE), AND JULIAN FIERREZ<sup>3</sup>

<sup>1</sup>Spain Research Center for Biometric Systems (CIBERS), Institute for the Protection and Security of the Citizen, Ager 01012, Spain  
<sup>2</sup>Centre de Recherche en Informatique, Université de Lausanne, CH-1015, Switzerland  
<sup>3</sup>Research Group in Biometric Systems (GRIBS), Universidad Autónoma de Madrid, Madrid 28049, Spain

Corresponding author: J. Galbally (javier.galbally@icac.es, correio.es)

This work was supported in part by the CAM under Project S2009/TIC-1485, in part by the Ministry of Economy and Competitiveness through the IIS-III-SHIELD Project under Grant TIN2012-34081, in part by the TABULA RASA Project under Grant FP7-ICT-257201, in part by the HEAT Project under Grant FP7-512724 through the European Union, and in part by the CiberBio Universidad Autónoma de Madrid-Spain.

**ABSTRACT** In recent decades, we have witnessed the evolution of biometric technology from the first pioneering works in face and voice recognition to the current state of development wherein a wide spectrum of highly accurate systems may be found, ranging from largely deployed modalities, such as fingerprint, face, or iris, to more marginal ones, such as signature or hand. This path of technological evolution has naturally led to a critical issue that has only started to be addressed recently: the resistance of this rapidly emerging technology to external attacks and, in particular, to spoofing. Spoofing, referred to by the term presentation attack in current standards, is a purely biometric vulnerability that is not shared with other IT security solutions. It refers to the ability to fool a biometric system into recognizing an illegitimate user as a genuine one by means of presenting a synthetic forged version of the original biometric trait to the sensor. The entire biometric community, including researchers, developers, standardizing bodies, and vendors, has thrown itself into the challenging task of proposing and developing efficient protection methods against this threat. The goal of this paper is to provide a comprehensive overview on the work that has been carried out over the last decade in the emerging field of anti-spoofing, with special attention to the mature and largely deployed face modality. The work covers theories, methodologies, state-of-the-art techniques, and evaluation databases and also aims at providing an outlook into the future of this very active field of research.

**INDEX TERMS** Biometrics, security, anti-spoofing, face.

### 1. INTRODUCTION

"Fingerprints cannot lie, but liars can make fingerprints". Unfortunately, this paraphrase of an old quote attributed to Mark Twain<sup>1</sup> has been proven right in many occasions now. And not only for fingerprints, but also for many other biometric traits such as face, iris, voice or even gait.

Every technology has its own time. Since the first pioneering works on automatic voice and face recognition over 40 years ago [1]–[3], steady and continuous progress has been made in the development of biometric technology. Driven by the very appealing new security biometric paradigm "forget about cards and passwords, you are your own key", researchers from many different fields such as image processing, computer vision or pattern recognition, have applied the newest techniques in each of these areas to improve the

performance of biometric systems [4]. This path of technological evolution has permitted the use of biometrics in many diverse activities such as forensics, border access control, surveillance or on-line commerce.

In this scenario of constant expansion, and as a consequence of its own natural progress, new concerns are arising regarding biometric technology different from the mere improvement of its recognition performance. Among these new issues and challenges that have emerged around biometrics, its resilience against external threats has lately drawn a significant level of attention.

Currently it is an accepted fact that, as the deployment of biometric systems keeps growing year after year in such different environments as airports, laptops or mobile phones, users are also becoming more familiar with their use in everyday life and, as a result, their security weaknesses are better

**ABSTRACT** In recent decades, we have witnessed the evolution of biometric technology from the first pioneering works in face and voice recognition to the current state of development wherein a wide spectrum of highly accurate systems may be found, ranging from largely deployed modalities, such as fingerprint, face, or iris, to more marginal ones, such as signature or hand. This path of technological evolution has naturally led to a critical issue that has only started to be addressed recently: the resistance of this rapidly emerging technology to external attacks and, in particular, to spoofing. Spoofing, referred to by the term presentation attack in current standards, is a purely biometric vulnerability that is not shared with other IT security solutions. It refers to the ability to fool a biometric system into recognizing an illegitimate user as a genuine one by means of presenting a synthetic forged version of the original biometric trait to the sensor. The entire biometric community, including researchers, developers, standardizing bodies, and vendors, has thrown itself into the challenging task of proposing and developing efficient protection methods against this threat. The goal of this paper is to provide a comprehensive overview on the work that has been carried out

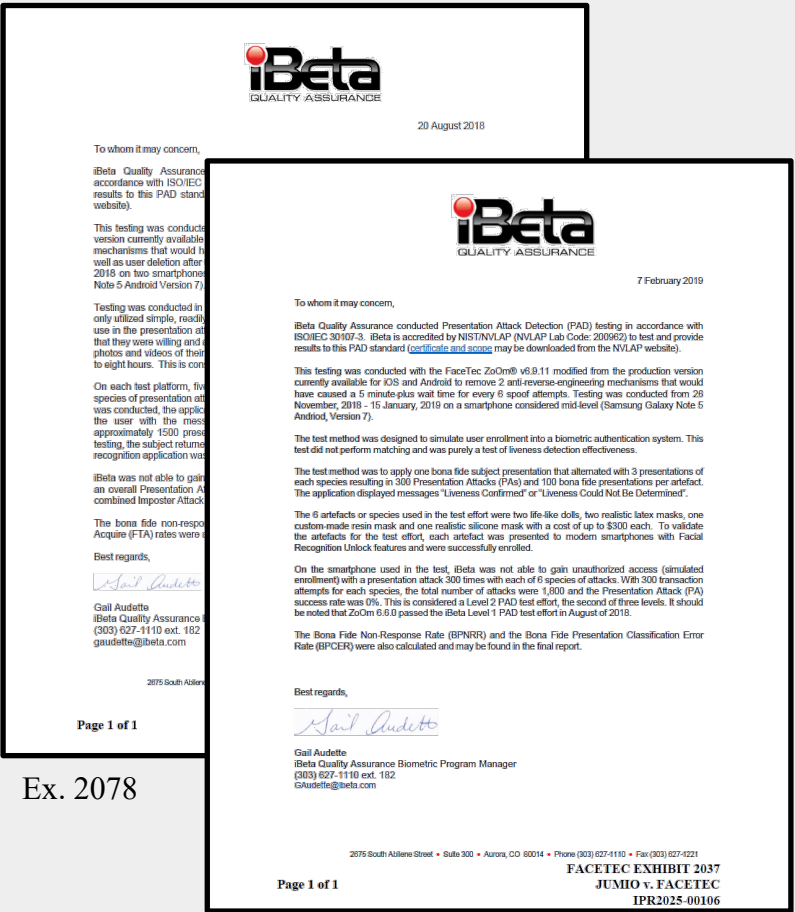
As a wrap up conclusion it may be stated that, although a great amount of work has been done in the field of spoofing detection and many advances have been reached, attacking methodologies have also evolved becoming more and more sophisticated. As a consequence, there are still big challenges to be faced in the protection against direct attacks, that will hopefully lead in the coming years to a new generation of more secure biometric systems.

Page 1 of 23

FACETEC EXHIBIT 2047  
JUMIO v. FACETEC  
IPR2025-00106

Ex. 2047, Abstract, 1548

# FaceTec's Software Satisfied a Long-Felt Need



Ex. 2078

Ex. 2037

## How to Participate in the Bounty Program

Read and agree to the Terms and Conditions outlined below, and then successfully Spoof or Bypass FaceTec's Liveness Detection with a method that qualifies as Level 1, 2, 3, 4 or 5 on the [Liveness.com](http://www.liveness.com) (<http://www.liveness.com>) Threat Vector Scale, reproduce it, and be paid a bounty as follows:

| 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<br><br>\$90,000<br>Total  |
| Level 2 | Commercially available lifelike dolls, and resin, latex & silicone 3D masks up to USD\$300 in price.                                                                                      |                                                                                                                                                                                                                                                       | Browser, iOS, & Android: \$30,000<br><br>\$90,000<br>Total  |
| Level 3 | Custom-made ultra-realistic 3D masks, sculptures, wax heads, etc. up to USD\$3,000 in creation costs.                                                                                     |                                                                                                                                                                                                                                                       | Browser, iOS, & Android: \$40,000<br><br>\$120,000<br>Total |
| 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. | <p>3D FaceScan<br/>Tampering<br/>(<a href="https://dev.facetec.com/security-best-practices#facemap-tampering">https://dev.facetec.com/security-best-practices#facemap-tampering</a>)</p>                                                                                                                                                 | Browser, iOS, & Android: \$60,000<br><br>\$180,000<br>Total |
| Level 5 | Successfully take over the camera feed & inject previously captured frames that result in the FaceTec Server responding with Liveness Success.                                            | <p>ManyCam<br/>(<a href="https://manycam.com/">https://manycam.com/</a>)<br/>Vcam<br/>(<a href="https://www.e2esoft.com/vcam/">https://www.e2esoft.com/vcam/</a>)<br/>vlc2Cam (<a href="https://vlc2vcam.com/">https://vlc2vcam.com/</a>)<br/>FakeWebcam<br/>(<a href="https://www.fakewebcam.com/">https://www.fakewebcam.com/</a>)</p> | Browser, iOS, & Android: \$40,000<br><br>\$120,000<br>Total |

Ex. 2046

# Jumio's Response Lacks Credibility

## Jumio's Position

“[N]one of [FaceTec's] evidence mentions a need for liveness based on ‘three-dimensionality.’”

106Reply, 33; 107Reply, 32; 108Reply, 30; 109Reply, 32

- Petitioner narrowly circumscribes the need as one for liveness based on three-dimensionality
- Petitioner improperly conflates the industry need (liveness detection) with FaceTec's innovative solution (liveness based on three-dimensionality)

# Jumio Tried and Failed to Meet This Need and Licensed FaceTec's Software



## Jumio Adds Biometric Facial Recognition to Netverify

By David Penn Posted on October 24, 2016  
Categories: Jumio



Adding biometric facial recognition to its flagship Netverify digital ID-verification platform will enable Jumio to offer a "three-pronged approach to the KYC process on mobile," the company said today. The facial recognition technology combines with Netverify's Face Match and ID-verification functionality to provide financial services companies, banks, and other businesses with a greater ability to prevent digital fraud.

Jumio CEO Stephen Stunt referenced the recent unauthorized, account opening scandal at Wells Fargo in discussing the need for better anti-fraud solutions. "It's critical to look beyond existing multifactor-authentication solutions whenever any digital transaction takes place," Stunt said. "The addition of biometric facial recognition, combined with ID verification, will ... help ensure that the individual in front of the screen is who they say they are."

<https://finovate.com/jumio-adds-biometric-facial-recognition-netverify/>  
Page 1 of 2

FACETEC EXHIBIT 2048  
JUMIO v. FACETEC  
IPR2025-00106 1/2

The biometric facial recognition technology Jumio is adding to Netverify will add "liveness" detection to the platform. "Liveness" detection combats fraudsters who attempt to use static images to trick authentication systems. By monitoring for and identifying even the most minute facial movements, "liveness" detection combines well with other tools like Face Match to grow customer conversions, as well as reduce fraud. And because both "liveness" detection and Face Match work quickly ("no more than five seconds"), the customer experience remains smooth and efficient.

Ex. 2048, 2

# Jumio Tried and Failed to Meet This Need and Licensed FaceTec's Software



Fraudsters evolve. So should your identity solution.

With many traditional identity verification solutions, users are asked to take a picture of their government-issued ID using a smartphone or computer webcam. The problem is, many fraudsters can pass these tests with the legitimate passports or driver's licenses they have stolen. The IDs are legit, they just don't belong to the person who is attempting to do business with you.



Intimidate and Deter Fraudsters with Liveness Detection

Jumio has pioneered liveness detection technology to thwart fraudsters' evolving and sophisticated attempts to assume another individual's identity. Starting by requiring users to take a selfie or a picture of themselves with a customized handwritten note, Jumio's Netverify takes identity verification to the next level.

Liveness detection for mobile or web helps you:

- ✓ Ensure your customer or user is physically present
- ✓ Ensure the user's selfie is legitimate
- ✓ Minimize fraud and the resulting costs of unauthorized transactions
- ✓ Maintain a positive customer experience

## 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

Page 1 of 2

FACETEC EXHIBIT 2049  
JUMIO v. FACETEC  
IPR2025-00106

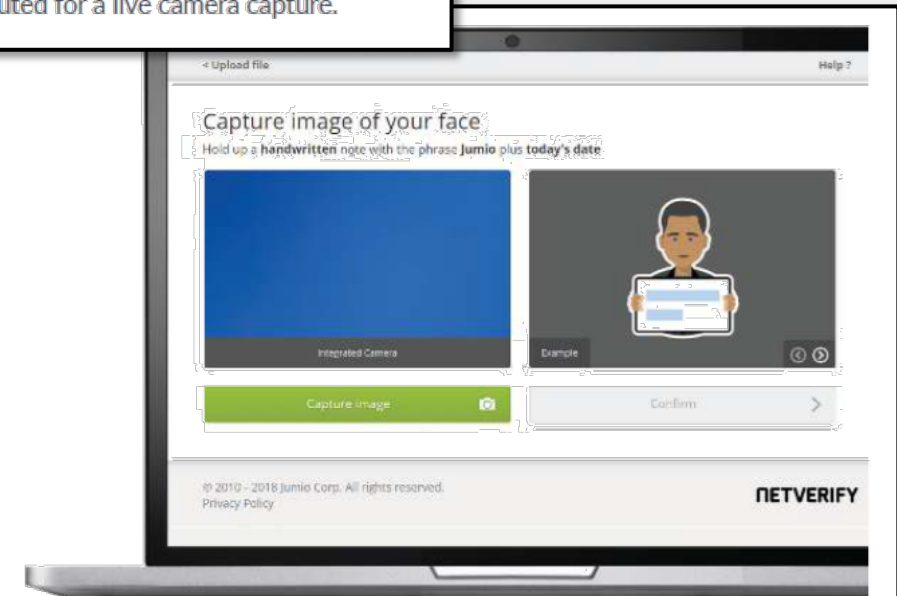


## Eyeball Tracking for Liveness Check

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.

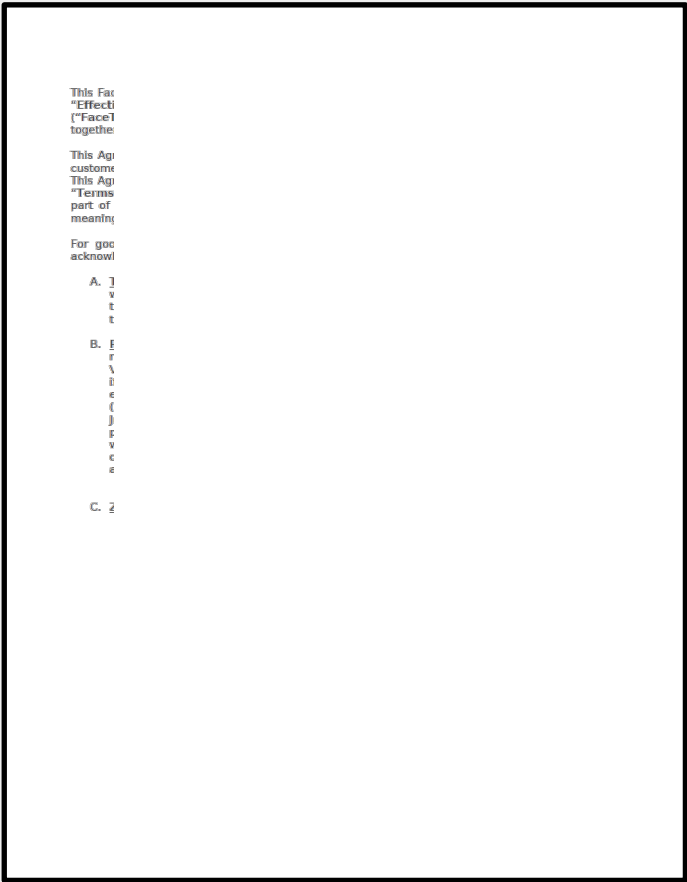
Unlike many ID verification solutions that only support smartphone image capture, Jumio supports your laptop and desktop users with a process designed to the unique fraud risks of a computer-based platform. For example, consider that in the age of Photoshop, it's not terribly difficult to take a picture of a stolen driver's license and use that as a selfie.

Jumio's Liveness Detection for Web prompts the user to create a handwritten note with a custom phrase and the current date. The user must then take a picture of themselves holding the note during the selfie capturing process.

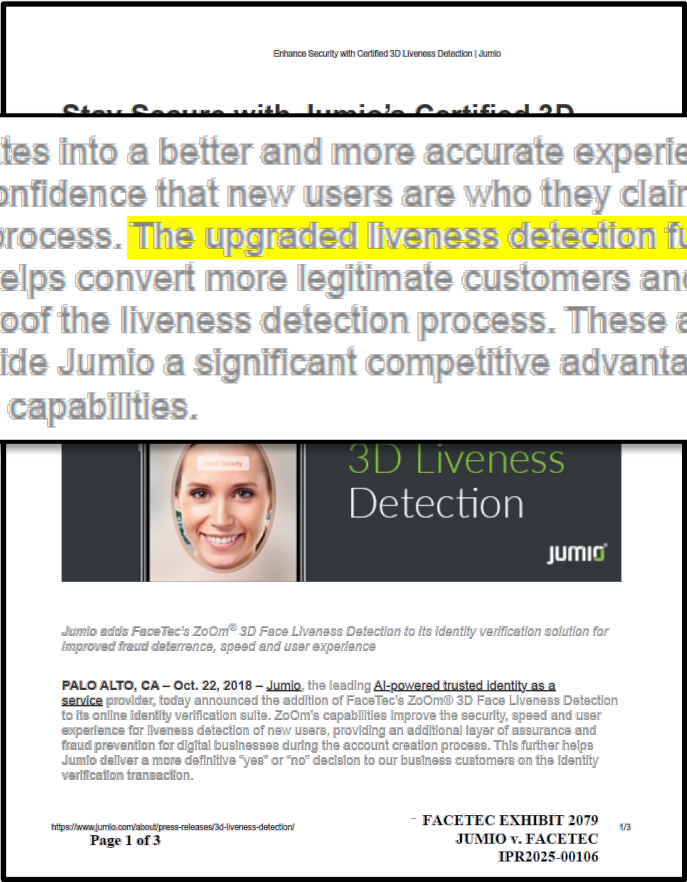


Ex. 2049, 1-2

# Jumio Tried and Failed to Meet This Need and Licensed FaceTec's Software



Ex. 2073  
Second Rose Decl., ¶54



Ex. 2079, 2

# Jumio's Response Lacks Credibility

## Jumio's Position

“[A]n ‘upgrade’ does not necessarily mean Petitioner’s previous approach failed or that Petitioner abandoned previous approaches.”

