

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

CARBYNE BIOMETRICS, LLC,
Patent Owner.

IPR2024-00507
Patent 11,475,105 B2

Before JAMESON LEE, ARTHUR M. PESLAK, and
STEVEN M. AMUNDSON, *Administrative Patent Judges*.

LEE, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Apple Inc. (“Petitioner”) filed a Petition requesting an *inter partes* review of claims 2, 4–6, 12, 15, 21, 23–25, 31, and 34 (“challenged claims”) of U.S. Patent No. 11,475,105 B2 (Ex. 1001, “the ’105 patent”). Paper 3 (“Pet.”). Carbyne Biometrics, LLC (“Patent Owner”) filed a Preliminary Response. Paper 8 (“Prelim. Resp.”). Petitioner filed an authorized Preliminary Reply. Paper 9 (“Prelim. Reply”). Patent Owner filed an authorized Preliminary Sur-reply. Paper 10 (“Prelim. Sur-reply”).

We have authority to determine whether to institute an *inter partes* review. *See* 35 U.S.C. § 314 (2018); 37 C.F.R. § 42.4(a) (2024). An *inter partes* review may not be instituted unless the information presented in the Petition “shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a). Upon consideration of the contentions and the evidence of record before us, we conclude Petitioner has not shown a reasonable likelihood that it would prevail in establishing the unpatentability of at least one challenged claim of the ’105 patent.

Accordingly, we decline to institute *inter partes* review.

II. BACKGROUND

A. *Real Parties in Interest*

Petitioner identifies itself as real party in interest. Pet. 1. Patent Owner identifies itself as real party in interest. Paper 4, 2.

B. *Related Matters*

The parties each identify the following litigation as related to the ’105 patent (Pet. 1; Paper 4, 2): *Carbyne Biometrics, LLC v. Apple Inc.*, 1:23-cv-00324 (WDTX).

Petitioner further identifies *Samsung Electronics Co., Ltd. v. RightQuestion, LLC*, IPR2022-00244 (PTAB) (Terminated July 26, 2022), which involved an ancestral patent of the '105 patent, as a related matter. Pet. 1–2.

IPR2024-00334 is a proceeding involving U.S. Patent No. 11,514,138 B1, based on Application 17/027,481, from which the application that issued as the '105 patent is a continuation-in-part application.

Petitioner has filed another petition in IPR2024-00333 against different claims of the '105 patent, i.e., claims 1, 9–11, 14, 18, 28–30, 33, and 35.

C. The '105 Patent

The '105 patent is directed to authentication techniques to provide credentials to a service. Ex. 1001, 1:43–52. The goal is to reduce practices such as password re-use and/or selection of poor quality passwords. *Id.* Specifically, the '105 patent pertains to authentication translation and states:

Authentication translation is disclosed. A request to access a resource is received at an authentication translator, as is an authentication input. The authentication input corresponds to at least one stored record. The stored record is associated at least with the resource. In response to the receiving, a previously stored credential associated with the resource is accessed. The credential is provided to the resource.

Id. at code (57). Figure 1 of the '105 patent is reproduced below:

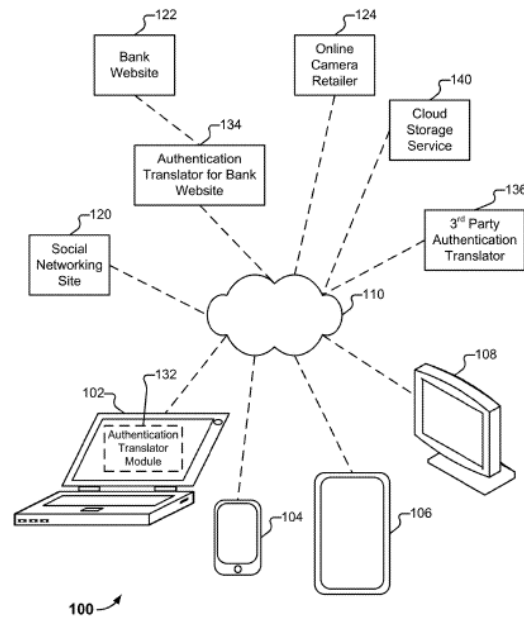


FIG. 1

Figure 1 illustrates an embodiment of an environment in which authentication translation is provided. Ex. 1001, 2:62–63. Various client service devices 102–108 are connected through one or more networks (represented as single network cloud 110) to various services 120–124, which are also referred to as sites. *Id.* at 2:63–67.

