

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

UNILOC 2017 LLC,
Patent Owner.

IPR2020-00441
Patent 8,949,954 B2

Before PATRICK M. BOUCHER, STACY B. MARGOLIES, and
MICHAEL T. CYGAN, *Administrative Patent Judges*.

BOUCHER, *Administrative Patent Judge*.

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

In response to a Petition (Paper 1, “Pet.”) filed by Google LLC (“Petitioner”), we instituted an *inter partes* review of claims 1–4, 6, 9, and 12–14 of U.S. Patent No. 8,949,954 B2 (Ex. 1001, “the ’954 patent”). Paper 13 (“Dec.”). During the trial, Uniloc 2017 LLC (“Patent Owner”) filed a (corrected) Response (Paper 17, “PO Resp.”), Petitioner filed a Reply (Paper 19, “Reply”), and Patent Owner filed a Sur-reply (Paper 21, “Sur-reply”). An oral hearing was held with the parties, and a copy of the transcript was entered into the record. Paper 29 (“Tr.”).

We have jurisdiction under 35 U.S.C. § 6. This Decision is a Final Written Decision under 35 U.S.C. § 318(a) as to the patentability of the claims on which we instituted trial. Based on the record before us, Petitioner has shown, by a preponderance of the evidence, that claims 1–4, 6, 9, and 12–14 are unpatentable.

I. BACKGROUND

A. The ’389 Patent

1. Overview

The ’954 patent “relates to a method and system for providing customer notification and authorization of remote requests for access to customer account information.” Ex. 1001, 1:17–20. Figure 7 of the ’954 patent is reproduced below.

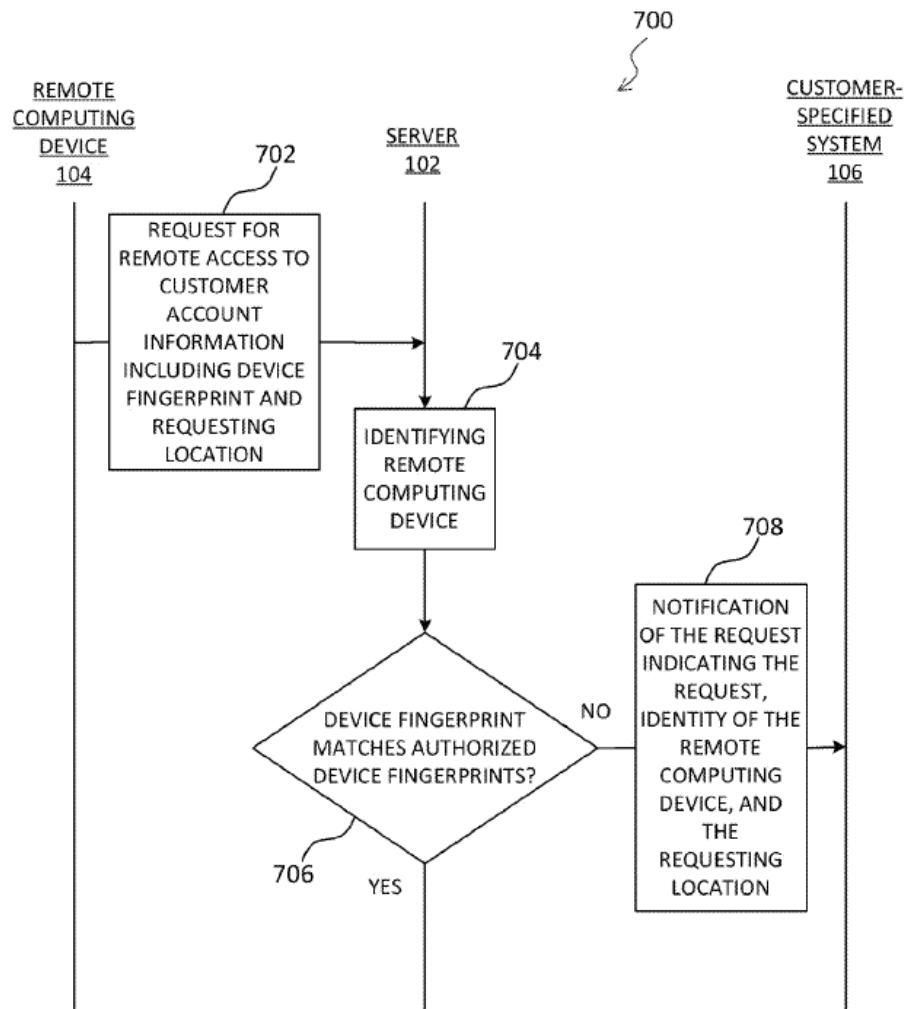


FIG. 7

Figure 7 is a “transaction flow diagram” that illustrates how a remote computing device requests remote access to customer account information through a server. *Id.* at 9:42–46. For purposes of illustration, the ’954 patent describes transaction flow diagram 700 “in the context . . . of a customer or a hacker requesting remote access to . . . bank account information.” *Id.* at 9:46–50.

At step 702, remote computing device 104 transmits a request for remote access to customer account information. *Id.* at 9:55–56. The request can include a “device fingerprint” and a “requesting location” of remote computing device 104. *Id.* at 9:57–59. “For example, a person can request remote access to the bank account information from a laptop in a different state. Such a laptop can be an authorized laptop or an unknown laptop.” *Id.* at 9:59–62. An “unknown laptop” differs from an “authorized laptop” because “[t]he authorized laptop can be a system in which the customer with authority to access the bank account information has approved for use in obtaining access to the bank account information” and because “[t]he authorized laptop’s device fingerprint may be stored as an authorized device fingerprint.” *Id.* at 9:63–67. The “unknown laptop,” by contrast, “can be a system that the customer with authority to access the bank account information has not approved for use in obtaining access to the bank account information.” *Id.* at 9:67–10:3. Accordingly, the unknown laptop’s device fingerprint is not indicated as an authorized device fingerprint. *Id.* at 10:3–6.

At step 704, server 102 identifies remote computing device 104, such as by using the device fingerprint and requesting location of remote computing device 104. *Id.* at 10:7–11. At step 706, server 102 determines whether the device fingerprint of remote computing device 104 matches an authorized device fingerprint, such as by performing a comparison with a stored list of authorized device fingerprints. *Id.* at 10:21–27. If a match is found, server 102 may approve the remote access request. *Id.* at 10:52–56. But if no match is found, server 102 proceeds to step 708. *Id.* at 10:31–33. “For example, in the case where the person is using the unknown laptop to request remote access to the bank account information, the device fingerprint

of the unknown laptop utilized will not match an authorized device fingerprint.” *Id.* at 10:33–36.

At step 708, server 102 transmits a notification of the request to customer-specified system 106, indicating “the request, identity of the remote computing device 104, and the requesting location.” *Id.* at 10:37–41. “This allows the customer to determine whether to grant or deny access to the bank account information by the unknown laptop.” *Id.* at 10:46–48.

Figure 8 of the ’954 patent is reproduced below.

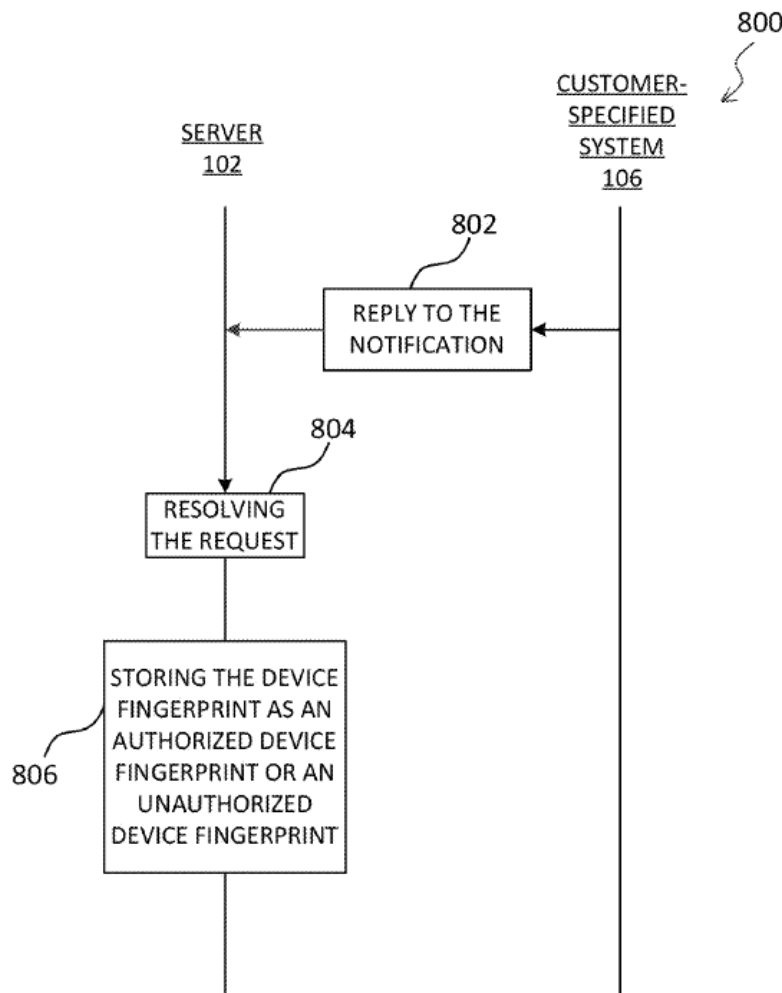


Figure 8 is a “transaction flow diagram [that] illustrates additional steps to the transactional flow diagram 700 (FIG. 7).” *Id.* at 10:60–65. At step 802,

customer-specified system 106 transmits a reply to the notification, which “may include an approval or disapproval to the server 102.” *Id.* at 11:3–5. “Thus, the customer can approve or disapprove the request for remote access by the unknown laptop. For example, if the customer knows that she or someone she wishes to access the bank account information is the one using the unknown laptop, she can approve the request.” *Id.* at 11:8–13. Reply 802 can also include the device fingerprint of customer-specified system 106 so that server 102 can authenticate the reply. *Id.* at 11:14–17.

At step 804, server 102 resolves the request, such as by approving or disapproving the request based on reply 802 received from customer-specified system 106. *Id.* at 11:18–21. At step 806, server 102 stores the device fingerprint as an authorized device fingerprint or an unauthorized device fingerprint in accordance with the approval or disapproval. *Id.* at 11:41–50.

2. Illustrative Claim

Independent claim 1 is illustrative of the challenged claims and is reproduced below with a key limitation emphasized.

1. A system for authorizing a request for remote access to customer account information, comprising:

a server configured to receive the request via a network from a remote computing device; a database storing the customer account information accessible by the server; and

memory accessible by the server and storing a customer notification program which, when executed by the server, performs steps for

(a) identifying, responsive to the server receiving the request, the remote computing device fingerprint and by a requesting location;

(b) determining whether the device fingerprint matches any of a number of device fingerprints previously authorized to access the customer account information;

(c) *sending*, responsive to determining a mismatch between the device fingerprint and each of the previously authorized device fingerprints, *a notification of the request to an address of a separate device specified by the customer*, the notification indicating (i) the request, (ii) identity of the remote computing device, and (iii) the requesting location;

(d) resolving the request responsive to a reply to the notification; and

(e) if resolving the request responsive to a reply to the notification results in permitting authorized access to the customer account information by the remote computing device, storing the device fingerprint as a previously authorized device fingerprint and associating the device fingerprint with the customer account information.

Ex. 1001, 12:2–34 (emphasis added).

3. Prosecution History

When the application that matured into the '954 patent was filed, independent claim 1 was presented in the following form:

1. A system for authorizing a request for remote access to customer account information, comprising:

a server configured to receive the request via a network from a remote computing device; a database storing the customer account information accessible by the server; and

memory accessible by the server and storing a customer notification program which, when executed by the server, performs steps for

(a) identifying, responsive to the server receiving the request, the remote computing device by a device fingerprint and by a requesting location;

(b) determining whether the device fingerprint matches any of a number of device fingerprints authorized to access the customer account information; and

(c) sending, responsive to determining a mismatch between the device fingerprint and each of the previously authorized device fingerprints, a notification of the request to a customer-specified address, the notification indicating (i) the request, (ii) identity of the remote computing device, and (iii) the requesting location.

Ex. 1004, 568. In a first Office Action, the Examiner rejected claim 1, as well as other claims, as unpatentable under 35 U.S.C. § 103(a) over U.S. Patent Publ. No. 2004/0254890 (“Sancho”) and U.S. Patent No. 8,370,265 (“Coulter”). *Id.* at 492–506. After the Applicant traversed this prior-art rejection without amending the claims, *id.* at 140–156, the Examiner issued a Final Office Action maintaining the rejection, *id.* at 76–120.

