

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

NOBOTS LLC,
Patent Owner.

IPR2022-00941
Patent 10,423,885 B2

Before JOSIAH C. COCKS, BARBARA A. PARVIS, and
ROBERT J. WEINSCHENK, *Administrative Patent Judges*.

Opinion for the Board filed by COCKS, *Administrative Patent Judge*.

Opinion dissenting filed by WEINSCHENK, *Administrative Patent Judge*.

COCKS, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

Nobots LLC - Ex. 2022 IPR2026-00429 Google LLC v. Nobots
--

I. INTRODUCTION

A. Background

Google LLC (“Petitioner”) filed a Petition (Paper 1, “Pet.”) requesting *inter partes* review of claims 1–20 (“the challenged claims”) of U.S. Patent No. 10,423,885 B2 (Ex. 1001, “the ’885 patent”). We instituted the petitioned review as to claims 3–9, 11, and 13–20. Paper 13 (“Institution Decision” or “Inst. Dec.”).¹

Nobots LLC (“Nobots” or “Patent Owner”) filed a Patent Owner Response (Paper 16, “PO Resp.”) to oppose the Petition. Petitioner filed a Reply (Paper 22, “Pet. Reply”) to the Patent Owner Response. Patent Owner filed a Sur-reply (Paper 26, “PO Sur-reply”) to the Reply. We conducted an oral hearing on August 31, 2023. A transcript has been entered into the record. Paper 32 (“Tr.”).

We have jurisdiction under 35 U.S.C. § 6(b)(4) and § 318(a). This Decision is a final written decision under 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73 as to the patentability of claims 3–9, 11, and 13–20 of the ’885 patent. We determine that Petitioner has shown by a preponderance of the evidence that claims 3–9, 11, and 13–20 are unpatentable.

B. Related Matters

The parties state that the ’885 patent was asserted in *Nobots LLC v. Google LLC*, Civil Action No. 6:21-cv-01290 (W.D. Tex., Waco Division).

¹ As we noted in our Institution Decision, in a Preliminary Response filed prior to institution, Patent Owner expressed that claims 1, 2, 10, and 12 had been disclaimed under 35 U.S.C. § 253(a). Inst. Dec. 2 (recognizing Ex 2103, “Disclaimer in Patent Under 37 CFR 1.321(a)”). Accordingly, those claims are not part of this proceeding.

Pet. xi; Paper 5, 1.² Patent Owner further states that the '885 patent was asserted in *Nobots LLC v. Google LLC*, No. 1:22-cv-00585 (W.D. Tex., Austin Division). Paper 6, 1. Patent Owner also identifies IPR2022-00940 as a related proceeding. Paper 6, 1.³

C. The '885 Patent

The '885 patent is titled “Systems, Methods and Apparatus for Evaluating Status of Computing Device User.” Ex. 1001, code (54). The Abstract of the '885 patent is reproduced below:

Methods, systems and apparatus for assessing the likely status of an operator of a computing device interacting with a server as a human operator or an autonomic computer application, such as a “bot” are described herein. By monitoring at least some data, e.g., biometric data, generated at the client computing device, a comparison can be made between the monitored data and model data relating to human interaction with the computing device. The results of the comparison can lead to a value that represents the likelihood that the monitored data results from human interaction.

Id. at code (57).

The '885 patent further summarizes its disclosure as being “for assessing the likely user status of a computing device interacting with a server where computing device is in bi-directional operative communication with the server wherein the status is one of a human

² In its filing of updated mandatory notices, Patent Owner indicates that the noted proceeding is “now terminated.” Paper 6, 1.

³ The Petition in IPR2022-00940 was filed on the same day as the Petition in the instant proceeding, and involves a related patent (U.S. Patent No. 9,595,008 B1).

operator or a computer executable program (also referred to herein as a ‘bot’).” *Id.* at 2:18–24.

By way of background, the ’885 patent explains that it became necessary for builders of web sites to develop “tests” to distinguish between human users and bots. The ’885 patent further describes the following:

Carnegie Mellon University coined the term “CAPTCHA” (Completely Automated Public Turing test to tell Computers and Humans Apart) for these types of tests. A common type of CAPTCHA requires that the user type the letters, digits or characters of a distorted image appearing on the screen. The objective is to create an image that a bot cannot easily parse but that is discernable by a human. Such efforts have been successful in preventing non-adaptive software from recognizing the imaged characters, but people intent on abusing these sites have designed ways to circumvent the CAPTCHA, such as through specially tuned character recognition programs.

Id. at 1:28–39.

“Current CAPTCHA technology is visual or auditory in nature, requiring the human user to answer a test that should be simple to most humans but difficult for non-humans, e.g., bots.” *Id.* at 1:60–63. The ’885 patent describes additional assessment measures, beyond an auditory or visual CAPTCHA test, involving a comparison of “acquired and/or available data relating to the operation of the computing device to suitable models embodying human user derived data (model data).” *Id.* at 2:25–27.

“[A]cquired” data can include “active” data such as “pointing device vector movements,” “key stroke combinations,” or “time differentials” between “stimulus” (e.g., dialog box displays or radio buttons on a computer screen) and a user response’s response to such stimulus. *Id.* at 2:65–3:10.

“[A]vailable” data can include “[p]assive” data such as “browser cookies,” “destination IP histories,” and a computer’s “IP address.” *Id.* at 3:17–22.

Assessment of such data may be used to establish “a probability value” as to whether a particular operator is a human or a bot. *Id.* at 2:24–31.

D. Challenged Claims

Petitioner offers challenges to claims 3–9, 11, and 13–20 of the ’885 patent. As noted above, independent claim 1, which was the only independent claim of the ’885 patent, has been disclaimed. We reproduce now disclaimed claim 1 along with dependent claim 3 as representative of the subject matter of the ’885 patent.

1. [1PRE] A method comprising:

[1A] testing for a presence of biometric data associated with an operator of a computing device attempting to access a server;

[1B] controlling access to the server by at least one of:

[1C] denying access of the computing device attempting to access the server when the biometric data is not present;

[1D] or not denying access of the computing device attempting to access the server when some biometric data is present.

3. A method as claim 1 recites, further comprising identifying whether the biometric data matches previously recorded biometric data.

Ex. 1001, 5:42–52, 56–58 (using claim element identifiers [1PRE] – [1D] as presented in the Petition (*see, e.g.*, Pet. 12–19)).

E. Alleged Grounds of Unpatentability

In its Petition, Petitioner asserts the following grounds of unpatentability:⁴

Ground #	Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1	1–3, 5, 6, 8, 10, 12–16, 18–20	103	O’Sullivan, ⁵ Willner ⁶
2	1–8, 10–20	103	O’Sullivan, Willner, Broder ⁷
3	1, 9	103	O’Sullivan, Willner, Tanzer ⁸
4	1, 2, 10, 12	102/103	Meek ^{9, 10}
5	1–3, 5, 6, 8, 10, 12	103	Meek, Willner
6	1–3, 5, 6, 8, 10, 12	103	Meek, Kroll ¹¹
7	1–8, 10–12	103	Meek, Willner, Broder

⁴ For completeness, we reproduce all the grounds and associated claims as they are presented in the Petition even though claims 1, 2, 10, and 12 have been statutorily disclaimed.

⁵ U.S. Patent Application Publication No. US 2008/0319774 A1 published Dec. 25, 2008 (“O’Sullivan,” Ex. 1006).

⁶ U.S. Patent Application Publication No. US 2009/0024971 A1 published Jan. 22, 2009 (“Willner,” Ex. 1005).

⁷ U.S. Patent Application Publication No. 2008/0147456 A1 published Jun. 19, 2008 (“Broder,” Ex. 1011).

⁸ U.S. Patent Application Publication No. US 2007/0255818 A1 published Nov. 1, 2007 (“Tanzer,” Ex. 1012).

⁹ U.S. Patent Application Publication No. US 2005/0278253 A1 published Dec. 15, 2005 (“Meek,” Ex. 1008).

¹⁰ We note that all of the claims 1, 2, 10, and 12 to which this ground would have applied have been disclaimed. Accordingly, this Ground 4 is no longer applicable to this proceeding. We note that the parties also do not address Ground 4 based only on Meek as a part of the trial.

¹¹ U.S. Patent No. US 6,405,922 B1 issued Jun. 18, 2002 (“Kroll,” Ex. 1010).

Ground #	Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
8	1–8, 10–12	103	Meek, Kroll, Broder
9	1, 9	103	Meek, Willner, Tanzer
10	1, 9	103	Meek, Kroll, Tanzer
11	1, 13–16, 18–20	103	Meek, Kitts ¹²
12	1, 13–16, 18–20	103	Meek, O’Connell ¹³
13	1, 13–20	103	Meek, Kitts, Broder
14	1, 13–20	103	Meek, O’Connell, Broder

Pet. 1.

F. Testimonial Evidence

Petitioner relies on the Declaration (Ex. 1003) and Reply Declaration (Ex. 1042)¹⁴ of Daniel P. Lopresti, Ph.D.

Patent Owner relies on the Declaration of Dr. Samuel Russ (Ex. 2104).¹⁵

II. ANALYSIS

A. Principles of Law

A petition must show how the construed claims are unpatentable under the statutory grounds it identifies. 37 C.F.R. § 42.104(b)(4).

To establish anticipation under 35 U.S.C. § 102, “all of the elements and limitations of the claim must be shown in a single prior art reference,

¹² U.S. Patent Application Publication No. US 2008/0114624 A1 published May 15, 2008 (“Kitts,” Ex. 1009).

¹³ U.S. Patent Application Publication No. US 2007/0239604 A1 (published Oct. 11, 2007) (“O’Connell,” Ex. 1007).

¹⁴ Exhibit 1042 was submitted in conjunction with Petitioner’s Reply.

¹⁵ Patent Owner indicates that a prior Declaration of Dr. Samuel Russ (Ex. 2101) is withdrawn. PO Resp. 5.

arranged as in the claim.” *Karsten Mfg. Corp. v. Cleveland Golf Co.*, 242 F.3d 1376, 1383 (Fed. Cir. 2001).

A claim is unpatentable under § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) when in evidence, objective indicia of non-obviousness (i.e., secondary considerations). *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

In an instituted *inter partes* review, a petitioner has the burden to show unpatentability by a preponderance of the evidence. 35 U.S.C. § 316(e). The burden of persuasion never shifts to Patent Owner. *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015).

B. Level of Ordinary Skill in the Art

In determining the level of skill in the art, we consider the type of problems encountered in the art, the prior art solutions to those problems, the rapidity with which innovations are made, the sophistication of the technology, and the educational level of active workers in the field. *Custom Accessories, Inc. v. Jeffrey-Allan Indus. Inc.*, 807 F.2d 955, 962 (Fed. Cir. 1986); *Orthopedic Equip. Co. v. U.S.*, 702 F.2d 1005, 1011 (Fed. Cir. 1983).

Petitioner contends that “a person of ordinary skill (“POSA”) would have had a bachelor’s degree in computer science or a related field with coursework relating to computer science, plus two years’ academic and/or industry experience in computer security. More education could substitute for experience, and vice versa.” Pet. 3–4 (citing Ex. 1003 ¶¶ 36–40). Patent Owner does not dispute this proposed level of skill. PO Resp. 15–16.

We adopt Petitioner’s proposal as reasonable and consistent with the prior art. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (the prior art may reflect an appropriate level of skill in the art).

C. Claim Construction

We construe claims in the same manner used in a civil action under 35 U.S.C. § 282(b) “including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” 37 C.F.R. § 42.100(b). When applying that standard, we interpret the claim language as it would have been understood by one of ordinary skill in the art in light of the specification. *Wasica Fin. GmbH v. Cont’l Auto. Sys., Inc.*, 853 F.3d 1272, 1279–80 (Fed. Cir. 2017). Thus, we give claim terms their ordinary and customary meaning as understood by an ordinarily skilled artisan. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc). Only terms that are in controversy need to be construed, and then only to the extent necessary to resolve the controversy. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Matal*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).