Client device 102 is a notebook computer owned by user Alice and includes a camera, a microphone, and a fingerprint sensor. *Id.* at 2:67–3:3. Client device 104 is a smartphone owned by user Alice and includes a camera. *Id.* at 3:3–4. Client device 106 is a tablet owned by user Bob and includes a camera and a fingerprint sensor, and device 106 is sometimes used by Bob’s son Charlie. *Id.* at 3:5–7. Client device 108 is a kiosk located in the lobby of a hotel, and it includes a camera and a microphone. *Id.* at 3:7–9.

Service 120 is a social networking site; service 122 is a website of a bank; service 124 is the online store of a boutique camera retailer; each

service requires a username and password (and/or a cookie) from a user prior to giving that user access to protected content and/or other features. Ex. 1001, 3:15–20. A user need not type such user names and passwords into the devices whenever required by a service, but can authenticate to an “authentication translator” which will provide the appropriate credentials to the service “on the user’s behalf.” *Id.* at 3:21–26.

For example, notebook computer 102 includes authentication translator module 132 that provides authentication translation services. Ex. 1001, 3:29–31. Devices 104–108 can also include, but need not include, their own respective authentication translator modules. *Id.* at 3:31–33. The owner of bank website 122 operates authentication translator 134 associated with the bank. *Id.* at 3:34–35. Authentication translator 136 provides authentication services to a variety of businesses, including online camera retailer 124. *Id.* at 3:35–38.

Figure 2 of the ’105 patent is reproduced below:

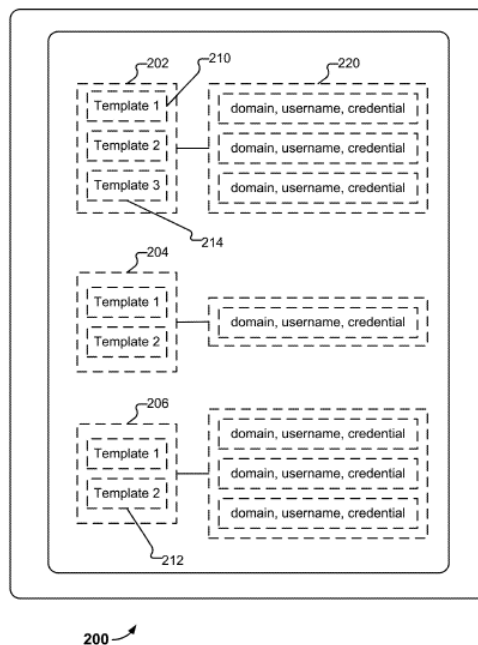


FIG. 2

Figure 2 shows an embodiment of credential information stored on a device 200. Ex. 1001, 3:38–39. Device 200 stores three user profiles 202–206, each of which contains a username and one or more templates associated with the user. *Id.* at 3:39–42. A template is a collection of biometric features, where a fingerprint is an example of a biometric feature. *Id.* at 3:42–44. A representation of a single fingerprint may be included in multiple templates, such as in different resolutions in accordance with different protocols, e.g., warm or cold conditions and/or by itself or in combination with multiple fingerprints). *Id.* at 3:48–53. When other biometrics are employed, for example facial recognition, voice print, or retina scan, corresponding features are included in the template. *Id.* at 3:53–56.

Policies can be included in profiles that govern how matches are to be performed. *Id.* at 4:3–5. Policies can specify threshold/tolerances for what constitutes a match, and can specify that different levels of matches can result in different levels of access to different resources. *Id.* at 4:5–8. A profile is associated with a vault, for example vault 220. *Id.* at 4:9. A vault, in turn, contains triples specifying a service provider/domain, a username, and a credential. *Id.* at 4:9–11.

Regarding policies, the '105 patent further describes:

Policies can also be associated with devices, or with all vaults on a device. Such a policy may state that vaults can only be backed up to computational devices of the same brand, or to computational devices that satisfy software requirements associated with the policy, such as having anti-virus software or using an operating system that is the most recent version or the version before that, but not older.

Ex. 1001, 19:28–35.