The Applicant responded to the Final Office Action by amending the claims, particularly amending step (c) of independent claim 1 to replace “sending . . . a notification of the request to *a customer specified address*” with “sending . . . a notification of the request to *an address of a separate device specified by the customer.*” *Id.* at 45 (emphases added).¹ The Applicant argued that the prior art cited by the Examiner “teaches sending

¹ In reproducing independent claim 1 in this amendment, step (a) was recited as “identifying . . . the remote computing device fingerprint and by a requesting location,” rather than reproducing the original language of “identifying . . . the remote computing device *by a device* fingerprint and by a requesting location.” Ex. 1004, 45 (emphasis added). Although the words “by a device” were omitted, no markings were included to indicate any intent by the Applicant to remove those words from the claim language. *See id.* The omission apparently propagated to issued claim 1, which also does not include the words “by a device.” We address this omission as a matter of claim construction below.

customer notification only to the same device, *not a separate device specified by the consumer.*” *Id.* at 164 (emphasis added). In doing so, the Applicant sought to distinguish the prior art as “fail[ing] to address and . . . not solv[ing] the problem of initial transaction requests from stolen devices (ones that are used to commit fraud for the first time).” *Id.* “By contrast,” the Applicant explained to the Examiner, “applicant’s invention teaches use of alternate devices.” *Id.* at 165. After considering this argument, the Examiner asserted that “applicant’s argued feature of: ‘a separate device specified by the consumer’ [wa]s not presently recited in applicant’s claim 1.” *Id.* at 80.

The Applicant similarly argued, in slightly different context, that the prior art “fails to teach sending alert notifications to separately specified user devices as taught by applicant’s claim 1.” *Id.* at 165. The Examiner found this argument equally unpersuasive because “applicant’s presently presented claim 1 does not recite the, ‘sending alert notifications to separately specified user devices.’” *Id.* at 80.

The Applicant accordingly amended claim 1 to recite the language that appears in the challenged issued claim, namely “sending . . . a notification of the request to an address of a separate device specified by the customer.” *Id.* at 45. Although Petitioner highlights the Examiner’s latter comment that the original version of claim 1 did not recite “sending alert notifications to separately specified devices,” it is apparent from the prosecution history that *both* of the Examiner’s comments identified above contributed to the Applicant’s amendment. *Id.* at 52 (“The Final Action states further that ‘*applicant’s argued feature of “a separate device specified by the consumer”* [or, “customer”] *is not presently recited [in] claim 1.*’; and

that claim 1 moreover does not recite ‘sending alert notifications to separately specified user devices.’ . . . Accordingly, applicant herein amends claim 1 to overcome this position.” (first alteration in original)).

Following an interview between the Examiner and Applicant, independent claim 1 was further amended by the Examiner to place it in condition for allowance by adding steps (d) and (e) of the issued claim. *Id.* at 33–41 (Notice of Allowability with Examiner’s Amendment and Interview Summary).

B. Evidence

Petitioner relies on the following references:

Steinberg	US 2007/0136573 A1	June 14, 2007	Ex. 1005
Oberheide	US 2011/0219230 A1	Sept. 8, 2011	Ex. 1006
McDowell	US 2009/0260064 A1	Oct. 15, 2009	Ex. 1008
Yasushi	JP 2010-262532	Nov. 18, 2010	Ex. 1009 ²

In addition, Petitioner relies on a Declaration by Fabian Monroe, Ph.D. Ex. 1002. No cross-examination testimony of Dr. Monroe was entered into the record.

C. Instituted Grounds of Unpatentability

Petitioner challenges claims 1–4, 6, 9, and 12–14 on the following grounds. Pet. 3.

² Exhibit 1009 includes both the original published Japanese application and an English translation, with an affidavit by the translator attesting to the accuracy of the translation.

Claim(s) Challenged	35 U.S.C. § ³	References
1–4, 6, 12, 14	103(a)	Steinberg, Oberheide
1–4, 6, 9, 12, 14 ⁴	103(a)	Steinberg, Oberheide, McDowell
13	103(a)	Steinberg, Oberheide, Yasushi
13	103(a)	Steinberg, Oberheide, McDowell, Yasushi

D. Real Parties in Interest

The parties identify only themselves as real parties in interest. Pet. 1; Paper 4, 1. Petitioner additionally discloses that it “is a subsidiary of XXVI Holdings Inc., which is a subsidiary of Alphabet Inc.,” but asserts that “XXVI Holdings Inc. and Alphabet Inc. are not real parties-in-interest to this proceeding.” Pet. 1 n.1. Patent Owner additionally discloses that it “is owned by CF Uniloc Holdings LLC.” Paper 4, 1.

E. Related Matters

A related district court proceeding involving the ’954 patent, *Uniloc 2017 LLC v. Google LLC*, No. 5:20-cv-04355 (N.D. Cal.), which originated as *Uniloc 2017 LLC v. Google LLC*, No. 2:18-cv-00504 (E.D. Tex.), has

³ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), amended various provisions of 35 U.S.C. Because the ’954 patent was filed before March 16, 2013 (the effective date of the relevant amendment), the pre-AIA versions of those provisions apply.

⁴ Petitioner identifies two separate grounds: (1) “Ground 2,” which challenges claim 9 as unpatentable under 35 U.S.C. § 103(a) over Steinberg, Oberheide, and McDowell; and (2) “Ground 4,” which challenges claims 1–4, 6, 9, 12, and 14 as unpatentable under 35 U.S.C. § 103(a) over Steinberg, Oberheide, and McDowell. Pet. 3. Because both grounds involve the same statutory basis and the same prior art, we identify them collectively in the table.

been dismissed for lack of subject-matter jurisdiction. *See* Pet. 1; Paper 4, 2; Ex. 3001; Paper 20 (citing *Uniloc 2017 LLC v. Google LLC*, No. 4:20-cv-5345) (N.D. Cal.)). In addition, *Uniloc 2017 LLC v. Google LLC*, No. 2:18-cv-00458 (E.D. Tex.), which also involved the '954 patent, was dismissed without prejudice. Pet. 1; PO Resp. 4.

II. ANALYSIS

A. Legal Principles

A claim is unpatentable for obviousness under 35 U.S.C. § 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 nonobviousness, i.e., secondary considerations.⁵ *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

Additionally, the obviousness inquiry typically requires an analysis of “whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) (requiring “articulated reasoning with some rational underpinning to support the legal conclusion of

⁵ The parties do not address objective indicia of nonobviousness, which accordingly do not form part of our analysis.

obviousness”)); see *In re Warsaw Orthopedic, Inc.*, 832 F.3d 1327, 1333 (Fed. Cir. 2016) (citing *DyStar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co.*, 464 F.3d 1356, 1360 (Fed. Cir. 2006)).

B. Level of Ordinary Skill in the Art

In determining whether an invention would have been obvious at the time it was made, we consider the level of ordinary skill in the pertinent art at the time of the invention. *Graham*, 383 U.S. at 17. “The importance of resolving the level of ordinary skill in the art lies in the necessity of maintaining objectivity in the obviousness inquiry.” *Ryko Mfg. Co. v. Nu-Star, Inc.*, 950 F.2d 714, 718 (Fed. Cir. 1991). The “person of ordinary skill in the art” is a hypothetical construct, from whose vantage point obviousness is assessed. *In re Rouffet*, 149 F.3d 1350, 1357 (Fed. Cir. 1998). “This legal construct is akin to the ‘reasonable person’ used as a reference in negligence determinations” and “also presumes that all prior art references in the field of the invention are available to this hypothetical skilled artisan.” *Id.* (citing *In re Carlson*, 983 F.2d 1032, 1038 (Fed. Cir. 1993)).

Petitioner proposes that a person of ordinary skill in the art “would have had a bachelor’s degree in electrical engineering, computer science, or the equivalent thereof, and three or more years of experience with network security.” Pet. 4 (citing Ex. 1002 ¶¶ 17–19). According to Petitioner, “[s]ignificantly more practical experience could also qualify one not having the aforementioned education while, conversely, a higher level of education could offset a lesser amount of experience.” *Id.* (citing Ex. 1002 ¶¶ 17–19).

Petitioner supports its proposal with testimony by Dr. Monroe. Ex. 1002 ¶ 18.

Although Patent Owner contends that Petitioner’s proposal is “improper,” at least for failing to define thresholds for “significantly more practical experience” or “a higher level of education,” Patent Owner declines to offer its own proposal for the level of ordinary skill. PO Resp. 5–6.

We adopt Petitioner’s proposed articulation. Our Decision does not depend on nuanced distinctions in the degree to which additional education or experience may offset Petitioner’s proposed baseline articulation of the level of ordinary skill in the art.

C. Claim Construction

The Board uses “the same claim construction standard that would be used to construe the claim 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) (2019); *see Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc). The specification may reveal a special definition given to a claim term by the patentee. *Phillips*, 415 F.3d at 1316. If an inventor acts as his or her own lexicographer, the definition must be set forth in the specification with reasonable clarity, deliberateness, and precision. *Renishaw PLC v. Marposs Societa’ per Azioni*, 158 F.3d 1243, 1249 (Fed. Cir. 1998).

Although Petitioner “believes that no express constructions of the claims are necessary to assess whether the prior art reads on the challenged claims,” Petitioner nevertheless proposes constructions for several terms.

Pet. 7. Patent Owner instead “requests that the Board adopt the ordinary and customary meaning of the claim terms as understood by one of ordinary skill in the art.” PO Resp. 6. In addition, Patent Owner contends that certain of Petitioner’s proposed constructions were rejected in related district court litigation, and highlights those that Patent Owner considers “fatal” to Petitioner’s position. *Id.* at 8 (“Given the court’s preliminary constructions and the court’s remarks during the *Markman* hearing,[□] it should have been clear, and indeed Google even acknowledged, that the court had decided against adopting Google’s untenable claim construction positions addressed herein.” (footnote omitted)); *see also id.* at 9–16 (discussing certain specific claim recitations).

In particular, Patent Owner reiterates an argument that we considered during the preliminary phase of this proceeding, namely that “the Petition is impermissibly keyed to *multiple* erroneous claim constructions.” *Id.* at 7 (citing *Mentor Graphics Corp. v. Synopsys, Inc.*, 2015 WL 3637569 at *11 (PTAB June 11, 2015), *aff’d sub nom. Synopsys, Inc. v. Mentor Graphics Corp.*, 669 Fed. Appx. 569 (Fed. Cir. 2016); *United Microelectronics Corp. v. Lone Star Silicon Innovations LLC*, IPR2017-01513, Paper 10 at 4–5, 6 (PTAB May 22, 2018)); *see* Dec. 14–15. According to Patent Owner, the Petition is “tainted” by its emphasis on certain constructions that were rejected in related district court litigation, and this taint “appl[ies] with greater force at the post-institution stage.” PO Resp. 7–8; Sur-reply 5. Specifically, Patent Owner contends that Petitioner had an obligation to substantively address the district court’s constructions, and that Petitioner failed to meet that obligation. Sur-reply 1–2 (citing *OrthoPediatrics Corp. v. K2M, Inc.*, IPR2018-01548, Paper 9 at 10–11 (PTAB May 1, 2019)).

But as we explained in our Institution Decision, “[w]e have reviewed the decisions cited by Patent Owner and disagree that it would be prudent to deny the Petition merely because Petitioner has emphasized proposed constructions that differ from those adopted by the district court.” Dec. 14–15 (citing Exs. 2001 (district court preliminary Claim Construction Memorandum and Order), 2002 (district court adopting preliminary constructions)); *see also* Tr. 25:15–26:11 (Patent Owner acknowledging that at least *OrthoPediatrics* is not binding authority). That determination, which we further determine applies as fully at this stage of the proceeding, resulted in significant part from the fact that “Petitioner argues, for each of its constructions that deviate from the district court’s construction, that its analysis applies both for the construction it advocates and for the construction adopted by the district court.” Dec. 15 (citing Pet. 10–13, 38, 43–44, 47); *see also* Tr. 7:5–8 (Petitioner asserting that “[w]hat [Patent Owner’s] argument misses however is that our IPR petition addressed both our alternative constructions as well as the district court’s constructions”).

We accordingly address construction of the following claim recitations, and determine that no further express constructions are required for purposes of this Decision. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (“[W]e need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy.’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

1. “device fingerprint”

Independent claim 1 recites a “device fingerprint,” which Petitioner contends should be construed as “a bit string (or bit array) that uniquely identifies the device, which includes or is derived from both user-configurable and non-user-configurable data specific to the remote computing device.” Pet. 9 (citing Ex. 1002 ¶ 50). This proposed construction differs from the construction adopted by the district court, which instead construed “device fingerprint” as “a bit string (or bit array) that substantially uniquely identifies a device and that includes (or is derived from) user-configurable data and non-user-configurable data specific to the device.” Ex. 2001, 57–62 (preliminary construction by magistrate judge); Ex. 2002 (adoption of preliminary construction by district judge).