106Reply, 33-34; 107Reply, 32-33; 108Reply, 30-31; 109Reply, 32-33

- Petitioner makes no affirmative statement that the systems it employed before licensing FaceTec’s software were successful

# *Industry Skepticism*

# More than a Lack of Enthusiasm

## Jumio's Position

“The other statements FaceTec cites amount to, at most, a lack of enthusiasm.”

106Reply, 34; 107Reply, 33; 108Reply, 31; 109Reply, 33

# The Industry Was Skeptical of FaceTec's Software

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 occurs as you move your face closer to the phone's camera, and analyzes how the distortion in images taken when you want to get into, say, a stock trading app, compare to that in images already stored on the phone.

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).

Yet Rich Mogull, analyst and CEO at security research company Securosis, says that being totally software-based means "it would need additional hardware protection to achieve equivalent levels of security" to Apple's face-scanning technology.

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

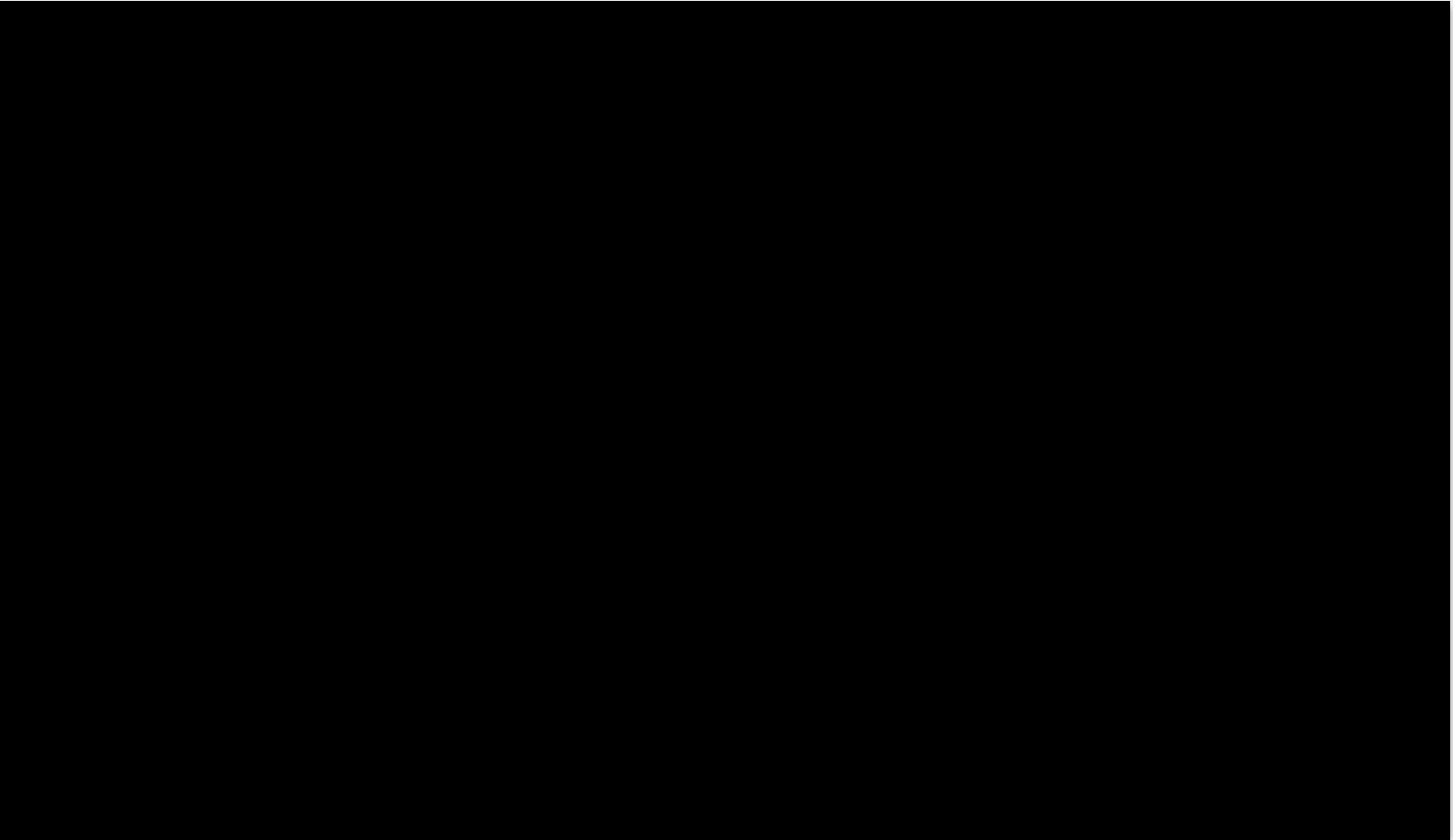
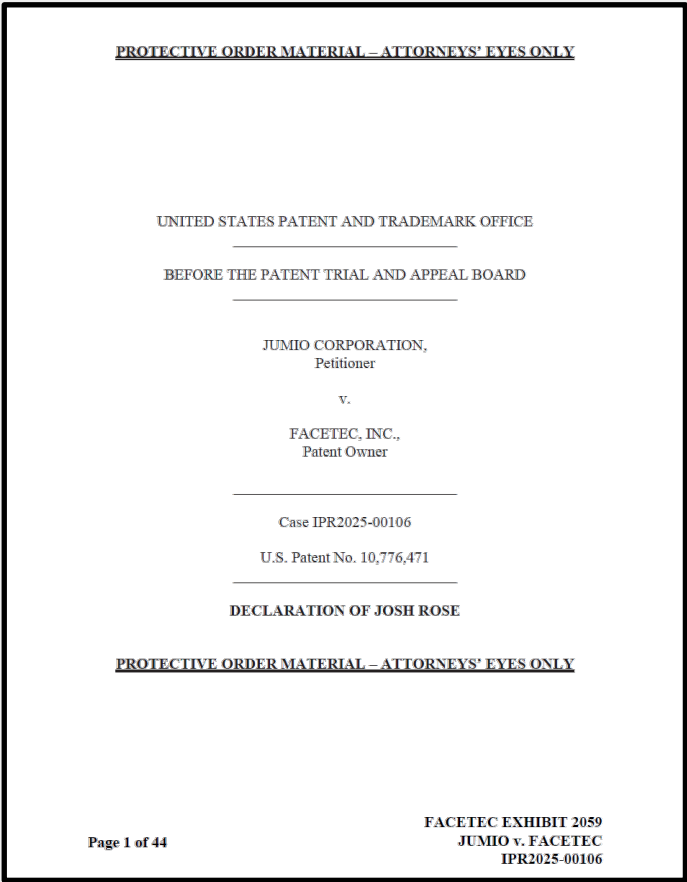
"But I'd be shocked if it was as usable or secure as alternative methods we now see being adopted," he adds.



Ex. 2050, 2-3

# *Commercial Success*

# FaceTec's Software Is Commercially Successful



Ex. 2059, ¶52

# FaceTec's Software Is Commercially Successful

Request a Quote - FaceTec

**Request a Pricing Quote**

Please fill out the following information about your company and use case, and we will get back to you as soon as possible.

**General Information**

Company Name \*  
Country \*  
Industry \*  
Company Type \*

**Contact Information**

Name \*  
Phone \*  
Email \*

**Usage Details**

You are \*  
How did you hear about FaceTec? \*  
Please Describe Your Use Case \*

**Requested Features**

Biometric Features Required\*  
Optional Free Features

**Usage Projections**

Projected Individual Users For First Year \*

102

FACETEC EXHIBIT 2068  
JUMIO v. FACETEC  
EPR2025-00106

## Requested Features

### Biometric Features Required\*

- ☐ 3D Liveness Checks & 3D Face Matching (Note: All Face Matching (/intro-3d-face-matching#matching-api) is Free, Unlimited Usage)
- ☐ 3D Liveness Checks Only (No Face Matching, even though it's Free)

### Optional Free Features

- ☐ Compare User's Face to their Photo ID Document
- ☐ Audit Trail Image For Each Session
- ☐ Match 3D User's Face to 2D Photo ID or Govt DB
- ☐ OCR Text From Photo ID Documents
- ☐ Scan Barcodes & NFC Chips from Photo ID Documents
- ☐ OCR Text From Other Documents (Utility Bill, W2, etc.)
- ☐ Cross Platform Support (Webcam, ATM, IoT, etc.)
- ☐ 1:N Face Search for Deduplication & Fraud Detection
- ☐ UR Code Encoder for Issuing Authorities
- ☐ UR Code Matcher/Scanner for Relying Parties

Ex. 2068



# Jumio's Response Lacks Credibility

## Jumio's Position

“ZoOm has many non-customer facing features (e.g., camera security, encryption, deletion of liveness data) that [FaceTec] believes are critical to its success.”

106Reply, 34-35; 107Reply, 33-34; 108Reply, 32; 109Reply, 33-34

- Petitioner fails to acknowledge that none of those “non-customer facing features” are explicitly paid for
- Prior to mid-2025, the only feature customers paid for was performing 3D liveness checks

# FaceTec's Objective Evidence Confirms Patentability

- ✓ Industry Praise
- ✓ Copying
- ✓ Long-Felt Need, Failures of Others, and Licensing
- ✓ Industry Skepticism
- ✓ Commercial Success

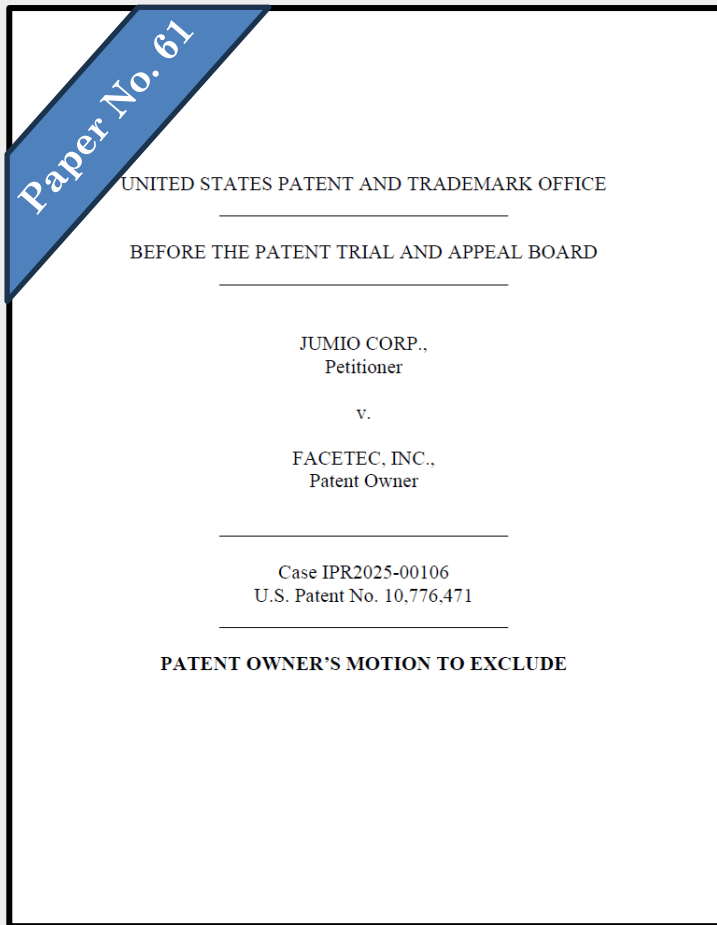


# **Jumio's Obviousness Case Does Not Reach Claims**

# Jumio's Arguments Fail for Three Independent Reasons



# All Claims Are Patentable – Reason 1



- Jumio's arguments are based on an expert who is not a POSITA
- 213-page second declaration does not repair this
- Both declarations should be excluded



106POR, 27-30; 106Sur-Reply, 27-28; 107POR, 27-31; 107Sur-Reply, 24-25;  
108POR, 27-30; 108Sur-Reply, 26-27; 109POR, 27-31; 109Sur-Reply, 27-28;  
Paper 61

## All Claims Are Patentable – Reason 2

- Tanii is not analogous to the FaceTec patents

Tanii then provides a procedure to correct this distortion by enlarging the image's peripheral areas relative to the center to produce an undistorted image. *Id.*, [0056]; *Daft*, ¶¶111-13.

106Pet., 11-12

- No motivation to combine with Derakhshani or Zhang



## All Claims Are Patentable – Reason 3

- Derakhshani and Zhang both require distortion to operate
- But Tanii “account[s]” for distortion by “correcting” (removing) it.
- Dr. Daft admits Tanii’s “critical feature” is correcting distortion

113. Tanii’s critical feature, however, is by providing a procedure to correct this type of distance-induced distortion by enlarging the image’s peripheral areas relative to the center to produce an undistorted image. Ex-1007, [0056]

Ex. 1003, ¶113



# All Claims Are Patentable

Any one of these faults individually dooms Jumio's arguments



106POR 27-64; 106Sur-Reply, 16-28; 107POR, 27-63; 107Sur-Reply, 16-26;  
108POR, 27-61; 108Sur-Reply, 16-27; 109POR, 27-64; 109Sur-Reply, 16-28;  
Paper No. 61

# Dr. Daft's Testimony Must be Excluded

## All Claims Are Patentable – Reason 1

- Jumio's arguments are based on an expert who is not a POSITA
- 213-page second declaration does not repair this
- Both declarations should be excluded



106POR, 27-30; 106Sur-Reply, 27-28; 107POR, 27-31; 107Sur-Reply, 24-25;  
108POR, 27-30; 108Sur-Reply, 26-27; 109POR, 27-31; 109Sur-Reply, 27-28;  
Paper 61

# Correct Level of Skill

# Dr. Daft Fails to Qualify Under The Correct Level of Skill

Dr. Daft is a “**physics-and-waves kind of guy**”

5 Q. A lot of your work at Siemens related to  
6 ultrasound imaging systems; is that correct?

7 A. That's correct. I'm a **physics-and-waves kind**  
8 **of guy.**

Ex. 2082, 40:5-8

## B. The Appropriate Level of Skill Requires Biometric Security, Facial Authentication, and Three-Dimensional Computer Vision

The appropriate level of ordinary skill is:

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**.



*Kyocera*, 22 F.4<sup>th</sup> at 1376-77 : “To offer expert testimony from the perspective of a skilled artisan in a patent case—like for claim construction, validity, or infringement—a **witness must at least have ordinary skill in the art**. Without that skill, the witness' opinions are neither relevant nor reliable.”

106POR, 27-30; 106Sur-Reply, 27-28; 107POR, 27-31; 107Sur-Reply, 24-25;  
108POR, 27-30; 108Sur-Reply, 26-27; 109POR, 27-31; 109Sur-Reply, 27-28;  
Paper 61, 5-10; Paper 67, 1-2

106POR, 28-29

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

# The Correct Level of Skill Requires Facial Biometric Security, Three-Dimensional Computer Vision

## Jumio Admits

The FaceTec patents describe “**facial-authentication systems and methods** to distinguish a **three-dimensional face from a two-dimensional picture** of a face by looking for well-known optical effects... that naturally occur in images to different degrees due to the **three-dimensionality of a face** and the distance between the face and the camera”

106Pet., 4; 107Pet., 3-4; 108Pet., 4; 109Pet., 4

The patents involve facial recognition authentication systems

### 1. Field of the Invention

The disclosed embodiments relate to biometric security. More specifically, the disclosed embodiments relate to a facial recognition authentication systems. 30

’471, 1:28-30.

The patents are about facial authentication

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, 1:50-56

106POR, 27-30; 106Sur-Reply, 27-28; 107POR, 27-31; 107Sur-Reply, 24-25; 108POR, 27-30; 108Sur-Reply, 26-27; 109POR, 27-31; 109Sur-Reply, 27-28; Paper 61, 5-10; Paper 67, 2-4

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

# The Correct Level of Skill Requires Facial Biometric Security, Three-Dimensional Computer Vision

## Jumio Admits

The FaceTec patents describe “**facial-authentication systems and methods** to distinguish a **three-dimensional face from a two-dimensional picture** of a face by looking for well-known optical effects... that naturally occur in images to different degrees due to the **three-dimensionality of a face** and the distance between the face and the camera”

106Pet., 4; 107Pet., 3-4; 108Pet., 4; 109Pet., 4

Two-dimensional “computer vision” is insufficient

“...even a deep understanding of two-dimensional vision systems would not aid in understanding the necessary mathematics and science behind understanding the ‘**expected differences**’ / ‘**expected distortion**’ of **faces** in images under perspective distortion.”

Ex. 2061 (“Turk”), ¶41

“Computer vision” includes irrelevant ultrasonic imaging

“ultrasonic imaging relies on the propagation of sound waves through tissue to measure internal structures....[it does not rely] on the necessary physics to capture surface geometry, light intensity, or distortions of a face from images taken from ranges closer to 20 or 30cm from the face”

Ex. 2061 (“Turk”), ¶49

106POR, 27-30; 106Sur-Reply, 27-28; 107POR, 27-31; 107Sur-Reply, 24-25; 108POR, 27-30; 108Sur-Reply, 26-27; 109POR, 27-31; 109Sur-Reply, 27-28; Paper 61, 5-10; Paper 67, 3-4

# The Correct Level of Skill Requires Facial Biometric Security, Three-Dimensional Computer Vision

## Jumio Admits

The FaceTec patents describe “**facial-authentication systems and methods** to distinguish a **three-dimensional face from a two-dimensional picture** of a face by looking for well-known optical effects... that naturally occur in images to different degrees due to the **three-dimensionality of a face** and the distance between the face and the camera”

106Pet., 4; 107Pet., 3-4; 108Pet., 4; 109Pet., 4

### “Optics” alone is insufficient

“...an eye doctor with a few years of practice, holding a Bachelor’s in physics and some software development experience, who has **never used a biometrics system**” would qualify.  
Optics also includes unrelated artisans, like “those working in laser development, optical communications, optical materials (such as semiconductor optoelectronics), quantum optics, illumination systems, or optical metrology.”