The credential for a service provider or domain can be a password or a cryptographic key. *Id.* at 4:14–17. The '105 patent describes that profiles, templates, and vaults are collectively referred to as “authentication information” and that in some embodiments secure storage techniques are used to store at least a portion of the authentication information. *Id.* at 4:18–23. Profiles and vaults can be updated while in secure storage, and if that occurs, they are encrypted before being written back to insecure storage, which may in turn propagate them to external backup storage. *Id.* at 4:44–48. Figure 3 is reproduced below:

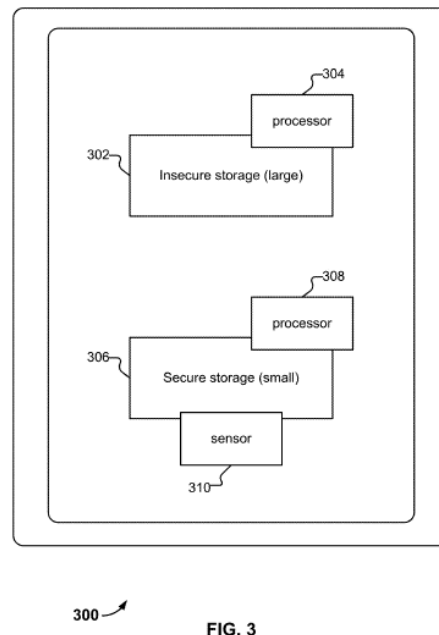


Figure 3 shows an embodiment using secured storage to hold authentication information. *Id.* at 4:21–25.

Mobile phone 300 includes large and insecure storage 302 attached to fast processor 304, and smaller but secure storage 306 is attached to dedicated processor 308 and sensor 310, which can be a camera or a fingerprint reader. *Id.* at 4:25–29. “Users (and applications) can read from and write to the insecure storage area. However, users cannot access the

secure storage area, and the fast processor can only communicate with the dedicated processor/sensor via a restricted API.” *Id.* at 4:29–33.

D. Illustrative Base Claim

Claims 1 and 18 are independent. Neither claim 1 nor claim 18 is challenged in the Petition. However, challenged claims 2, 4–6, 12, and 15 each depend, directly or indirectly, from claim 1, and challenged claims 21, 23–25, 31, and 34 each depend, directly or indirectly, from claim 18. Ex. 1001, 25:14–27:20. Thus, each of claims 2, 4–6, 12, and 15 includes all of the limitations of claim 1, and each of claims 21, 23–25, 31, and 34 includes all of the limitations of claim 18. 35 U.S.C. § 112(d). Claim 1 is illustrative and reproduced below:

1. [1.0] A system, comprising:
 - [1.1] one or more processors configured to:
 - [1.2] receive, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;
 - [1.3a] access at least one record stored on the first device, the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access,
 - [1.3b] wherein the credential information comprises a cryptographic key;
 - [1.4] receive authentication input from the user;
 - [1.5] determine that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;
 - [1.6] retrieve at least a portion of the credential information from the at least one record stored in the first device;
 - [1.7] facilitate access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the

credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and

[1.8] based at least in part on the first device being a same brand as a second device, initiate a backup, to the second device, of at least a portion of the at least one record; and

[1.9] a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.

Ex. 1001, 24:47–25:13.¹

E. Prior Art and Declaration Evidence

Petitioner relies on the following evidence:²

¹ The bracketed heading labels correspond to those used by Petitioner to reference the claim elements. *See* Pet. 20–35. We use the same labels here for ease of reference, understanding, and consistency.

² The '105 patent issued from Application No. 17/123,018, filed Dec. 15, 2020, which is a continuation-in-part of Application No. 17/027,481, filed Sept. 21, 2020, now Patent No. 11,514,138, which is a continuation of Application No. 16/773,767, filed Jan. 27, 2020, now Patent No. 10,929,512, which is a continuation of Application No. 16/563,715, filed Sept. 6, 2019, now Patent No. 10,824,696, which is a continuation of Application No. 16/273,797, filed Feb. 12, 2019, now Patent No. 10,521,568, which is a continuation of Application No. 15/042,636, filed Feb. 12, 2016, now Patent No. 10,360,351, which is a continuation of Application No. 13/706,254, filed Dec. 5, 2012, now Patent No. 9,294,452. Ex. 1001, codes (21), (22), (63). The '105 patent also claims priority to Provisional Application 61/587,387, filed Jan. 17, 2012, and Provisional Application 61/569,112, filed Dec. 9, 2011. *Id.* at code (60).