Both Petitioner’s and the district court’s constructions require that the bit string or array include or be derived from both “user-configurable” and “non-user-configurable” data specific to the device. In particular, in adopting its construction, the district court agreed, as do we, that the specification of the ’954 patent and its prosecution history “discuss[] using user-configurable data and non-user-configurable data to make a device fingerprint.” Ex. 2001, 59 (citing Ex. 1001, 7:24–44; Ex. 1004, 149–150).

The principal difference in the constructions is that Petitioner’s proposal requires that the bit string or array “uniquely identifies” the device, while the district court’s adopted construction requires only that the bit string or array “substantially uniquely identifies” the device. On this point, the district court observed that “[t]he specification also refers to this data string being ‘unique,’” and further noted that the specification of the ’954 patent “explains that ‘unique’ does not refer to absolute uniqueness but

rather a probability of uniqueness.” *See id.* at 59, 61. In particular, the specification states that “the *desired degree of uniqueness* may be set to a practical level such as 99.999999% or higher, to achieve a *probability* of less than 1 in 100,000,000 that any two remote computing devices will generate identical fingerprints.” Ex. 1001, 7:51–55 (emphases added).

We apply the same claim-construction standard as the district court, and we agree with the court’s analysis. Accordingly, we construe “device fingerprint” in the same manner as the district court, i.e., as “a bit string (or bit array) that substantially uniquely identifies a device and that includes (or is derived from) user-configurable data and non-user-configurable data specific to the device.”

2. “*an address of a separate device specified by the customer*”

Independent claim 1 recites “sending . . . a notification of the request to an address of a separate device specified by the customer.” Ex. 1001, 12:19–23. In deciding whether to institute this proceeding, we applied a preliminary construction of this phrase as “an address of a separate device, the separate device having been specified by the customer.” Dec. 15–18. Patent Owner agrees that this is the “correct construction.” PO Resp. 14. In contrast, Petitioner “stands by” the construction advocated by its Petition, namely that the phrase refers to “an address specified by the customer, where the address is for a separate device.” Reply 3; Pet. 10. That is, the disagreement between the parties is whether the claim language requires that the *address* of the separate device be specified by the customer rather than requiring specification of the *separate device* itself.

Although we have reconsidered our preliminary construction in light of the parties' further arguments, we adopt that preliminary construction for this Final Written Decision and conclude that the claims require specification of the *separate device* by the customer. In doing so, we note that this is the same construction arrived at by the district court under the same claim-construction standard that we apply. Ex. 2001 (preliminary construction by magistrate judge), 62–65; Ex. 2002 (adoption of preliminary construction by district judge).

First, we agree with the district court that “the most natural reading of the disputed term is that the phrase ‘specified by the customer’ modifies the closest noun phrase, namely ‘a separate device.’” Ex. 2001, 64. In addition, the district court noted that dependent claim 20 of the '954 patent “reinforces this natural reading because Claim 20 relies on Claim 1 for antecedent basis for ‘the customer-specified separate device.’” *Id.*; see Ex. 1001, 14:42–44. We also note the specific distinction between claim 20's recitation and that of independent claim 15, which recites “a customer-specified address.” Ex. 1001, 13:35–36. Viewed together, the set of claims thus specifically distinguishes between a customer-specified address and a customer-specified separate device.

Petitioner observes that the specification of the '954 patent includes references to a “customer-specified address,” a fact acknowledged by the district court in the Texas litigation proceeding. See Pet. 10–11; Ex. 2001, 64; see also Ex. 1001, 2:13–24, 4:57–5:9, 5:62–6:1, 6:16–19, 6:34–40 (each referring to a “customer-specified address”). But as the district court observed, the specification also “use[s] ‘customer-specified’ with reference

to a ‘device’ or a ‘system.’” Ex. 2001, 64 (citing Ex. 1001, 3:39–43, 5:41–43, 5:48–49, 8:30–32).

We also agree with the district court that, “even if [Petitioner] were correct that the specification only referred to a ‘customer specified address,’ ‘it is improper to read limitations from a preferred embodiment described in the specification—even if it is the only embodiment—into the claims absent a clear indication in the intrinsic record that the patentee intended the claims to be so limited.’” Ex. 2002, 2 (quoting *Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 913 (Fed. Cir. 2004)). Petitioner has identified no such indication in the intrinsic record.

In addition to these considerations, we find that the prosecution history more strongly supports the district court’s construction than Petitioner’s proposed construction. As noted in our summary of the prosecution history above, the claim language was amended during prosecution from reciting “to a customer-specified address” to reciting “to an address of a separate device specified by the customer.” See Ex. 1004, 45. Such amendment addressed the Examiner’s concerns that the original claim language did not support the Applicant’s patentability arguments because it did not recite “a separate device specified by the consumer” and did not recite “sending alert notifications to separately specified user devices.” *Id.* at 52. In the context provided by those concerns, it appears that the amendment shifted claim scope to encompass the separate device being specified by the customer, rather than the address being specified by the customer. Indeed, even Petitioner characterizes that prosecution history as involving an amendment “to specify that the device is customer-specified.” Pet. 11 (citing Ex. 1004, 45).

Accordingly, we adopt a construction of “an address of a separate device specified by the customer” as “an address of a separate device, the separate device having been specified by the customer.”

3. *“determining whether the device fingerprint matches any of a number of device fingerprints previously authorized to access the customer account information”*

Independent claim 1 recites “determining whether the device fingerprint matches any of a number of device fingerprints previously authorized to access the customer account information.” Ex. 1001, 12:15–18. Petitioner proposes that the phrase be construed as “determining whether the device fingerprint matches any of the device fingerprints on the whitelist of devices previously authorized to access the customer account information.” Pet. 12 (citing Ex. 1002 ¶ 56). But as Patent Owner observes, in considering construction of this phrase, the district court identified multiple flaws with Petitioner’s proposed construction. PO Resp. 15.

The district court noted that Petitioner’s proposed construction replaces “a number of” with “the,” such that the “determining” step would thereby “involve *all* of the recited device fingerprints.” Ex. 2001, 66. We agree with the district court that Petitioner’s proposed construction “cannot be reconciled with the plain meaning of ‘a number of’ as meaning some number of, not necessarily all.” *Id.* In addition, we agree with the district court’s further conclusion that Petitioner “fails to demonstrate any need or purpose for introducing the technical term ‘whitelist,’ which would tend to confuse rather than clarify the scope of the claims.” *Id.* at 68. That conclusion was based on a careful analysis of that portion of the prosecution

history identified by Petitioner, which relied on the claim language itself and which the district court found “is readily understandable on its face.” *Id.*

Although we reject Petitioner’s proposed construction for the “determining” limitation in favor of the plain and ordinary meaning of that limitation, we nevertheless disagree with Patent Owner’s contention that Petitioner’s advocacy for that construction is fatal to Petitioner’s position. Like the “address” limitation discussed above, Petitioner provides analysis both under its proposed construction and under the plain-and-ordinary meaning adopted by the district court. *See* Pet. 41–44.

For the “determining” limitation, we accordingly do not find it necessary to expressly construe the term.

4. *“identifying . . . the remote computing device fingerprint and by a requesting location”*

Independent claim 1 recites “identifying . . . the remote computing device fingerprint and by a requesting location.” Ex. 1001, 12:12–14. During the preliminary phase of this proceeding, we adopted Petitioner’s proposal to insert the words “by a device” as follows: “identifying . . . the remote computing device *by a device* fingerprint and by a requesting location.” Dec. 18 (citing Pet. 11). On its face, the “identifying” limitation is grammatically awkward, and Petitioner explains that its proposal “clarifies the apparent erroneous deletion of ‘by a device’ because ‘by a device’ was present in claim 1 as originally filed.” Pet. 11–12 (citing Ex. 1004, 568). Petitioner’s contention is consistent with our independent review of the prosecution history. *See supra* n.1. Patent Owner “does not take a position on this issue,” and we adopt Petitioner’s proposed construction for this Final

Written Decision. See PO Resp. 16. In particular, we find support for Petitioner’s proposed construction in the standard for correction of errors.

A district court may “correct an error in a patent by interpretation of the patent where no certificate of correction has been issued . . . only if (1) the correction is not subject to reasonable debate based on consideration of the claim language and the specification and (2) the prosecution history does not suggest a different interpretation of the claims.” *Novo Indus., LP v. Micro Molds Corp.*, 350 F.3d 1348, 1354 (Fed. Cir. 2003); see also *CBT Flint Partners, LLC v. Return Path, Inc.*, 654 F.3d 1353, 1358 (Fed. Cir. 2011) (holding obvious errors in a claim may be corrected in construing the claim). As we stated in our Institution Decision, see Dec. 18–19, the Board has applied this same standard in Board proceedings. *E.g.*, *Research Prods. Corp. v. Honeywell Int’l Inc.*, IPR2018-00976, Paper 6 at 13 (PTAB Nov. 7, 2018); *Apple Inc. v. Achates Reference Publ’g, Inc.*, IPR2013-00080, Paper 22 at 10–12 (PTAB June 3, 2013); *Fitbit, Inc. v. Valencell, Inc.*, 2020 WL 3815662 at *6 (Fed. Cir. July 8, 2020) (explaining that “there is foundation for such authority [of the Board to correct errors] in the America Invents Act . . . and precedent has provided guidelines for district courts to correct errors in issued patents,” and holding it was error not to correct a “conspicuous” and undisputed error related to antecedent basis). Further, “[t]he preferable agency action is to seek to serve the agency’s assignment under the America Invents Act, and to resolve the merits of patentability.” *Fitbit*, 2020 WL 3815662 at *6. But “courts may not redraft claims, whether to make them operable or to sustain their validity.” *Chef Am., Inc. v. Lamb-Weston, Inc.*, 358 F.3d 1371, 1374 (Fed. Cir. 2004). The burden is on Petitioner to show

that a claim contains the kind of error that may be corrected in construing the claim. 37 C.F.R. § 42.20(c).

In this instance, we agree with Petitioner that the form of the “identifying” limitation in the issued patent results from an evident error and that Petitioner’s proposed construction is supported by the specification. Pet. 12 (citing Ex. 1001, 10:7–20, Fig. 7). Petitioner’s proposed construction is therefore a reasonable construction of the claim language. Furthermore, the district court also adopted such a construction, to which the parties agreed. *Id.*; Ex. 2001, 9. Accordingly, we adopt Petitioner’s proposed construction for this Final Written Decision.

D. Scope and Content of the Prior Art

1. Steinberg

Steinberg describes “improved authentication of interacting parties comprising the use of two or more forms of authentication, each of which uses at least two methods of authenticating users.” Ex. 1005 ¶ 44. Figure 11A of Steinberg is reproduced below.