In the Petition, Petitioner contends that all claim terms should be given their “ordinary and customary meaning as understood by a [person of

ordinary skill in the art] and the patent’s prosecution history.” Pet. 4. Petitioner further contends that such meaning for the following terms is made explicit in the ’885 patent: “model data,” “issued data,” and “interest data.” *Id.* at 5 (citing Ex. 1001, 2:59–3:51).

In the Institution Decision, we gave all terms their ordinary and customary meaning and determined, at that time, that it was unnecessary to make that meaning explicit for any term. *See* Inst. Dec. 8–10.

In Patent Owner’s Response, Patent Owner provides a proposed claim construction for the term “not denying access” that appears in claim 1. PO Resp. 12–15. In Petitioner’s Reply, Petitioner expresses disagreement with Patent Owner as to the meaning of “not denying access,” and offers its own views on the meaning of the term. Pet. Reply 1–4. In Patent Owner’s Sur-Reply, Patent Owner expresses disagreement with Petitioner. PO Sur-reply 7–14.

We address below the claim construction issues necessary to resolve this proceeding.

1. “not denying access”

Claim 1 is a method claim that includes steps involving the term “access.” Those steps are reproduced below:

[1B] controlling access to the server by at least one of:

[1C] denying access of the computing device attempting to access the server when the biometric data is not present;

[1D] or not denying access of the computing device attempting to access the server when some biometric data is present.

Ex. 1001, 5:46–52 (reproduced with claim elements identifiers [1B] – [1D] used in the Petition.)

The above-noted limitations, thus, recite that access to a server is controlled such that denying access of a computing device occurs if biometric data is not present, or “not denying access” occurs when biometric data is present.

a) Summary of Patent Owner’s Arguments from Patent Owner’s Response

Patent Owner contends that during parallel litigation, Petitioner proposed that “‘not denying access’ does not mean granting access,” but that “Petitioner contradicts this position by implicitly construing ‘not denying access’ as including ‘granting access.’” PO Resp. 13. Patent Owner argues that “a POSA would understand that ‘denying access,’ ‘granting access,’ and ‘not denying access’ are separate and distinct actions.” *Id.* (citing Ex. 2014 ¶ 77) In Patent Owner’s view, “‘not denying access’ does not refer to or encompass ‘granting access’ or ‘denying access.’” *Id.* at 15.

Patent Owner also contends that dependent claims 3–20 provide some support for the construction of “not denying access” that it advocates. PO Resp. 14–15. Patent Owner discusses claims 3, 16, and 18 as exemplary.

Claim 3 recites “identifying whether the biometric data matches previously recorded biometric data.” Ex. 1001, 5:56–58. According to Patent Owner, “[t]his identification occurs only if some biometric data is present, meaning that [1D] has occurred and access has not yet been granted. Thus, claims 3–20 all require claim 1 to detect some biometric data and therefore not deny access.” PO Resp. 14–15.

In connection with claim 16, Patent Owner contends the following:

Claim 16 confirms this. There, access to the server is granted upon fulfillment of the probability factor test described in claim 13. Ex-1001, 6:60-63. But Claim 13 itself depends on claim 1.

Accordingly, “granting access” in claim 16 can occur only subsequent to the “not denying access” that occurs in [1D]. Ex-2104 ¶76. As a subsequent step in the claimed method, “granting access” must be separate and distinct from its prerequisite step, “not denying access.” *Id.*

Id. at 15.

As to claim 18, Patent Owner contends that “[c]laim 18 denies access, but only after the determination of ‘not denying access’ required by [1D] Ex. 1001, 7:3–7. Thus, ‘denying access,’ like ‘granting access,’ is a separate and distinct action from ‘not denying access.’” *Id.*

b) Summary of Petitioner’s Arguments from Petitioner’s Reply

In response to Patent Owner’s arguments, Petitioner contends the following:

[1D]’s “not denying access . . . when some biometric data is present” simply means **not** “denying access . . . when some biometric data is present.” It is met by any method that does “not” deny access based on some biometric data being present. EX1042, [0003]-[0005]. This is not a “separate and distinct action[]” from “granting access” (POR, 13), or from any other action that is not “denying access . . . when some biometric data is presents.” EX1042, [0004]-[0011].

Pet. Reply 1.

Petitioner also contends the following:

Nobots mischaracterizes Google’s district-court claim-construction proposal by suggesting Google agreed that [1D] excludes “granting access.” POR, 13. Google only said “‘not denying access’ does not **mean** granting access” (EX2002, 4^[footnote omitted]—i.e., [1D] does not **require** granting access. But [1D] does encompass “granting access.” [1D] is **broader** than “granting access”—it generically encompasses many possible actions that do “not” include “denying access . . . when some biometric data is presents.” EX1043, [0012]-[0013].

Id. at 3.

In conjunction with Patent Owner’s discussion of the dependent claims as proposed support for its position on “not denying access,” Petitioner contends that “[e]ach action in dependent claims 3-20 is an action (like those in the specification) that, when some biometric data is present does something other than simply denying access.” *Id.* at 2. Petitioner further contends the following:

Contrary to the [PO Resp.] at 14-15, the actions in dependent claims need not occur “subsequent to” or “after” [1D]. Nothing in the claims recites such a temporal/sequential requirement . . . POSAs would have understood that the dependent-claim actions are *part of* a process for performing [1D]—one that is “not” a process that denies access when some biometric data is present.

Pet. Reply 4 (citing Ex. 1042 ¶ 14–15).

c) Summary of Patent Owner’s Arguments from Patent Owner’s Sur-Reply

In its Sur-reply, Patent Owner reiterates its view that “not denying access” does not encompass “granting access.” PO Sur-reply 7–8. Patent Owner also contends the claims do require a “temporal-sequential construction” (*id.* at 10), and that “[t]he dependent limitations are thus separate from [1D], occurring only when some diametric data has been detected and access has not been denied. *Id.* at 8; *see id.* at 8–14.

d) Analysis

Having considered the parties’ respective positions, we conclude that Petitioner’s view as to meaning of “not denying access” is more consistent with the ’885 patent, and the record at hand, than Patent Owner’s view. In that respect, we agree that “not denying access” is “broader” than “granting access” and encompasses other possible acts in which access is not denied,

including an act of granting access. *See* Pet. Reply 3. We discern no inconsistency in Petitioner’s representations in this proceeding as to the meaning of “not denying access” that Petitioner advanced in the district court litigation. *See* PO Resp. 13. We note that Patent Owner contends the following:

Petitioner’s district court proposal—that “‘not denying access’ does not mean ‘granting access’” (Response, 13)—refutes its new position. If “not denying access” encompasses “granting access,” at least sometimes “not denying access” necessarily **does mean** “granting access.” Thus, “not denying access” cannot encompass “granting access.”

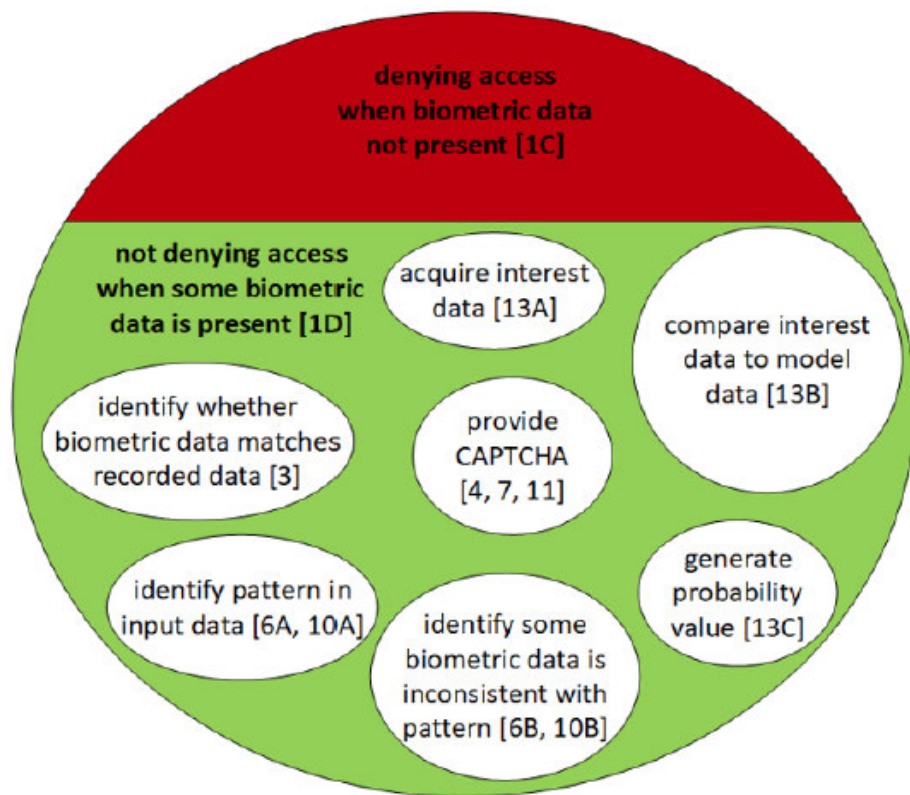
PO Sur-reply 8.

Patent Owner’s conclusion, however, that “not denying access cannot encompass ‘granting access’” simply is not supported by the record. To that end, contrary to Patent Owner’s view, Petitioner’s representation that “‘not denying access’ does not mean granting access” is consistent with its position that “not denying access,” although not being synonymous, or co-extensive, with “granting access,” nevertheless, still encompasses an act of granting access. It follows readily from the ordinary understanding of “granting access,” that, if access is granted, then such access has not been denied.

Furthermore, we note that neither Patent Owner nor Dr. Russ points to any portion of the ’885 patent as a part of the Patent Owner Response or Sur-reply that supports Patent Owner’s position that an act of “not denying access” is, itself, something regarded as a “separate and distinct” action from “granting access.” *See, e.g.,* PO Resp. 13; Ex. 2104 ¶¶ 71–77. The portions of the Specification that Patent Owner and Dr. Russ do cite simply do not support the position that the ’885 patent restricts “not denying access” to some type of independent or distinct contemplated action entirely separate

from an act of granting access. *See, e.g.*, PO Resp. 13–14 (citing Ex. 1001, 4:59–5:2, 5:42–52; 5:2–10); Ex. 2104 ¶¶ 71–77 (citing same portions of Ex. 1001).

Further still, because the record does not establish that “not denying access” is some type of separate action that is performed in the context of the ’885 patent, it does not follow that there is a “temporal/sequential” requirement as a part of the dependent claims, such that the actions set forth in those claims must be performed “subsequent to” or “after” step [1D]. *See* PO Resp. 14–15; PO Sur-reply 9. Rather, we find persuasive Petitioner’s view that the claims do not have a “temporal/sequential” requirement in the manner proposed by Patent Owner and that “POSAs would have understood that the dependent-claim actions are *part of* a process for performing [1D]—one that is ‘not’ a process that denies access when some biometric data is present.” Pet. Reply 4. Petitioner provides an illustration capturing its positions as to the claim requirements, which we reproduce below:



Pet. Reply 3. The image above is characterized by Petitioner as showing “Exemplary actions encompassed by [1D].” *Id.* We agree with Petitioner that the image is in accord with how a person of ordinary skill in the art would understand the claims of the ’885 patent based on the record at hand, including the Specification of that patent. *See id.*

We observe that Patent Owner characterizes the claimed invention as “a Multi-Layered Test Protocol” intended to “identify bots.” *See* PO Resp. 8–12. Patent Owner further contends that the “multi-layer test” includes “a first-pass binary test and additional test layers,” and, in support of that contention, points to column 2, lines 24–39 and column 4, lines 59–39 of the ’885 patent. *Id.* at 9. Those cited portions describe, for instance, “a first layer of testing that simply checks if there were valid mouse movements and/or key strokes inputted by the user of a computing device that is

attempting to access a server resource ‘protected’ from bots.” *Id.* at 4:59–63. The cited portions also characterize the disclosure as a “basic ‘if-then’ check.” *Id.* at 4:63. Thus, the test protocol as set forth in the cited portions is directed to an initial basic assessment of biometric data to check for the potential presence of a bot rather than a human user. Significantly, we do not discern that the above-noted portions of the ’885 patent cited by Patent Owner describe an act of “not denying access” as a stand-alone act apart from additional inquiries such as, assessing whether input data matches previously recorded data. *See, e.g., id.* at 5:7–10,¹⁶ 5:14–17.¹⁷ Neither do we discern that any other portion of the Specification describes “not denying access” in such a manner.¹⁸

We note that Patent Owner contends that its proposed “multi-layer protocol” provides that “if biometric data (either real or pseudo) is detected, the protocol does not simply grant (or deny) access, but rather proceeds to the next layer of testing.” PO Resp. 9 (citing Ex. 1001, 4:59–5:2). To the extent that the ’885 patent may describe an embodiment involving multi-layers, the ’885 patent simply does not preclude a scenario, even as a part of a multi-layer protocol, in which access is granted to the server if some

¹⁶ “Exploiting this premise allows a second level knockout assessment to deny user access if the input data exactly (or statistically sufficiently) matches previously recorded data.” Ex. 1001, 5:7–10.