Turk, ¶40

### Non-facial “biometrics” is insufficient

“biometrics [includes]... **fingerprints, palmprints, faces, irises, retinas, ears, voices, signatures, gaits, hand veins, odor, and DNA.** ... two years of experience with identifiers unrelated to the face would ... not equip them with the necessary skills to understand and implement the Challenged Patents. For example, someone having experience with **fingerprint biometrics** would not have the necessary experience to understand the facial biometrics involved in the Challenged Patents.”

Turk, ¶43

106POR, 27-30; 106Sur-Reply, 27-28; 107POR, 27-31; 107Sur-Reply, 24-25; 108POR, 27-30; 108Sur-Reply, 26-27; 109POR, 27-31; 109Sur-Reply, 27-28; Paper 61, 5-10; Paper 67, 3-4

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

# Dr. Daft Fails to Qualify Under The Correct Level of Skill

## Jumio Admits

Dr. Daft qualifies for having “over two years experience in computer vision,” over two years in fingerprint-based “biometrics and biometric security,” and over 25 years with “optical effects.”

106Reply, 21-22; 107Reply, 20-21; 108Reply, 18-19; 109Reply, 20-21

### B. The Appropriate Level of Skill Requires Biometric Security, Facial Authentication, and Three-Dimensional Computer Vision

The appropriate level of ordinary skill is:

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**.

✓ Computer vision

✗ Biometric security, facial authentication, **and** three-dimensional computer vision

✗ Facial biometrics

106POR, 28-29

106POR, 27-30; 106Sur-Reply, 27-28; 107POR, 27-31; 107Sur-Reply, 24-25; 108POR, 27-30; 108Sur-Reply, 26-27; 109POR, 27-31; 109Sur-Reply, 27-28; Paper 61, 5-8; Paper 67, 3-4

# Dr. Daft Fails to Qualify Under The Correct Level of Skill

## B. The Appropriate Level of Skill Requires Biometric Security, Facial Authentication, and Three-Dimensional Computer Vision

The appropriate level of ordinary skill is:

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**.

106POR, 28-29

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

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

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

Ex. 2082, 74:1-11



*Interactive Commc'ns Int'l v. Blackhawk Network*, IPR2024-00465, Paper 40, 4 (Director Oct. 9, 2025): "Having determined that Mr. Hutton is not credible as to multiple material aspects of his testimony, it would be inappropriate in this instance to rely on this testimony for the other grounds."

106POR, 27-30; 106Sur-Reply, 27-28; 107POR, 27-31; 107Sur-Reply, 24-25;  
108POR, 27-30; 108Sur-Reply, 26-27; 109POR, 27-31; 109Sur-Reply, 27-28;  
Paper 61, 4-7; Paper 67, 2-4



# Jumio's Level of Skill is Unreasonably Low

# Jumio's Level of Skill is Unreasonably Low

The '471 Patent describes facial-authentication systems and methods to distinguish a three-dimensional face from a two-dimensional picture of a face by looking for well-known optical effects—such as a “fish-eye” effect—that naturally occur in images to different degrees due to the three-dimensionality of a face and the distance between the face and the camera. *Id.*, 1:64-67, 28:34-58. The patent 106Pet., 4

A person of ordinary skill in the art (“POSITA”) in August 2014 would have had 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. *Daft*, ¶¶129-31. Formal education can substitute for work 106Pet., 5

106POR, 27-30; 106Sur-Reply, 27-28; 107POR, 27-31; 107Sur-Reply, 24-25; 108POR, 27-30; 108Sur-Reply, 26-27; 109POR, 27-31; 109Sur-Reply, 27-28; Paper 61, 4-7; Paper 67, 2-4



DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

# Jumio's Level of Skill is Unreasonably Low

The '471 Patent describes facial-authentication systems and methods to distinguish a three-dimensional face from a two-dimensional picture of a face by looking for well-known optical effects—such as a “fish-eye” effect—that naturally occur in images to different degrees due to the three-dimensionality of a face and the distance between the face and the camera. *Id.*, 1:64-67, 28:34-58. The patent 106Pet., 4

A person of ordinary skill in the art (“POSITA”) in August 2014 would have had 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. *Daft*, ¶¶129-31. Formal education can substitute for work

**Computer vision:** too broad

A biometric system measures one or more physical or behavioral characteristics (see Figure 1.2), including fingerprint, palmpoint, face, iris, retina, ear, voice, signature, gait, hand vein, odor, or the DNA<sup>4</sup> information of an individual to determine or verify his identity. These characteristics are referred to by different terms such as traits,

4

1 INTRODUCTION

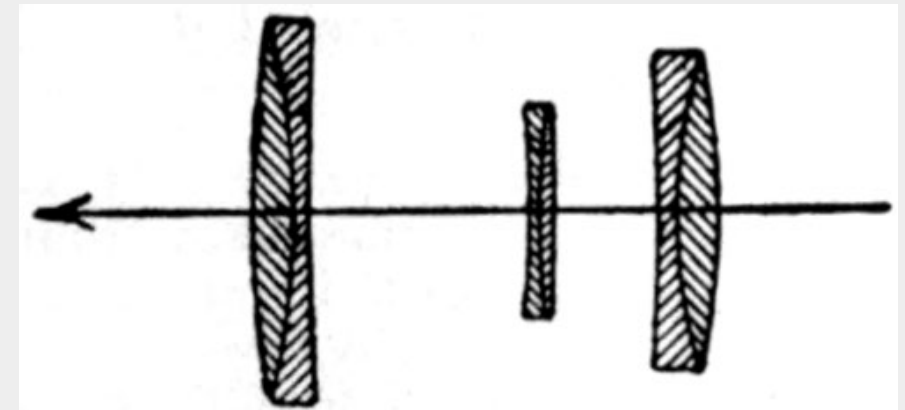
ify his identity. These characteristics are referred to by different terms such as traits,

**Biometrics:** too broad

Ex. 1018, 3-4



**Optics:** too broad



106Pet, 5; 106POR, 27-29; Ex. 2061, ¶¶39, 40, 41, 43; Paper 61, 6-7; Paper 67, 2-4

# Jumio’s Level of Skill is Unreasonably Low

|                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Jumio’s Position</b>                                                                                                                                                                                                    |
| The FaceTec patents are <b>not limited</b> to facial authentication systems, instead identifying “non-facial authentication systems, such as ‘an optical reader’ and ‘fingerprint systems’ as related art.”<br>Paper 66, 6 |

The “non-facial authentication systems” are cited for their shortcomings

1. Field of the Invention

The disclosed embodiments relate to biometric security. More specifically, the disclosed embodiments relate to a facial recognition authentication systems.

30

’471, 1:28-30

The patent at its core is about facial authentication

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, 1:50-56

# Dr. Daft's Declaration

# Dr. Daft's Declaration Contains a Critically Inaccurate Assertion

132. I was at least a POSITA **as of the earliest-possible effective filing date** of the Challenged Patents, and I still am.

Ex. 1003 ("Daft"), ¶132

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

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

Ex. 2082, 68:13-17

9 Q. Okay. Other than for the case, have you worked  
10 for any other companies that do -- that work on -- that  
11 provide biometric security systems?

12 A. When I worked at **General Electric**, I was  
13 involved in a project that was also fingerprint related.  
14 **That was for a military application through Lockheed**  
15 **Martin.**

Ex. 2082, 12:9-15

19 This fingerprint project was a smaller thing;  
20 so I didn't include it in my CV.

21 Q. How much time would you say you worked on the  
22 fingerprint project for?

23 A. **A few weeks.**

Ex. 2082, 13:19-23

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

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

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

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

Ex. 2082, 74:1-11

106POR, 29-30; 107POR, 29-31; 108POR, 29-30; 109POR, 29-31;  
Paper 61, 8, 11-12; Paper 67, 4

# Dr. Daft's Declaration Contains a Critically Inaccurate Assertion

132. I was at least a POSITA **as of the earliest-possible effective filing date** of the Challenged Patents, and I still am.

Ex. 1003 ("Daft"), ¶132

13 Q. Had you done two years of work experience in  
14 the **field of biometrics in August 2014?**  
15 A. Putting together my experience at GE and my  
16 **work at Qualcomm,** that would be the two years work  
17 **experience.**

Ex. 2082, 68:13-17

1 Q. Can you please describe for me your experience  
2 in fields related to biometrics as of **August of 2014?**  
3 A. Yes. The work experience that I had done  
4 involved a project, when I worked at General Electric,  
5 that was a biometric fingerprint recognition. And  
6 the -- that was for law enforcement and military  
7 applications.  
8 As well as that, I had experience when **I was a**  
9 **consultant to Qualcomm.** And there the biometric work  
10 was on an improved way of having **fingerprint**  
11 authentication for cell phones.

Ex. 2082, 74:1-11

22 Q. So, if I understand correctly, **that Qualcomm**  
23 project was in 2012?  
24 A. I am going to say that **was probably 2016,**  
25 **sometime around then.**

Ex. 2082, 22:22-25

106POR, 29-30; 107POR, 29-31; 108POR, 29-30; 109POR, 29-31;  
Paper 61, 8, 11-12; Paper 67, 4

## Dr. Daft vs. Dr. Turk

Dr. Daft is a “**physics-and-waves kind of guy**”

Contradiction on “biometric security”

**Daft Declaration** (Ex. 1003, ¶38):

**biometric security:** using “unique biological information...to **authenticate the identity of an individual** and serve as a ‘key’ to provide access to some resource.”

**Daft Deposition** (Ex. 2082, 35:18-22):

**biometric security:** “protection of the biometric data which the system acquires as part of its operation.”

5 Q. A lot of your work at Siemens related to  
6 ultrasound imaging systems; is that correct?  
7 A. That's correct. I'm a **physics-and-waves kind**  
8 **of guy.**

Ex. 2082, 40:5-8

## Dr. Daft vs. Dr. Turk

Dr. Turk has years of relevant experience

4. I believe that I am well qualified to serve as a technical expert in this matter based upon my educational and professional experience, including my 25+ years of experience in biometrics, biometric security, facial authentication, and computer vision, including three-dimensional computer vision.

Ex. 2061, ¶4

# Dr. Daft’s Testimony Should Be Excluded Under FRE 702



*Kyocera Senco Indus. Tools Inc., v. ITC*, 22 F.4<sup>th</sup> 1369, 1376-77 (Fed. Cir. 2022): “To offer expert testimony from the perspective of a skilled artisan in a patent case—like for claim construction, validity, or infringement—a witness must at least have ordinary skill in the art. Without that skill, the witness' opinions are neither relevant nor reliable.”



*Sundance, Inc. v. DeMonte Fabricating Ltd.*, 550 F.3d 1356, 1363 (Fed. Cir. 2008): “[I]t is an abuse of discretion to permit a witness to testify as an expert on the issues of noninfringement or invalidity unless that witness is qualified as an expert in the pertinent art.”



*Interactive Commc’ns Int’l v. Blackhawk Network*, IPR2024-00465, Paper 40, 4 (Director Oct. 9, 2025): “Having determined that Mr. Hutton is not credible as to multiple material aspects of his testimony, it would be inappropriate in this instance to rely on this testimony for the other grounds.”

**Paper No. 61**

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

JUMIO CORP.,  
Petitioner

v.

FACETEC, INC.,  
Patent Owner

Case IPR2025-00106  
U.S. Patent No. 10,776,471

PATENT OWNER’S MOTION TO EXCLUDE

# Dr. Daft's Opinion is Inadmissible and Was the Subject of Proper Objections

- Dr. Daft lacks the threshold competence to offer testimony through the lens of a POSITA.

*Kyocera*, 22 F.4th at 1377-78.

- This is not merely a question of credibility or weight.

*Kyocera*, 22 F.4th at 1377-78.

- Patent Owner's objections under § 42.64(b)(1) were "sufficiently particular."
- Section 42.64(b)(1) requires that an objection identify "the grounds for the objection with sufficient particularity to allow correction in the form of supplemental evidence."



*Kyocera*, 22 F.4<sup>th</sup> at 1376-77 : "[T]o be qualified to offer expert testimony on issues from the vantage point of an ordinarily skilled artisan in a patent case, **an expert must at a minimum possess ordinary skill in the art.**"

Ex. 1004. Patent Owner further objects to Exhibit 1003 under FRE 702 as providing testimony that is not the product of reliable principles and methods. Dr. Daft offers opinions on the background technology, claim construction, disclosures in the prior art, and motivations to combine the prior art **without demonstrating that Dr. Daft's experience allows him to reliably opine on these issues.** See Ex. 1003 at

Paper 21, 3; *see also* Paper 53, 1-2

# Dr. Daft Has Never Been “Qualified...As an Expert” In “Biometric Security”

Held himself out as expert in “biosensing” technology;  
never “qualified” as expert

5           A.    “He has worked on the development of 'biosensor  
6           systems' and at least one fingerprint scanner and  
7           considers himself an expert in 'biosensing' technology.”

8           Q.    So is it fair to say that you offered yourself  
9           as an expert in biosensing technology in this case?

10          A.    That isn't exactly the word that I would use,  
11          but I see that's what the court said here.

16          Q.    Okay. Did the court in this case qualify you  
17          as an expert in biometric security?

18          A.    My understanding of the history of this case is  
19          that, after this document was issued by the court, the  
20          parties settled. So it did -- so I did a deposition,  
21          but I did not do -- do a trial testimony because the  
22          matter had settled.

Ex. 2082, 53:5-11, 55:16-22

17.    I have trial and deposition experience and have been qualified by the  
courts as an expert on optical devices and biometric security.

Ex. 1003, ¶17.

Never “qualified” as an expert

12          Q.    Were you aware that the testimony in Case  
13          Number 9 that you gave was the subject of a motion to  
14          exclude?

15          A.    I was not.

Ex. 2082, 60:12-15

16          Q.    Did the court in Case Number 9 qualify you as  
17          an expert in biometric security?

18          A.    I don't know what the court said about me, if  
19          anything. I did two depositions, and then the case  
20          settled.

Ex. 2082, 59:16-20

# Dr. Daft Has Never Been “Qualified...As an Expert” In “Biometric Security”

- Dr. Daft has **not** been “**qualified** by the courts as an expert on ... biometric security” as he stated.

17. I have trial and deposition experience and have been qualified by the courts as an expert on optical devices and biometric security.

Ex. 1003, ¶17.

2 Q. Was Case Number 1 related to biometric  
3 security?

4 A. It was not.

Ex. 2082, 48:2-4.

15 Q. So Case Number 2 also was not related to  
16 biometric security; right?

17 A. Case Number 2 is not related to biometric  
18 security.

Ex. 2082, 48:15-18

7 A. The technology in Case Number 3 involved  
8 software for mobile radio systems.

9 Q. Was this case related to biometric security?

10 A. No, it wasn't.

Ex. 2082, 49:7-10

8 Q. Did the technology in Case Number 4 relate to  
9 biometric security?

10 A. It did not.

Ex. 2082, 50:8-10

24 Q. Was this case related to biometric security?

25 A. It was not.

Ex. 2082, 50:24-25

9 Q. What was the technology involved in Case Number  
10 6?

11 A. This involved optical systems that measure  
12 biometric information from the wearer of the device.

13 Q. Was this case related to biometric security?

14 A. It was not.

Ex. 2082, 51:9-14

# All Claims Are Patentable – Reason 1

Once Dr. Daft's testimony is excluded, Jumio's case fails.



*Aspex Eyewear, Inc. v. Concepts In Optics, Inc.*, 111 F. App'x 582, 588 (Fed. Cir. 2004) "This is not one of those rare cases where the invention is so simple that expert testimony is not required."



**Tanii Is Not Analogous Art**

**No Motivation to Combine Tanii with Derakhshani  
or Zhang**



## All Claims Are Patentable – Reason 2

- Tanii is not analogous to the FaceTec patents

Tanii then provides a procedure to correct this distortion by enlarging the image's peripheral areas relative to the center to produce an undistorted image. *Id.*, [0056]; *Daft*, ¶¶111-13.

- Thus, no motivation to combine with Derakhshani or Zhang



106POR, 57-64; 106Sur-Reply, 24-26; 107POR, 56-63; 107Sur-Reply, 22-24; 108POR, 55-61; 108Sur-Reply, 24-26; 109POR, 57-64; 109Sur-Reply, 24-26

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

# Tanii is Not Analogous Art to the FaceTec Patents



*Sanofi-Aventis Deutschland GmbH v. Mylan Pharms. Inc.*, 66 F.4<sup>th</sup> 1373, 1377:

“Two separate tests define the scope of analogous prior art: (1) whether the art is from the **same field of endeavor**, regardless of the problem addressed and, (2) if the reference is not within the field of the inventor's endeavor, whether the reference still is **reasonably pertinent to the particular problem** with which the inventor is involved.”

**Tanii is Not From the Same Field of Endeavor**

# Tanii is Not From The Same Field of Endeavor as the FaceTec Patents



*Sanofi-Aventis Deutschland GmbH v. Mylan Pharms. Inc.*, 66 F.4<sup>th</sup> 1373, 1377:

“Two separate tests define the scope of analogous prior art: **(1) whether the art is from the same field of endeavor, regardless of the problem addressed and,** (2) if the reference is not within the field of the inventor's endeavor, whether the reference still is reasonably pertinent to the particular problem with which the inventor is involved.”

# Tanii is Not From The Same Field of Endeavor as the FaceTec Patents

Jumio: Tanii is analogous for “identifying and accounting for distortions”

Also Jumio: Tanii “account[s]” for distortion by correcting (removing) it

Also Jumio: removing distortion is Tanii’s “critical feature”

Tanii is analogous because “both are concerned with identifying and accounting for distortions of [3D] faces in images captured using a camera” (same field of endeavor). (EX1003, ¶110; EX1001, Abstract; EX1007, Abstract, [0068]-[0069].) Further, both address the same lens-induced distortion problems known in Paper No. 10, 5

Tanii then provides a procedure to correct this distortion by enlarging the image’s peripheral areas relative to the center to produce an undistorted image. *Id.*, [0056]; *Daft*, ¶¶111-13.