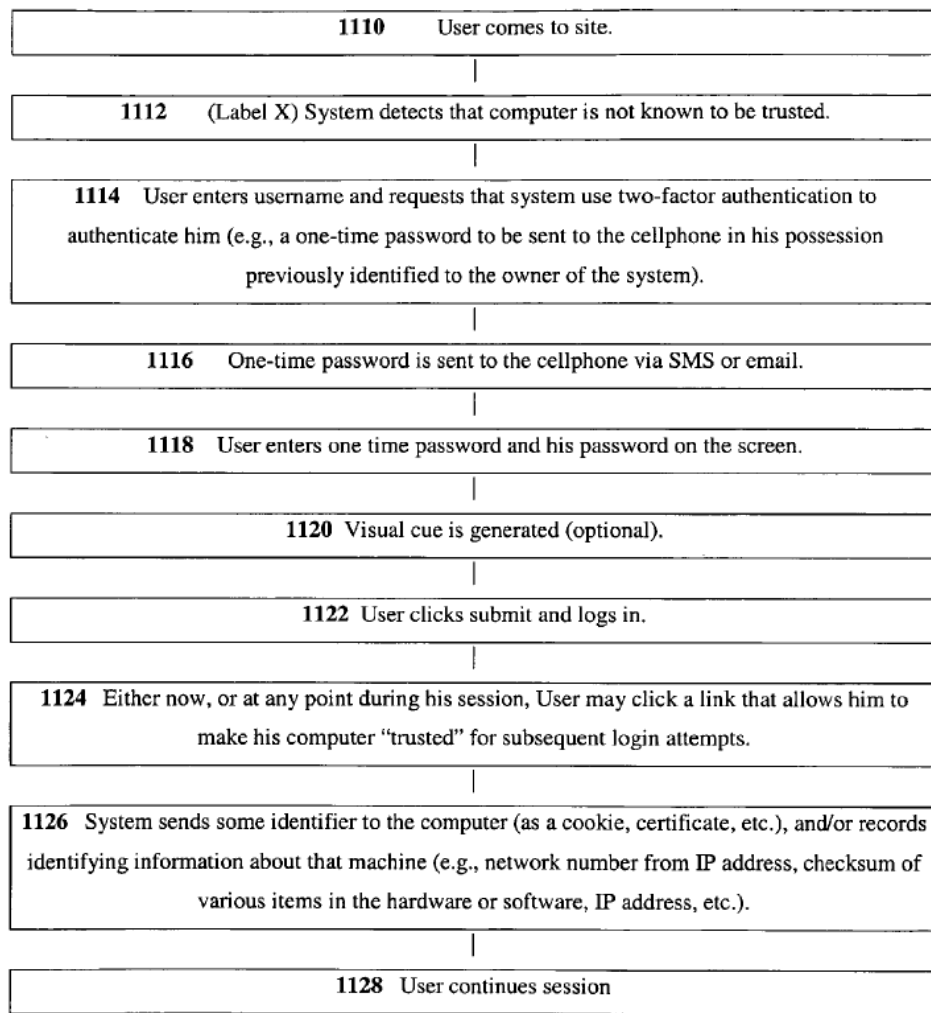


FIG. 11A

Figure 11A depicts an exemplary process flow described by Steinberg. *Id.* ¶ 48. When a user visits a site at step 1110 and logs into a system that does not recognize the user's computer as known to be associated with the user at step 1112, two-factor authentication is initiated. *Id.* Thus, at step 1114, the user enters a username and "he asks for a one-time password to be sent to the cell phone in his possession previously identified to the owner of the system." *Id.* At step 1116, a one-time password is sent to the cell phone so that the user may enter it with his password at step 1118 to log in at step 1112 (with a visual cue optionally generated at step 1120). *Id.*

At some time during the logged-in session, the user may identify his computer as “trusted” for subsequent login attempts, as indicated at step 1124. *Id.* Thereafter, the system sends an identifier, such as in the form of a cookie or certificate, to the user’s computer at step 1126, with the user continuing the session at step 1128. *Id.*

2. Oberheide

Oberheide relates “specifically to a new and useful system and method of notifying mobile devices to complete transactions in the digital security field.” Ex. 1006 ¶ 2. Figure 1 of Oberheide is reproduced below.

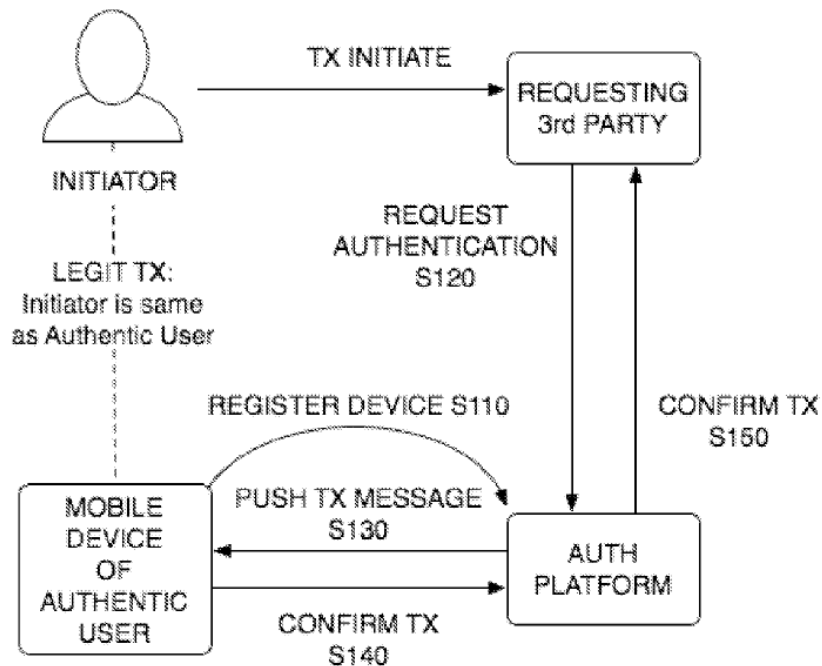


FIGURE 1

Figure 1 illustrates a method for authenticating a transaction. *Id.* ¶ 4. Six steps are illustrated in the drawing: (1) registering an “authority device” for an account on an “auth platform” at step S110; (2) receiving a transaction request from an initiator to the auth platform at step S120; (3) messaging the

authority device with the transaction request at step S130; (4) receiving an authority agent response from the authority device to the auth platform at step S140; and, if the authority agent response confirms the transaction, (5) communicating a confirmed transaction to the initiator at step S150; or, if the authority agent response denies the transaction, (6) communicating a denied transaction to the initiator at step S152. *Id.* ¶ 9.

Two points with respect to this authentication method are relevant to Petitioner’s challenges. First, registration step S110 “preferably occurs prior to a transaction request, and is preferably performed during an initial setup of an account on the auth platform.” *Id.* ¶ 11. Second, the “authority device,” which may be a “mobile device” such as a mobile phone, is notified by SMS (i.e., short message service) when the transaction request is received from the initiator by the auth platform at step S120. *Id.*

3. McDowell

McDowell “relates to a system and method of verifying transactions to reduce fraud.” Ex. 1008 ¶ 2. The system and method allow consumers to register devices used to conduct transactions with a verification system. *Id.* ¶ 22. Figure 1 of McDowell is reproduced below.

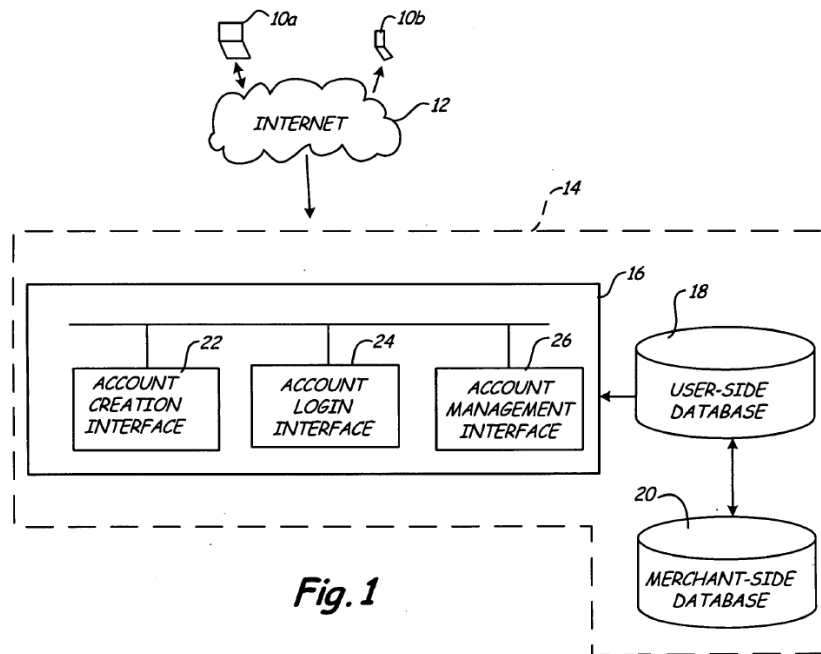


Fig. 1

Figure 1 is a block diagram illustrating communication between user devices 10a and 10b, Internet 12, and user-side verification system 14, which includes user-side server 16, user-side database 18, and merchant-side database 20. *Id.* ¶ 25. User-side server 16 includes account creation interface 22, account login interface 24, and account management interface 26. *Id.* “[U]ser-side server 16 may store and communicate webpages or interfaces . . . to user devices 10a and 10b, allowing a user to enter information via the interface and communicate the information back to user-side server 16 for parsing.” *Id.* ¶ 28. “[U]ser-side database 18 stores information related to an account created by a user that is responsible for storing entity data, device identifiers, as well as account related information such as username/password, user-selected means of notification, device type (e.g., computer, cell phone, cell phone brand, etc.), etc.” *Id.* ¶ 25. “Merchant-side database [20] stores entity/device pairs and receives verification requests from requesting servers (e.g., merchants, third-parties,

etc.) that include entity/device pairs with which the merchant-side database compares with stored values to verify transactions.” *Id.*

4. *Yasushi*

Yasushi is related to login verification. Ex. 1009 ¶ 6 (“The aim of this invention is to provide a server, method and program not only enabling easy recognition by the user themselves of the occurrence of unlawful login, but also enabling the performance of secure verification of the subject, in respect of the operations of a login lock thereafter.”). In *Yasushi*’s system, a “notification mail” is generated in response to receipt of a login request. *Id.* ¶ 8. A server “transmits [the] notification mail including a message notifying said user to the mail address of the user themselves from whom there was a login request.” *Id.* ¶ 9.

Figure 6⁶ of *Yasushi* is reproduced below.

⁶ Petitioner erroneously refers to this drawing as “Figure 13,” but *Yasushi* includes only seven drawings. See Pet. 77–78.

[Figure 6]

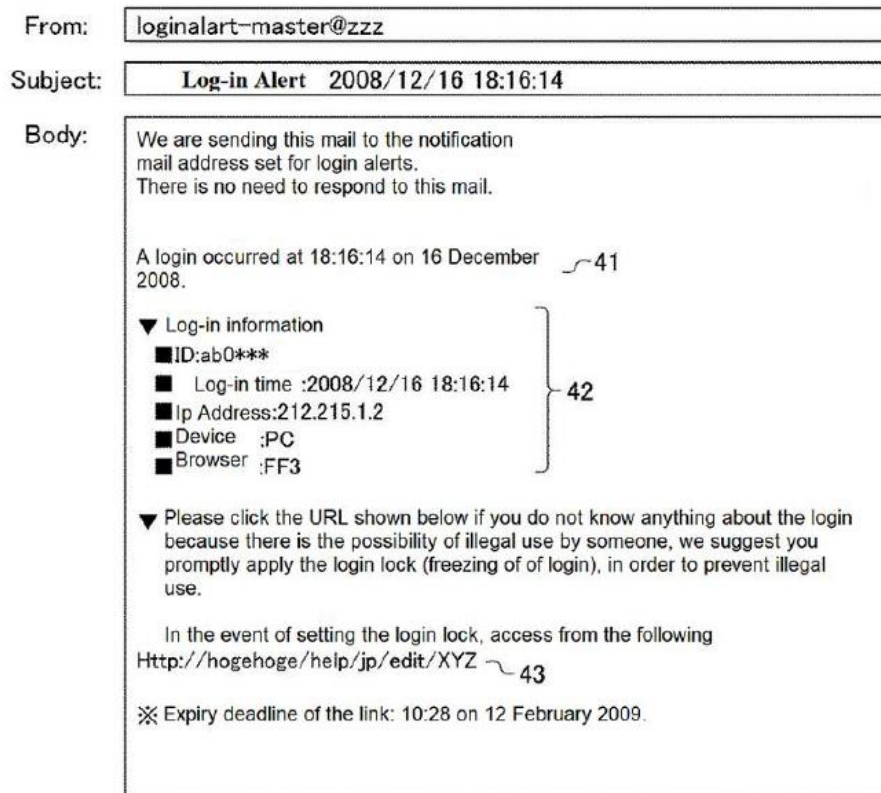


Figure 6 provides an example of Yasushi’s “notification mail.” *Id.* ¶ 33.

E. Combination of Steinberg and Oberheide

Petitioner challenges claims 1–4, 6, 12, and 14 as unpatentable under 35 U.S.C. § 103(a) over Steinberg and Oberheide. Pet. 14–70.

1. Independent Claim 1

Petitioner provides a detailed analysis that relies generally on the steps identified in Figure 7 of Steinberg, reproduced above, as meeting the steps performed by the customer notification program recited in independent claim 1. See Pet. 14–70. For certain aspects of this claim, Petitioner

additionally relies on Oberheide, contending that one of ordinary skill in the art would have combined the teachings of Steinberg and Oberheide because both references “relate to authorizing, in a networking context, a requested access or transaction.” *Id.* at 26. Supported by the testimony of Dr. Monroe, Petitioner contends that, because both references are “in the same or similar technical field,” a person of ordinary skill in the art would have had reason to consider Oberheide’s teachings when implementing Steinberg’s system. *Id.* (citing Ex. 1002 ¶ 102). Patent Owner does not dispute Petitioner’s reasoning for effecting the combination, *see generally* PO Resp. 26–33, and we credit Dr. Monroe’s uncontroverted testimony on this point in concluding that Petitioner articulates persuasive reasoning, supported by rational underpinning, for the combination. In discussing specific limitations below, particularly the “sending” limitation, we address Petitioner’s reasoning in greater detail.

a. Preamble

The preamble of independent claim 1 recites a “system for authorizing a request for remote access to customer account information.” Ex. 1001, 12:2–3. In addressing the preamble, Petitioner observes that Steinberg “discloses that in response to a user ‘attempt[ing] to access a [web] site’ . . . , one of several actions is taken, including ‘allowing access [or] blocking access.’” Pet. 14 (quoting Ex. 1005 ¶¶ 46, 65) (alterations by Petitioner). Petitioner further identifies multiple drawings of Steinberg, and their associated discussion, as supporting its position that Steinberg discloses the preamble, particularly that Steinberg’s users are “customers” and that Steinberg’s accounts contain “customer account information.” *Id.* at 15–21.