¹⁷ “Alternatively, if samples are used, an exact match could then invoke a more intensive comparison with the same stored datasets, where again access can be denied when an exact or statistically sufficient match is found.” Ex. 1001, 5:14–17.

¹⁸ We note in passing, as does Petitioner (*see* Pet. Reply 1), that the particular phrase “not denying access” does not appear anywhere in the Specification of the ’885 patent.

biometric data is present. Also, significantly, the claims themselves do not include language that gives rise to “multi-layer protocol” that somehow precludes granting access to a server when biometric data is determined to be present.

Accordingly, having considered the parties’ respective positions, we conclude that Petitioner has the better position as to how a skilled artisan would understand the “not denying access” step that is [1D]. In particular, we do not agree with Patent Owner that “not denying access” is understood from the ’885 patent as being a separate action entirely divorced from “granting access.” *See, e.g.*, PO Resp. 12–15; PO Sur-reply 7–14. Rather, we agree with Petitioner, and determine that “not denying access” encompasses “granting access.” *See, e.g.*, Pet. Reply 1–4. Furthermore, in connection with that determination, and based on the record before us, we also agree with Petitioner that actions described in the dependent claims are undertaken as a part of the process of “not denying access.” *See id.* at 4.

2. *Additional Interpretation Matters Concerning the “Controlling Access” Steps*

Although not presented expressly by Patent Owner as a matter of claim construction of any particular claim term, in reviewing Patent Owner’s Response and Sur-reply, we discern that Patent Owner is of the view that the “controlling access” step of claim 1, i.e., [1B], and the two sub-steps of denying or not denying access [1C] and [1D], must be performed based on the “mere presence or absence” of biometric data. *See, e.g.*, PO Sur-reply 7 (“the claimed multi-layered test protocol required by all claims . . . keys off the *mere presence or absence* of biometric data.” (emphasis added)); PO Response 10 (“[t]he binary “if-then’ first pass evaluation is reflected in the

elements of claim 1, which tests for the *mere presence* of biometric data.” (emphasis added). Patent Owner argues that its position is supported by an embodiment of the ’885 patent that describes a multi-layered test protocol with a “first layer” constituting a “first-pass binary test” for the presence or absence of biometric data that is a “‘basic ‘if-then’ check’ that minimizes computations (and associated processing power), and is thus ‘essentially without [computational] overhead.’” *See, e.g.*, PO Resp. 9 (citing Ex. 1001, 4:59–5:2). Thus, we understand that Patent Owner is of the view that the “denying access” step [1C] and the “not denying access” step [1D] cannot be met if anything other than the mere recognition of the presence or absence of biometric data, e.g., processing of that biometric data, occurs as a part of those access actions, because doing so would incur some computational overhead and thus not constitute the if-then “first layer” testing disclosed in the above-noted embodiment of the ’885 patent.

We again reproduce steps [1B] through [1D]:

[1B] controlling access to the server by at least one of:

[1C] denying access of the computing device attempting to access the server when the biometric data is not present; or

[1D] not denying access of the computing device attempting to access the server when some biometric data is present.

Ex. 1001, 5:46–52 (reproduced with claim elements identifiers [1B] – [1D] used in the Petition.)

Notably, claim 1 does not set forth “a binary ‘if-then’” evaluation that “tests for the mere presence of biometric data,” as Patent Owner argues. PO Resp. 10; Sur-reply 7. Although the steps do require that biometric data be not present (i.e., absent) in denying access and some biometric data be

present in not denying access, the claims do not use language mandating that it is exclusively such presence or absence that must be considered.

Furthermore, we agree with Petitioner that “[c]laim 1 is nowhere limited to a ‘basic,’ ‘if-then,’ ‘first layer,’ or ‘binary’ test/check,” and “[n]othing in claim 1 limits the amount of computational ‘overhead’ incurred.” Pet. Reply 6–7. Although it may be the case that the particular embodiment of the ’885 patent cited by Patent Owner does describe a first layer test with a “‘basic ‘if-then’ check”” (PO Resp. 9) for controlling server access based only on the presence or absence of biometric data, the language of the claims does not include corresponding description dictating they must also have that requirement. We agree with Petition that the law ‘expressly reject[s] the contention that [even] if a patent describes only a single embodiment, the claims . . . must be construed as limited to the embodiment.” Pet. Reply 7 (quoting *Phillips v. AWH Corp.*, 415 F.3d 1303, 1323 (Fed. Cir. 2005) (en banc)).¹⁹

In our view, the record does not support a determination that step [1D] requires that the determination of whether to deny or not deny access must be based only on the presence or absence of biometric data.

¹⁹ The Dissent relies on the discussion in the ’885 patent of the noted embodiment laying out a multi-layer test including a “first pass evaluation” of only the presence of biometric data in concluding that “the language of claim 1 requires determining whether to deny access to a server based *only* on whether biometric data is present *before* performing the additional steps recited in the dependent claims.” See *infra* Dissent § A. We note that the claims, themselves, do not characterize any recited steps as requiring only a first-pass evaluation of the presence of biometric data before evaluating other data. Neither “only” nor “before” appears in the language of claim 1, or any other claim.

3. *Remaining Claim Terms*

We determine that it is unnecessary to expressly construe any other claim term. *See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (Only terms in controversy must be construed and only to the extent necessary to resolve the controversy); *see also Nidec*, 868 F.3d at 1017 (citing *Vivid Techs* in the context of an *inter partes* review).

D. All Relevant Proposed Grounds

We discern that there are thirteen proposed grounds that remain involved in this proceeding.²⁰ For those thirteen grounds, Petitioner lays out in detail, supported by the testimony of Dr. Lopresti, where it believes all the required features of claims 3–9, 11, and 13–20 are present in the prior art, and why a person of ordinary skill in the art would have had reason combine the teachings of the prior art. *See* Pet. 5–65.

With respect to Grounds 1–3 (grounds based on O’Sullivan), Patent Owner contends that the Grounds “Do Not Control Server Access Based on the Mere Presence of Biometric Data.” *See* PO Resp. 22–29; PO Sur-reply 14–15. Also, in connection with those grounds, Patent Owner argues that they “do not teach ‘not denying access’ when some biometric data is present, as required by claims 3–20.” PO Resp. 33–34; *see* PO Sur-reply 16–17.

For Grounds 5–14 (grounds based on Meek), Patent Owner contends that they also do not account for the “not denying access” requirement of the claims. PO Resp. 30–33; PO Sur-reply 17–18.

²⁰ Numbered in this Final Written Decision (*see supra* § I.D), and also by the parties, as Grounds 1–3 and 5–14 (*see* Pet. 1; PO Resp. 16–17).

With respect to all of Grounds 1–3 and 5–14, Patent Owner contends that Petitioner has not met its “burden to provide a reasonable expectation of success[.]” PO Resp. 34–68; PO Sur-reply 18–33.²¹

For reasons discussed below, we conclude that Petitioner has shown by a preponderance of the evidence that claims 3–9, 11, and 13–20 are unpatentable. We begin with a brief summary of the prior art relied upon in the Petition.

1. Summary of Prior Art

a) O’Sullivan

O’Sullivan is titled “Pixel Cluster Transit Monitoring for Detecting Click Fraud.” Ex. 1006, code (54). O’Sullivan’s Abstract is reproduced below:

Detecting click fraud that includes a processing device that receives data related to a cursor movement towards an advertisement displayed on a web page. The processing device analyzes the cursor movement data and determines a confidence level useable in the determination of click fraud, the confidence level responsive to the analysis of the cursor movement. The received data includes data that the cursor on the web page has transited at least one pixel cluster on the web page prior to a clicking the advertisement. In one embodiment, a click fraud is detected when the click occurred without the cursor crossing a pixel cluster, and no click fraud occurring when the click occurred after the cursor crossed a pixel cluster.

Id. at code (57).

²¹ As a part of its Sur-reply, in connection with its arguments pertaining to reasonable expectation of success, Patent Owner also contends that Petitioner has relied on “improper reply arguments and evidence.” *See* PO Sur-reply 23–27.

b) Willner

Willner is titled “Cursor Path Vector Analysis for Detecting Click Fraud.” Ex. 1005, code (54). Willner’s Abstract is reproduced below:

A system and method for detecting click fraud where data is received corresponding to a tracking movement of a cursor on a web page. The movement of the cursor is associated with at least one vector. The at least one vector represents at least a portion of the cursor movement. A confidence level useable in the determination of click fraud is determined. The confidence level is responsive to analysis of the at least one vector representing at least a portion of the cursor movement.

Id. at code (57).

Willner’s Figures 2 and 3 are reproduced below:

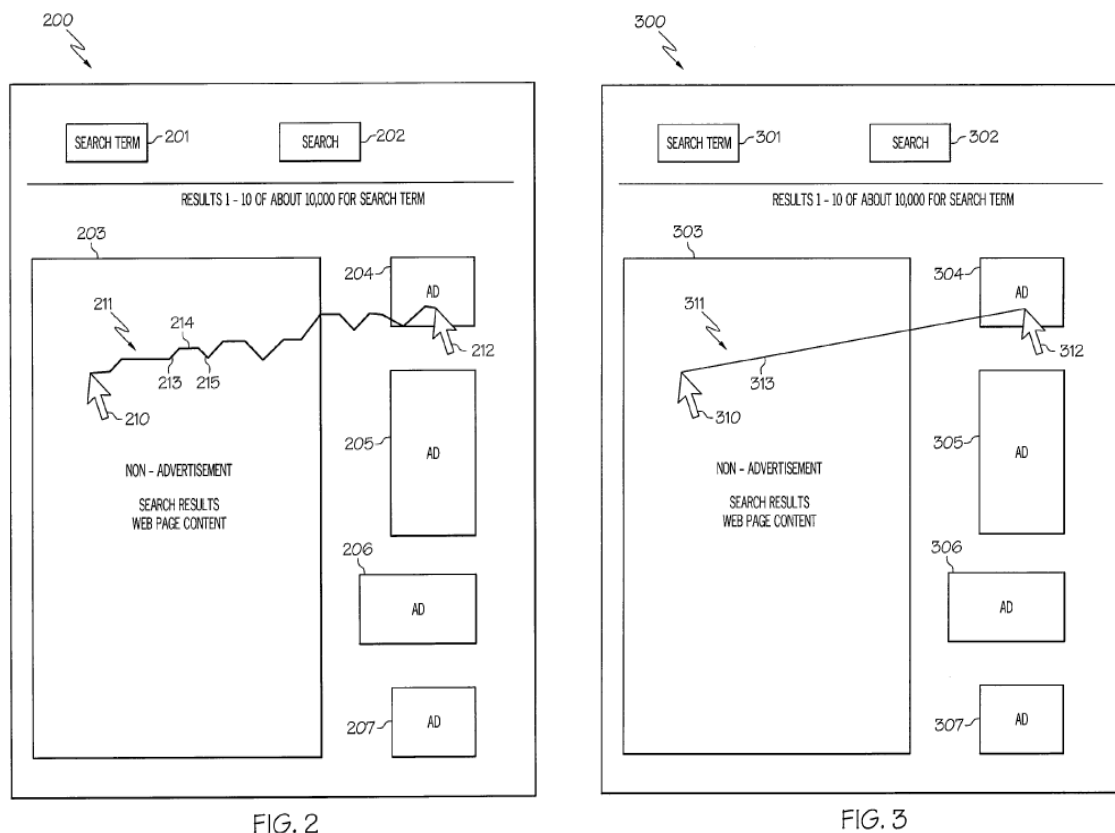


Figure 2 above shows a diagram of a web page illustrating a human-like cursor movement according to an embodiment. *Id.* ¶ 17. Figure 3 above is a diagram of a web page showing cursor movement resembling click fraud,

i.e., movement by a bot, according to an embodiment. *Id.* ¶ 18. The path traveled by a cursor (211 in Figure 2, 311 in Figure 3) may be mapped into vectors and analyzed to assess whether the cursor movement has been provided by a human operator or a bot. *Id.* ¶¶ 46–48.