Name	Patent Document	Exhibit
Kesanupalli ³	US Patent No. 8,799,666 B2	1006
Jakobsson '351 ⁴	US Patent No. 10,360,351 B2	1011
Cheng ⁵	US Pub. App. 2004/0117636 A1	1008
Hubner ⁶	US Pub. App. 2012/0150808 A1	1030
Kodama ⁷	EP 2 079 023 A2	1010

Petitioner also relies on the Declaration of Patrick McDaniel, Ph.D. (Ex. 1003). Patent Owner has not submitted any declaration testimony.

F. The Asserted Grounds of Unpatentability

Petitioner asserts that the challenged claims of the '105 patent are unpatentable based on the following grounds (Pet. 10):

Claims Challenged	35 U.S.C. §	References/Basis
2, 4, 12, 15, 21, 23, 31, 34	103	Kesanupalli, Cheng, Kodama
5, 6, 24, 25	103	Kesanupalli, Cheng, Kodama, Hubner
2, 4, 12, 15, 21, 23, 31, 34	103	Jakobsson '351, Kodama
5, 6, 24, 25	103	Jakobsson '351, Kodama, Hubner

³ Issued Aug. 5, 2014, from Application No. 12/731,050, filed Mar. 24, 2010. Ex. 1006, codes (21), (22), (45).

⁴ Issued July 23, 2019, from Application No. 15/042,636, filed Feb. 12, 2016, which is a continuation of Application No. 13/706,254, filed Dec. 5, 2012, now Patent No. 9,294,452. Ex. 1011, codes (21), (22), (45), (63). Jakobsson '351 also claims priority to Provisional Application 61/587,387, filed Jan. 17, 2012, and Provisional Application 61/569,112, filed Dec. 9, 2011. *Id.* code (60). Jakobsson '351 is an ancestral patent to which the '105 patent claims priority through a chain of continuation applications including a continuation-in-part application. Ex. 1001, code (63).

⁵ Published June 17, 2004. Ex. 1008, code (43).

⁶ Published June 14, 2012. Ex. 1030, code (43).

⁷ Published July 15, 2009. Ex. 1010, code (43).

G. Effective Filing Date and Applicable Law

The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112–29, 125 Stat. 284, 287–88 (2011), in § 3(n)(1), provides that the amendments made by this section “shall apply to any application for patent, and to any patent issuing thereon, that contains or contained at any time—(A) a claim to a claimed invention that has an effective filing date as defined in section 100(i) of title 35, United States Code, that is on or after [expiration of the 18 month period beginning on the date of enactment of the AIA (September 16, 2011)].”⁸ AIA § 3(n)(1).

Petitioner asserts that dependent claim 16 of Application No. 17/123,018 as initially filed on December 15, 2020, which issued as the ’105 patent, recites “the backup is performed in response to a determination that the first device is of the same brand as the second device.” Pet. 6 (citing Ex. 1002, 417). Petitioner also asserts:

As confirmed by Dr. McDaniel, no disclosure exists in any application to which the ’018 App claims priority—including the pre-AIA ’254 App—that provides written description support for a backup being performed **in response to a determination** that the first device is **of the same brand** as the second device. APPL-1003, ¶¶36–41. Accordingly, AIA § 3(n)(1) dictates the ’105 patent be evaluated under post-AIA §§102, 103.

Id.

Similarly, Petitioner asserts that the effective filing date of each challenged claim is no earlier than the actual filing date of Application No. 17/123,018, December 15, 2020, because all independent claims of the challenged claims require initiating a backup based at least in part on a first

⁸ The date of enactment of the AIA is September 16, 2011.

device being of the same brand as a second device. Pet. 5–7. Petitioner explains:

As confirmed by Dr. McDaniel, no written description exists in any application to which the '018 App claims priority for initiating backup to a second device based at least in part on the first device ***being a same brand*** as a second device. APPL-1003, ¶¶36-41. To the extent passages of the '018 App discuss the term “brand” (*i.e.*, those portions corresponding to 13:28-33 and/or 19:29-35 of the '105 patent), these passages are not found in any application to which the '018 App claims priority. *Id.* These passages fall under a heading “ADDITIONAL EMBODIMENTS.” APPL-1001, 11:30; APPL-1002, 18. This heading begins a portion of the '018 App’s specification that spans pages numbered 18 to 36; in contrast, the originally filed specification of the U.S. Application 17/027,481 of which the '018 App is a CIP, does not include this heading and begins its claim recitation at its page 17. APPL-1002, 395-414; APPL-1005, 38.