We agree, and Patent Owner does not dispute, that Steinberg discloses a “system for authorizing a request for remote access to customer account information.” *See generally* PO Resp. 26–33. Because we find that the preamble of independent claim 1 is thereby disclosed by Steinberg, we need not address whether the preamble is limiting.

b. “server”

Claim 1 further recites that the system comprises “a server configured to receive the request via a network from a remote computing device.” Ex. 1001, 12:4–5. For this limitation, Petitioner contends that Steinberg discloses such a server or, alternatively, that it would have been obvious to a person of ordinary skill in the art in light of Steinberg and Oberheide. Pet. 21–28.

With respect to Steinberg, Petitioner observes that the system is described in terms of the Internet and an illustrative depiction that involves a user visiting a web site requiring authentication. *Id.* at 21–25. Petitioner relies on uncontested testimony by Dr. Monroe to support its inference that Steinberg’s web site is thereby “implemented with a web server configured to receive a request via a network from the user’s remote computing device using a web browser.” *Id.* at 23–24 (citing Ex. 1002 ¶ 96).

With respect to Petitioner’s alternative position involving the combination of Steinberg and Oberheide, Petitioner observes that Oberheide describes its auth platform as an “internet accessible server” that “communicates with a client of an initiating agent (‘remote computing device’) to initiate the transaction request.” *Id.* at 27 (citing Ex. 1006 ¶ 10, Fig. 2). Petitioner reasons that a person of ordinary skill in the art would

thus have been motivated to configure Steinberg’s system to implement a server configured to receive the request via a network from a remote computing device. *Id.* at 28 (citing Ex. 1002 ¶ 104). Uncontroverted testimony by Dr. Monroe supports Petitioner’s contention that such an implementation would have been “nothing more than the combination of known components and technologies, according to known methods, to produce predictable results.” *Id.* (citing Ex. 1002 ¶ 105).

Patent Owner does not dispute Petitioner’s reasoning with respect to either its principal position relying exclusively on Steinberg or its alternative position relying on the combination of Steinberg and Oberheide, *see generally* PO Resp. 26–33, and we find Petitioner’s showing persuasive with respect to this limitation for both of Petitioner’s alternative positions. Ex. 1005 ¶¶ 45, 46; Ex. 1006 ¶ 10; Ex. 1002 ¶¶ 93–105.

c. “database”

Independent claim 1 recites that the system also includes “a database storing the customer account information accessible by the server.” Ex. 1001, 12:5–6. Petitioner contends that such a database is disclosed or suggested by the combination of Steinberg and Oberheide. Pet. 29–31. In doing so, Petitioner observes that Steinberg discloses a “database” that stores data corresponding to a user. *Id.* at 29 (citing Ex. 1005 ¶¶ 25, 26, 50, 51, 66; Ex. 1002 ¶ 106). In addition, Petitioner reasons, in a manner similar to that discussed above for the preamble, that such data are customer account information, and supports that reasoning with testimony by Dr. Monroe. *Id.* at 29–30; Ex. 1002 ¶ 106.

With respect to the limitation’s required accessibility “by the server,” Petitioner further reasons that a person of ordinary skill in the art “would have been motivated to configure *Steinberg*’s database to store customer account information accessible by the server of the combined *Steinberg-Oberheide* system, because having such information be accessible by the server would have predictably enabled processing of such information by the server.” Pet. 31. Dr. Monroe’s testimony supports this reasoning, particularly his assertion that a skilled artisan “would have recognized that configuring data of a database to be accessible to a server was a basic architectural principle for a computer system having a server, especially in the context of web servers.” Ex. 1002 ¶ 110 (citing Ex. 1008 ¶¶ 25, 28, 35).

We find this evidence and reasoning persuasive, and Patent Owner does not dispute this aspect of Petitioner’s analysis. *See generally* PO Resp. 26–33. We thus conclude that Petitioner makes a persuasive showing with respect to the “database” limitation. Ex. 1005 ¶¶ 25, 26, 50, 51, 66; Ex. 1002 ¶¶ 106–111.

d. “memory”

Independent claim 1 recites that the system also includes “memory accessible by the server and storing a customer notification program,” with the program performing a number of steps “when executed by the server.” Ex. 1001, 12:9–11. In addressing this “memory” limitation, Petitioner observes that Steinberg discloses that its process be implemented in “executable code.” Pet. 32 (citing Ex. 1005 ¶¶ 23 (“executable code implementations”), 44 (“At its broadest level, the present invention comprises . . . novel executable code that may be used on computer based

systems as known in the art of security and authentication.”)). Dr. Monroe testifies that a person of skill in the art would have understood such disclosure as “disclosing a computer program that is stored in memory and executed by the server of *Steinberg*’s system.” Ex. 1002 ¶ 112. Petitioner additionally reasons that it would have been obvious specifically to implement a “customer notification program” in light of Oberheide’s disclosure of a push notification service:

[A person of ordinary skill in the art] would have been motivated to configure the server in the combined *Steinberg-Oberheide* system to include memory accessible by the server for storing a customer notification program which, when executed by the server, performs steps for various functions relating to the access request.

Pet. 34 (citing Ex. 1002 ¶¶ 117–119). Although we agree with this reasoning, which is not contested by Patent Owner, we note that the specific steps recited in the claim, and which we address more fully below, define the scope of the “customer notification program.”

We conclude that Petitioner provides persuasive evidence and reasoning to make a persuasive showing with respect to the “memory” limitation. Ex. 1005 ¶¶ 23, 44; Ex. 1005 ¶¶ 112–119.

e. “identifying”

The first of the five steps that independent claim 1 recites for the “customer notification program” is “identifying, responsive to the server receiving the request, the remote computing device [by a device] fingerprint and by a requesting location.” Ex. 1001, 12:12–14 (alteration in accordance with adopted claim construction discussed *supra*, § II.C.3.). Petitioner

reasons that, “because *Steinberg* discloses that the user’s computing device used for logging in is identified in response to the user coming to the site for the login request, the combined *Steinberg-Oberheide* system . . . discloses identifying the computing device in response to the server receiving the request.” Pet. 35 (citing Ex. 1002 ¶ 121). In advancing this reasoning, Petitioner addresses the “device fingerprint” and “requesting location” aspects of the limitation separately.

First, as discussed above, we construe “device fingerprint” as “a bit string (or bit array) that substantially uniquely identifies a device that includes (or is derived from) user-configurable data and non-user-configurable data specific to the device.” *See supra*, § II.C.1. Petitioner observes that “[t]he components of *Steinberg*’s device profile for identifying the user’s device include both user-configurable and non-user configurable data, such as the checksum of various items in the hardware or software, browser version, IP address, network number, time zone of device, and clock offset.” Pet. 36 (citing Ex. 1005 ¶¶ 46–48; Ex. 1002 ¶ 124). For instance, Petitioner identifies the “browser version” and “time zone,” which *Steinberg* discloses as among the “various properties to which future sessions can be compared,” as examples of “user-configurable data.” *Id.* at 35–36; Ex. 1005 ¶ 45.

Petitioner also identifies as examples of “non-user-configurable data” the IP address and checksum of various hardware items that *Steinberg* describes as used to record identifying information about a machine. Pet. 36; Ex. 1005 ¶ 48. In support of this identification, Dr. Monroe testifies that “[a] person of ordinary skill in the art would have known that a computing device’s hardware, e.g., a computer processor’s serial number or

the MAC address assigned to a device, can be fixed (i.e., not user-configurable).” Ex. 1002 ¶ 123.

Petitioner reasons, supported by Dr. Monroe’s testimony, that “[c]ombining both types of properties (user-configurable and non-user-configurable) would have provided a robust identifier for the device, and this would have been a straightforward extension of generating the one or more components of the device profile.” Pet. 39. In addition, Petitioner reasons, also supported by Dr. Monroe’s testimony, that one or more components of Steinberg’s device profile are stored as a bit string because “[t]he collection of various identifying information of the user’s device that are recorded and stored in a device profile on *Steinberg’s* system discloses values that, like any other value stored in a computer system, are represented electronically as a string of one or more binary digits (e.g., ‘0’'s and ‘1’'s).” *Id.* at 37–38 (citing Ex. 1002 ¶ 126). Patent Owner does not dispute these aspects of Petitioner’s analysis. *See generally* PO Resp. 26–33.

Second, for the “requesting location,” Petitioner observes that Steinberg discloses identifying the geolocation of a device requesting access and that “[a] user can be authenticated based on the fact that a device he is known to carry [i.e., a trusted device verification] is **in the location from which he is currently accessing the system.**” Pet. 40 (quoting Ex. 1005 ¶ 45 (alterations by Petitioner), citing Ex. 1005 ¶ 44, claims 19, 38, Fig. 11F; Ex. 1002 ¶¶ 132–133). Petitioner supports its contention that Steinberg thus discloses identifying the remote computing device by a requesting location with testimony by Dr. Monroe. Ex. 1002 ¶¶ 133.

In addition to supporting its separate contentions that Steinberg discloses identifying the remote computing device by a device fingerprint

and that Steinberg discloses identifying the remote computing device by a requesting location, Petitioner addresses the limitation's requirement of using *both*. See Pet. 41. Specifically, Dr. Monroe testifies that “a person of ordinary skill in the art would have recognized that the requesting location can be used to identify the device separately from the device profile (‘device fingerprint’).” Ex. 1002 ¶ 134. This leads Dr. Monroe to conclude that such a skilled artisan “would have found it foreseeable to identify the computing device seeking access by its requesting location in addition to identification by the device profile (‘device fingerprint’).” *Id.* ¶ 135. Petitioner relies on this testimony to argue that the proposed implementation of using both the device fingerprint and requesting location “would have been a mere combination of known components, according to known methods, to produced predictable results.” Pet. 41 (citing *KSR*, 550 U.S. at 416).

Patent Owner does not dispute Petitioner's analysis of the “identifying” limitation, *see generally* PO Resp. 26–33, and we conclude, in light of the above discussion, that Petitioner makes a persuasive showing. Ex. 1005 ¶¶ 45–48; Ex. 1002 ¶¶ 120–135.

f. “determining”

The second of independent claim 1's five steps executed by the “customer notification program” is “determining whether the device fingerprint matches any of a number of device fingerprints previously authorized to access the customer account information.” Ex. 1001, 12:15–18. Building on its analysis of the “identifying” limitation, Petitioner observes that Steinberg discloses that a computer may be considered

“trusted” after it has been authorized to log in, as illustrated at step 1124 of Steinberg’s Figure 11, reproduced above. Pet. 42–43 (citing Ex. 1005 ¶ 48). The section of Steinberg cited by Petitioner also discloses making use of such “trusted” status for a subsequent log-in attempt by “check[ing] that the user is accessing from [a] trusted device” by comparing the “identifying information about that machine (e.g., network number from IP address, checksum of various items in the hardware or software, IP address, etc.” with stored information. Ex. 1005 ¶ 48.

As explained above, in its analysis of the “identifying” limitation, Petitioner drew a correspondence between such identifying information about the machine and the generation of a device fingerprint for the machine. In light of Steinberg’s further disclosure of using “trusted” status for subsequent log-in attempts, Petitioner reasons that, “in the context of authenticating a user making an access request, *Steinberg* discloses determining whether a computer’s profile matches any of a number of profiles known for a user, and further discloses matching a device identifier to a user.” Pet. 42 (citing Ex. 1002 ¶ 136). Patent Owner does not contest Petitioner’s showing with respect to this element. *See generally* PO Resp. 26–33.