c) Broder

Broder is titled “Methods of Detecting and Avoiding Fraudulent Internet-Based Advertisement Viewings.” Ex. 1011, code (54). Broder’s Abstract is reproduced below:

Non human entities such as automated web crawlers or malicious click-fraud programs can skew the tracking of clicks on web site advertisements. Thus, it is desirable to filter out page views caused by such automated entities. To achieve this goal, a web site may interject an intermediate web page after a web viewer selects an advertising link but before the web viewer is sent to the advertiser's designated web site. The intermediate web page allows for a response from the web viewer. The system then analyzes the web viewer's response to the intermediate web page (if any) along with other information using an adjustable testing policy to make a determination as to whether the web viewer is a human or non-human entity. An adjustable interject policy may be used to determine if an interjection should occur after a web viewer has selected an advertisement and before the web viewer is directed to the advertiser's designated web site. In this manner, the number of web viewers that are subjected to the intermediate web page is reduced.

Id. at code (57).

Broder's Figure 5 is reproduced below:

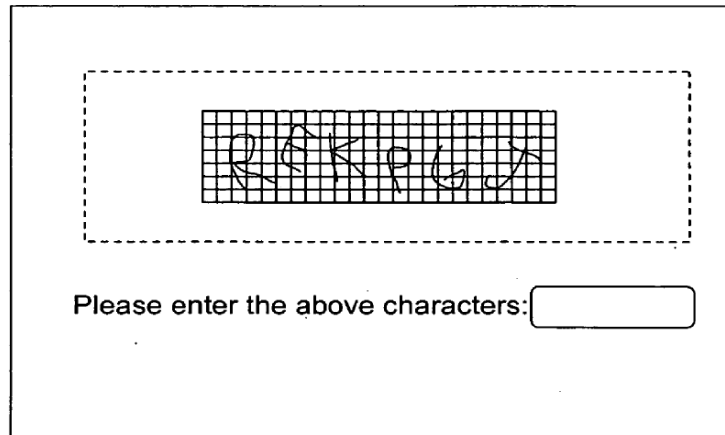


Figure 5

Figure 5 above “illustrates an example embodiment of an intermediate web page that illustrates on[e] example of a Completely Automated Public Turning test to tell Computers and Humans Apart (CAPTCHA).” *Id.* ¶ 21. Broder explains that in situations in which a “web site is being attacked by a malicious robot program, that web site may elect to use a CAPTCHA intermediate page in order to filter out all of the accesses by the malicious robot program.” *Id.* ¶ 41.

d) Tanzer

Tanzer is titled “Method of Detecting Unauthorized Access to a System or an Electronic Device.” Ex. 1012, code (54). Tanzer’s Abstract is reproduced below:

Characteristics of a user's behavior on an electronic device are captured and stored. These stored characteristics are compared to the characteristics of a subsequent user purporting to be the same person. If the differences in the characteristics are such that fraud is suspected, an alert is activated.

Id. at code (57).

e) Meek

Meek is titled “Verifying Human Interaction to a Computer Entity by Way of a Trusted Component on a Computing Device or the Like.” Ex. 1008, code (54). Meek’s Abstract is reproduced below:

A method describes user interaction in combination with sending a send item from an application of a computing device to a recipient. The computing device has an attestation unit thereon for attesting to trustworthiness. The application facilitates a user in constructing the send item, and pre-determined indicia are monitored that can be employed to detect that the user is in fact expending effort to construct the send item. The attestation unit authenticates the application to impart trust thereto, and upon the user commanding the application to send, a send attestation is constructed to accompany the send item. The send attestation is based on the monitored indicia and the authentication of the application and thereby describes the user interaction. The constructed send attestation is packaged with the constructed send item and the package is sent to the recipient.

Id. at code (57).

f) Kroll

Kroll is titled “Keyboard Signature Security System.” Ex. 1010, code (54). Kroll’s Abstract is reproduced below:

A method is taught for analyzing the keystroke signature of a keyboard customer. The signature is compared to a database of previously stored keystroke sequences to allow for a statistical test for the identity of the user. This method allows for the use of varying keyboards to facilitate electronic commerce over the Internet from arbitrary terminals and personal computers.

Id. at code (57).

g) Kitts

Kitts is titled “Click-Fraud Protector.” Ex. 1009, code (54). Kitts summarizes its disclosure below:

Determining the probability that a user or program fraudulently initiated a web-page request is described herein. A web service executing on a server includes a data-mining component, computation component, and auction component. The data-mining component is configured to determine attributes associated with the web-page request. The computation component is configured to calculate a probability that the web-page request was fraudulently initiated. To calculate this probability, the attributes and other parameters are fed into a statistical model. The auction component is configured to locate one or more advertisements to display on the web page based on the probability. The auction component is also configured to restrict the advertisements for display based on advertiser-specified target criteria. Once an advertisement is located, the advertisement is rendered along with the web page.

Ex. 1009 ¶ 9.

Kitts further describes that the types of attributes that can be analyzed “include, without limitation, an internet protocol (IP) address of the client-computing device, . . . date, time, geographic location, metadata, key words, HTML tabs, or other characteristics associated with the page request.” *Id.* ¶ 46.

h) O’Connell

O’Connell is titled “User-Browser Interaction-Based Fraud Detection System.” Ex. 1007, code (54). O’Connell’s abstract is reproduced below:

Systems, methods and media for detecting fraudulent behavior during an Internet commerce session are disclosed. Embodiments of a method may include establishing an e-commerce session with a user and requesting fraud detection analysis of user-browser interaction during the e-commerce session. Embodiments may also include receiving fraud detection results for the e-commerce session, where the fraud detection results may provide an indication of a comparison between the user's interaction with a browser during the e-commerce session and known fraudulent behavior.

Embodiments may also include performing an action based on the fraud detection results. Determining the fraud detection results may include determining user-browser interaction data associated with the session and comparing the user-browser interaction data to known fraudulent human or automated program behavior. Performing the action based on fraud detection results may include one or more of completing an e-commerce transaction, requesting additional authentication, denying the requested action, etc.

Id. at code (57).

O'Connell further describes that

[f]actors that may represent potential fraudulent behavior by an automated program and thus raise potential security issues may include data that is entered too rapidly, a mouse pointer tha[t] never moves, a large form that is filled out without the browser window scrolling, data transmitted in a form without keystrokes being recorded, or other factors.

Id. ¶ 48.

2. *Grounds 1–3: O'Sullivan Based Grounds*

In the Institution Decision, we made a general assessment as to Petitioner's evaluation of the teachings of Sullivan and Willner. *See* Inst. Dec. 17. In particular, we observed the following:

[T]here a common theme in the teachings of the prior art of record. Namely, most, if not all, of that prior art on which Petitioner relies is directed to systems, techniques, and procedures for assessing the presence of fraudulent behavior in connection with activity on the Internet. Each of Petitioner's relevant proposed grounds includes assessment of the teachings of each of the prior art references, explanation as to how those teachings constitute the features required by the claims, and reasoning as to why a person of ordinary skill would have combined those teachings.

For instance, with respect to the ground including O'Sullivan and Willner, Petitioner explains where all of the features of claims 3, 5, 6, 8, 13–16, and 18–20 are found in those two references. *See* Pet. 10–35. In conjunction with that

explanation, Petitioner notes that O’Sullivan describes a system that determines if click fraud is occurring and as a result a server of the system “may then take appropriate action based” on that determination. Pet. 10 (quoting Ex. 1006 ¶ 48). Petitioner then turns to the teachings of Willner that readily convey to a person of ordinary skill in the art that “appropriate action” in a circumstance in which such fraud is detected, e.g., when an advertisement has been clicked on, includes “‘deny[ing] the action of click,’ thus ‘withholding the click response,’ when the ‘click [is] considered fraudulent.’” *Id.* at 10–11 (quoting Ex. 1005 ¶ 36; Ex. 1003 (Lopresti Declaration) ¶ 77).

Id.

We reiterate those observations as a part of this Final Written Decision. As noted above, during trial Patent Owner now argues that, as concerns all of Grounds 1–3, Petitioner: (1) does account adequately for requirements of controlling server access based on the presence of biometric data (*see* PO Resp. 22–29; PO Sur-reply 14–15); (2) does not adequately account for the requirement of “not denying access” when some biometric data is present (*see* PO Resp. 33–34; PO Sur-reply 16–17; and (3) has not shown a reasonable expectation of success in combining the teachings of the prior art (*see* PO Resp. 34–68; PO Sur-reply 18–33. We consider each of Grounds 1–3 below with Patent Owner’s arguments in mind.

a) Ground 1: O’Sullivan and Willner

Petitioner contends that all the features of claims 3, 5, 6, 8, 11 and 13–16, and 18–20 are present in O’Sullivan and Willner, and that a person of ordinary skill in the art would have had adequate reason to combine the

teachings of those references. *See* Pet. 5–35.²² As noted above, Patent Owner disagrees.

(1) Controlling Access Based on Biometric Data

(a) Summary of the Parties’ Positions

In the Petition, Petitioner provides discussion of the combined teachings of O’Sullivan and Willner in which, based on movement of a cursor on a screen (i.e., biometric data), access to a server is controlled. *See* Pet. 10–12 (§ III.C), 17–19 (§§ III.D.5, III.D.4). Those referenced portions of the Petition are directed to a summary of the proposed combination of O’Sullivan and Willner and Petitioner’s accounting for claim elements [1C] and [1D]. Specifically, Petitioner contends that “[a]s discussed *supra* § III.C, the O’Sullivan-Willner combination controls this access by displaying the website when no fraud is detected (meeting [1D] as discussed *infra* § III.D.5) and denying access when fraud is detected (meeting [1C] as discussed *infra* § III.D.4).” Pet. 17 (citing Ex. 1003 ¶ 86).

In the Patent Owner Response, Patent Owner argues that, although “O’Sullivan uses biometric data as the *starting point* for computing and generating a confidence factor[,]. . . it is the confidence factor, and not the mere *presence* or absence of biometric data, that is used as the basis for the ultimate determination of click fraud and the decision to grant or deny.” PO Resp. 24 (citing Ex. 1006 ¶ 32; Ex. 2104 ¶ 83). Apparently, it is Patent Owner’s view that use of a generated confidence level to ultimately deny or grant access is something different than a “basic” “if-then” decision

²² We again note that although claims 1, 2, 10, and 12 are addressed in the Petition, those claims have been disclaimed. *See* Inst Dec. 2; Ex. 2103.

“eliminating computational overhead” to deny or not deny access based “mere[ly]” on biometric data that claim 1 is alleged to require. *Id.* at 22–29.