Id. at 7.

Patent Owner asserts that “the Petition contains no actual analysis of the actual Provisionals.” Prelim. Resp. 43. According to Patent Owner, it “properly disclosed support for the ‘same brand’ backup in the Provisional.”

Id. at 44. Patent Owner explains:

Here, the Provisional application (Ex. 1005 at 298) discusses “synchronization of data between device 110 . . . and cloud storage or other storage 101.” Ex. 1005 (Provisional) at 315 (Fig. 5). The Provisional further discusses that a “secure channel” can be established between the two entities to authenticate each other and that “[i]t is determined, *based on policies and the identity and access history of device 110* what data to upload 502 to storage 101 *from device 110 . . .*” *Id.* (emphasis added) (reproduced below).

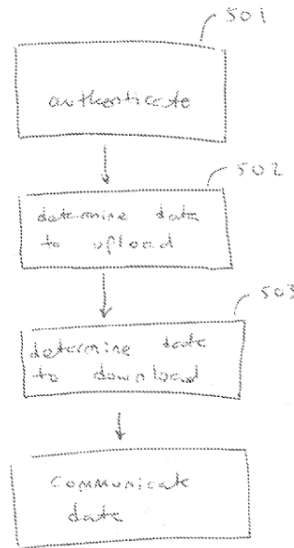


FIG 5

Fig 5 shows an example of synchronization of data between device 110, including component 114, and cloud storage or other storage 101. A secure channel can have been established, e.g., using SSL, after which the entities 110 and 101 authenticate to each other 501. It is determined, based on policies and the identity and access history of device 110 what data to upload 502 to storage 101 from device 110 and component 114, and similarly, what data to download from storage 101 to device 110 and component 114. All data is encrypted using keys stored at least in part by component 114.

Ex. 1005 (Provisional) at 315 (Fig. 5). A determination “based on” *policies* and the *identity of the device* would have conveyed to a POSITA that the backup could have been based on a policy including the device being of the same brand as the second device. *See, e.g.,* Ex. 1001 (’105 Patent) at 19:29–35 (“Such a *policy* may state that vaults can only be backed up to computational *devices of the same brand.*”) (emphasis added). Petitioner and its expert completely disregard this statement and the backup discussions in the Provisional.

Prelim. Resp. 44–45 (alterations and emphasis in original).

These assertions of Patent Owner are unavailing. First, in light of Petitioner’s application of Jakobsson ’351 as prior art, Patent Owner bears the burden of production to present persuasive argument that its claims are entitled to the benefit of a filing date prior to the date of Jakobsson ’351 as prior art. *See Dynamic Drinkware, LLC v. National Graphics, Inc.*, 800 F.3d 1375, 1379–1380 (Fed. Cir. 2015).

Second, as to Patent Owner’s arguments regarding support being found in Provisional Application No. 61/587,387, filed Jan. 17, 2012, we are not sufficiently persuaded. The disclosure Patent Owner refers to in the provisional application is this: “It is determined, based on policies and the identity and access history of device 110 what data to upload 502 to storage 101 from device 110 and component 114, and similarly, what data to download from storage 101 to device 110 and component 114.” Ex. 1005, 315 (cited at Prelim. Resp. 45).

The test for written description support is whether the application reasonably would have conveyed to one with ordinary skill in the art “the inventor possessed the invention at the time of that original disclosure.” *Pandrol USA, LP v. Airboss Ry. Prods., Inc.*, 424 F.3d 1161, 1165 (Fed. Cir. 2005); *see also Vas-Cath Inc. v. Mahurkar*, 935 F.2d 1555, 1563–64 (Fed. Cir. 1991) (“the applicant must also convey with reasonable clarity to those skilled in the art that, as of the filing date sought, she or he was in possession of the invention”).