106Pet., 11-12

113. Tanii’s critical feature, however, is by providing a procedure to correct this type of distance-induced distortion by enlarging the image’s peripheral areas relative to the center to produce an undistorted image. Ex-1007, [0056]

Ex. 1003, ¶113

# Tanii is Not From The Same Field of Endeavor as the FaceTec Patents

## Jumio Argues

Tanii is analogous to the FaceTec patents because both are “concerned with identifying and accounting for distortions”

Paper No. 10 (106), 5; Paper No. 10 (107), 5; Paper No. 10 (108), 5; Paper No. 10 (109), 5



106POR, 58; 106Sur-Reply, 26; 107POR, 57; 107Sur-Reply, 24; 108POR, 55-56; 108Sur-Reply, 25-26; 109POR, 58; 109Sur-Reply, 26; Ex. 2061, ¶¶150-154

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

# Tanii is Not From The Same Field of Endeavor as the FaceTec Patents



*Sanofi-Aventis Deutschland GmbH v. Mylan Pharms. Inc.*, 66 F.4<sup>th</sup> 1373, 1377: “Two separate tests define the scope of analogous prior art: ~~(1) whether the art is from the same field of endeavor, regardless of the problem addressed and,~~ (2) if the reference is not within the field of the inventor's endeavor, whether the reference still is reasonably pertinent to the particular problem with which the inventor is involved.”

# Tanii is Not Reasonably Pertinent

## Tanii Is Not “Reasonably Pertinent” to Problems Faced By the Inventor

**Jumio admits:** Tanii “account[s]” for distortion by correcting (*removing*) it

Tanii then provides a procedure to correct this distortion by enlarging the image’s peripheral areas relative to the center to produce an undistorted image. *Id.*, [0056]; *Daft*, ¶¶111-13.

106Pet., 11-12

471 Patent: “account[s]” for distortions by *using* it

The ’471 Patent describes facial-authentication systems and methods to distinguish a three-dimensional face from a two-dimensional picture of a face by looking for well-known optical effects—such as a “fish-eye” effect—that naturally occur in images to different degrees due to the three-dimensionality of a face and the distance between the face and the camera. *Id.*, 1:64-67, 28:34-58. The patent

106Pet., 4

106POR, 58-60; 106Sur-Reply, 26; 107POR, 57-59; 107Sur-Reply, 24; 108POR, 56-57; 108Sur-Reply, 25-26; 109POR, 58-60; 109Sur-Reply, 26; Ex. 2061, ¶¶155-161

## Tanii Is Not “Reasonably Pertinent” to Problems Faced By the Inventor

**Jumio admits:** Tanii “account[s]” for distortion by correcting (*removing*) it

Tanii then provides a procedure to **correct this distortion** by enlarging the image’s peripheral areas relative to the center to **produce an undistorted image.** *Id.*, [0056]; *Daft*, ¶¶111-13.

107Pet., 11-12

606 Patent: “account[s]” for distortions by *using* it

The ’606 Patent describes systems and methods to **distinguish real, three-dimensional faces from two-dimensional pictures of a face** during a facial-authentication process. Ex-1001, 1:67-2:3. To do so, the ’606 Patent proposes evaluating images captured by the facial-authentication system for **well-known optical effects—such as “perspective,” “fish-eye,” or “barrel” distortion—that** naturally occur in images and exist to different degrees depending upon (among other factors) the distance between the object and the camera. *Id.*, 29:10-43; *Daft*,

107Pet., 3-4

106POR, 58-60; 106Sur-Reply, 26; 107POR, 57-59; 107Sur-Reply, 24; 108POR, 56-57; 108Sur-Reply, 25-26; 109POR, 58-60; 109Sur-Reply, 26; Ex. 2061, ¶¶155-161

# Tanii does **not** detect faces

23 So would you agree that the main object in  
24 Tanii is a user's face?  
25 A Here, it's described that way. In a lot of  
Page 174  
1 other places in this reference, it's just referred to  
2 as the object.  
3 Q Okay.  
4 A It seems like it could be other things.

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

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

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

14 A Yeah, I think so.

106POR, 37-38; 106Sur-Reply, 24-25; 107POR, 38-39; 107Sur-Reply, 22-23;  
108POR, 37-38; 108Sur-Reply, 23-24; 109POR, 37-38; 109Sur-Reply, 24-25

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

## Tanii Is Not “Reasonably Pertinent” to Problems Faced By the Inventor

### Jumio admits: patent relates to preventing spoofing by looking for fish-eye effect (perspective distortion)

The '471 Patent describes facial-authentication systems and methods to distinguish a three-dimensional face from a two-dimensional picture of a face by looking for well-known optical effects—such as a “fish-eye” effect—that naturally occur in images to different degrees due to the three-dimensionality of a face and the distance between the face and the camera. *Id.*, 1:64-67, 28:34-58. The patent

106Pet., 4

The system may also incorporate other security features when the “zoom in” movement is used as shown in FIGS. 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.

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 appear as much as 30% wider and 15% taller relative to a person’s face when the image is taken at a close proximity as compared to when the image is taken at a distance. The differences in the relative dimensions are caused by the relatively larger differences in focal length of the various facial features when the person is imaged close to the lens as compared to the relatively equal distances in focal length when the person is imaged at a distance farther from the lens.

’471, 28:34-58

## Tanii Is Not “Reasonably Pertinent” to Problems Faced By the Inventor

**Jumio admits:** patent relates to preventing spoofing by looking for fish-eye effect (perspective distortion)

The '606 Patent describes systems and methods to distinguish real, three-dimensional faces from two-dimensional pictures of a face during a facial-authentication process. Ex-1001, 1:67-2:3. To do so, the '606 Patent proposes evaluating images captured by the facial-authentication system for well-known optical effects—such as “perspective,” “fish-eye,” or “barrel” distortion—that naturally occur in images and exist to different degrees depending upon (among other factors) the distance between the object and the camera. *Id.*, 29:10-43; *Daft*, ¶¶66. The patent proposes capturing at least two images of the face: one “close,” one

107Pet., 3-4

The system may also incorporate other security features when the “zoom in” movement is used as shown in FIGS. 13A and 13B. The zoom in feature is typically from moving the device closer or further from the user, but a camera zoom function is also contemplated. When images are taken at relatively close distances between the subject and the camera, the images are distorted through what is known as perspective distortion. Some texts may refer to this distortion as fish-eye type distortion, but perspective distortion is a more accurate technical terminology. Further, lenses configured as wide-angle lenses may contribute barrel distortion (a type of lens distortion) in an image. Other types of lens distortions are also present. These distortions may be tracked for different types of lenses for different devices. The degree of distortion experienced by a user performing the “zoom in” movement to fit their face within the screen displayed prompts may vary and is dependent on the type of optics used in the camera’s lens, the type of distortion, and other factors.

The distortion becomes more obvious 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 appear as much wider and taller relative to a person’s face when the image is taken at a close proximity as compared to when the image is taken at a distance. The differences in the relative dimensions are caused by the relatively larger differences in distances between the various facial features and the camera when the person is imaged close to the lens as compared to the relatively equal distances between the facial features and the camera when the person is imaged at a distance farther from the lens.

‘606, 29:10-43

## Tanii Is Not “Reasonably Pertinent” to Problems Faced By the Inventor

### Jumio admits: patent relates to preventing spoofing by looking for fish-eye effect (perspective distortion)

The '471 Patent describes facial-authentication systems and methods to distinguish a three-dimensional face from a two-dimensional picture of a face by looking for well-known optical effects—such as a “fish-eye” effect—that naturally occur in images to different degrees due to the three-dimensionality of a face and the distance between the face and the camera. *Id.*, 1:64-67, 28:34-58. The patent

106Pet., 4

This effect may be used to increase the security of the 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 authentication, authentication images may be obtained at both the close and far distances from the lens to determine if they match with the enrollment information obtained from the enrollment 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, 29:3-19



*In re Clay*, 966 F.2d 656, 659-60 (Fed. Cir. 1992): invention directed to “storage” of refined hydrocarbons; prior art directed to extraction of crude petroleum.  
**“The Board clearly erred in considering [prior art] to be within the same field of endeavor....”**

106POR, 58-60; 106Sur-Reply, 26; 107POR, 57-59; 107Sur-Reply, 24;  
108POR, 56-57; 108Sur-Reply, 25-26; 109POR, 58-60; 109Sur-Reply, 25-26

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

# Tanii is Not Analogous Art to the FaceTec Patents



*Sanofi-Aventis Deutschland GmbH v. Mylan Pharms. Inc.*, 66 F.4<sup>th</sup> 1373, 1377: “Two separate tests define the scope of analogous prior art: ~~(1) whether the art is from the same field of endeavor, regardless of the problem addressed and, (2) if the reference is not within the field of the inventor's endeavor, whether the reference still is reasonably pertinent to the particular problem with which the inventor is involved.~~”



# No Motivation to Combine Tanii with Derakhshani or Zhang



## All Claims Are Patentable – Reason 3

- Tanii “account[s]” for distortion required by Derakhshani and Tanii by “correcting” (removing) it.
- Tanii’s “critical feature” is correcting distortion

113. Tanii’s critical feature, however, is by providing a procedure to correct this type of distance-induced distortion by enlarging the image’s peripheral areas relative to the center to produce an undistorted image. Ex-1007, [0056]

Ex. 1003, ¶113



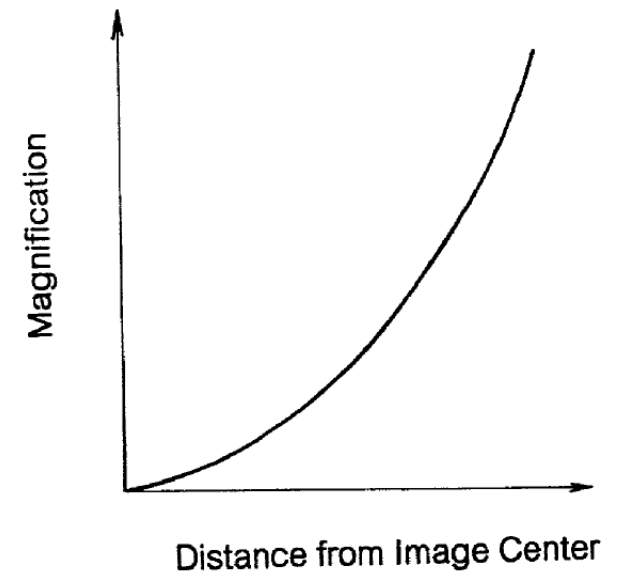
# Tanii Enlarges Objects

Tanii presumes the object is in the center of the frame

[0072] FIG. 13 is a drawing showing sections 821 and 822 that are set in the image 82 in order to detect the size of the image of the main object within the overall image. The section 822, however, includes the section 821. It is deemed in general that the exaggeration warp becomes more significant as the proportional size of the main object image relative to the overall image increases. In addition, because the main object can be deemed to be located in the center of the image at all times, by setting the sections 821 and 822 in the image 82 depending on the distance from the center of the image, and by changing the degree of correction based on the comparison of the size of the main object image with these sections 821 and 822, appropriate warp correction may be realized.

Tanii enlarges images at a rate proportional to distance from the center

Fig.8



# Tanii Does Not Detect Faces

## Jumio Argues

“FaceTec is also wrong that Tanii does not detect a face.”

106Reply, 4; 107Reply, 4; 108Reply, 4; 109Reply, 4

*At most, Tanii teaches detecting an object exists*

23            So would you agree that the main object in  
24   Tanii is a user's face?

25            A    Here, it's described that way.    In a lot of

Page 174

1   other places in this reference, it's just referred to  
2   as the object.

3            Q    Okay.

4            A    It seems like it could be other things.

Ex. 1059, 174:23-174:4

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

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

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

14            A    Yeah, I think so.

Ex. 1059, 174:5-14

106POR, 37-38, 44-45; 106Sur-Reply, 24-25; 107POR, 38-39, 45-46; 107Sur-Reply, 23-24; 108POR, 37-38, 44-45; 108Sur-Reply, 24-25; 109POR, 37-38, 44-46; 109Sur-Reply, 25-26; Ex. 2061 ¶73

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

# Tanii Does Not Detect Three-Dimensionality or Expected Distortion

**Jumio Argues**

“Tanii teaches detecting three-dimensionality and expected distortion.”  
106Reply, 5; 107Reply, 5; 108Reply, 5; 109Reply, 5

Tanii detects the size of an object and a distance to the object

97.Moreover, contrary to the Board’s statements about Tanii, it is my opinion that Tanii does not teach or suggest “evaluating distance induced distortions in a face caused by the camera’s lens and the distance from the object.” Paper No. 17, 32-33. Tanii detects the size of an “object” in the frame and a “distance” to the object. *See, e.g.*, Ex. 1007, ¶¶[0072], [0074], [0076]-[0077], [0079], [0097]-[0098] (size); [0096]-[0098], [0100]-[0102] (distance). Tanii does not evaluate

Ex. 2061, ¶97

Tanii enlarges images based on distance to the object

|    |   |                                                         |
|----|---|---------------------------------------------------------|
| 11 | Q | Okay. So Tanii determines the distance                  |
| 12 |   | between the main object and the cellular phone and then |
| 13 |   | applies different levels of correction depending on the |
| 14 |   | distance, yes?                                          |
| 15 | A | That's how it's described here, yes.                    |

Ex. 1059, 176:11-15

106POR, 37-38, 44-45; 106Sur-Reply, 24-25; 107POR, 38-39, 45-46; 107Sur-Reply, 23-24; 108POR, 37-38, 44-45; 108Sur-Reply, 24-25; 109POR, 37-38, 44-46; 109Sur-Reply, 25-26; Ex. 2061 ¶73

# Tanii Enlarges Objects, Does Not Detect Faces

## Jumio Argues

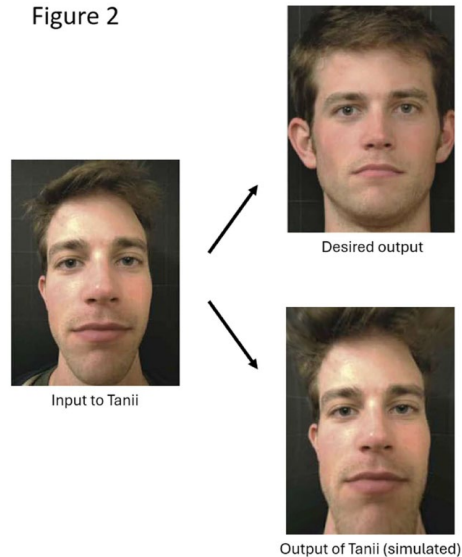
“Tanii teaches detecting three-dimensionality and expected distortion.”

106Reply, 5; 107Reply, 5; 108Reply, 5; 109Reply, 5

Enlarging an image merely stretches pixels on a flat surface

Distortion in Tanii is not related to distance to the object

Figure 2



16 Q And different distances may have different  
17 degrees of distance-induced distortion, right?  
18 A It's -- that's also a complicated question.  
19 The distortion that's being talked about here  
20 is not a function of the distance to the object. It's  
21 a function -- it's a function of the distances within  
22 the object. For example, if it were a face --  
23 Q Okay.  
24 A -- the various parts of the face are at a  
25 different distance to the camera.

106POR, 37-38, 44-45; 106Sur-Reply, 24-25; 107POR, 38-39, 45-46; 107Sur-Reply, 23-24; 108POR, 37-38, 44-45; 108Sur-Reply, 24-25; 109POR, 37-38, 44-46; 109Sur-Reply, 25-26; Ex. 2061 ¶73

Ex. 1059, 176:16-25

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

# Tanii Enlarges Objects, Does Not Detect Faces

## Jumio Argues

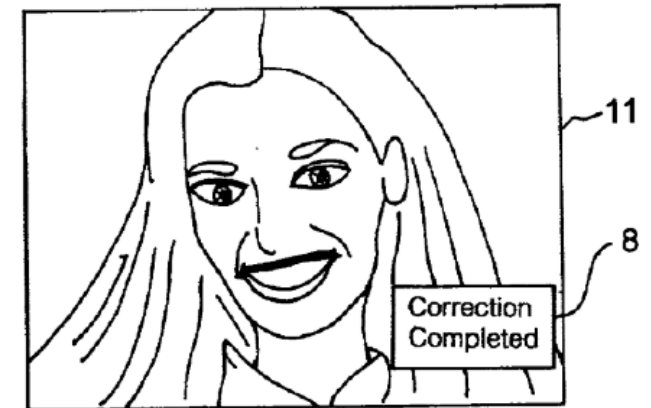
“Tanii teaches detecting three-dimensionality and expected distortion.”

106Reply, 5; 107Reply, 5; 108Reply, 5; 109Reply, 5

Tanii needs the user to determine whether to perform correction; it cannot detect distortion on its own

[0058] FIG. 9 is a drawing showing an example of the display of a corrected image on the display 11. As shown in FIG. 9, when a corrected image is displayed, the display controller 203 displays in synthesis with the corrected image a phrase 8 that indicates that correction was performed by the warp corrector 201. Consequently, the user can easily recognize whether or not warp correction was performed, and is prevented from forgetting to initiate correction.

Fig.9



106POR, 37-38, 44-45; 106Sur-Reply, 24-25; 107POR, 38-39, 45-46; 107Sur-Reply, 23-24; 108POR, 37-38, 44-45; 108Sur-Reply, 24-25; 109POR, 37-38, 44-46; 109Sur-Reply, 25-26; Ex. 2061 ¶¶69-73, 97, 173-74

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

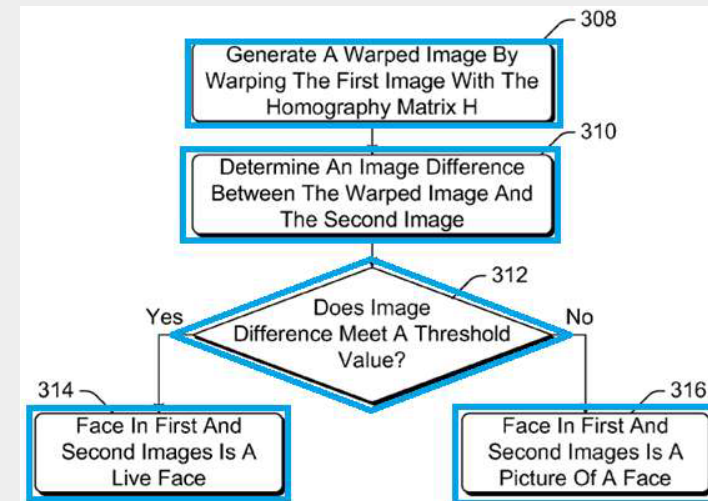
# No Motivation to Combine Either Reference with Tanii

Derakhshani and Zhang both require distortion to operate

- Derakhshani: Blur / parallax across multiple images
- Zhang: “warped image”

authentication), 16:44-18:4 (three-dimensional verification). To verify three-dimensionality, Derakhshani exploits one or more known optics principles, such as: (1) adjusting the *focus* distance of the camera to determine whether different facial features exhibit different amounts of blur across multiple images, indicating the face has depth; and/or (2) evaluating whether “parallax” exists between two images captured from different camera positions, also indicating the face has depth. *Id.*, 16:44-17:11, 17:45-18:4; *Daft*, ¶¶101-02.