In the Reply, Petitioner contends that “[c]laim 1 is nowhere limited to a ‘basic,’ ‘if-then,’ ‘first layer,’ or ‘binary’ test/check,” and “[n]othing in claim 1 limits the amount of computational ‘overhead’ incurred, nor excludes calculating a confidence factor.” Pet. Reply 6–7. Petitioner also submits that “Nobots doesn’t dispute that O’Sullivan-Willner denies access when biometric data is not present, and does not simply grant or deny access when biometric data is present, but instead analyzes the data to determine whether to grant/deny.” *Id.* at 7.

Petitioner alternatively contends that, even if Patent Owner’s interpretation of the requirements of claim 1 on this matter were correct (e.g., a “basic” or “binary” test requirement), “O’Sullivan includes a binary first-layer test of whether applets are triggered by ‘cursor movement . . . over associated pixel clusters.” *Id.* at 7 (citing Ex. 1006 ¶ 30; Pet. 30). Petitioner contends that Patent Owner admits that such test is a “yes/no determination” as to cursor movement, and a “no” results in access denial, even if the “no” determination “is expressed as ‘a high confidence level’ of fraud” thereby meeting the requirements set forth in claim 1 under Patent Owner’s interpretation. *Id.* at 7–8 (citing Pet. 17; PO Resp. 25; Ex. 1042 ¶¶ 26–27; Ex. 1006 ¶ 46).

Lastly, in the Sur-reply, Patent Owner reiterates its view that O’Sullivan’s disclosure of computational analysis to generate a “confidence factor,” which is used to control server access, is “not the presence or absence of biometric data.” PO Sur-reply 14. Patent Owner also discounts Petitioner’s alternative contention as to a “yes/no” determination made based on cursor movement. *Id.* at 15. According to Patent Owner, the outcome of

that determination is used in the confidence factor calculation, which ultimately controls server access, but that O’Sullivan “specifically teaches that it **does not** control server access using the binary determination.” *Id.* (citing Ex. 1006 ¶ 30).

(b) *Analysis*

Claim 1 includes the following recitations:

[1B] controlling access to the server by at least one of:

[1C] denying access of the computing device attempting to access the server when the biometric data is not present;

[1D] or not denying access of the computing device attempting to access the server when some biometric data is present.

See supra § I.D.

Thus, access to the server is controlled by either denying access when biometric data is not present, or not denying access when some biometric data is present. Although the claim describes two possible actions, we agree with Petitioner that “[c]laim 1 is nowhere limited to a ‘basic,’ ‘if-then,’ ‘first layer,’ or ‘binary’ test/check.” *See* Pet. Reply 6. We also agree that “[n]othing in claim 1 limits the amount of computational ‘overhead’ incurred, nor excludes calculating a confidence factor” in connection with the operation of at least one of [1C] or [1D]. *See Id.* at 6–7 (citing PO Resp. 22–23). Although the ’885 patent describes an embodiment in which initial input data (such as key strokes) is evaluated for detecting bots as a “basic ‘if-then’ check” to limit computational overhead in some capacity (*see, e.g.,* Ex. 1001, 4:59–5:2), that does not mean that such a requirement is imported to the controlling access options that are [1C] or [1D], which make no mention of a “basic ‘if-then’ check” or any computational overhead

concerns. It is notable that corresponding language is absent from the claims. As noted above, we agree with Petitioner that “the law ‘expressly reject[s] the contention that [even] if a patent describe only a single embodiment, the claims . . . must be construed as being limited to that embodiment.’” Pet. Reply 7 (quoting *Phillips v. AWH Corp.*, 415 F.3d 1303, 1323 (Fed. Cir. 2005) (en banc)). We do not find a basis on the record to limit the claims to what is described in the above-noted embodiment.

We further discern that Petitioner argues the following:

Nobots doesn’t dispute that O’Sullivan-Willner denies access when biometric data is not present, and does not simply grant or deny access when biometric data is present, but instead analyzes the data to determine whether to grant/deny. Petition, 17-19. Nothing different is described in the specification’s “first” (or second-third) layer. EX1001, 4:59-5:39; EX1042, [0025]. Nobots’s suggestion that the claims only allow performing data analysis “after” all aspects of claim 1 (including [1D]) (POR, 29) is unsupported by the claim language and inconsistent with the specification.

Pet. Reply 7.

We agree with Petitioner’s above-noted argument. That argument is consistent with our assessment of how a person of ordinary skill in the art would understand “not denying access” in the context of the ’885 patent. *See supra* § II.C.1. We also do not discern any disagreement from Patent Owner in Petitioner’s explanation that analysis performed as a part of the O’Sullivan-Willner combination includes determination of a “confidence factor” that is based on biometric data (e.g., tracked cursor movement) and ultimately used in a determination whether to deny or grant access to a server. *See, e.g.*, Pet. Reply 4–7; Pet. 18–19. We agree with Petitioner that a “confidence factor” that is determined based on the presence or absence of biometric data satisfies what is required by the claims. We disagree with

Patent Owner that the use of such a confidence factor to control access means that such access is not controlled based on the presence or absence of biometric data. *See* PO Sur-reply 14–15; PO Resp. 22–29.

As a result, we conclude that Petitioner has established that the combination of O’Sullivan and Willner accounts for the requirement in the claims of controlling access to a server based on the presence or absence of biometric data.²³

(2) Not Denying Access Based on Biometric Data

As discussed above, we conclude that “not denying access” to a server encompasses “granting access” to the server. *See supra* § II.C.1. As also discussed above, we disagree with Patent Owner and agree with Petitioner, that the claims do not have a “temporal/sequential requirement” as a part of some type of “multi-layered test protocol” that mandates that some separate or independent “not deny access” determination occurs, distinct, for instance, from a determination to grant access. *See supra* §§ II.C.2, II.C.3.

In the Petition, Petitioner contends the following:

In the O’Sullivan-Willner combination, mouse clicks “that crossed the pixel cluster and took a longer period of time would be judged not to be click fraud.” O’Sullivan, [0032], [0047]. When the click is determined valid, the advertiser’s webpage is displayed. O’Sullivan, [0040]. Thus, when some biometric data is present (cursor movement detected as transiting a pixel cluster and taking enough time to be human movement), the client

²³ We note that Petitioner’s “[a]lternative[.]” position involves a “yes/no” determination of cursor movement and an assessment of a “high confidence level” of fraud, and, if “no,” subsequent denial of access based on that determination. *See* Pet. Reply 7–8. We conclude that position also has merit to demonstrate that O’Sullivan discloses controlling server access based on biometric data, even if such control occurs after a confidence level is assessed.

computing device is not denied access. Lopresti-Declaration, [0088].

Pet. 18.

Thus, Petitioner contends that the combined teachings of O’Sullivan and Willner convey that in the circumstance when evaluation of mouse clicks results in a determination that the clicks are “valid” (i.e., the presence of some biometric information), then the “webpage is displayed,” i.e., access is granted. That is a scenario that clearly encompasses the claimed step of not denying access when some biometric information is present.

Petitioner also contends the following:

Nobots doesn’t dispute that O’Sullivan-Willner denies access when biometric data is not present, and does not simply grant or deny access when biometric data is present, but instead analyzes the data to determine whether to grant/deny. Petition, 17-19. Nothing different is described in the specification’s “first” (or second-third) layer. EX1001, 4:59-5:39; EX1042, [0025]. Nobots’s suggestion that the claims only allow performing data analysis “after” all aspects of claim 1 (including [1D]) (POR, 29) is unsupported by the claim language and inconsistent with the specification.

Pet. Reply 7 (citing Pet. Reply 1–4).

We agree with Petitioner. Patent Owner argues that “O’Sullivan’s confidence factor is analogous to the additional steps recited in” claim 13 “which generates a probability value which may represent ‘an assessment of likelihood that the operator of the computing device ... is a human being rather than [a bot]’,” and that “the method of claim 13 only generates this probability value after performing the basic binary test required by claim 1.” Yet, Patent Owner does not dispute that the combination of O’Sullivan and Willner conveys that, when biometric data is not present, access is ultimately denied, and if biometric data is present, access is not immediately granted or

denied, but instead further analysis occurs en route to a determination to take either action. In particular, Patent Owner recognizes that, when biometric data is present and in developing a confidence level that click fraud has occurred, O’Sullivan analyzes the biometric data to ultimately decide whether to grant or deny access. *See* PO Resp. 28 (“O’Sullivan thus analyzes the collected biometric data so that it can generate a confidence level, which is then used to make a determination of the likelihood of click fraud, leading to the ultimate decision of whether to grant or deny access.”) That reasonably accounts for what is required by the claims.

Petitioner further makes the following argument in its Reply:

Alternatively, even if Nobots’s interpretations were adopted, including importing such a temporal/sequential requirement into the claims, O’Sullivan-Willner meets [1D]. O’Sullivan detects biometric data using “applets...associated with pixel clusters” that “capture cursor movement...over the associated pixel clusters.” O’Sullivan, [0030]; Petition, 30. Because those applets are triggered when a pixel crossing occurs, an applet’s triggering and transmission of captured cursor movement is a determination of presence of biometric data. EX1042, [0020]. That must occur before O’Sullivan-Willner can further analyze the cursor movements captured by the applets, meeting the dependent-claim actions. Thus the determination that biometric data is present for [1D] occurs before the analysis of that data meeting dependent claims, and access is neither granted nor denied in the intervening time. EX1042, [0020].

Pet. Reply 5.

Thus, Petitioner also takes a position that during the time period in which the cursor movement (i.e., biometric data) is being analyzed by the applets, “access is neither granted nor denied.” In that circumstance, access is clearly not denied when biometric data is present, i.e., a determination to not deny access has occurred. That is so because the data is analyzed before any result of granting or denying access. Accordingly, even were we to

adopt Patent Owner's view that "not denying access" is some act that is distinguished from granting access, Petitioner's combination of O'Sullivan and Willner also accounts for that view.

We have considered Patent Owner's assertions that the "not denying access" limitation of the claims is not present in the grounds based on O'Sullivan and Willner. *See* PO Resp. 33–35; PO Sur-reply 16–17. For instance, Patent Owner contends the following:

In O'Sullivan-Willner, after O'Sullivan's single layer test determines that there is no click fraud, access to the server will be granted by displaying the advertisement, with appropriate charges to the advertiser. Petition, 10-11 (citing Ex-1006 ¶ 40, Ex-1005 ¶ 45); *id.* at 18 ("When the click is determined valid, the advertiser's webpage is displayed."). Petitioner argues that this means that "when some biometric data is present ... the client computing device is not denied access." *Id.* at 18. However, as previously discussed, "not denying access" does not encompass granting access, but rather means exactly what it says: withholding denial until a future decision is made to grant or deny access. *See* Section II.B. O'Sullivan-Willner does not teach this because it does not disclose a multilayered test, but grants access if the combination's algorithm determines the confidence factor does not indicate click fraud. *See* Petition, 11; Ex-2104 ¶106.

PO Rep. 33–34; *see also id.* at 29 (arguing that the probability value of claim 13 is generated "***after*** performing the basic binary test required by claim 1" and "[n]othing in O'Sullivan teaches or suggests this tiered, multi-step approach").

Those assertions, however, are premised on Patent Owner's mistaken view that "not denying access" does not encompass granting access to a server. They also do not account for the position noted in Petitioner's Reply that, in the O'Sullivan-Willner combination, "access is neither granted nor denied" when biometric data is being analyzed. *See, e.g.,* Pet. Reply 5.

Accordingly, we have considered Patent Owner’s arguments, but we conclude that Petitioner has set forth adequately in the Petition how the combined teachings of O’Sullivan and Willner satisfy the claim requirement of “not denying access of the computing device attempting to access the server when some biometric data is present.”

(3) Reasonable Expectation of Success

Patent Owner contends that Petitioner has not shown a reasonable expectation of success in combining O’Sullivan and Willner. *See* PO Resp. 35–49; PO Sur-reply 19–24. Patent Owner also contends that Petitioner’s discussion of reasonable expectation of success as a part of its Reply constitutes improper argument that should have been part of the Petition. *See* PO Sur-reply 24–27.