The disclosure in the provisional application as cited by Patent Owner regarding policies is broad and does not convey with reasonable clarity what specifically are the policies, such as a policy for backup based on whether the first and second devices are of the same brand. The broad disclosure does not provide written description support for the narrow and specific limitation recited in independent claims 1, 18, and 25, i.e., “based at least in part on the first device being a same brand as a second device, initiating a backup, to the second device, of at least a portion of the at least one record.” Ex. 1001, 25:7–10, 26:30–32, 28:23–25.

Patent Owner states: “A determination ‘based on’ *policies* and the *identity of the device* would have conveyed to a POSITA that the backup could have been based on a policy including the device being of the same brand as the second device.” Prelim. Resp. 45 (emphasis in original). The assertion is misplaced because it refers to what “could have been” a policy, rather than what policy the provisional application disclosure conveys the inventor actually possessed. What potentially “could have been” is mere speculation, not written description indicating possession.

Similarly, the disclosure of the provisional application does not provide adequate written description support for dependent claim 16 contained in Patent Application 17/123,018 as initially filed, which issued as the ’105 patent; claim 16 as initially filed recites: “the backup is performed in response to a determination that the first device is of a same brand as the second device.” Ex. 1002, 417.

For the foregoing reasons, we apply the AIA versions of 35 U.S.C. §§ 102 and 103. Also, we determine, on this record, that the effective filing date of all challenged claims of the ’105 patent is the actual filing date of Patent Application No. 17/123,018, December 15, 2020.

III. ANALYSIS

A. *Legal Standards*

A claim is unpatentable under 35 U.S.C. § 103 “if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains.” 35 U.S.C. § 103; *see 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) where in evidence, so-called secondary considerations of nonobviousness.⁹ See *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

B. Level of Ordinary Skill in the Art

Citing testimony from Dr. McDaniel, Petitioner asserts a person of ordinary skill in the art “would have had a bachelor’s degree in [] electrical engineering, computer engineering, computer science, or a related field, and at least two years of experience in the research, design, development, and/or testing of authentication techniques, and related firmware and software, or the equivalent, with additional education substituting for experience and vice versa.” Pet. 8 (citing Ex. 1003 ¶¶ 18–22).

On this record, we adopt Petitioner’s statement of the level of ordinary skill in the art, except for the qualifier “at least” which applies to experience and which would improperly extend the scope of experience to the realm of an expert. It is supported by the testimony of Dr. McDaniel and not disputed by Patent Owner (Prelim. Resp. 11). Further, it appears consistent with what is reflected by the content of the applied prior art. *Cf. Okajima v. Bourdeau*, 261 F.3d 1350, 1354–55 (Fed. Cir. 2001) (the applied prior art may reflect an appropriate level of skill).

⁹ The record does not include any evidence of secondary considerations of nonobviousness.

C. *Claim Interpretation*

We use the same claim construction standard that would be used to construe a 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). The claim construction standard set forth in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc) is applicable.

Claim terms are generally given their ordinary and customary meaning as would be understood by one with ordinary skill in the art in the context of the specification, the prosecution history, other claims, and extrinsic evidence including expert and inventor testimony, dictionaries, and learned treatises, although extrinsic evidence is less significant than the intrinsic record. *Phillips*, 415 F.3d at 1312–17. Usually, the specification is dispositive, and it is the single best guide to the meaning of a disputed term. *Id.* at 1315.

The specification may reveal a special definition given to a claim term by the patentee, or the specification or prosecution history may reveal an intentional disclaimer or disavowal of claim scope by the inventor. *Id.* at 1316. “There are only two exceptions to this general rule: 1) when a patentee sets out a definition and acts as his own lexicographer, or 2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution.” *Thorner v. Sony Comput. Entm’t Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012).

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). The disavowal, if any, can be effectuated by language in the specification or the prosecution history. *Poly-Am., L.P. v. API Indus., Inc.*, 839 F.3d 1131, 1136 (Fed. Cir. 2016).

Only those claim terms that are in controversy need to be construed, and only to the extent necessary to resolve the controversy. *Realtime Data, LLC v. Iancu*, 912 F.3d 1368 (Fed. Cir. 2019) (“The Board is required to construe ‘only those 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))).

D. Alleged Obviousness of Claims 2, 4, 12, 15, 21, 23, 31, and 34 over Kesanupalli, Cheng, and Kodama

1. Overview of Kesanupalli (Exhibit 1006)

Kesanupalli discloses systems and methods which relate to biometric authentication of users. Ex. 1006, 2:30–31. Biometric information refers to measurable biological characteristics of a user, such as fingerprint, facial characteristics, eye characteristics, and voice characteristics. *Id.* at 2:31–35.