106Pet., 7



Zhang, Fig. 3

# No Motivation to Combine Either Reference with Tanii

Jumio: Tanii “account[s]” for distortion required by Derakhshani and Zhang by correcting (removing) it

Removing distortion is Tanii’s “critical feature”

Tanii then provides a procedure to **correct this distortion** by enlarging the image’s peripheral areas relative to the center to **produce an undistorted image**. *Id.*, [0056]; *Daft*, ¶¶111-13.

Pet., 11-12

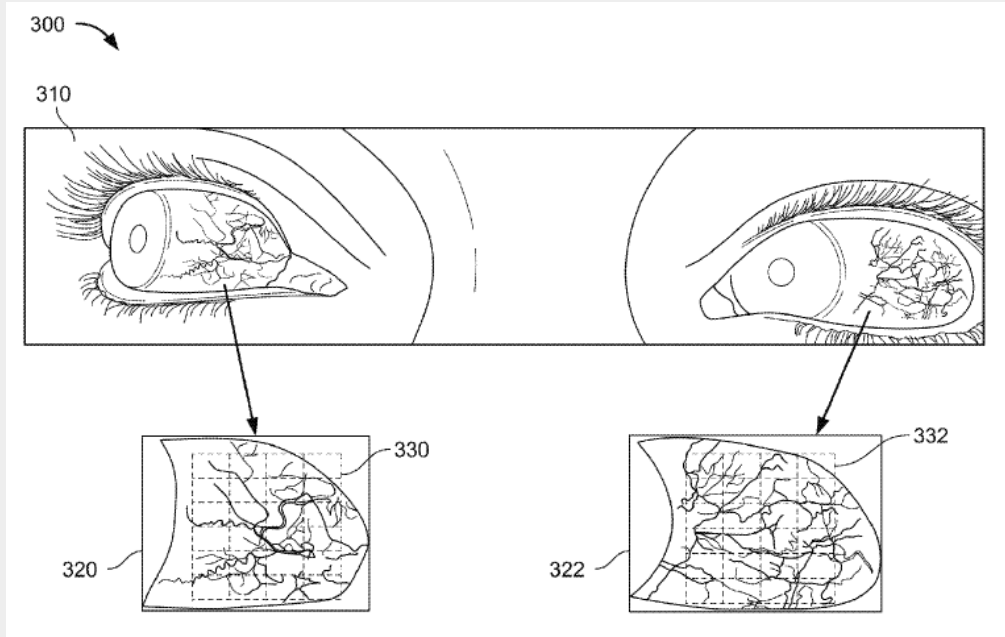
113. Tanii’s **critical feature**, however, is by providing a **procedure to correct this type of distance-induced distortion** by enlarging the image’s peripheral areas relative to the center to produce an undistorted image. Ex-1007, [0056]

Ex. 1003, ¶113



*Trivascular*, 812 F.3d 1056, 1068 (Fed. Cir. 2016): no error in rejecting argument to “substitute the recessed barbs of Samuels ’851 with the protuberances of Todd, since TriVascular’s proposed substitution would **destroy the basic objective of the barbs**, which is to *penetrate* surrounding tissue” (emphasis original).

# No Motivation to Combine Derakhshani with Tanii



Derakhshani  
6-12cm away from **eyes**

Tanii  
enlarging **face**

Fig.4A

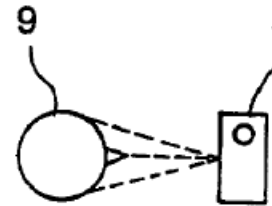
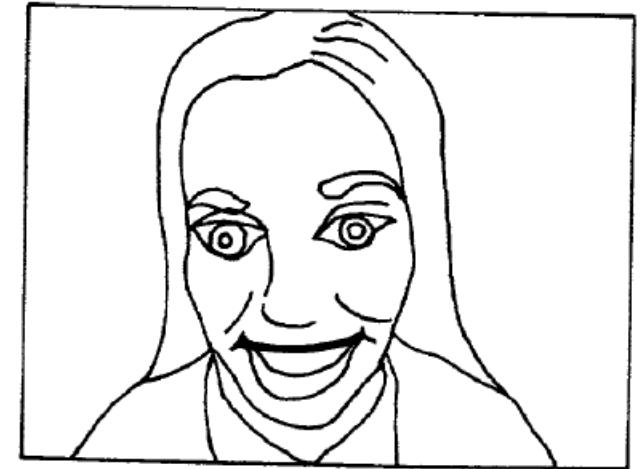
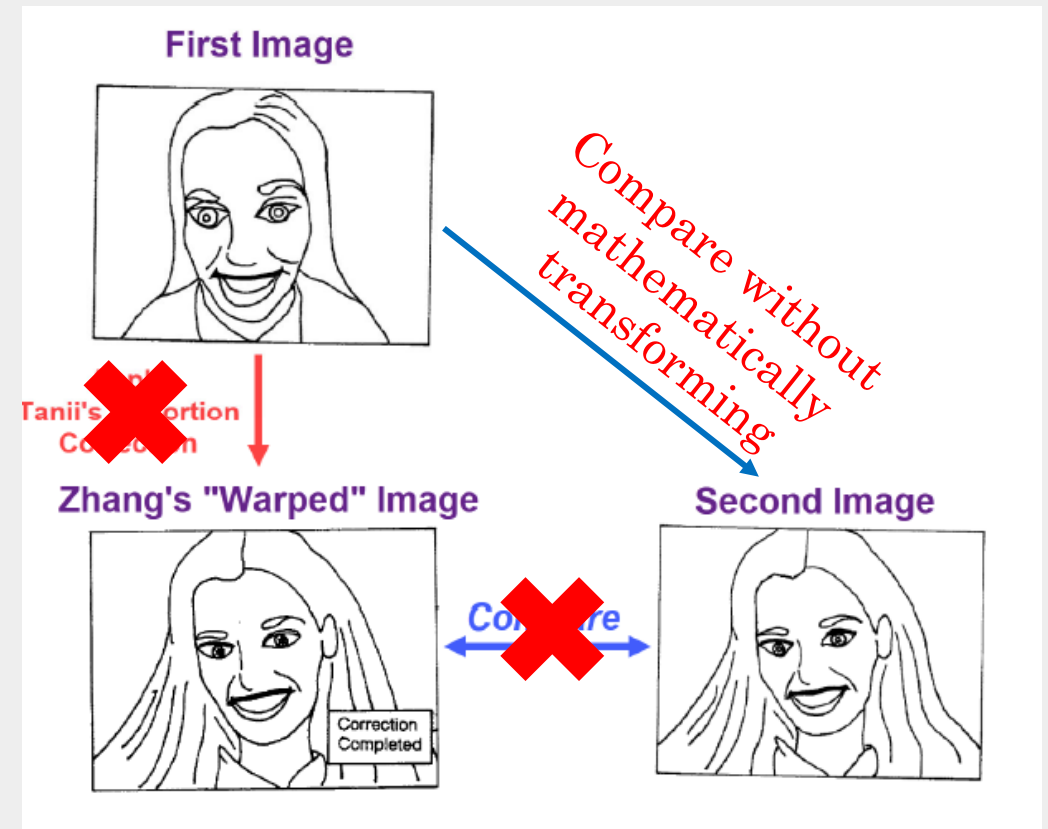


Fig.4B



# No Motivation to Combine Zhang with Tanii

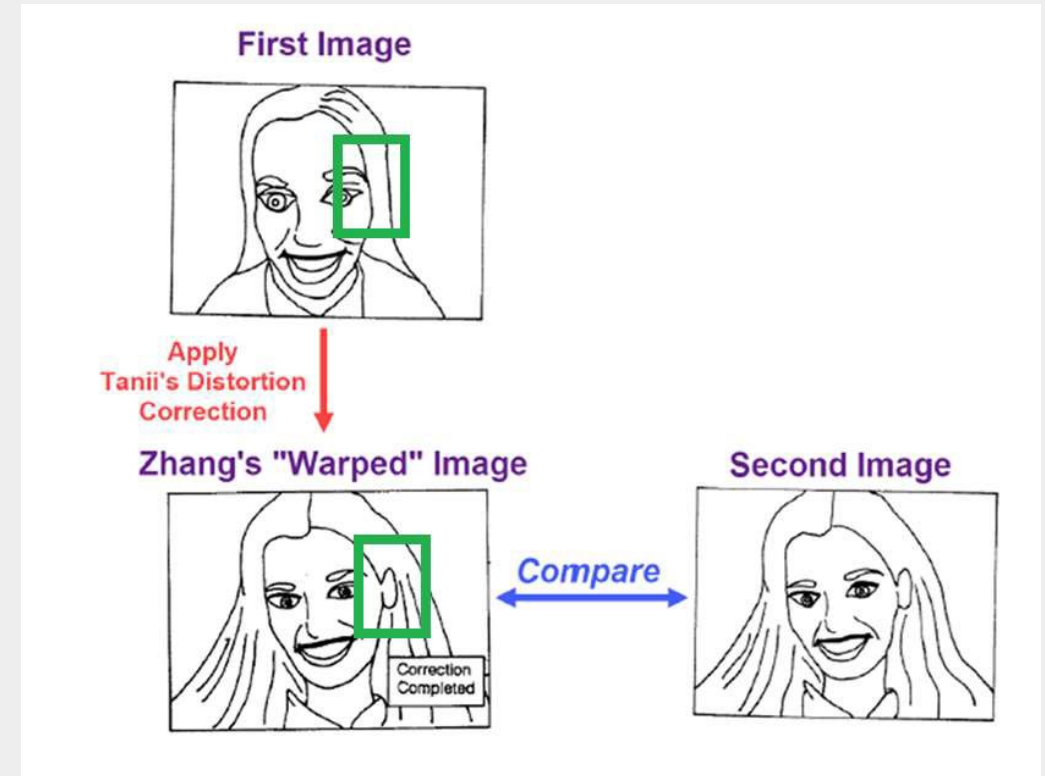
Jumio does not explain how to “compare” a warped image to a second image without “mathematically transform[ing]”



106Pet., 52 (annotated)

# No Motivation to Combine Zhang with Tanii

Tanii's purported distortion correction would not create ears in warped image that could not be seen in a first image.



106Pet., 52 (annotated, 106POR, 62)

# There Would Have Been No Motivation to Combine Either Derakhshani or Zhang with Tanii



*Medtronic, Inc. v. Teleflex Innovations S.a.r.l.*, 69 F.4th 1341, 1349 (Fed. Cir. 2023) (“The Board reasonably recognized that modifying a device in a manner that would undermine a purpose it shares with the challenged claims counsels against a motivation to make such modifications.”)



*In re Clay*, 966 F.2d 656, 660 (Fed. Cir. 1992) (“A person having ordinary skill in the art would not reasonably have expected to solve the problem of dead volume in tanks for storing refined petroleum by considering a reference dealing with plugging underground formation anomalies. The Board's finding to the contrary is clearly erroneous.”)

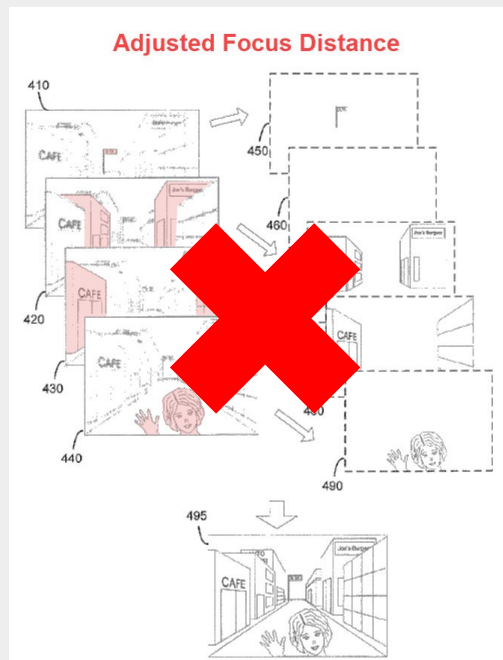
106POR, 45, 58-62; 106Sur-Reply, 26; 107POR, 46, 57-59, 61; 107Sur-Reply, 24; 108POR, 45, 56-58, 59; 108Sur-Reply, 25-26; 109POR, 46, 58, 60, 62; 109Sur-Reply, 26



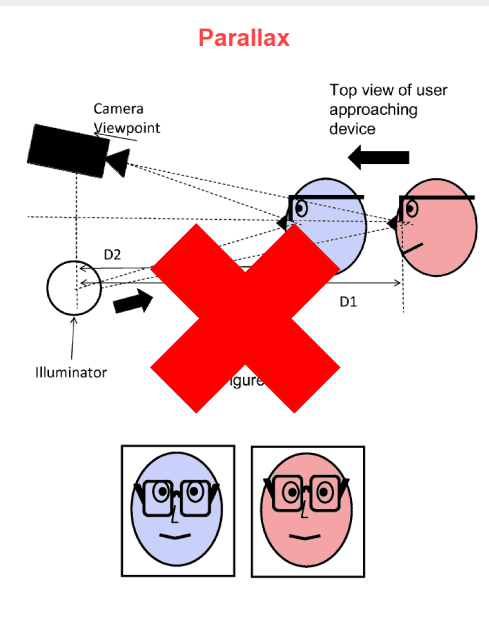
# Derakhshani (Ex. 1005) and Zhang (Ex. 1006)

# Derakhshani (Ex. 1005)

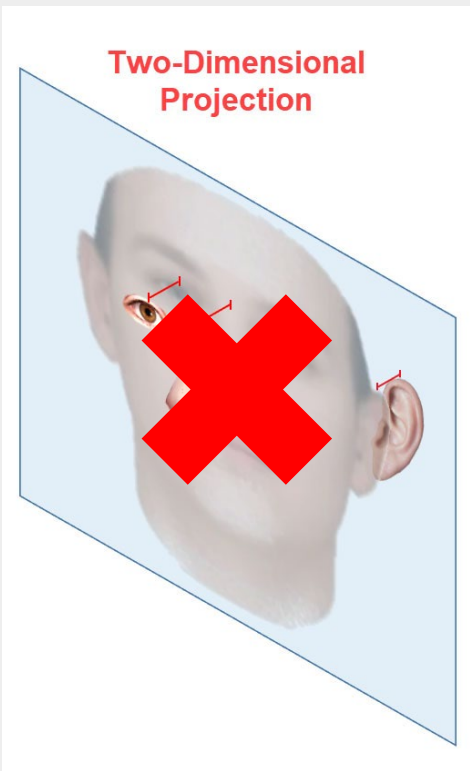
# Jumio is Wrong: Derakhshani Does Not Capture Face Images



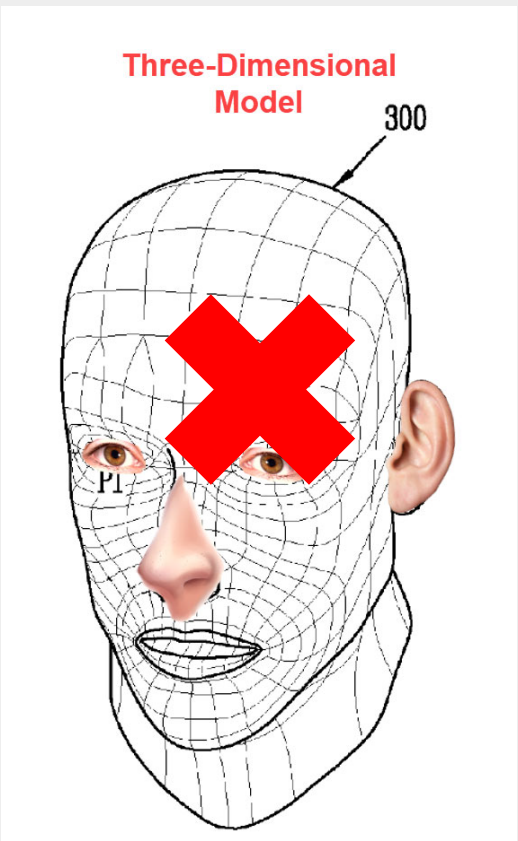
106Pet, 8



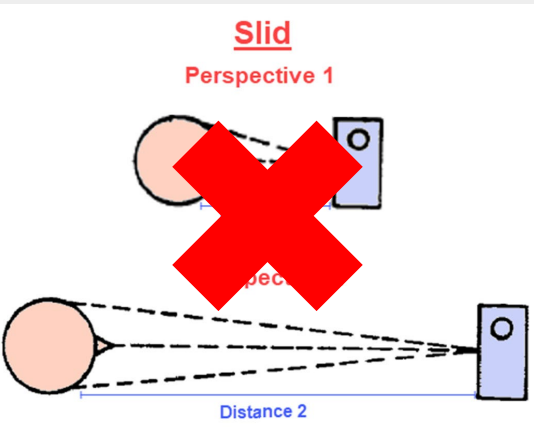
106Pet, 9



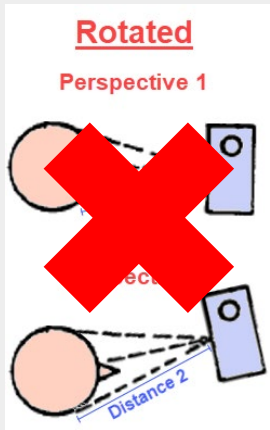
106Pet, 10, 29



106Pet, 10



106Pet, 23



106Pet, 23

# Derakhshani's Purpose: Capturing Eye Vasculature

## Jumio Argues

“nowhere does Derakhshani suggest a primary purpose of **capturing the eye vasculature**, or that it relies on images of the eyes only for the **spatial metric determination or user authentication**.”