Each of O’Sullivan and Willner is directed to the problem of detecting click fraud on web pages. *See, e.g.*, Ex. 1005, code (57); Ex. 1006, code (57). In doing so, each reference proposes that one approach is through tracking and analyzing cursor movement, which both references express can be an indicator that a bot is present rather than a human user. *See, e.g.*, Ex. 1005, code (57); Ex. 1006, code (57). In the Petition, Petitioner presented its proposed reasons as to why a person of ordinary skill in the art would have combined the teachings of O’Sullivan and Willner. *See* Pet. 10–12. As set forth in the Petition, if O’Sullivan’s “analysis ‘determine[s] [that] a click fraud is occurring . . . [t]he server . . . may then take appropriate action based on the analysis.’” Pet. 10 (citing Ex. 1005 ¶ 4). Petitioner relies on Willner’s disclosure as teaching one type of “appropriate action” is to “*deny* the action of click,’ thus ‘withhold the click response,’” when the ‘click [is] considered fraudulent.’” *Id.* at 10–11 (citing Ex. 1006 ¶ 45; Ex. 1003 ¶ 77).

Petitioner additionally reasons the following:

In the O’Sullivan-Willner combination a POSA would have been motivated to incorporate Willner’s vector pattern analyses as “other received data” (O’Sullivan, [0050]) for consideration in determining whether the curser movement is consistent with “[h]uman characteristics” (O’Sullivan, [0034]) or instead indicates clickbot fraud, to achieve the benefits Willner ([0033], [0036]) teaches of “exploit[ing] the stochastic pattern in curser movement vectors...to establish that a human is involved, as opposed to an automated tool.”

Id. at 12 (citing Ex. 1003 ¶¶ 79).

In the Institution Decision, based on Petitioner’s reasoning, including that noted above, we expressed the following:

We conclude, at this time, that Petitioner’s reasoning is sound, and amply supported by record evidence. We also conclude that the record readily conveys that a skilled artisan would have had a reasonable expectation of success in combining the teachings of O’Sullivan and Willner to arrive at the invention of the relevant claims of the ’885 patent. On the record before us, we are not satisfied that either Patent Owner’s arguments or the testimony of its declarant, Samuel Russ, Ph.D., suitably take into account what a person of ordinary skill in the art would have gleaned from the teachings of O’Sullivan and Willner. *See, e.g.*, Prelim Resp. 16, 25–27; Ex. 2101 ¶¶ 85–88. In that respect, and on the current record, we credit Dr. Lopresti’s testimony (e.g., Ex. 1003 ¶¶ 78, 79) over the countervailing testimony of Dr. Russ, as, in our view, Dr. Lopresti’s testimony better reflects what a skilled artisan would have understood in combining the teachings of O’Sullivan and Willner. Furthermore, although, as Patent Owner notes, the Petition does not use the specific phrase “reasonable expectation of success” (*see, e.g.*, Prelim. Resp. 15), that such an expectation is present flows intrinsically from Petitioner’s and Dr. Lopresti’s explanation underscoring the proposed ground.

Inst. Dec. 18–19.

Thus, for purposes of instituting trial, we found Petitioner’s arguments persuasive (and Dr. Lopresti’s supporting testimony credible) that a skilled artisan would have had adequate motivation to combine the teachings of O’Sullivan and Willner, and also that the record conveyed “a reasonable expectation of in doing so.” *Id.*

We discern that the primary thrust of Patent Owner’s arguments lies in the belief that a person of ordinary skill in the art would not have had a reasonable expectation of success in combining O’Sullivan’s “relatively simple” (PO Resp. 40) click fraud detection system with the “vastly more complex” (*id.* at 43) click fraud detection system of Willner. Although noting that Willner performs some of its analysis on a “client” device (PO Resp. 42 (citing Ex. 1005 ¶ 54)), Patent Owner contends that some of Willner’s data comparison operations “can only be done on [a] server.” *Id.* According to Patent Owner and Dr. Russ, such a circumstance may lead to potential “multiple issues” (PO Resp. 35), “difficulties” (*id.* at 44), or “problems” (*id.* at 46) that a person of ordinary skill in the art might have to address in combining some aspects of O’Sullivan and Willner. *See, e.g.*, PO Resp. 35–49; PO Sur-reply 19–22; Ex. 2104 ¶¶ 108–244. In effect, in our view, Patent Owner and Dr. Russ see fault in in the Petition with respect to reasonable expectation of success because the Petition did not step through every possible issue or difficulty that a skilled artisan might have cause to address in combining the teachings of O’Sullivan and Willner.

As Petitioner observes (*see* Pet. Reply 12),²⁴ however, notably absent from Patent Owner’s arguments (Or Dr. Russ’s testimony) is any contention that the types of issues or difficulties that may arise in implementing O’Sullivan’s teachings with Willner’s are those that are beyond the skill of an ordinarily skilled artisan. We also agree with Petitioner that “[t]he challenged claims recite no limitation on whether the method is performed client-side, server-side, or distributed between both.” *See* Pet. Reply 13 (citing Ex. 1042 ¶ 39). It follows readily that a “POSA would have reasonably expected success in achieving a workable implementation of any of the options—performing the method client-side, performing it server-side, or performing parts client-side and parts server-side—for each of the Petition’s grounds.” *See id.* at 14.

Furthermore, although Patent Owner regards O’Sullivan analysis of pixel clusters to detect click fraud as “simple,” as compared to Willner’s “complex” vector analysis for that same purpose, Patent Owner does not, in our view, adequately account what a person ordinary skill in the art, who is also a person of ordinary creativity, *see KSR*, 550 U.S. at 418, would have appreciated from the combined teachings of the references.²⁵ As Petitioner observes, O’Sullivan does not limit its system to only one type of data in its pursuit of rooting out click fraud. *See, e.g.,* Pet. Reply 10. Rather, O’Sullivan specifically contemplates that a wide range of data may be

²⁴ “Tellingly, Nobots never asserts (let alone establishes with evidence) that considering and resolving any of those ‘issues’ was beyond the POSA’s skill.” Pet. Reply 12.

²⁵ Here the parties agree that a skilled artisan has significant experience in computer science and security. *See* Pet. 4; PO Resp. 15.

analyzed in connection with its click fraud detection approach. For instance, O’Sullivan describes the following:

Data received may also include data gathered related to a timing of a view duration of the web page, data related to the transiting, data related to a speed of the cursor transiting each pixel cluster, data related to a click on the advertisement when initially displayed during a short time duration in one of a transparent or an invisible font, or data related to the clicking of the advertisement.

Ex. 1006 ¶ 50.

O’Sullivan also discloses that “other received data” may be used. *Id.* We agree with Petitioner, and Dr. Lopresti, that Willner’s vector analysis data is reasonably regarded as the type of data that O’Sullivan contemplates may be received as part of its click detection system. *See, e.g.*, Pet. 5–12; Ex. 1003 ¶ 74. Even if there is some possible incompatibility in some potential aspects of a combination of O’Sullivan and Willner, we agree with Petitioner that “[r]easonable expectation of success does not require ‘certainty that the [combination] would be successful in every instance.’” *See* Pet. Reply 20 (quoting *Eli Lilly & Co. v. Teva Pharms.*, 8 F.4th 1331, 1346 (Fed. Cir. 2021)).

Further still, with respect to Patent Owner’s contention that the Petition is “defective because it presents no evidence or analysis of a reasonable expectation of success, for any asserted grounds” (*see* PO Resp. 35), we do not agree. We take note that the Federal Circuit has observed that, while motivation to combine the teachings of the prior art requires an explicit analysis, “a finding of reasonable expectation of success can be implicit.” *See Elekta Limited v. Zap Surgical Systems, Inc.*, 81 F.4th 1368, 1376 (Fed. Cir. 2023). Moreover, “[e]vidence of reasonable expectation of success, just like evidence of a motivation to combine, ‘may flow from the

prior art references themselves, the knowledge of one of ordinary skill in the art, or in some cases, from the nature of the problem to be solved.’” *Id.* at 1377 (quoting *Brown & Williamson Tobacco Corp. v. Philip Morris Inc.*, 229 F.3d 1120, 1125 (Fed. Cir. 2000); *see also Merck & Cie v. Gnosis S.P.A.*, 808 F.3d 829, 836 (Fed. Cir. 2015) (“KSR does not require an explicit statement of a reasonable expectation of success in every case.”)).

Here, we conclude that: (1) the parties’ recognized level of ordinary skill in the art; (2), the knowledge of a skilled artisan as set forth by record evidence, including the teachings of O’Sullivan and Willner; and (3) the nature of the problem addressed in both of those references, i.e., click fraud detection, all support a determination that a skilled artisan would have had adequate reasons to combine O’Sullivan and Willner, and would have had a reasonable expectation of success in doing so. To that end, we find persuasive Petitioner’s arguments in the Petition as to reasoning to combine O’Sullivan and Willner, and also credit Dr. Lopresti’s supporting testimony. *See* Pet. 10–12; Ex. 1003 ¶¶ 77, 78.

We further discern that, in response to the challenges posed by Patent Owner pertaining to motivation to combine and reasonable expectation of success, Petitioner provides additional explanation and evidence. *See* Pet. Reply 10–22; Ex. 1042 ¶¶ 35–74. Patent Owner characterizes the new argument and evidence as “improper.” *See* PO Sur-reply. 18–20. A reply may incorporate new evidence in response to arguments made in a patent owner response and issues discussed in the institution decision, but it is certainly not the case that new evidence in a reply can go beyond what is permitted. *See* Consolidated Trial Practice Guide (Nov. 2019), 73 (“Petitioner may not submit new evidence or argument in reply that it could have presented earlier, e.g., to make out a *prima facie* case of

unpatentability.”) In this circumstance, however, Petitioner’s introduction and discussion of additional evidence as to reasonable expectation of success is tied directly to an initial determination made in the Institution Decision as to Petitioner’s establishment of reasonable expectation of success, and also is directly responsive to arguments challenging that establishment made by Patent Owner in the Patent Owner Response. Nevertheless, even discounting Petitioner’s argument and evidence made in the Reply as to this issue, we conclude that the Petition adequately demonstrates a reasonable expectation of success in combining the teachings of O’Sullivan and Willner.

(4) Conclusion

We have considered the parties’ respective positions on the question of whether Petitioner has shown that claims 3, 5, 6, 8, 10, 12–16, and 18–20 are unpatentable based on the teachings of O’Sullivan and Willner. We conclude that Petitioner has shown where all the features of those claims are found in O’Sullivan and Willner, and that a person of ordinary skill in the art would have adequate reason to combine those teachings, and a reasonable expectation of success in doing so. We conclude that Petitioner has shown by preponderance of evidence that claims 3, 5, 6, 8, 10, 12–16, and 18–20 are unpatentable over O’Sullivan and Willner. *See* Pet. 5–35.

b) Ground 2: O’Sullivan, Willner, and Broder

Petitioner contends that claims 3–8, 11, and 13–20 are unpatentable based on O’Sullivan, Willner, and Broder. *See* Pet. 35–38.

Patent Owner contends that this ground is deficient for the same reasons as it proposed for the Ground 1 based on O’Sullivan and Willner.

See PO Resp. 48. For the same reasons discussed above (*see supra* § II.D.2.a)), we do not agree with Patent Owner in that respect.

Patent Owner also contends that Petitioner has not sufficiently “explored or explained in the Petition or Lopresti declaration” how Broder’s teachings would be implemented in the combination of O’Sullivan-Willner. *Id.* at 47–48. As a result, Patent Owner contends that “a POSA would not have reasonably expected the proposed combination to succeed because the combination would simply not work.” *Id.* at 48.