Figure 2 of Kesanupalli is reproduced below:

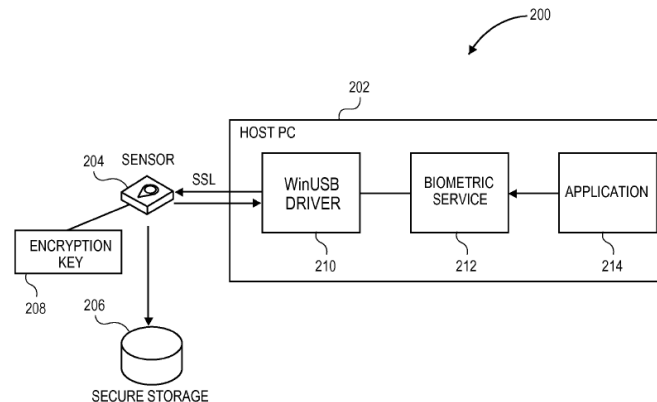


FIG. 2

Figure 2 illustrates sample system 200 for performing biometric user enrollment and authentication. Ex. 1006, 6:26–28. System 200 includes sensor 204, host PC 202, WinUSB driver 210, biometric service 212, application 214, and secure storage 206. *Id.* at 6:26–49.

During an enrollment process that uses a fingerprint sensor as the biometric sensor, a user swipes a finger across the fingerprint sensor several times to create a fingerprint template. Ex. 1006, 3:32–35. After creating a fingerprint template, the user provides user credentials, such as a password, cryptographic key, or random seed. *Id.* at 3:41–44. The system then binds the user's fingerprint template with the user's credentials and stores the template and the credentials in a secure storage device. *Id.* at 3:44–47.

During a subsequent user identification process, referred to as user verification process, a user swipes a finger across a fingerprint sensor. Ex. 1006, 3:52–53. The process then determines whether the user's fingerprint information matches a fingerprint template associated with the fingerprint sensor. *Id.* at 3:54–56. If the user's fingerprint information matches a fingerprint template, the user's credentials are released to the user and/or a service or process requesting the user verification. *Id.* at 3:56–59. The user credentials are not reeleased from the secure storage device until a matching fingerprint template is confirmed. *Id.* at 3:59–61.

Figure 9 is reproduced below:

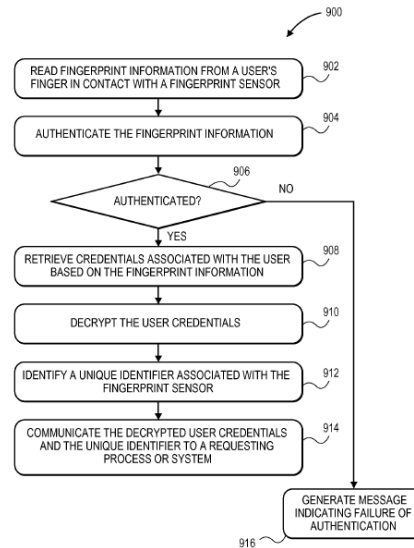


FIG. 9

Figure 9 illustrates a procedure for authenticating a user in a biometric authentication system. Ex. 1006, 2:6–7.

Kesanupalli describes that its system will send user credentials to a predetermined address or location:

The described systems and methods communicate user credentials to a specific address, location, or other recipient identifier. Thus, even if an imposter can gain access to the user credentials, the system will send those user credentials to a predetermined address or location, thereby preventing the imposter from attempting to have the user credentials sent to an alternate address or location. The address or location information is stored within the user credentials and is established as part of the enrollment process.

Ex. 1006, 4:3–11. Kesanupalli describes that its systems and methods are useful in performing Web site authentication. *Id.* at 4:36–37. Kesanupalli explains:

After a user has enrolled with a particular Web site that supports biometric authentication, subsequent visits to the same Web site cause the Web browser plug-in to detect that the user has already enrolled with the Web site. In this situation, the Web site prompts the user to perform user authentication (e.g., using

the biometric device). In the case of a fingerprint sensor, the user swipes their finger across the fingerprint sensor or places their finger on the fingerprint sensor. If the fingerprint information matches a fingerprint template associated with the fingerprint sensor, the Web browser plug-in releases user secrets from the user credentials. In particular embodiments, the fingerprint sensor releases an OTP token or an RSA signature instead of plain-text credential. After the credentials are released, they are communicated to the Web site to complete the user authentication process.