106Reply, 3; 107Reply, 3; 108Reply, 3; 109Reply, 3

The primary purpose of Derakhshani is capturing the vasculature of eyes for authentication and spatial metric

Abstract: “This specification describes technologies relating to biometric authentication **based on images of the eye**”

4:19-21: “features of an individual’s **visible vasculature in the whites of the eyes** may be used to identify or authenticate the individual.”

9:59-61: “authenticating an individual based on one or more **image of the white of an eye**”

5:42-45: “FIG. 3 is a diagram of an example image 300, including **portions showing vasculature of the whites of two eyes**, that is segmented for analysis. A captured image 310 may be obtained in a variety of ways.”

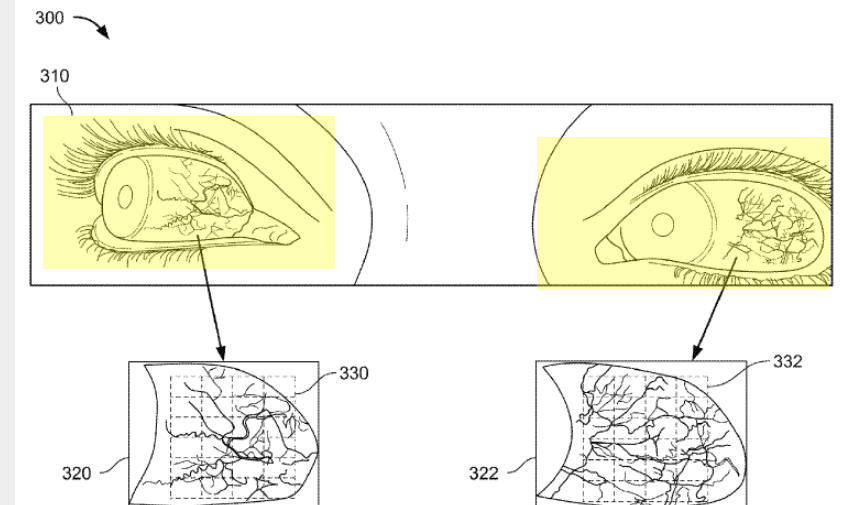


Fig. 3

106POR, 31-32; 106Sur-Reply, 16-17; 107POR, 31-32; 107Sur-Reply, 17-18;  
108POR, 31-32; 108Sur-Reply, 17-18; 109POR, 31-32; 109Sur-Reply, 16-17

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

# Jumio is Wrong: Derakhshani Does Not Capture Face Images

## Jumio Argues

“Derakhshani [still] captures an image of the head/face.”

106Reply, 1; 107Reply, 1; 108Reply, 1; 109Reply, 1

Jumio:

106Reply, 1

Ex. 1005, 3:5-7

(EX1005, 16:51-54, 17:16-17, 17:29-36.) It would be obvious for an image having multiple “landmarks (e.g., an eye, nose, mouth, *and* ear)” to be of the head/face.

(EX1005, 17:16-19; 3:5-7, 17:2-6; EX1059, 136:25-137:3.) Derakhshani also

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

Ex. 1005, 17:2-6

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 land-

be estimated. In some implementations, distances from the sensor (e.g. a camera) for multiple landmarks are estimated to form a topological map (consisting of a set of three-dimensional landmark positions) of the subject in the view of the sensor. The positions of these landmarks in the space viewed

Ex. 1005, 17:12-19

106Sur-Reply, 18-19; 107Sur-Reply, 17-18; 108Sur-Reply, 18; 109Sur-Reply, 17-18

# Jumio is Wrong: Derakhshani Does Not Capture Face Images

## Jumio Argues

“Derakhshani [still] captures an image of the head/face.”

106Reply, 1; 107Reply, 1; 108Reply, 1; 109Reply, 1

Jumio:

106Reply, 1

(EX1005, 16:51-54, 17:16-17, 17:29-36.) It would be obvious for an image having multiple “landmarks (e.g., an eye, nose, mouth, *and* ear)” to be of the head/face.

(EX1005, 17:16-19; 3:5-7, 17:2-6; EX1059, 136:25-137:3.) Derakhshani also

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 land-

Ex. 1005, 17:12-19

25 Q Okay. And Derakhshani also teaches capturing

Page 136

1 images having multiple landmarks within the same image,

2 right?

3 A I believe so.

4 Q Okay. So if Derakhshani is capturing an image

5 that has an ear, nose, mouth and eye, what type of

6 image is it capturing?

7 A Well, I don't think Derakhshani ever says that

8 it will capture images that include all of those.

9 Q Uh-huh.

10 A So they may well just be individual examples

11 that would never be in the same image.

12 If Derakhshani were to capture something with

13 all of those, it would be an image that is generally

14 different than the images that are shown in

15 Derakhshani, because those images generally don't cover

16 larger parts of the face that would include such

17 features.

Ex. 1059, 136:25-137:17.

# Jumio Redefines Derakhshani's Images

## Jumio Argues

Derakhshani's images do not need to capture vasculature or can capture blurry vasculature

106Reply, 2-4; 107Reply, 2-4; 108Reply, 2-4; 109Reply, 2-4

captured simultaneously both with enough precision. (POR, 43.) The spatial metric determination may use a close-up image that captures the eye vasculature in focus (having enough precision) and a further-away image that captures a landmark in focus (eye vasculature is blurred). (EX1059, 144:7-16.) The match

106Reply, 4

16:44-47, 17:45-47.) For example, a close-up image may capture the eye vasculature (with enough precision) for the match score and/or liveness score, and a further-away image for the liveness score. Because the liveness score

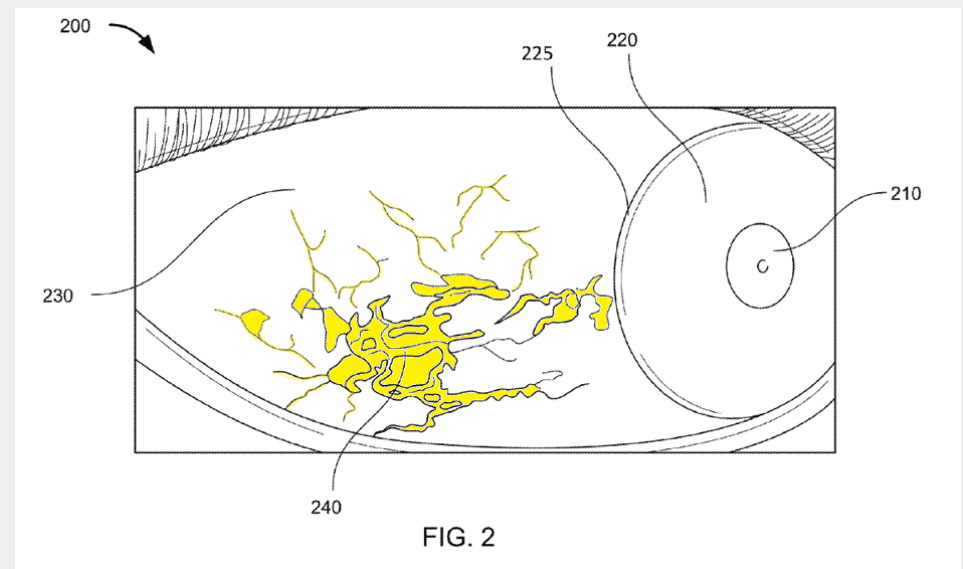
106Reply, 2

106POR, 31-34, 41-44, 46-48; 106Sur-Reply, 19-20; 107POR, 31-35, 41-44, 47-48; 107Sur-Reply, 19; 108POR, 31-34, 40-43, 45-47; 108Sur-Reply, 19; 109POR, 31-34, 41-44, 46-47; 109Sur-Reply, 19-20

Derakhshani: images must include vasculature

One or more images of an eye are obtained 602. The images include a view of a portion of a vasculature of the eye external to a corneal limbus boundary of the eye. The obtained images may be monochrome or represented in various color spaces (e.g., RGB, SRGB, HSV, HSL, or YCbCr). In some imple-

Ex. 1005, 10:25-27



Ex. 1005, Fig. 2

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

# Jumio Redefines Derakhshani's Images

## Jumio Argues

Turk agreed Derakhshani's images can capture blurry vasculature

106Reply, 2-4; 107Reply, 2-4; 108Reply, 2-4; 109Reply, 2-4

captured simultaneously both with enough precision. (POR, 43.) The spatial metric determination may use a close-up image that captures the eye vasculature in focus (having enough precision) and a further-away image that captures a landmark in focus (eye vasculature is blurred). (EX1059, 144:16.) The match

106Reply, 4

16:44-47, 17:45-47.) For example, a close-up image may capture the eye vasculature (with enough precision) for the match score and/or liveness score, and a further-away image for the liveness score. Because the liveness score

106Reply, 2

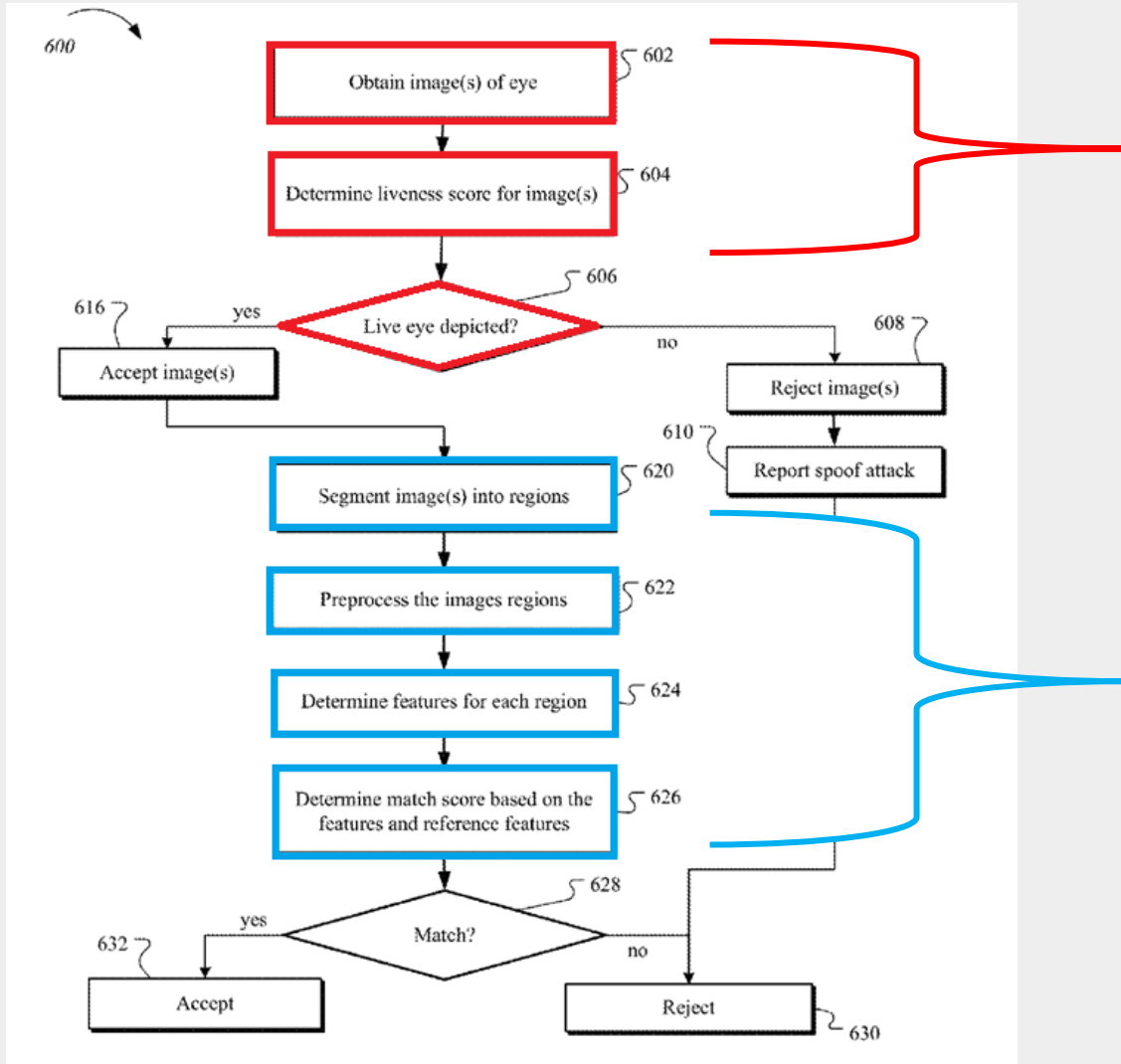
106POR, 31-34, 41-44, 46-48; 106Sur-Reply, 19-20; 107POR, 31-35, 41-44, 47-48; 107Sur-Reply, 19; 108POR, 31-34, 40-43, 45-47; 108Sur-Reply, 19; 109POR, 31-34, 41-44, 46-47; 109Sur-Reply, 19-20

Turk: "landmarks" (not vasculature) can be blurry

7 Q Okay. So Derakhshani's focus distance  
8 approach captures a plurality of images with different  
9 distances, right? We talked about that earlier.  
10 A Yes.  
11 Q Okay. And in that, would Derakhshani be  
12 capturing one image where a given landmark is in focus,  
13 and in another image, that same landmark is then  
14 blurry?  
15 A That is my understanding of how he's  
16 describing that process.

Ex. 1059, 144:7-16

# Derakhshani's Image Landmarks are Not Vasculature Features



Eye liveness detection uses image landmarks to determine a spatial metric and a liveness score.

Authentication of user relies on biometric features from eye vasculature

106POR, 31-34, 46-48; 106Sur-Reply, 20-22; 107POR, 31-35, 41-44, 47-48;  
108POR, 31-34, 40-43, 45-47; 108Sur-Reply, 20-21; 109POR, 31-34, 41-44, 46-47; 109Sur-Reply, 19-20

# Derakhshani's Image Landmarks are Not Vasculature Features

g. 1[d2]

Derakhshani discloses or suggests 1[d2]. *Daft*, ¶¶161-63.

Derakhshani discloses, as part of the verification process, “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). A POSITA would have understood Derakhshani's identification of landmarks constitutes creating data (specifically biometric data) because the identification uses a computer (which operates on data)

106Pet., 21-22

b. 5[b]

Derakhshani discloses or suggests 5[b]'s additional limitation. *Daft*, ¶¶215-16.

During the authentication process, Derakhshani calculates a match score based on the comparison of features extracted from the first and second image to the corresponding features in an enrollment reference record. *Derakhshani*, 13:62-66. The match score is then compared to a predetermined threshold. *Id.* 14:25-28. When the match score is within that predetermined threshold, it is determined that the user who is depicted in the captured image is the same individual associated with the enrollment reference record, and the user is authenticated. *Id.* 14:25-45; *Daft*, ¶216.

106Pet., 36

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;

Claim 1: “first data” = landmarks

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 only authenticating the user when the first data, the second data, or both match the enrollment data within a predetermined threshold.

Claim 5: “first data” = features of vasculature

106POR, 31-34, 46-48; 106Sur-Reply, 20-22; 107POR, 31-35, 41-44, 47-48; 108POR, 31-34, 40-43, 45-47; 108Sur-Reply, 20-21; 109POR, 31-34, 41-44, 46-47; 109Sur-Reply, 19-20; Paper 6 (106), 48-50, 50 n.9; Paper 6 (108), 46-48, 48 n.12 ; Paper 6 (109), 42-44, 44 n.9

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

# Derakhshani's Image Landmarks are Not Vasculature Features

g. 1[d2]

Derakhshani discloses or suggests 1[d2]. *Daft*, ¶¶161-63.

Derakhshani discloses, as part of the verification process, “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). A POSITA would have understood Derakhshani’s identification of landmarks constitutes creating data (specifically biometric data) because the identification uses a computer (which operates on data)

106Pet., 21-22

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 sensors, the focus distance may be adjusted for different images by adjusting a focus configuration setting for the 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

Ex. 1005, 16:44-54

b. 5[b]

Derakhshani discloses or suggests 5[b]’s additional limitation. *Daft*, ¶¶215-16.

During the authentication process, Derakhshani calculates a match score based on the comparison of features extracted from the first and second image to the corresponding features in an enrollment reference record. *Derakhshani*, 13:62-66. The match score is then compared to a predetermined threshold. *Id.* 14:25-28. When the match score is within that predetermined threshold, it is determined that the user who is depicted in the captured image is the same individual associated with the enrollment reference record, and the user is authenticated. *Id.* 14:25-45; *Daft*, ¶216.

106Pet., 36

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 detection methods may be used to extract features of the user’s vasculature. Examples of minutia detection processes are described in U.S. Pat. No. 7,327,860.

A match score is determined 626 based on the features and corresponding features from a reference record. The reference record may include data based at least in part on one or more reference images captured during an enrollment or registration process for a user. In some implementations, a match

Ex. 1005, 13:9-14, 62-66

106POR, 31-34, 46-48; 106Sur-Reply, 20-22; 107POR, 31-35, 41-44, 47-48; 108POR, 31-34, 40-43, 45-47; 108Sur-Reply, 20-21; 109POR, 31-34, 41-44, 46-47; 109Sur-Reply, 19-20; Paper 6 (106), 48-50, 50 n.9; Paper 6 (108), 46-48, 48 n.12 ; Paper 6 (109), 42-44, 44 n.9

# Derakhshani's Image Landmarks are Not Vasculature Features

## Jumio Argues

Landmarks in “reference record,” features compared to “reference record,” thus “features” and “landmarks” are synonymous  
106Reply, 9; 108Reply, 8; 109Reply, 8

FaceTec’s rebuttal that “landmarks” and “features” are not synonymous falls flat. (POR, 47-48.) Both “landmarks” and “features” are data of the reference record. The “relative positions of *landmarks* on a particular user’s face . . . [for] generat[ing] a three-dimensional model [] is stored as part of a *reference record*.” (EX1005, 17:32-36; EX1059, 134:8-135:15.) And “features” are extracted and “compare[d] . . . to [the] *reference record* in order to authenticate the user.” (EX1005, 4:19-24, 7:19-34, 9:59-67, 13:62-14:9; EX1059, 135:16-136:1; EX1060, ¶¶45-46.)

106Reply, 9

Derakhshani: reference record includes many things – like vasculature “features.”

used to store one or more reference records. A reference record may include data derived from one or more images of the white of an eye for a registered our authorized user of the secured device 450. In some implementations, the reference record includes complete reference images. In some implementations the reference record includes features extracted from the reference images. In some implementations the reference record includes encrypted features extracted from the reference images. In some implementations the reference record includes identification keys encrypted by features extracted from the reference images. To create a reference record for a new user and enrollment or registration process may be carried out. An enrollment process may include the capture of one or more reference images of the white of a new registered user’s eye. In some implementations, the enrollment process may be performed using the light sensor 420 and processing device 430 of authentication system 400.