Petitioner applies Broder’s teachings to account for a requirement in claims 4, 7, 11, and 17 of a “Completely Automated Turing test to tell Computers and Humans Apart (“CAPTCHA”)” requirement. Petitioner contends, in-part, the following:

In situations where the O’Sullivan-Willner combination determines that biometric data is present but suspicious of click fraud, a POSA would have been motivated to incorporate Broder’s technique to then interject a CAPTCHA page, to achieve the benefits Broder describes of “help[ing] determine if the entity that selected the advertisement link was a human or a non human entity” by “analyz[ing] the web viewer’s response to the intermediate [CAPTCHA] web page...along with other information” (e.g., the biometric data analyzed by O’Sullivan-Willner) “to make a determination as to whether the web viewer is a human or non-human entity.” Broder, [0029], [0010]; Lopresti-Declaration, [0122]-[0123]. O’Sullivan ([0048]) teaches that once the analysis O’Sullivan describes has detected possible fraudulent activity, “[t]he server...may then take appropriate action based on the analysis,” and Broder teaches that providing a CAPTCHA is an appropriate action when possible fraud is suspected. Lopresti-Declaration, [0123] (also citing O’Connell, [0032], corroborating POSA’s knowledge that “request[ing] additional authentication information” is “appropriate course of action” based on “fraud detection results”). A POSA would further have understood interjecting the CAPTCHA page to be desirable to slow down a clickbot

attempting click fraud. Lopresti-Declaration, [0123] (citing O’Connell, [0049], corroborating POSA’s knowledge that “slow[ing] down the automated program” helps to “make it less efficient (and thus useful”).

Pet. 36.

In the Reply, Petitioner contends that “Nobots ignores that the combination with Broder *modify* the base reference to interject a CAPTCHA *rather than* immediately granting or denying access.” Pet. Reply 28.

In its Sur-Reply, Patent Owner contends the following:

Petitioner argues that the Broder combinations modify the base references to interject a CAPTCHA instead of immediately granting or denying access. Reply, 28. But the Petition states, for each combination, that Broder’s interjected CAPTCHA is used only when the policy of **the underlying combination** first determines there is a **possible** fraud. Response, 46-47, 65-66. The Petition describes no modification of the underlying combinations to generate a “possible” fraud determination. *Id.* That the references refer to “possible” click fraud (Reply, 28-29) does not change their underlying logic or the proposed combination.

PO Sur-reply 32–33.

The record readily reflects that “CAPTCHA” is a well-known tool for use in click fraud detection systems. *See, e.g.*, Ex. 1011, Fig. 5 ¶¶ 21, 40 (“A well known type of CAPCHA requires that the web viewer to view [sic] a distorted image and then type in the letters and numbers displayed in the distorted image.”). Broder explains that in situations in which a “web site is being attacked by a malicious robot program, that web site may elect to use a CAPTCHA intermediate page in order to filter out all of the accesses by the malicious robot program.” *Id.* ¶41.

It is not apparent on the record why a person of ordinary skill in the art would not reasonably expect success in incorporating a well-known

CAPTCHA intermediate page of one click fraud detecting system (e.g., Broder) into other click fraud detecting systems (e.g., O’Sullivan and Willner). Patent Owner does not explain why a skilled artisan would not reasonably and readily “have understood interjecting the CAPTCHA page to be desirable to slow down a clickbot attempting click fraud” as is urged by Petition and Dr. Lopresti. *See, e.g.,* Pet. 36 (citing Ex. 1003 ¶ 123). We reject Patent Owner’s conclusory argument to the contrary.

Accordingly, we conclude that Petitioner has shown by a preponderance of the evidence that claims 3–8, 11, and 13–20 are unpatentable based on O’Sullivan, Willner, and Broder. *See* Pet. 35–38.

c) Ground 3: O’Sullivan, Willner, and Tanzer

Petitioner contends that claim 9 is unpatentable based on O’Sullivan, Willner, and Tanzer. Pet. 38–40.

Patent Owner contends that Ground 3 involving Tanzer “fails for the same reasons set forth for Ground 1.” PO Resp. 49. For the same reasons discussed above for Ground 1 (*see supra* § II.D.2.a)), we do not agree with Patent Owner’s challenges to Ground 3.

In considering the record before us, we conclude that Petitioner has shown by a preponderance of the evidence that claim 9 is unpatentable based on O’Sullivan, Willner, and Tanzer. *See* Pet. 38–40.

3. Grounds 5–14: Meek Based Grounds

Petitioner contends that Grounds 5–14 based on Meek taken with various other references including Willner, Kroll, Broder, Tanzer, Kitts, and O’Connell demonstrate the unpatentability of claims 3–9, 11, and 13–20. *See, e.g.,* Pet. 40–66; Pet. Reply 8–15; 22–27. Patent Owner disagrees. The

proposed basis of that disagreement is that Grounds 5–14 do not disclose the “not denying access” step [1D] (PO Resp. 30), and that a “POSA would not have reasonably expected the combination of Meek with any of the secondary references to success” (PO Resp. 49). *See, e.g.*, PO Resp. 49–68; PO Sur-reply 17–27; 29–33.

a) Not Denying Access Based Biometric Data

As discussed above, we conclude that “not denying access” to a server encompasses “granting access” to the server. *See supra* § II.C.1. Petitioner contends that Meek satisfies the “not denying access” step when some biometric data is present. *See* Pet. 45; Pet. Reply 8. Patent Owner disagrees on the basis that “not denying access” “does not mean simply granting access.” PO Resp. 30. According to Patent Owner, “[i]nstead, when some biometric data is present, the claimed method requires additional layers of testing, which are encompassed and described by subsequent claims.” *Id.*

Patent Owner also contends “Meek does not withhold denial as required by ‘not denying access,’ but instead **grants access.**” Further, Patent Owner argues the following: Thus, Meek makes an up/down decision as to whether to grant or deny access, based on a single-layer test: does the send attestation satisfy the predetermined policy? No matter what the policy—a single keystroke or mouse click, or several—the decision made is to grant access or to deny access. Ex-2104 ¶102. There is no subsequent test to further examine the biometric data as required by claims 3-20 of the ’885 Patent.

Id.

Because we conclude that the “not denying access” requirement of [1D] includes “granting access,” we do not agree with Patent Owner that Meek’s action of granting access to a server are distinct from what is required as a part of [1D].

We further note that Petitioner relies on modification of Meek based on the teachings of additional prior art references to account for features of the dependent claims. *See, e.g.*, Pet. 48–66; Pet. Reply 8–9. In particular, as Petitioner notes, its grounds based on Meek coupled with the teachings of other prior art references (e.g., Willner, Kroll, Broder, Tanzer, Kitts, and O’Connell) “assess whether the diametric data satisfies a policy before determining whether to grant/deny access,” and “involves additional assessment beyond just whether some biometric data is present.” Pet. Reply 9. The additional assessment means that, as a part of all of the proposed grounds based on Meek, access to the server is not denied in order to provide such assessment. That circumstance reasonably conveys all that is required of step [1D]. Patent Owner does not appear to address adequately Petitioner’s reliance on Meek’s teachings in combination with the teachings of the other prior art in urging that Petitioner’s grounds based on Meek lack the “not denying access” limitation of claim 1. Rather, Patent Owner bases its dispute solely on the belief that Meek’s disclosure of granting server access when biometric data is detected is in adequate to account for that feature. *See, e.g.*, PO Resp. 30–33. Although, as discussed above, we do not agree with Patent Owner on that basis, we also are not satisfied that Patent Owner presents any cogent reasoning as to why Petitioner’s grounds based on Meek taken together with the teachings of the additional prior art references does not reasonably meet the “not denying access” step [1D].

Accordingly, we conclude that Petitioner adequately accounts for the “not denying access” requirement of the claims.

b) Reasonable Expectation of Success

As with the grounds based on O’Sullivan, Patent Owner contends that a person of ordinary skill in the art would not have had a reasonable expectation of success in combining the teachings of Meek with any of the additional prior art teachings on which Petitioner relies (i.e., Willner, Kroll, Broder, Tanzer, Kitts, and O’Connell). *See* PO Resp. 49–68; PO Sur-reply 29–33. For the following reasons we do not agree with Patent Owner.

The primary basis for Patent Owner’s contention rests on similar reasoning as was proposed for the O’Sullivan grounds. Namely, according to Patent Owner, there is a dichotomy between systems in which it is a “client” computer that performs the bulk of computing requirements for the system and a “server” focused system in which the server handles the majority of the computing requirements. *See, e.g.*, PO Resp. 50–68; PO Sur-reply 29–33. In that respect, Patent Owner expresses that “in a ‘thick’ or ‘fat’ client model, much of the computation and software complexity required by the system resides at the client.” PO Resp. 50 (citing Ex. 2104 ¶ 144). Whereas, according to Patent Owner, “[i]n a ‘thin client’ / ‘fat server’ model, much of the computation and software complexity resides at the server.” *Id.* (citing Ex. 2104 ¶ 146). Patent Owner further contends the following:

[S]tarting with one working system (such as Meek) and adding another system to it can require extensive redesign of the system architecture. Ex-2104 ¶ 155 (citing Ex-2109). The decisions made to implement one system constrain that system, and attempts to add features may require major changes to the overall architecture. *Id.* Therefore, a POSA recognized that making modifications to a system required careful evaluation of the impact that any changes would have on the systems’ functionality, before one could conclude that the modified system would be reasonably expected to successfully function.

Id. This is even more important when attempting to combine “thick client” and “thin client” systems, given their substantial difference as previously discussed. *Id.*

PO Resp. 53.

Thus, Patent Owner argues that a skilled artisan may need to evaluate the potential impacts of modifications in combining “thick client” and “thin client” systems. According to Patent Owner, Meek “uses a ‘thick client’ approach,” while “the secondary references in Grounds 5-14 use a ‘thin client’ or ‘fat server’ approach. *Id.* at 54 (citing Ex. 2104 ¶¶ 166–168). Patent Owner then contends that a skilled artisan would need to consider “issues” such as “processing and data storage capabilities” and “computational power” that “must be resolved in order to determine whether there is a reasonable expectation of success.” *Id.* at 55–58. Notably, as Petitioner observes, Patent Owner “does not establish that ‘resolving’ any such ‘issues’ was beyond the POSA’s skill.” *See* Pet. Reply 22.

Petitioner also contends the following:

Nobots’s arguments regarding whether “starting with one working system (such as Meek) and adding another system to it can require extensive redesign of the system architecture” (POR, 53) are irrelevant because the Petition’s Grounds do not require designing a working Meek-alone system and then **redesigning** it. POSAs could design a system combining the references’ teachings from the beginning. EX1042, [0075]-[0077]. Combining references’ teachings “does not require an actual, physical substitution of elements.” *In re Mouttet*, 686 F.3d 1322, 1332 (Fed. Cir. 2012). “The test for obviousness is not...bodily incorporat[ion]” of features, but “what the combined teachings of the references would have suggested.” *MCM Portfolio v. Hewlett-Packard*, 812 F.3d 1284, 1294 (Fed. Cir. 2015).

Id. at 23.

We agree with Petitioner that an obviousness analysis does not require a demonstration of how elements in the prior art would be physically

substituted, or bodily incorporated, into a system. Indeed, obviousness does not require a rigid showing of the actual contours of any one particular system that may emerge from the combined teachings of the prior art. Rather, the obviousness inquiry is “flexible” and must take into account the “background knowledge, creativity, and common sense of the person of ordinary skill in the art.” *See Perfect Web Techs., Inc. v. InfoUSA, Inc.*, 587 F.3d 1324, 1329 (Fed. Cir. 2009). We agree with Petitioner that the record at hand reasonably conveys that a person of ordinary skill and creativity in the art would have reasonably expected success in combining the teachings of the prior art in a variety of ways irrespective of whether such combination implements certain computing functions on a “client side” device, “server side” device, or a combination of the two. *See* Pet. Reply 24–27. That such implementation of the teachings of the various references may involve addressing difficulties or problems does not demand a conclusion of non-obviousness as a “a person of ordinary skill often will be able to fit the teachings of multiple patents together like pieces of a puzzle.” *See KSR*, 550 U.S. at 402.