We conclude that Petitioner has identified persuasive disclosure of the limitation by Steinberg. Ex. 1005 ¶ 48; Ex. 1002 ¶¶ 136–140.

g. “sending”

The third step recited by independent claim 1 for the “customer notification program” is “sending, responsive to determining a mismatch between the device fingerprint and each of the previously authorized device

fingerprints, a notification of the request to an address of a separate device specified by the customer, the notification indicating (i) the request, (ii) identity of the remote computing device, and (iii) the requesting location.” Ex. 1001, 12:19–25. Petitioner addresses this limitation in two parts, namely the requirement of sending a notification and the details of what the notification indicates.

i. Sending a Notification

For the aspect of the “sending” limitation that requires a notification be sent “to an address of a separate device specified by the customer,” Petitioner points to Steinberg’s disclosure addressing “the risk of man-in-the-middle attacks and similar attacks.” Pet. 44–47 (citing, *inter alia*, Ex. 1005 ¶ 53). In the cited section, Steinberg provides the following description:

Specifically, these techniques may comprise the following: (1) sending a warning message (via email, instant messenger, SMS, or [through] another channel of communication) that may be visible, audible, or otherwise sensed and may be in the form of either in a one-time-password message, through some signal on a user’s screen, speakers, via telephone or other device, or separately to a user when access is attempted from an unrecognized device (or a device recognized, but not recognized as belonging to the particular user whose credentials were used), such that the invention would include sending this message in situations in which the correct username of a user was sent, but not the correct password, or in situations in which the correct username and password for a user are submitted, or in other scenarios where a “risky” situation may have occurred; or (2) presentation of a visual, audible, or otherwise easily recognizable cue to users and the presentation is only performed when users login in from either a machine with a trusted user or a device from which they themselves are trusted.

Ex. 1005 ¶ 53. According to Petitioner, this discloses “send[ing] an out-of-band communication (e.g., warning notification) to an address specified by the customer (e.g., a phone number or email address), where the address is for a separate device.” Pet. 46–47. Although we agree with Petitioner’s characterization of Steinberg’s disclosure, this aspect of Petitioner’s argument does not support Petitioner’s position under the claim construction we adopt because it is directed at the *address* being specified by the customer, rather than the *separate device*. See *supra*, § II.C.2 (construing “an address of a separate device specified by the customer” as “an address of a separate device, the separate device having been specified by the customer”).

Petitioner provides further argument, though, that the same disclosure is sufficient also to meet our applied construction:

For at least the same reasons, the combined *Steinberg-Oberheide* system discloses sending the out-of-band communication to an address of a separate device, *the separate device* having been specified by the user (“customer”) (and thus also meets the district court’s preliminary construction . . .), because the cell phone of *Steinberg*’s user is a separate device and has been specified by the user.

Pet. 47 (citations omitted). In light of this argument, we disagree with Patent Owner’s assertion that “[t]he Petition offers no theory for how the cited disclosure in Steinberg concerning either *a phone number* or *an e-mail address* maps onto ‘a separate device specified by the customer.’” PO Resp. 18. Rather, Petitioner’s alternative position that a cell phone may be identified by the phone number associated with that cell phone is supported by both the express teachings of the prior art and Dr. Monroe’s testimony,

which is not controverted by any contrary expert testimony offered by Patent Owner. *See* Reply 1.

First, with respect to Steinberg’s express disclosure, Petitioner identifies repeated references in which Steinberg refers to a cell phone as having been specified by a customer. *See id.* at 6–7. For example, in describing Figure 11A of Steinberg, reproduced above, Steinberg explains that the two-factor authentication identified of step 1114 sends a one-time password to the “*cell phone . . . previously identified to the owner of the system.*” Ex. 1005 ¶ 48 (emphasis added); *see also id.* ¶ 49 (same in the context of Figure 11B). This is, moreover, consistent with Steinberg’s summary characterization of such two-factor authentication as “entail[ing] the sending of a one-time password to a *pre-agreed cellphone* via SMS or via email.” *Id.* ¶ 45 (emphasis added). In addition, Petitioner notes that Steinberg “relies on the physical cell phone to enable certain location-based functionality even apart from [these] disclosures.” Reply 7 (citing Ex. 1005 ¶ 45).

Second, Dr. Monroe specifically testifies that “a person having skill in the art would have understood that the cell phone of *Steinberg’s* user . . . is a separate device and has been specified by the user in order for the user to receive the out-of-band communication.” Ex. 1002 ¶ 145. Patent Owner urges that we disregard such testimony: “The declaration of Dr. Monroe is unavailing and should be afforded no weight because it simply copies (quite literally verbatim, including which words are italicized) the same erroneous claim construction and the same tainted reasoning set forth in the Petition.” PO Resp. 25. But as we noted in the Institution Decision, “Dr. Monroe’s Declaration differs from Petitioner’s argument through specific assertion of

his opinion that *a person of skill in the art would have understood* Steinberg’s cell phone to have been a separate device specified by the customer.” Dec. 27 (citing Ex. 1002 ¶ 145). Although we indicated that “[s]uch an opinion can be meaningfully explored through cross-examination during trial” and that “the record would benefit from evidentiary development of this issue,” *id.*, Patent Owner declined to offer cross-examination testimony of Dr. Monroe. See Reply 8 (“Uniloc has not established any basis for doubting Dr. Monroe’s credibility: it offers no expert testimony of its own, no cross-examination testimony, and indeed no evidence at all.”). We accordingly credit Dr. Monroe’s testimony as to how a person of ordinary skill in the art would have understood Steinberg’s disclosure.

Although Patent Owner contends that “[a] cell phone number allegedly ‘associated with’ a cell phone is insufficient under the claim language and intrinsic evidence,” the ’954 patent is notably similar in its description of requiring that the notification be sent “to an address of a separate device specified by the customer.” See PO Resp. 27. Specifically, the ’954 patent explains that a “customer-specified system” is “a system located at or associated with the customer-specified address.” Ex. 1001, 8:30–32. And the ’954 patent explains that “when the customer-specified address is a telephone number, the customer-specified system can include a mobile phone and a computer.” *Id.* at 9:36–39. The specification thus describes specification of a telephone number that is “associated with” a cell phone to specify the separate device, just as in Steinberg. Accordingly, we find the relied-upon teachings of Steinberg consistent with the meaning the

'954 patent's specification provides for the recited "to an address of a separate device specified by the customer."

As we noted in the Institution Decision, "it is not apparent how the '954 patent otherwise contemplates that a customer could specify the separate device." Dec. 27–28. In response to our observation in the Institution Decision that "Patent Owner provides no alternative mechanism supported by the intrinsic record for us to consider," *id.*, Patent Owner contends that "the '954 patent does indeed provide at least one such alternative mechanism, such as by previously storing a device fingerprint of a device as being an authorized device fingerprint." PO Resp. 29 n.4 (citing Ex. 1001, 2:21, 4:59, 11:41–46). We explored this contention at some length during the oral hearing. *See, e.g.*, Tr. 28:9–30:4, 31:11–42:14. In elaborating on this contention, Patent Owner described an example involving multiple "iterations" of a customer requesting remote access to customer account information. *See id.* at 36:9–37:14.

In this example, according to Patent Owner, the first "iteration" occurs when a customer attempts to access customer account information using a device that has never been authorized to do so. *Id.* at 36:13–20. This might happen, for instance, when the customer uses a laptop that has never previously been used to access the customer account information. *See id.* at 41:14–15, 42:1–10 (Patent Owner agreeing that hypothetical corresponds to its position). After following the procedure described in the '954 patent and summarized above (such as by confirming authorization by the customer with a previously authorized device like the customer's cell phone), a device fingerprint for the previously unauthorized device (like the laptop) is stored at the server. *Id.* at 36:11–20, 41:15–20. The previously unauthorized

device (laptop) then becomes an authorized device, with the device fingerprint acting to identify the device. *Id.* at 36:21–37:2, 41:15–20. According to Patent Owner, the newly authorized device is a “device specified by the customer” based on the fingerprint of the device. *Id.* at 35:3–23, 38:18–20.

A second “iteration” occurs in this scenario when the customer later attempts to access the customer account information with a further unauthorized device (like a desktop computer). *Id.* at 36:21–37:3, 41:20–24. When a notification is sent to the first previously unauthorized device (laptop) in an effort to authorize the second unauthorized device (desktop), the claim language is met, according to Patent Owner, because the notification is sent to “an address of a separate device specified by the customer.” *Id.* at 41:20–42:10. Critical to Patent Owner’s theory is its position that, by relying on the device fingerprint to identify the device, this scenario provides for specification of the separate device by the customer without specifying the address.

We find Patent Owner’s multi-iteration scenario insufficient to discount the otherwise clear disclosure of the ’954 patent that a “customer-specified system . . . is a system located at or associated with the customer-specified address.” *See* Ex. 1001, 8:30–32. Patent Owner offers no expert testimony that a person of ordinary skill in the art would have understood the claim language to be referring to such a multi-iteration scenario, much less limited exclusively to such a scenario. And, as Petitioner points out, “[t]he ’954 patent variously discloses that a ‘server’ (Ex. 1001 at 5:11-13), a ‘remote computing device’ (*id.* at 8:6-7), or a ‘logic’ (*id.* at 9:20-22) stores a device fingerprint, but does not disclose that a customer specifies the

separate device using the fingerprint or how that would be accomplished.”
Reply 10–11.

To reiterate, there is no indication that Patent Owner’s multi-iteration scenario limits the specifying to a device fingerprint. That is, the claim only requires that the device be “specified by” the user, not that the device be specified by its fingerprint by the user. As discussed above, Steinberg describes the user specifying a singular device—“the cell phone in his possession previously identified to the owner of the system,” Ex. 1005 ¶ 48—and, therefore, teaches that limitation as detailed by Petitioner.

Patent Owner also contends that
public communications from the Federal Communications
Commission (“FCC”) show that a person of ordinary skill in the
art would **not** have, and should **not** have, accepted or
understood Steinberg’s mere cell phone number to also identify
a separate device specified by the customer, especially for
security purposes as a trusted device.

PO Resp. 31. To support this contention, Patent Owner provides a copy of a current FCC consumer guide to cell-phone fraud that warns of “SIM cloning fraud,” in which a scammer steals a cell phone’s electronic serial number (“ESN”) and mobile identification number (“MIN”) combinations to clone the user’s cell phone. Ex. 2007, 1. “After cloning,” the FCC guide warns, “both the legitimate and the fraudulent cell phones have the same ESN/MIN combination and cellular providers cannot distinguish the cloned cell phone from the legitimate one.” *Id.* In addition, Patent Owner provides an earlier FCC communication from the year 2002 that similarly warns against cell-phone cloning fraud. Ex. 2008.

Although Petitioner contends that at least the current FCC consumer guide is “unauthenticated” and “contains inadmissible hearsay,” we agree with Patent Owner that this government publication is self-authenticating and falls within the public-records exception to the hearsay rule. Reply 16; Sur-reply 18. But we do agree with Petitioner that Patent Owner “has not established that the document is relevant to the understanding of a [person of ordinary skill in the art] at the time of the alleged invention of the ’954 patent, much less to the understanding of *Steinberg*.” Reply 16–17. At best, Patent Owner’s additional evidence shows only that *fraud* may be used to evade what is otherwise confirmed by the ’954 patent, *Steinberg*, and Dr. Monroe’s testimony, namely that a person of ordinary skill in the art would have understood that a cell phone can be specified by a user with a cell-phone number.

Patent Owner’s argument that the cell-phone number does not “specify” a cell phone when there is an association of a cell-phone number with “multiple devices, such as a mobile phone and a computer,” is also unavailing. See PO Resp. 27–29 (citing Ex. 1001, 9:35–39). As Petitioner replies, “nothing in the claims . . . precludes a customer from specifying more than one device.” Reply 14. In addressing a variation of this argument made on the preliminary record, we indicated that “Patent Owner’s attorney argument is insufficient on the current record to overcome the evidentiary basis that undergirds Petitioner’s argument.” Dec. 26. The evidentiary record on this point has not been developed such that we reach a different conclusion now. That is, Petitioner supports its position with testimony by Dr. Monroe that “a person having skill in the art would have understood that the cell phone of *Steinberg*’s user (‘customer’) is a separate device and

has been specified by the user in order for the user to receive the out-of-band communication.” Ex. 1002 ¶ 145. We accord weight to Dr. Monroe’s uncontroverted testimony, particularly as inadequately counterbalanced by Patent Owner’s attorney argument.

In light of these various considerations, we conclude that Petitioner makes a persuasive showing with respect to the aspect of the “sending” limitation that requires a notification be sent “to an address of a separate device specified by the customer.”

ii. What the Notification Indicates

In addressing the specific content of the notification in the Steinberg-Oberheide combination, Petitioner observes that Steinberg discloses sending a “communication comprising information detailing the geolocation information (in the form of text or a map) that shows where the user is accessing a given application or site from so that the user can detect any fraudulent access.” Pet. 49 (quoting Ex. 1005 ¶ 53). Steinberg thus discloses that the notification includes at least an indication of the requesting location, and Petitioner relies on Oberheide as providing further details regarding an indication of the request itself and the identity of the remote computing device. *See id.* at 50.