Ex. 1005, 7:20-37

# Derakhshani Doesn't Verify Ears/Features on Side Of Head

Using ears/features to focus a sensor does not mean *verifying* anything about the ear/feature

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 sensors, the focus distance may be adjusted for different images by adjusting a focus configuration setting for the 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

Ex. 1005, 16:47-54

Turk never agrees that Derakhshani teaches “verifying” reduced visibility

|    |   |                                                         |
|----|---|---------------------------------------------------------|
| 11 | Q | Okay. And in that, would Derakhshani be                 |
| 12 |   | capturing one image where a given landmark is in focus, |
| 13 |   | and in another image, that same landmark is then        |
| 14 |   | blurry?                                                 |
| 15 | A | That is my understanding of how he's                    |
| 16 |   | describing that process.                                |

Ex. 1059, 144:11-16

# Derakhshani's Landmarks Aren't Biometric Data

## Jumio Argues

Derakhshani's image landmarks are  
"biometric data"

106Reply, 10; 107Reply, 4; 108Reply, 9; 109Reply, 9

"image landmarks" are not useful for identification

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

Ex. 1005, 16:51-54

17:16-19 references a "spoofing" photograph

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 land-

Turk: "biometric data" must be useful for identification; Derakhshani silent on this

because these image landmarks can be "a background object." *Id.* As explained above, even the landmarks identified that could be part of a user – including an iris, eye corner, or ear – are not "biometric data" in the context of Derakhshani because there is no discussion of how to identify a user using those landmarks.

Ex. 2061, ¶118

|    |   |                                                        |
|----|---|--------------------------------------------------------|
| 21 | Q | Okay. Is there a requirement that the term             |
| 22 |   | "biometric data," as used for the FaceTec patents, be  |
| 23 |   | used for authentication?                               |
| 24 | A | I think we discussed this before. I think              |
| 25 |   | that data should be useful for identification. Whether |
| 1  |   | it's used or not is a different question.              |

Ex. 1059, 48:21-49:1

106POR, 48; 106Sur-Reply, 22; 108POR, 43-44; 108Sur-Reply, 19; 109POR, 49; 109Sur-Reply, 22

**Zhang (Ex. 1006)**

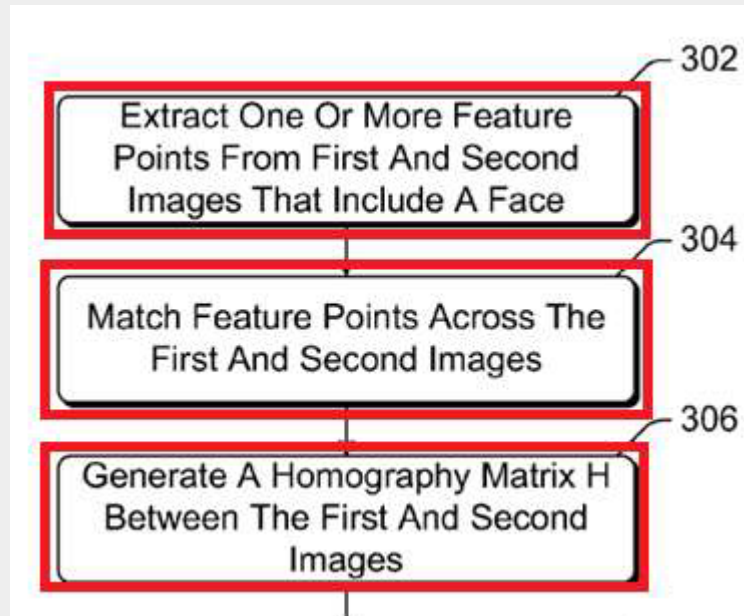
# Expected Distortion Based on Movement

- Patents require detecting captured images having “expected distortions” resulting from movement of a camera between taking images

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.

‘471, 38:39-45

## Zhang's Feature Points vs. Different Locations

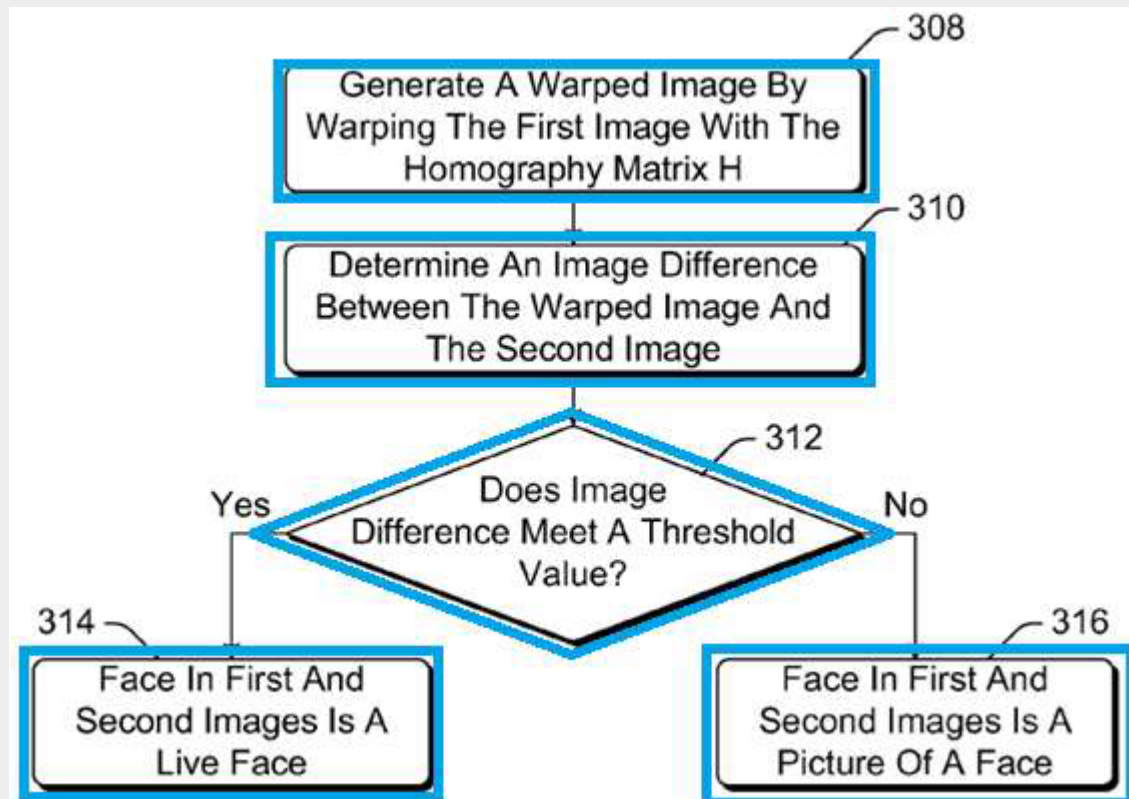


Ex. 1006, Fig. 3

Zhang extracts and matches “feature points” from first and second images and generates homography matrix  $H$  using the feature points.

Zhang warps the first image using homography matrix  $H$  and compares the warped image to the second image at “different locations” for comparison to a threshold.

Ex. 1006, Fig. 3



# Zhang's "Image Difference" is Not Related to "Movement"

[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 the second image are superimposed and the difference in color or intensity values at the same pixels (locations) in the two images is determined. In other words, for each location [u,v] in the warped image, the difference between the color or intensity value at the location [u,v] in the warped image and the location [u,v] in the second image is determined. The differences determined for these different locations are then combined to generate the image difference. The differences can be combined in different manners, such as being averaged together, being added together, and so forth.

[0033] A determination is then made as to whether the image difference determined in act 310 meets a threshold value (act 312). The image difference can meet the threshold value by, for example, being greater than the threshold value, being greater than or equal to the threshold value, and so forth. This threshold value can be, for example 10 in situations where the color values can be one of 256 gray levels. This threshold value can be a fixed value (e.g., 10 gray levels) or can be a relative value (e.g., 5% of the number of possible color or intensity values).

“Image difference:” a comparison of color/intensity values at the same [u,v] locations across images

“Image difference” is compared to a “threshold value”

# Zhang’s “Image Difference” is Not Related to “Movement”

[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 the second image are superimposed and the difference in color or intensity values at the same pixels (locations) in the two images is determined. In other words, for each location [u,v] in the warped image, the difference between the color or intensity value at the location [u,v] in the warped image and the location [u,v] in the second image is determined. The differences determined for these different locations are then combined to generate the image difference. The differences can be combined in different manners, such as being averaged together, being added together, and so forth.

Zhang’s “image difference” fails to meet “movement” requirement

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.

Dr. Turk:

‘471, 38:29-45

|    |   |                                                        |
|----|---|--------------------------------------------------------|
| 12 | Q | Okay. So would you agree that Zhang                    |
| 13 |   | anticipates there to be an image difference when there |
| 14 |   | is a live face being imaged?                           |
| 15 | A | No, I wouldn't say Zhang anticipates anything.         |
| 16 |   | Zhang calculates, as we've gone through briefly the    |
| 17 |   | homography matrix, does a warping, does a comparison   |
| 18 |   | and then checks to see if that comparison is above or  |
| 19 |   | below a threshold.                                     |

106POR, 40, 49-51; 106Sur-Reply, 22; 107POR, 40-41, 48-50; 107Sur-Reply, 20; 108POR, 43, 48-49; 108Sur-Reply, 21-22; 109POR, 40-41, 49-50; 109Sur-Reply, 22; Ex. 2061, ¶¶126-128

Ex. 1059, 27:12-19

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

# Zhang's Feature Points are Not Selected Locations

## Jumio Argues

Jumio: the same locations are used for “feature points” and for “different locations”  
106Reply, 12-13; 107Reply, 11-12; 108Reply, 10-11; 109Reply, 11-12

FaceTec misreads Zhang. Zhang teaches matching feature points across first and second images by “identifying the locations of the same feature points in each of the two images.” (EX1006, [0028]-[0029].) Zhang uses the feature points to generate the homography matrix. (EX1006, [0028]-[0029].) When comparing the images, Zhang uses the same extracted feature points having respective “locations” to determine color/intensity value differences. (EX1006, [0031]; EX1060, ¶¶70-72.)

106Reply, 12-13

106POR, 35-37, 51-53; 106Sur-Reply, 23-24; 107POR, 35-38, 50-53; 107Sur-Reply, 20-22; 108POR, 34-37, 49-52; 108Sur-Reply, 20-21; 109POR, 34-37, 51-53; 109Sur-Reply, 23-24

Zhang: “feature points” are different from “different locations”

[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 multiple pixels. These feature points can be extracted in a variety of different conventional manners, such as using template matching algorithms, feature matching algorithms, and so forth. In one or more embodiments, techniques for extract-

[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 the second image are superimposed and the difference in color or intensity values at the same pixels (locations) in the two images is determined. In other words, for each location [u,v] in the warped image, the difference between the color or intensity value at the location [u,v] in the warped image and the location [u,v] in the second image is determined. The differences determined for these different locations are then combined to generate the image difference. The differences can be combined in different manners, such as being averaged together, being added together, and so forth.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

# Zhang’s Feature Points are Not Selected Locations

Jumio Argues

Jumio: the same locations are used for “feature points” and for “different locations”  
106Reply, 12-13; 107Reply, 11-12; 108Reply, 10-11; 109Reply, 11-12

FaceTec misreads Zhang. Zhang teaches matching feature points across first and second images by “identifying the locations of the same feature points in each of the two images.” (EX1006, [0028]-[0029].) Zhang uses the feature points to generate the homography matrix. (EX1006, [0028]-[0029].) When comparing the images, Zhang uses the same extracted feature points having respective “locations” to determine color/intensity value differences. (EX1006, [0031]; EX1060, ¶¶70-72.)

106Reply, 12-13

Turk: every pixel is at a location

17 A When it says "the same locations," it means a  
18 location in the warped image is being compared to the  
19 same location in the second image. And that's being  
20 done at a number of locations, but those locations are  
21 independent and separate from the earlier determination  
22 of locations that we discussed, the feature locations.

Ex. 1059, 25:17-22

15 BY MS. NGUYEN:  
16 Q Okay. Is there a reason why Zhang used  
17 "location" for both?  
18 A Yes. Because in an image, every piece of  
19 information, every pixel, is at a location. So we're  
20 pretty much always talking about locations in images  
21 when we talk about image data.

Ex. 1059, 26:7-21

106POR, 35-37, 51-53; 106Sur-Reply, 23-24; 107POR, 35-38, 50-53; 107Sur-Reply, 20-22; 108POR, 34-37, 49-52; 108Sur-Reply, 20-21; 109POR, 34-37, 51-53; 109Sur-Reply, 23-24

# Zhang-Tanii Doesn't Verify Anything About Ears/Features

Zhang does not expressly disclose verifying the presence of a user's ears in one image and absence in another. But as Tanii shows, the absence or presence of an ear is a natural result of the distance between the user and camera. Specifically, given sufficient distance between the face and camera, the ears are captured because there is enough distance for light rays from the ears to reach the camera sensor. *See Tanii*, [0047]-[0048], Figs. 3A-B; *Daft*, ¶¶325-26.

But when a face is too close, the ears will not be captured because light rays from the ears cannot reach the camera sensor. *See Tanii*, [0048], Figs. 4A-B; *Daft*, ¶326.

This was a well-known consequence of distance-induced distortion when capturing images of a face. *See Daft*, ¶326.

Accordingly, a POSITA would have appreciated (based on Tanii) that the presence of a user's ears in one image and absence of the user's ears in another image at a closer distance would further indicate a three-dimensional face, and a POSITA would have found it obvious to modify Zhang to verify this. *Daft*, ¶326.

106Pet., 68-69

The Petition does not even plead that Zhang in view of Tanii teaches “verifying” anything about ears or features

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.

# Zhang's Feature Points Aren't Biometric Data

## Jumio Argues

Zhang's "feature points" are "biometric data"  
106Reply, 15-16; 107Reply, 10; 108Reply, 9; 109Reply, 14-15

Zhang discloses processing the first image to extract "feature points" from the image. *Zhang*, [0027] ("[O]ne or more feature points are extracted from two 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."). A POSITA would have understood these extracted feature points to be biometric data that identifies unique physical characteristics of a face. *See* §§VII.D.3.g (1[d2]), VII.D.3.j (1[d5]); *Daft*, 106Pet., 71-72

Turk: "biometric data" must be useful for identification and authentication

21 Q Okay. Is there a requirement that the term  
22 "biometric data," as used for the FaceTec patents, be  
23 used for authentication?  
24 A I think we discussed this before. I think  
25 that data should be useful for identification. Whether  
1 it's used or not is a different question.  
2 Q Okay. So, in your opinion, it's a requirement  
3 that biometric data, as used in the FaceTec patents, be  
4 useful for authentication?  
5 MR. JOHNS: Objection; form.  
6 BY MS. NGUYEN:  
7 Q Is that right?  
8 A Yeah, I think that's a fair summary.

Ex. 1059, 48:21-49:8

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

'471, 39:12-13

# Motion to Strike

# Jumio's New Arguments - Derakhshani 'Spoofing' Photograph

- Jumio newly argues a “spoofing” photograph teaches an image “having multiple landmarks.”

(EX1005, 16:51-54, 17:16-17, 17:29-36.) It would be obvious for an image having multiple “landmarks (e.g., an eye, nose, mouth, *and* ear)” to be of the head/face.

(EX1005, 17:16-19; 3:5-7, 17:2-6; EX1059, 136:25-137:3.) Derakhshani also

106Reply, 1

a further-away image for the liveness score. Because the liveness score determination uses images of non-eye landmarks, the further-away image captures more than the eye, *e.g.*, it captures the eye, nose, mouth, and ear—*i.e.*, the face.

(EX1005, 17:16-19.) Capturing an image of the eye vasculature does not preclude

106Reply, 2

(POR, 41-42.) It points to figures “depicting only eyes” and a non-limiting

“placing [a] sensor 6-12cm from the eye” for support, but ignores other disclosures of capturing images of non-eye landmarks. (EX1005, 16:44-54 (describing images with “a nose, an ear, or a background object”), 17:16-17 (describing “landmarks

(e.g., an eye, nose, mouth, and ear)” in an image); POR, 41-42.) And

106Reply, 2-3

Derakhshani’s teachings are not strictly from the figures. (POR, 41.) Turk

admitted the figures do not show a disclosed embodiment (captured image of the nose, ear, mouth, and eye). (EX1059, 137:4-17; EX1005, 17:16-19.) FaceTec is

106Reply, 3

See also Ex. 1060 (Daft), ¶¶13, 20, 23-25, 28, 38, 40, 46, 48, 50.

## Jumio's New Arguments - Derakhshani 'Spoofing' Photograph

- Jumio newly argues a “spoofing” photograph teaches an image “having multiple landmarks.”

FaceTec's attempt to improperly separate “landmarks” from the eye vasculature is also clearly wrong because Derakhshani names the eye as a landmark. (EX1005, 17:16-17 (“*landmarks (e.g., an eye, nose, mouth, and ear)*”); POR, 47.) FaceTec's argument that liveness detection is not part of Derakhshani's

106Reply, 9

Derakhshani discloses “an eye, nose, mouth, and ear” (what FaceTec refers to as “image” landmarks)—*i.e.*, “biometric data.” (EX1005, 17:16-19; EX2061, ¶112.) FaceTec argues “image landmarks” are not a “mapping of facial features.”

106Reply, 10

See also Ex. 1060 (Daft), ¶¶13, 20, 23-25, 28, 38, 40, 46, 48, 50.

## Jumio's New Arguments – Derakhshani New Obviousness Position

- Jumio newly argues it would be obvious that an image with multiple landmarks is of a head or face.

(EX1005, 16:51-54, 17:16-17, 17:29-36.) It would be obvious for an image having multiple “landmarks (e.g., an eye, nose, mouth, *and* ear)” to be of the head/face.

(EX1005, 17:16-19; 3:5-7, 17:2-6; EX1059, 136:25-137:3.) Derakhshani also

106Reply, 1

a further-away image for the liveness score. Because the liveness score determination uses images of non-eye landmarks, the further-away image captures more than the eye, *e.g.*, it captures the eye, nose, mouth, and ear—*i.e.*, the face.