Patent Owner urges that incorporating the teachings of the pertinent prior art references into Meek’s client-side system would be “difficult, if not impossible” for a skilled artisan to accomplish. PO Resp. 56 (citing Ex. 2104 ¶174). Neither Patent Owner nor Dr. Russ, however, justifies that postulation with any evidence or cogent reasoning as to why the types of problems that a skilled artisan might confront in modifying Meek’s system gives rise to the “impossib[ility]” of combining Meek’s teachings with those of the cited prior art. Patent Owner and Dr. Russ also do not credibly explain why challenges or “difficulties” that a skilled artisan might face as a

part of the proposed combinations abjectly “preclude a determination of reasonable expectation of success.” PO Resp. 58.

As discussed above, we conclude that the Meek based grounds account for the [1D] requirement of “not denying access” when some biometric data is present. We also observe that Patent Owner does not contend that any other features required by the claims are absent from the prior art. We have considered all of Patent Owner’s arguments that a person of ordinary skill in the art would not have had a reasonable expectation of success in combining the teachings of the prior art. *See* PO Resp. 49–68; PO Sur-reply 29–33. As with the proposed grounds based on O’Sullivan, we conclude that, based on the record at hand, including (1) the parties’ recognized level of ordinary skill in the art; (2), the knowledge of a skilled artisan as set forth by record evidence; and (3) the nature of the problem addressed by all of those references, i.e., click fraud or bot detection, Petitioner has adequately established that a skilled artisan would have had adequate reasons to combine the teachings of Meek, Willner, Kroll, Broder, Tanzer, Kitts, and O’Connell, and would have had a reasonable expectation of success in doing so. *See* Pet. 40–66; Pet. Reply 8–15, 22–27.²⁶

²⁶ As with the O’Sullivan based grounds, we reject Patent Owner’s argument that Petitioner’s Reply and Dr. Lopresti’s Reply Declaration in responding to Patent Owner’s arguments pertaining to reasonable expectation of success constitute impermissible new argument and evidence. *See* PO Sur-Reply 18–27. In any event, even discounting Petitioner’s argument and evidence made in the Reply as to this issue, we conclude that the Petition adequately demonstrates a reasonable expectation of success in combining the teachings of Meek with the other pertinent prior art references.

III. CONCLUSION

In summary, we determine that a preponderance of the evidence establishes that claims 3–9, 11, and 13–20 of the ’885 patent are unpatentable.²⁷ Those determinations are shown in the following table:²⁸

Claim(s)	35 U.S.C. §	References/Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
3, 5, 6, 8, 13–16, 18–20	103	O’Sullivan, Willner	3, 5, 6, 8, 13–16, 18–20	
3–8, 11, 13–20	103	O’Sullivan, Willner, Broder	3–8, 11, 13–20	
9	103	O’Sullivan, Willner, Tanzer	9	
3, 5, 6, 8	103	Meek, Willner	3, 5, 6, 8	
3, 5, 6, 8	103	Meek, Kroll	3, 5, 6, 8	
3–8, 11	103	Meek, Willner, Broder	3–8, 11	
3–8, 11	103	Meek, Kroll, Broder	3–8, 11	
9	103	Meek, Willner,	9	

²⁷ As noted *supra* (§ A.1 n.1), claims 1, 2, 10, and 12 were challenged in the Petition but have been disclaimed. Accordingly, we do not reach any patentability determination as to those claims as a part this Final Written Decision.

²⁸ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner’s attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. See 37 C.F.R. §§ 42.8(a)(3), (b)(2).

		Tanzer		
9	103	Meek, Kroll, Tanzer	9	
13–16, 18–20	103	Meek, Kitts	13–16, 18–20	
13–16, 18–20	103	Meek, O’Connell	13–16, 18–20	
13–20	103	Meek, Kitts, Broder	13–20	
13–20	103	Meek, O’Connell, Broder	13–20	
Overall Outcome			3–9, 11, 13– 20	

IV. ORDER

Upon consideration of the record before us, it is:

ORDERED that claims 3–9, 11, and 13–20 of the ’885 patent have been shown to be unpatentable;

FURTHER ORDERED that, because this is a final written decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

NOBOTS LLC,
Patent Owner.

IPR2022-00941
Patent 10,423,885 B2

Before JOSIAH C. COCKS, BARBARA A. PARVIS, and
ROBERT J. WEINSCHENK, *Administrative Patent Judges*.

WEINSCHENK, *Administrative Patent Judge*, dissenting.

I respectfully dissent from the majority’s decision that Petitioner has shown by a preponderance of the evidence that claims 3–9, 11, and 13–20 are unpatentable.

A. Claim Construction

Patent Owner argues that claim 1 recites a “first pass evaluation” that performs “a simple check for the **presence** of biometric data.” PO Resp. 13; *see also id.* at 10 (“The binary ‘if-then’ first pass evaluation is reflected in the elements of claim 1, which test for the mere presence of biometric data.”). I agree. In my view, the language of claim 1 requires determining whether to deny access to a server based *only* on whether biometric data is

present *before* performing the additional steps recited in the dependent claims. Specifically, the phrase “denying access . . . when the biometric data is not present” indicates that when biometric data is not present, the claimed method simply denies access to the server. *Id.* at 5:47–49. The phrase “not denying access . . . when some biometric data is present” indicates that when some biometric data is present, the claimed method does not deny access and may proceed to perform additional steps, such as those recited in the dependent claims,¹ to determine whether to deny access to the server. *Id.* at 5:50–52, 5:56–58, 5:64–67.

This reading of the claim language is supported by the written description of the ’885 patent. Specifically, the ’885 patent describes “a first layer of testing that simply checks if there were valid mouse movements and/or key strokes inputted by the user of a computing device that is attempting to access a server.” *Id.* at 4:59–63. “[I]f no activity is recorded there is a very high probability that the user is actually a bot,” so “access is denied.” *Id.* at 4:65–5:2. This “first pass evaluation” is advantageous because it “is essentially without overhead since there are no computations being carried out.” *Id.* at 4:63–5:1. The ’885 patent explains that when some biometric data is present, there is “a second level knockout assessment to deny user access if the input data exactly (or statistically sufficiently) matches previously recorded data.” *Id.* at 5:3–10. And, “[i]n robust embodiments of the invention, a third layer of testing may be employed that compares recorded pointer movements and key strokes to previously

¹ For example, claims 3 and 5 recite “identifying whether the biometric data matches previously recorded biometric data” and “denying access . . . when the biometric data matches previously record biometric data.” Ex. 1001, 5:56–58, 5:64–67.

recorded activity for a given input page that was knowingly created by humans.” *Id.* at 5:28–32. In other words, like the claim language, the written description of the ’885 patent describes a first pass evaluation that determines whether to deny access to the server based only on whether biometric data is present before performing additional steps.

B. O’Sullivan Grounds

Patent Owner argues that Petitioner does not show sufficiently that the asserted grounds including O’Sullivan teach determining whether to deny access to a server based only on whether biometric data is present. PO Resp. 23 (“does not teach th[e] first layer binary test”). I agree. In my view, the portions of O’Sullivan cited by Petitioner teach determining whether to deny access to a server based on analyzing characteristics of a cursor’s movement, not based only on whether the cursor moved. *See* Pet. 17–19; Pet. Reply 6–8; Ex. 1006 ¶ 30 (“The data . . . , e.g., when the click occurs, the transit and the timer information, are used . . . to create a confidence factor.”); *id.* ¶ 32 (“where the mouse click occurred very quickly”); *id.* ¶ 34 (“[h]uman characteristics of such a movement could be stored and compared”); *id.* ¶ 35 (“calculate a signature, including timing, trajectory, and the like”); *id.* ¶ 40 (“monitors the transition of a cursor movement” and “determines a confidence factor”); *id.* ¶ 43 (“When the click occurs, the transit and the timer may be used to create a confidence factor.”); *id.* ¶ 46 (“a confidence level is determined based on the time duration, the transiting and the

clicking”)²; *id.* ¶ 47 (“where the mouse click occurred very quickly”); *id.* ¶ 48 (“the collected data to be processed”); *id.* ¶ 50 (“analyze the cursor movement data collected”); *id.* ¶ 52 (“analyze the cursor movement”).

Petitioner argues that “O’Sullivan includes a binary first-layer test of whether applets are triggered by ‘cursor movement . . . over the associated pixel clusters.’” Pet. Reply 7 (citing Ex. 1006 ¶ 30). I disagree. Even if Petitioner is correct that O’Sullivan’s applet is triggered simply by a cursor’s movement, the applet still determines whether to deny access to the server based on analyzing characteristics of the cursor’s movement. *Id.* ¶ 30 (“The data . . . , e.g., when the click occurs, the transit and the timer information, are used . . . to create a confidence factor.”). And, contrary to Petitioner’s assertion, Patent Owner’s declarant does not admit that O’Sullivan teaches denying access to the server “because no cursor movement is detected.” Pet. Reply 7–8 (citing Ex. 1042 ¶ 26). Rather, Patent Owner’s declarant states that the client “checks for the cursor movement . . . *as well as* timing information” and then the server performs “the confidence factor analysis” to determine whether to deny access. Ex. 2104 ¶ 111 (emphasis added).

For the foregoing reasons, in my view, Petitioner does not show sufficiently that the asserted grounds including O’Sullivan teach all the limitations of the challenged claims.

² Petitioner points out that the “time duration” in O’Sullivan’s paragraph 46 is “optional.” Pet. Reply 8; Ex. 1006 ¶ 46. Even if Petitioner is correct, O’Sullivan’s paragraph 46 still teaches determining whether to deny access to the server based on a confidence level calculated using at least “the transiting and the clicking.” Ex. 1006 ¶ 46.

C. Meek Grounds

Patent Owner argues that Petitioner does not show sufficiently that the asserted grounds including Meek teach determining whether to deny access to the server based only on whether biometric data is present before performing the additional steps recited in the challenged dependent claims. PO Resp. 30 (“does not teach th[e] multilayer protocol”). I agree. In my view, the portions of Meek cited by Petitioner teach determining whether to deny access to a server based on whether a single policy is satisfied. *See* Pet. 43–45; Pet. Reply 8–10; Ex. 1008 ¶ 50 (“a pre-determined policy”); *id.* ¶ 51 (“the policy may for example set forth . . . a minimum number of keyboard taps, a minimum number of mouse clicks”); *id.* ¶ 52 (“if the policy is in fact satisfied by the send attestation 18, the send item 14 is honored, accepted, and acted upon”); *id.* ¶ 53 (“if the policy is not in fact satisfied by the send attestation 18, the send item 14 is denied”).

Petitioner argues that “in some examples, [Meek’s] policy can specify ‘a’ (singular) keystroke or mouse click as the minimum number required to demonstrate human effort,” and thus determines whether the deny access to the server based only on whether biometric data is present. Pet. 44.

Petitioner argues that Meek’s policy also can determine (or be modified to determine) whether to deny access to the server based on an analysis of the biometric data as recited in the challenged dependent claims. *See, e.g., id.* at 47–48 (“identifies patterns in input data”); *id.* at 49 (“incorporate Willner’s cursor movement analysis as part of Meek’s policy.”); *id.* at 61 (“Meek compares the monitored interest data . . . to known patterns.”). In other words, according to Petitioner, Meek’s policy can determine whether to deny access based on whether biometric data is present *or* based on an analysis of the biometric data. But Petitioner does not identify specific

evidence indicating that Meek's policy determines whether to deny access to the server based only on whether biometric data is present *before* performing the additional steps recited in the challenged dependent claims. *See id.* at 40–66; Pet. Reply 8–10.

For the foregoing reasons, in my view, Petitioner does not show sufficiently that the asserted grounds including Meek teach all the limitations of the challenged claims.

IPR2022-00941
Patent 10,423,885 B2

FOR PETITIONER:

Elisabeth H. Hunt
Richard F. Giunta
Adam R. Wichman
WOLF, GREENFIELD & SACKS, P.C.
ehunt-ptab@wolfgreenfield.com
rgiunta-ptab@wolfgreenfield.com
awichman-ptab@wolfgreenfield.com

FOR PATENT OWNER:

Stephen D. Zinda
James H. Hall
J. David Cabello
CABELLO HALL ZINDA, PLLC
stephen@chzfirm.com
james@chzfirm.com
david@chzfirm.com