Because Oberheide discloses that a user sends a reply confirming or denying a requested transaction, Petitioner reasons that “the request” is indicated by the notification. *Id.* at 51. In addition, because Oberheide discloses that the notification includes an “entity name” and IP address, Petitioner reasons that the “identity of the remote computing device” and “the requesting location” are also indicated. *Id.* at 52–53. Petitioner

supports these identifications and reasoning with testimony by Dr. Monroe. Ex. 1002 ¶¶ 154–157. Petitioner thus reasons that the elements required by claim 1 for the recited “notification of the request” are met by the combination of Steinberg and Oberheide, and that “[t]his would have been a predictable and straightforward configuration, because *Steinberg* discloses sending a warning message for security reasons in the context of an access request and because *Oberheide* similarly discloses alerting the user to transaction requests so that they can be confirmed or denied.” *Id.* at 53 (citing Ex. 1005 ¶ 53; Ex. 1006 ¶¶ 9, 13; Ex. 1002 ¶¶ 159–160).

This reasoning is persuasive and is not disputed by Patent Owner. *See generally* PO Resp. 26–33. We accordingly conclude that Petitioner makes a persuasive showing for all aspects of the “sending” limitation of independent claim 1.

h. “resolving”

The fourth of independent claim 1’s five steps executed by the “customer notification program” is “resolving the request responsive to a reply to the notification.” Ex. 1001, 12:26–27. Petitioner contends that Steinberg discloses that the system resolves the request when a user enters the one-time password that was sent to a pre-agreed (authorized) device into the currently unauthorized device. Pet. 53–54 (citing Ex. 1005 ¶ 48, Fig. 11A; Ex. 1002 ¶ 161). The request is resolved by Steinberg, according to Petitioner, when the one-time password and expected password match, such that the user is granted access with the unauthorized device. *Id.* (citing Ex. 1005 ¶ 48; Ex. 1002 ¶ 161). Petitioner supports this reasoning with uncontroverted testimony by Dr. Monroe. Ex. 1002 ¶ 161.

Petitioner additionally reasons that, to the extent Steinberg does not explicitly disclose resolving the request responsive to the reply to the notification, it would have been obvious to implement such a feature in view of Oberheide. Pet. 54–57. Petitioner specifically points to Oberheide’s approval or denial of a transaction based on a reply to the notification. *Id.* at 54–55 (citing Ex. 1006 ¶¶ 9, 14, 15, Figs. 1, 2; Ex. 1002 ¶ 164). Petitioner reasons, supported by testimony of Dr. Monroe, that such a feature “would have been a predictable way to improve security, and would have been a straightforward implementation,” in alignment with Steinberg’s expressed objective of increasing security by providing a warning message to a user regarding attempted access. *Id.* at 56 (citing Ex. 1005 ¶¶ 5, 44, 53; Ex. 1002 ¶¶ 165–167).

This aspect of Petitioner’s argument is not contested by Patent Owner, and we find Petitioner’s reasoning persuasive. We accordingly conclude that Petitioner makes a persuasive showing with respect to the “resolving” limitation under both of its alternative theories. Ex. 1005 ¶¶ 5, 44, 48, 53; Ex. 1006 ¶¶ 9, 14, 15; Ex. 1002 ¶¶ 161–170.

i. “storing” and “associating”

The fifth and final step recited by independent claim 1 as executed by the “customer notification program” is “if resolving the request responsive to a reply to the notification results in permitting authorized access to the customer account information by the remote computing device, storing the device fingerprint as a previously authorized device fingerprint and associating the device fingerprint with the customer account information.” Ex. 1001, 12:28–34. This limitation has two distinct steps that are

performed with respect to the device fingerprint when resolving the request that permits access to the customer account information, namely “storing” it as a previously authorized device fingerprint and “associating” it with the customer account information.

For the first of these, “storing,” Petitioner observes that Steinberg discloses that, when the user opts to make the previously unauthorized device “trusted,” Steinberg’s system “records identifying information about that machine (e.g., network number from IP address, checksum of various items in the hardware or software, IP address, etc.) at step 1126, and thereafter, user continues his session.” Pet. 59 (quoting Ex. 1005 ¶ 48). Petitioner thus reasons that when the user selects the previously unauthorized device as “trusted” for a future login, the Steinberg-Oberheide system records (or “stores”) the device profile, including the device fingerprint. *Id.* at 60. Petitioner supports this reasoning, which is not contested by Patent Owner, with testimony by Dr. Monroe. Ex. 1002 ¶ 175.

For the second aspect of this limitation, “associating,” Petitioner relies on Steinberg’s general disclosure of associating device profiles with customer account information. Pet. 60 (citing Ex. 1002 ¶¶ 176–178; Ex. 1005 ¶¶ 46, 48, Figs. 4, 11A). Accordingly, Petitioner reasons, “when the user selects his/her computer to be a ‘trusted’ computer for a future login, the combined *Steinberg-Oberheide* system . . . associates the stored device profile (‘device fingerprint’) as one known for this user.” *Id.* (citing Ex. 1002 ¶ 176). Petitioner supports this reasoning, which is not contested by Patent Owner, with testimony by Dr. Monroe. Ex. 1002 ¶ 176.

Petitioner further addresses this limitation's requirement that the "storing" and "associating" be performed "if resolving the request responsive to a reply to the notification results in permitting authorized access to the customer account information by the remote computing device" by contending that such a feature would have been obvious in view of Oberheide. Pet. 60–62. Petitioner supports this contention with testimony by Dr. Monroe that the device fingerprint would have been recognized by a person of ordinary skill in the art as "a convenient, foreseeable piece of data to store as an identifier for a previously authorized device (e.g., one that has been allowed access and has been assigned 'trusted' status as in *Steinberg*) and to associate with the customer account information for such registration." Ex. 1002 ¶ 178. Dr. Monroe also supports Petitioner's reasoning that a person of ordinary skill in the art would thus "have found it beneficial to associate the device profile ('device fingerprint') with the customer account information so that when a device is recognized, access to the correct customer account can be provided." Pet. 62 (citing Ex. 1002 ¶ 178).

Patent Owner does not contest this aspect of Petitioner's argument, *see generally* PO Resp. 26–33, and Petitioner's reasoning is persuasive, particularly in light of the uncontroverted supporting testimony provided by Dr. Monroe. Ex. 1005 ¶¶ 46, 48; Ex. 1002 ¶¶ 171–179.

j. Summary

For each limitation of independent claim 1, Petitioner has persuasively identified where that limitation is taught by its proposed combination of *Steinberg* and *Oberheide*, and has provided persuasive reasoning, supported

by rational underpinning, to effect the combination of teachings from Steinberg and Oberheide. We therefore conclude that Petitioner shows, by a preponderance of the evidence, that independent claim 1 is unpatentable under 35 U.S.C. § 103(a) over Steinberg and Oberheide.

2. Dependent Claim 2

Claim 2 depends from independent claim 1 and recites that “the reply is received from the address of the separate device specified by the customer.” Ex. 1001, 12:35–36. For this claim, Petitioner observes that Oberheide discloses that the auth platform, which Petitioner identifies with the “server” recited in underlying independent claim 1, “receives ‘an authority agent response from the authority device’ and thereby ‘process[es] [the] response.’” Pet. 63 (quoting Ex. 1006 ¶ 14; citing Ex. 1006, Figs. 1, 2; Ex. 1002 ¶ 181) (alterations by Petitioner). In light of this disclosure, Petitioner reasons that, in the combined Steinberg-Oberheide system, “the reply to the notification is received from the address of the separate device specified by the user (‘customer’).” *Id.* (citing Ex. 1002 ¶ 181; Ex. 1006 ¶¶ 9, 14, 15, Figs. 1, 2).

Patent Owner does not contest Petitioner’s analysis of claim 2 outside of its arguments directed at underlying independent claim 1. PO Resp. 33–34. Petitioner’s analysis is supported by testimony by Dr. Monroe, and we find it persuasive. *See* Ex. 1002 ¶¶ 180–181. We accordingly conclude that Petitioner shows, by a preponderance of the evidence, that dependent claim 2 is unpatentable under 35 U.S.C. § 103(a) over Steinberg and Oberheide.

3. Dependent Claim 3

Claim 3 depends from independent claim 1 and recites that “the notification further interrogates for an answer approving or disapproving the request,” with “the resolving step further compris[ing] approving or disapproving the request according to the answer.” Ex. 1001, 12:37–41. Petitioner addresses these related limitations by noting that Oberheide explicitly discloses a “push notification service” that “push[es] a notification to a secondary device for authentication or authorization.” Pet. 64; Ex. 1006 ¶ 13. Because Oberheide’s notification message may include “options for a transaction response” that include acceptance or rejection of a transaction, Petitioner reasons that claim 3’s interrogation for an answer and the approval or disapproval according to the answer are disclosed. Pet. 64–65.

Patent Owner does not contest Petitioner’s analysis of claim 3 outside of its arguments directed at underlying independent claim 1. PO Resp. 33–34. Petitioner’s analysis is supported by testimony by Dr. Monroe, and we find it persuasive. See Ex. 1002 ¶¶ 182–185. We accordingly conclude that Petitioner shows, by a preponderance of the evidence, that dependent claim 3 is unpatentable under 35 U.S.C. § 103(a) over Steinberg and Oberheide.

4. Dependent Claim 4

Claim 4 depends from claim 3 and further recites “storing, responsive to approving the request, the device fingerprint as a previously authorized device fingerprint.” Ex. 1001, 12:42–44. As discussed above in connection with the “storing” and “associating” limitation of independent claim 1, Petitioner persuasively shows that the Steinberg-Oberheide combination it proposes includes “storing the device fingerprint as a previously authorized

device fingerprint” in response to a reply to the notification. *Supra* § II.E.1.i. Petitioner builds upon that showing with its argument for claim 3 to contend that the further requirement of claim 4 of storing the device fingerprint response to approving the request would have been obvious. Pet. 65–66. Specifically, with uncontroverted testimonial support by Dr. Monroe, Petitioner contends that “it would have been obvious to configure the combined *Steinberg-Oberheide* system so that if the answer provided by the user approves the access request, then the device profile (‘device fingerprint’) is stored in the memory or the database and is associated with the customer account information.” *Id.* at 66 (citing Ex. 1002 ¶ 187).

This contention (which is not contested by Patent Owner, PO Resp. 33–34) is persuasive, particularly when tied to Petitioner’s showing with respect to the “storing” and “associating” limitation of independent claim 1. We accordingly conclude that Petitioner shows, by a preponderance of the evidence that claim 4 is unpatentable under 35 U.S.C. § 103(a) over *Steinberg* and *Oberheide*.

5. *Dependent Claim 6*

Claim 6 also depends from claim 3, reciting that “the notification program interrogates by effecting display of selectable answers on a user interface.” Ex. 1001, 12:48–50. To address this requirement, Petitioner points to *Steinberg*’s disclosure of providing at least the “requesting location” aspect of the notification “in the form of text or a map” as an example of effecting a display of information to the user. Pet. 67 (citing Ex. 1005 ¶¶ 15, 44, claim 28; Ex. 1002 ¶ 189). In addition, Petitioner identifies *Oberheide*’s disclosure that a notification message sent to the

secondary device may include “options for a transaction response” that include “to accept or reject a transaction” or “multiple-choice options.” *Id.* at 67–68 (citing Ex. 1006 ¶¶ 13–14).

Petitioner reasons that, in light of these disclosures, the combined Steinberg-Oberheide system renders obvious the additional limitation of claim 6. *Id.* at 67–68. Petitioner’s reasoning is uncontested by Patent Owner and supported by Dr. Monroe’s testimony, and we find it persuasive. *See* Ex. 1002 ¶¶ 188–190; PO Resp. 33–34. We accordingly conclude that Petitioner shows, by a preponderance of the evidence, that claim 6 is unpatentable under 35 U.S.C. § 103(a) over Steinberg and Oberheide.

6. *Dependent Claim 12*

Claim 12 depends from independent claim 1 and recites that “the requesting location comprises a geographic location.” Ex. 1001, 13:9–10. In addressing this limitation, Petitioner observes that both Steinberg and Oberheide disclose that the requesting location can be a “geographic location” because both references refer to the “geolocation” of an IP address, which Dr. Monroe testifies refers to a “geographic location.” Pet. 68–69; Ex. 1002 ¶ 192 (“It is my opinion that a person of ordinary skill in the art would have understood that “geolocation” refers to a *geographic* location.”).

Petitioner’s reasoning is persuasive and not contested by Patent Owner. *See* PO Resp. 33–34. We accordingly conclude that Petitioner shows, by a preponderance of the evidence, that claim 12 is unpatentable under 35 U.S.C. § 103(a) over Steinberg and Oberheide.