(EX1005, 17:16-19.) Capturing an image of the eye vasculature does not preclude

106Reply, 2

(POR, 41-42.) It points to figures “depicting only eyes” and a non-limiting

“placing [a] sensor 6-12cm from the eye” for support, but ignores other disclosures of capturing images of non-eye landmarks. (EX1005, 16:44-54 (describing images with “a nose, an ear, or a background object”), 17:16-17 (describing “landmarks

(e.g., an eye, nose, mouth, and ear)” in an image); POR, 41-42.) And

106Reply, 2-3

See also Ex. 1060 (Daft), ¶¶20, 25, 28, 50

## Jumio's New Arguments – Derakhshani New Obviousness Position

- Jumio newly argues it would be obvious in response to unfavorable testimony, not an argument made by FaceTec.

25 Q Okay. And Derakhshani also teaches capturing  
Page 136  
1 images having multiple landmarks within the same image,  
2 right?  
3 A I believe so.  
4 Q Okay. So if Derakhshani is capturing an image  
5 that has an ear, nose, mouth and eye, what type of  
6 image is it capturing?  
7 A Well, I don't think Derakhshani ever says that  
8 it will capture images that include all of those.  
9 Q Uh-huh.  
10 A So they may well just be individual examples  
11 that would never be in the same image.  
12 If Derakhshani were to capture something with  
13 all of those, it would be an image that is generally  
14 different than the images that are shown in  
15 Derakhshani, because those images generally don't cover  
16 larger parts of the face that would include such  
17 features.

Ex. 1059, 136:25-137:17.

## Jumio's New Arguments – Derakhshani's “Further-Away” Images

- Jumio newly argues Derakhshani teaches capturing close-up images (with vasculature) and further-away images (*without* or with *blurry* vasculature).

cannot capture the head/face. (POR, 40-41.) Derakhshani's spatial metric determination uses multiple images captured at different distances. (EX1005, 16:44-47, 17:45-47.) For example, a close-up image may capture the eye vasculature (with enough precision) for the match score and/or liveness score, and a further-away image for the liveness score. Because the liveness score determination uses images of non-eye landmarks, the further-away image captures more than the eye, *e.g.*, it captures the eye, nose, mouth, and ear—*i.e.*, the face. (EX1005, 17:16-19.) Capturing an image of the eye vasculature does not preclude

106Reply, 2

*Third*, FaceTec is wrong that the eye vasculature and face need to be captured simultaneously both with enough precision. (POR, 43.) The spatial metric determination may use a close-up image that captures the eye vasculature in focus (having enough precision) and a further-away image that captures a landmark in focus (eye vasculature is blurred). (EX1059, 144:7-16.) The match score determination may use the close-up image. (EX1060, ¶¶28-29.)

106Reply, 4

See also Ex. 1060 (Daft), ¶¶13, 23-24, 26-27, 29, 38

# Jumio's New Arguments – Derakhshani's “Further-Away” Images

- Jumio never used the word “vasculature” in its Petition or Dr. Daft’s declaration.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

JUMIO CORPORATION,  
Petitioner

FACETEC, INC.,  
Patent Owner

IPR2025-00106; IPR2025-00107  
U.S. Patent Nos. 10,776,471; 11,776,472

DECLARATION OF  
IN SUPPORT OF PETITION  
OF U.S. PATENT NOS. 10,776,471

*vasculature*

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

JUMIO CORPORATION,  
Petitioner

v.

FACETEC, INC.,  
Patent Owner

IPR2025-00106  
U.S. Patent No. 10,776,471

PETITION FOR *INTER PARTES* REVIEW  
OF U.S. PATENT NO. 10,776,471

Mail Stop PATENT BOARD  
Patent Trial and Appeal Board  
U.S. Patent & Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450

*vasculature*

## Jumio's New Arguments – Zhang's motion estimation

- Jumio newly references Zhang's motion estimation technique for the 00106 proceeding

[0034].) As Turk testified, this “binary decision” of authenticating based on color/intensity value differences exceeding a threshold is predetermined (EX1059, 27:12-30:11)—*i.e.*, expected. And a live face having a three-dimensional structure exhibits the distortion of the '471. Given these teachings, the Board correctly found Zhang teaches elements 1[d6]/10[f] and 1[d7]/10[g]. (DI, 45; EX1060, ¶¶59-64, 66-67.)

106Reply, 11-12

60. Zhang's authentication process 200 is depicted in the flowchart of Figure 2 below. The authentication process involves accessing multiple images of the user and determining whether motion is present. Process 400 includes extracting feature points (act 404), determining whether motion is present. Process 400 includes extracting feature points (act 404), determining whether motion is present. Process 400 includes extracting feature points (act 404), determining whether motion is present.

63. Motion estimation: Process 400 shows how Zhang determines whether motion is present. Process 400 includes extracting feature points (act 404), determining whether motion is present. Process 400 includes extracting feature points (act 404), determining whether motion is present.

64. In fitting characteristics to a plane in act 410, Zhang determines whether the face is a live face by analyzing characteristics of facial components or feature points. Zhang determines a first value by determining the change in distance from a particular feature: “a maximum distance from a particular feature (e.g., tip of a nose).” (EX1006, [0045].) Zhang also determines a second value by determining the change in distance between two facial components: “the distance

- Improper attempt to skirt word limits/incorporation-by-reference prohibition

## Jumio's New Arguments – Zhang in view of Derakhshani

- Jumio newly relies on Derakhshani to repair deficiencies in its Zhang grounds).
- Jumio also relies on Derakhshani to create a new obviousness position, relating Zhang's "live face" to Derakhshani's "live eye"

The prior art confirms. Derakhshani explains "the intensity or color scale can be zoomed in to reveal more subtle changes in the level of the detected image signal. If the captured images are of a *live eye*, it is expected that the range of *color or intensity values detected will continue to vary continuously*. In contrast, a spoofed image (e.g., a digital photograph presented to the sensor) may exhibit large discontinuous jumps corresponding to halftones."). (EX1005, 19:30-37.) Thus, a live face exhibits expected distance-induced distortion via differences in color/intensity values. (EX1060, ¶65.)

106Reply, 12

# Requirements of FaceTec Patents

# All Claims Require Capture of a Face at Two Distances

- “Ultimate goal:” matching a face of a user to an identity or image
- Jumio patents relate to “*facial-authentication* systems and methods”

With the ultimate goal of matching a face of a user to an identity or image stored in a database 124, to authenticate the user, the ID App may first process the image captured by the camera 114, 134 to identify and locate the face that is in the image. As shown in FIG. 1, there may be the face 108.

'471, 7:39-43; '910, 7:32-36

The '471 Patent describes facial-authentication systems and methods to distinguish a three-dimensional face from a two-dimensional picture of a face by looking for well-known optical effects—such as a “fish-eye” effect—that naturally occur in images to different degrees due to the three-dimensionality of a face and the distance between the face and the camera. *Id.*, 1:64-67, 28:34-58. The patent

106Pet., 4

# All Claims Require Capture of a Face at Two Distances

- Images are captured at different distances and processed to detect expected distortion to understand whether face is flat or three-dimensional

FIG. 13A

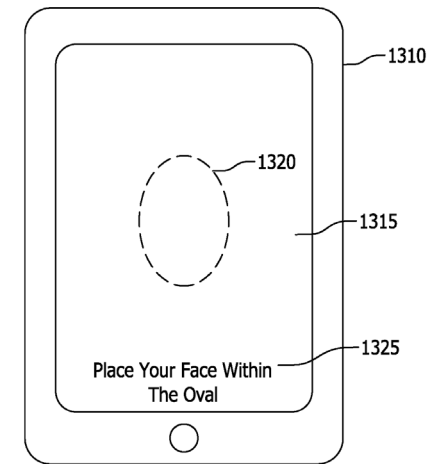
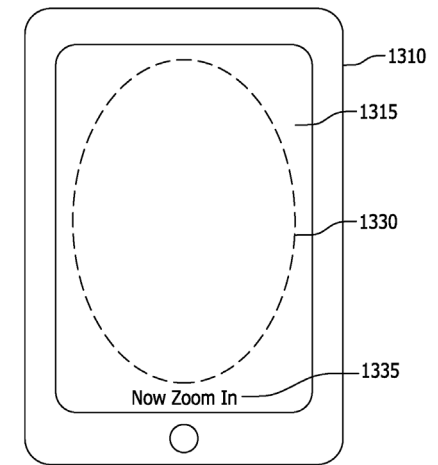


FIG. 13B



# Capture of Images of a Face – Undisputed

'606

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 with the camera of the computing device at a first distance from the user;

10. A system for verifying three-dimensionality of a user's face using **images of the user's face** captured using a camera equipped computing device, the system comprising:

...

capture at least **one first image of the user** taken with the camera of the computing device when the camera is located a first distance from the user;

19. 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:

receiving first biometric data generated from **at least one first image of the user** taken with the camera of the computing device located at a first distance from the user;

'938

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;

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;

8. A method for determining when a user, based on images of the user's face, does not exhibit three-dimensionality, the method comprising:

capturing **at least one first image of the user's face** taken with a camera located at a first distance from the user's face, the camera associated with a computing device;

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;

20. A method for determining whether a user exhibits three-dimensionality, the method comprising:

capturing at least one **first image of a user's face** taken with a camera located a first distance from the user, the camera associated with a computing device;

# Capture of Images of a Face – Disputed

'471

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;

'910

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;

## Intuitive User Training and Enhanced Security by “Zooming”

In one embodiment, the system is configured to aid the user to easily learn to authenticate with the system. As shown in FIG. 13A, once enrollment or authentication is begun as described previously, the system causes the user's mobile device 1310 to display a small oval 1320 on the screen 1315 while the mobile device 1310 is imaging the user. Instructions 1325 displayed on the screen 1315 instruct the user to hold the mobile device 1310 so that his or her face or head appears within in the oval 1320. Because the oval 1320 is small, the user is required to hold the mobile device 1310 away from his or her body, such as by straightening his or her arm while holding the mobile device 1310. The maximum arm length and face size is unique to the user. In other embodiment, the arm may not be fully straightened such as to accommodate operation when space is not available, such as in a car or in a crowded location. It is noted that while the small oval 1320 is shown centered in the display, it may be positioned anywhere on the screen 1315.

FIG. 13A

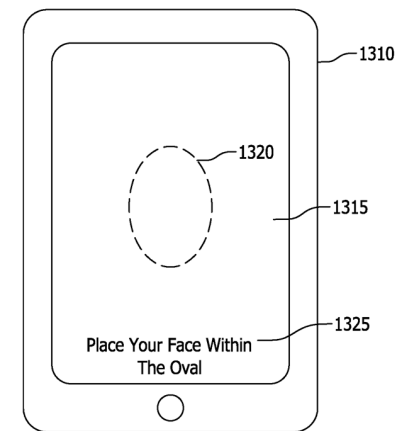
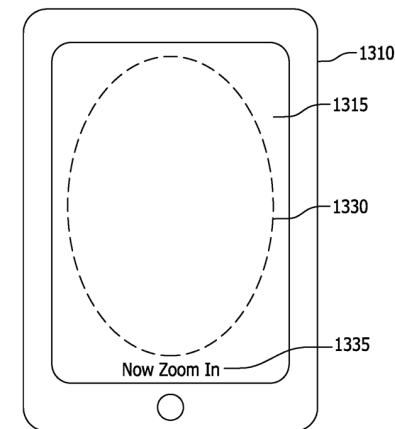


FIG. 13B



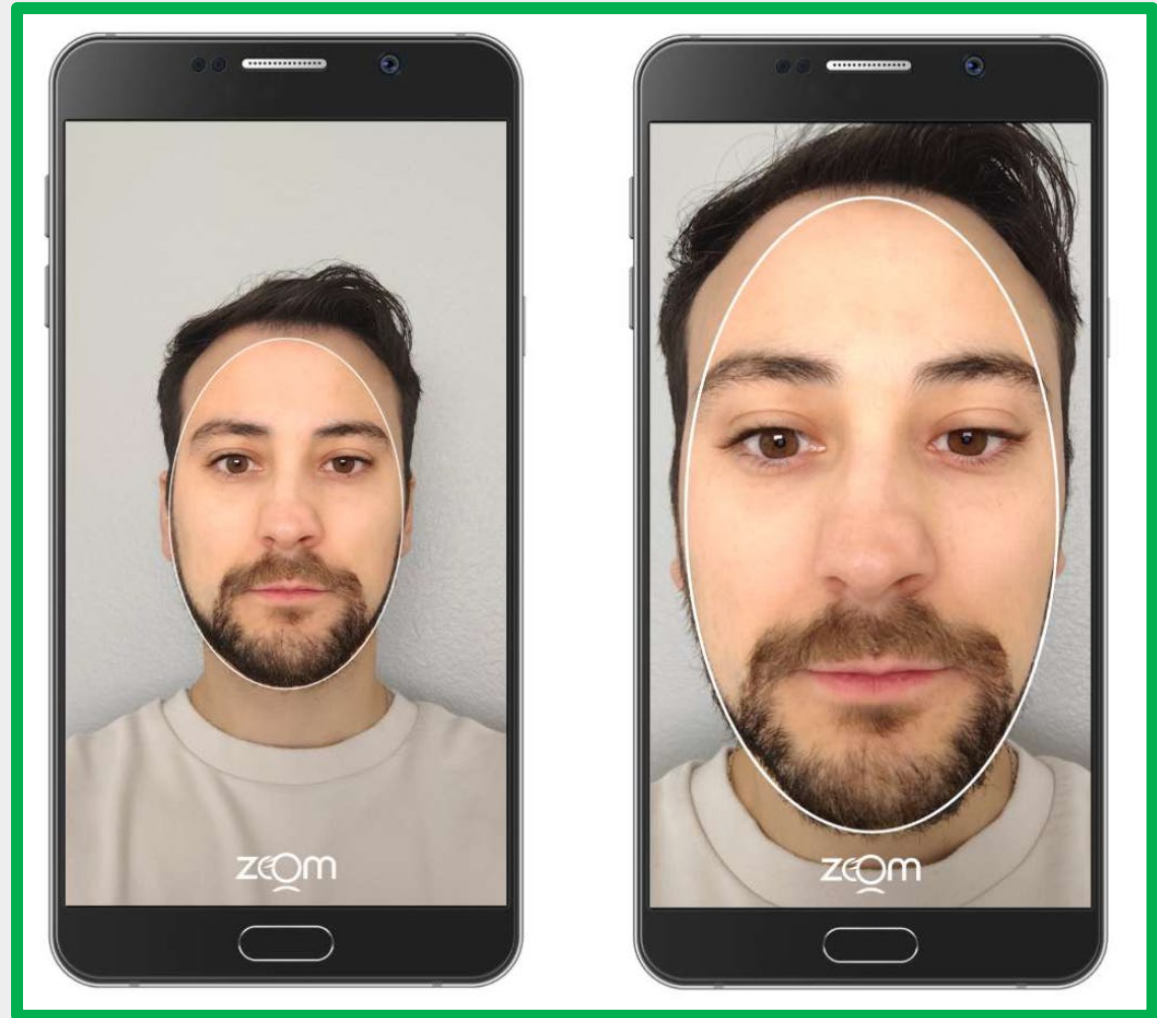
# Capture of Images of a Face – Disputed Claims

'471 (similar in '910)

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;

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.



# Capture of Images of a Face – Disputed Claims

'471

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;

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.

14. The method according to claim 13, wherein the one or more prompts are ovals on the screen within which the face of the user is placed to capture the at least one first image and the at least one second image.

'910

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;

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.

14. The method according to claim 13, wherein the one or more prompts are an oval shape guide on the screen within which an image of a face of the user is aligned to capture the at least one first image and the at least one second image.

FIG. 13A

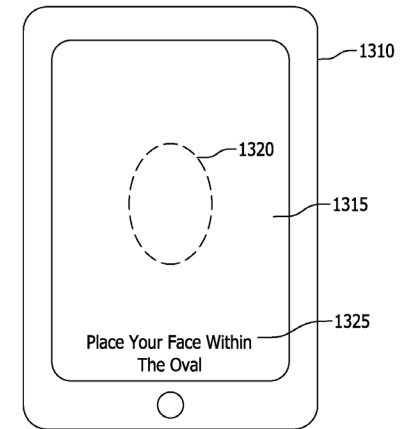
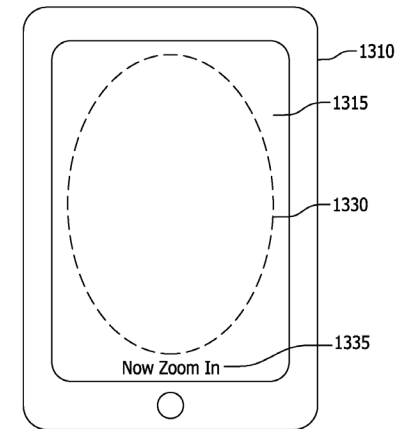


FIG. 13B



# Hoyos (Ex. 1010)

# Hoyos Determines Reflections From Eyes, Not Faces

The Petitions do not even plead that Hoyos teaches reflections from a face

face. *Daft*, ¶378. Hoyos, however, teaches that measuring reflectance of displayed images is a well-known method to verify the liveness of the user. *Hoyos*, [0018]-[0019]; [0033]-[0035]. A POSITA would have been motivated to modify Zhang to

106Pet., 79

The patent requires detecting a reflection off of a user's face

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.

147. Hoyos detects reflections from human eyes, not a *face*, as required by the explicit language of claim 18. Capturing reflections from an eye is materially different from analyzing reflections from the face. The human eye is a smooth, curved, and highly reflective surface that behaves similarly to a mirror or calm water. For example, the eye exhibits specular reflection that preserves the shape and pattern of the light source. In contrast, facial skin is a complex, textured surface that acts as a diffuse reflector. This fundamental difference in surface properties means that the techniques used to process reflections from the eye are not transferable to facial reflection analysis. Moreover, the face includes heterogeneous regions (such as hair, nostrils, and blemishes) that reflect light differently or not at all. Additionally, the eye occupies a relatively small area of the face, requiring close-range optics and high resolution for reflectance analysis. Eyes can also reflect things like QR codes while it would be more difficult to read a QR code reflected off of a face. Ex. 1001 ('471 patent), 3:35-43 (discussing reflecting a QR code off of a user's eye).

Ex. 2061, ¶147