7. Dependent Claim 14

Claim 14 depends from independent claim 1 and recites that “the notification further indicates a time of the request.” Ex. 1001, 13:16–17. To address this limitation, Petitioner identifies Oberheide’s explicit disclosure that the notification indicates a “time of transaction,” which Dr. Monroe testifies would have been understood by a person of ordinary skill in the art as referring to “a time of the transaction *request* because *Oberheide* discloses to ‘alert a user to [a] transaction request.’” Pet. 70 (alteration by Petitioner); Ex. 1002 ¶ 195 (quoting Ex. 1006 ¶ 9) (emphasis by Dr. Monroe).

In light of this identification and supporting testimony, Petitioner makes a persuasive showing, which is not contested by Patent Owner. PO Resp. 33–34. We accordingly conclude that Petitioner shows, by a preponderance of the evidence, that claim 14 is unpatentable under 35 U.S.C. § 103(a) over Steinberg and Oberheide.

F. Combination of Steinberg, Oberheide, and McDowell

Petitioner challenges claims 1–4, 6, 9, 12, and 14 as unpatentable under 35 U.S.C. § 103(a) over Steinberg, Oberheide, and McDowell. Pet. 71–75, 79–81.

1. Claims 1–4, 6, 12, and 14

As discussed above, Petitioner challenges claims 1–4, 6, 12, and 14 as unpatentable under 35 U.S.C. § 103(a) over Steinberg and Oberheide. *See* Pet. 14–70. Petitioner’s additional challenge of these claims over the further

combination with McDowell presents an alternative for addressing the “database” recited in independent claim 1. *Id.* at 79.

As Petitioner notes, McDowell’s verification system includes a database, such as user-side database 18, that is accessible by a server, such as user-side server 16, for storing and communicating information. *Id.* (citing Ex. 1008 ¶¶ 25, 28, Fig. 1). Petitioner reasons that a person of skill in the art would have been motivated to use a database, like that taught by McDowell, for storing customer account information in the Steinberg-Oberheide system. *Id.* at 80. In providing such reasoning, Petitioner provides testimony by Dr. Monroe that incorporating such a database would “have been a mere combination of known components and technologies, according to known methods, to produce predictable results.” Ex. 1002 ¶ 216. In addition, Dr. Monroe testifies that “a skilled person would have recognized *McDowell*’s usage of a database to be a straightforward application of basic computing principles, and would have been motivated in light of *McDowell*’s disclosures to include a database for storing the customer account information.” *Id.* In addition to testifying that the resulting combination of Steinberg, Oberheide, and McDowell would have been “a foreseeable configuration,” Dr. Monroe identifies “additional benefits” to the combination that include “rapid search and retrieval of the information.” *Id.*

Patent Owner does not contest Petitioner’s further incorporation of McDowell into the Steinberg-Oberheide combination outside of its arguments directed at the combination of Steinberg and Oberheide alone. PO Resp. 25–26, 33. Because we find that Petitioner articulates persuasive reasoning, supported by rational underpinning, to effect the further

combination with McDowell, and persuasively identifies disclosure of the “database” limitation of claim 1 in that combination, we determine that Petitioner makes a persuasive showing. This showing also applies to each of claims 2–4, 6, 12, and 14 by virtue of their dependence from claim 1.

We accordingly conclude that Petitioner shows, by a preponderance of the evidence, that claims 1–4, 6, 12, and 14 are unpatentable under 35 U.S.C. § 103(a) over Steinberg, Oberheide, and McDowell.

2. Claim 9

Claim 9 depends from independent claim 1 and recites that “the number of device fingerprints are stored in a second database accessible by the server.” Ex. 1001, 12:60–62. Petitioner contends that this feature would have been obvious over the combination of McDowell with the Steinberg-Oberheide system described above. Pet. 71–75, 81. In particular, Petitioner contends that McDowell discloses the use of multiple databases in the context of its verification system, including user-side database 18 and merchant-side database 20 illustrated in Figure 1, reproduced above. *Id.* at 73 (citing Ex. 1008 ¶¶ 25, 28; Ex. 1002 ¶ 202). User-side database 18 “stores information related to an account created by a user that is responsible for storing . . . device identifiers,” among other information. Ex. 1008 ¶ 25. Merchant-side database 20 stores entity/device pairs and receives verification requests from requesting servers operated by merchants and other third parties. *Id.* ¶ 38. As Petitioner asserts, “[t]he device/entity pairs stored in user-side database 18 are provided to merchant-side database 20 to prevent fraudulent transactions from unregistered devices, by permitting a

merchant to authenticate a device requesting a transaction.” Pet. 74 (citing Ex. 1008 ¶ 38; Ex. 1002 ¶ 203).

Petitioner reasons that a person of ordinary skill in the art would have been motivated by such teachings to configure the Steinberg-Oberheide system such that the recited “number of device fingerprints”—i.e., device fingerprints previously authorized to access the customer account information, as recited in underlying claim 1—are stored in a second database accessible by the server. *Id.* (citing Ex. 1002 ¶ 204). Dr. Monroe testifies in support of this reasoning a person of ordinary skill in the art would have found it useful to store the device fingerprints in a second database “so that the fingerprints (which pertain to a variety of devices) could be securely stored separately from the customer account information (which such a skilled person would have recognized need not be conceptually grouped with the variety of devices).” Ex. 1002 ¶ 205. Dr. Monroe also specifically testifies that such a skilled person would have found it beneficial to configure the second database to be accessible by the server so that the customer notification program could access the fingerprints. *Id.* In addition, Dr. Monroe testifies to certain benefits of storing the device fingerprints in a second database that would have been predictable to a person of ordinary skill in the art. *Id.* ¶¶ 205–206. Such benefits include rapid search and retrieval of the device fingerprints, scalability over a single database, data redundancy, and fault tolerance. *Id.*

Patent Owner does not contest this aspect of Petitioner’s analysis, PO Resp. 33–34, which we find persuasive and supported by the evidence of record. We accordingly conclude that Petitioner shows, by a preponderance

of the evidence, that claim 9 is unpatentable under 35 U.S.C. § 103(a) over Steinberg, Oberheide, and McDowell.

G. Obviousness over Steinberg, Oberheide, and Yasushi

Petitioner challenges claim 13 as unpatentable under 35 U.S.C. § 103(a) over Steinberg, Oberheide, and Yasushi. Pet. 75–79. Claim 13 depends from independent claim 1 and recites that “the identity of the remote computing device includes information selected from the group consisting of manufacturer name, model name, and device type.” Ex. 1001, 13:11–14.

As discussed above, Petitioner makes a persuasive showing that the combination of Steinberg and Oberheide teaches all limitations of independent claim 1, and articulates persuasive reasoning for effecting that combination of teachings. *Supra*, § II.E.1. Because Yasushi, like Steinberg and Oberheide, is directed to computer-security applications, Petitioner reasons that a person of ordinary skill in the art would have had reason to consider its teachings when implementing the combined Steinberg-Oberheide system. Pet. 76. Petitioner particularly notes Yasushi’s disclosure of a server that transmits a “notification mail” when a login request is received so that “[t]he user themselves can easily be made aware of the occurrence of an unlawful login.” *Id.* at 76–77 (quoting Ex. 1009 ¶ 9). An example of such a “notification mail” is reproduced above in our summary of Yasushi, and illustrates login information that may be included. *See supra* Section II.D.4; Ex. 1009, Fig. 6. For instance, the notification may indicate the login time, IP address, type of device used (such as “PC” or

“mobile terminal”), and the type of browser making the request. Ex. 1009 ¶ 71, Fig. 6.

Petitioner specifically identifies the indication of the type of device used as meeting the “device type” element of claim 13’s Markush group. Pet. 78–79. According to Petitioner, a person of ordinary skill in the art would have been motivated in light of Yasushi “to configure the combined *Steinberg-Oberheide* system so that the identity of the computer seeking access (‘the remote computing device’) includes device type.” *Id.* at 78 (citing Ex. 1002 ¶ 212). Petitioner supports this contention with uncontroverted testimony by Dr. Monroe that a skilled artisan “would have recognized that providing information in the notification message that indicates the device type of a device requesting an access would have been beneficial . . . , so the user can determine whether the request is fraudulent based on the requesting device’s identity (e.g., its type).” Ex. 1002 ¶ 212. Dr. Monroe further testifies that such a configuration “would have been a mere combination of known components and technologies, according to known methods, to produce foreseeable results.” *Id.*

Patent Owner does not contest Petitioner’s challenge of claim 13 outside of its arguments directed at underlying independent claim 1. PO Resp. 33–34. Petitioner’s reasoning for the combination of Yasushi with Steinberg and Oberheide is supported by rational underpinning, and we therefore find that Petitioner makes a persuasive showing both with respect to the rationale for effecting the combination and with respect to the features of such a combination. We conclude that Petitioner shows, by a preponderance of the evidence, that claim 13 is unpatentable under 35 U.S.C. § 103(a) over Steinberg, Oberheide, and Yasushi.

H. Obviousness over Steinberg, Oberheide, McDowell, and Yasushi

Petitioner challenges claim 13 as unpatentable under 35 U.S.C. § 103(a) over Steinberg, Oberheide, McDowell, and Yasushi. Pet. 81–82. According to Petitioner, “*Steinberg* in combination with *Oberheide* and *McDowell* discloses or suggests the limitations of claim 1,” and “*Steinberg* in combination with *Oberheide*, *McDowell*, and *Yasushi* discloses or suggests the limitations of claim 13 for at least the same reasons as discussed above [for the combination of Steinberg, Oberheide, and Yasushi].” *Id.* As noted immediately above, Patent Owner does not contest Petitioner’s challenge of claim 13 outside of its arguments directed at underlying independent claim 1. PO Resp. 33–34.

As discussed above, Petitioner makes a persuasive showing that the combination of Steinberg, Oberheide, and McDowell teaches all limitations of independent claim 1, and articulates persuasive reasoning for effecting that combination of teachings. *Supra*, § II.F.1. In addition, Petitioner makes a persuasive showing that the limitation of claim 13 is taught by Yasushi and articulates persuasive reasoning for combining that teaching with Steinberg and Oberheide. *Supra*, § II.G. Petitioner proposes the same modification of the Steinberg-Oberheide-McDowell system with Yasushi as made for the Steinberg-Oberheide system with Yasushi. Pet. 81–82. That argument is supported by testimony by Dr. Monroe, and we find it persuasive. Ex. 1002 ¶¶ 218–219.

Accordingly, we conclude that Petitioner shows, by a preponderance of the evidence, that claim 13 is unpatentable under 35 U.S.C. § 103(a) over Steinberg, Oberheide, McDowell, and Yasushi.

III. APPOINTMENTS CLAUSE

Patent Owner presents an argument that Administrative Patent Judges “are principal officers under the Appointments Clause of the Constitution . . . , but undisputedly are not appointed through the constitutionally-mandated mechanism of appointment for principal officers.” PO Resp. 34. According to Patent Owner, “only Congress can fix the IPR statutory scheme, and this case must be dismissed.” *Id.* at 37. This argument is foreclosed by the Supreme Court’s recent decision in *U.S. v. Arthrex, Inc.*, 141 S. Ct. 1970 (2021).

IV. CONCLUSION⁷

The table below summarizes our conclusions as to the challenged claims.

⁷ 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).

Claim(s)	35 U.S.C. §	References	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–4, 6, 12, 14	103(a)	Steinberg, Oberheide	1–4, 6, 12, 14	
1–4, 6, 9, 12, 14	103(a)	Steinberg, Oberheide, McDowell	1–4, 6, 9, 12, 14	
13	103(a)	Steinberg, Oberheide, McDowell	13	
13	103(a)	Steinberg, Oberheide, McDowell, Yasushi	13	
Overall Outcome			1–4, 6, 9, 12–14	

V. ORDER

It is

ORDERED that, based on a preponderance of the evidence, claims 1–4, 6, 9, and 12–14 of U.S. Patent No. 8,949,954 B2 have been shown to be unpatentable;

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

IPR2020-00441
Patent 8,949,954 B2

For PETITIONER:

Naveen Modi
Joseph Palys
Daniel Zeilberger
Arvind Jairam
Jason Heidemann
PAUL HASTINGS LLP
naveenmodi@paulhastings.com
josephpalys@paulhastings.com
danielzeilberger@paulhastings.com
arvindjairam@paulhastings.com
jasonheidemann@paulhastings.com

For PATENT OWNER:

Ryan Loveless
Brett Mangrum
James Etheridge
Brian Koide
Jeffrey Huang
ETHERIDGE LAW GROUP PC
ryan@etheridgelaw.com
brett@etheridgelaw.com
jim@etheridgelaw.com
brian@etheridgelaw.com
jeff@etheridgelaw.com