Ex. 1006, 5:9–24. Kesanupalli also describes that “different user credentials are associated with each Web site with which the user enrolls.” *Id.* at 5:35–37.

2. *Overview of Cheng (Ex. 1008)*

Cheng discloses a method “to securely backup and restore a user’s portable biometrics-based authentication device without compromising the security thereof.” Ex. 1008, code (57). The method has a two-tier backup encryption structure which allows decryption of lower-tier data only when upper tier data has been decrypted and validated. *Id.* The lower-tier data contain encrypted electronic identity of a user and authentication information associated therewith such as private keys and corresponding certificates. *Id.* The upper-tier data contain the encrypted lower-tier data and the user’s biometrics information. *Id.* Figure 2 of Cheng is reproduced below:

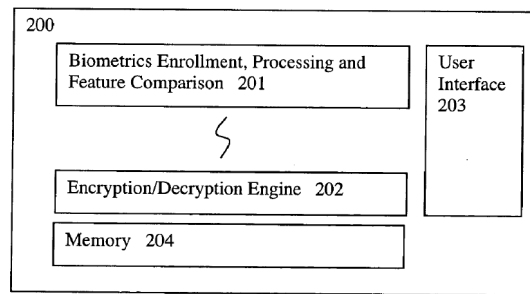


FIG. 2

Figure 2 shows a sample portable biometrics-based authentication device according to Cheng. Ex. 1008 ¶ 22. Portable device 200 includes user-interface means 203, memory means 204, encryption/decryption engine 202, and biometrics processing means 201. *Id.* Onboard microprocessor and communication means are not shown. *Id.*

Cheng describes that to backup a device, the lower-tier data are first enciphered using a first encryption means, and the upper-tier data are then enciphered using a second encryption means. Ex. 1008 ¶ 8. Cheng describes:

In an embodiment, the encryption keys for both the upper and lower tiers are separately generated within the device. In a preferred embodiment, the device obtains a first encryption key from a first user service bureau. The lower tier data is encrypted with this encryption key. Then, the device obtains a second encryption key from a second user service bureau, which may or may not be the same as the first user service bureau, and the upper tier data are further encrypted using the second encryption key, generating a multiple-encrypted backup file. The multiple-encrypted backup file is then copied to a storage medium of user's choice.

Ex. 1008 ¶ 8. Cheng further describes:

The storage means could be, for instance, an online proprietary or Internet-based storage service, a remote server, a floppy disk, a hard drive, a data drive, a CD-ROM, an optical storage means,

a removable disk, a smart card, a memory storage device or any other storage media capable of storing data. The user service bureau could be proprietary or Internet-based and could also provide the storage service.

Id. ¶ 29.

To restore already backed-up data onto a new device, Cheng states as follows:

To restore the multiple-encrypted backup data onto a new biometrics-based authentication device, the user first needs to enroll the relevant biometrics in the new device and upload the multiple-encrypted backup data onto the device, then contact the corresponding user service bureau to obtain an access clearance to the encrypted lower and upper tier encryption keys. The access clearance enables the device to establish a secure connection with the user service bureau service. Upon establishing the secure connection, the restore process begins automatically. The device first requests the upper tier data decryption key from the user service bureau server to decipher the encrypted upper tier data. The device then compares the decrypted backup biometrics data with the newly enrolled biometrics data. If they match, then the newly enrolled biometrics data are replaced with the decrypted backup biometrics data. Only then, will the system confirm the match to the user service bureau server and request the lower tier decryption key. Once the lower tier decryption key is received, the lower tier data is deciphered and stored in the device. This completes the restore process. If they do not match, the restore process is terminated. When the restore process is complete or otherwise terminated, the device automatically disconnects from the user service bureau and communicates the results to the user.

Id. ¶ 9.

3. *Overview of Kodama (Ex. 1010)*

Kodama relates to a system and method for mitigating risk of third party using backup data without authorization when restoring such backup data onto a user device such as an HDD (hard disk drive) recorder.

Ex. 1010, code (57). An online backup service system first registers authentication information of a user and also the authentication information of an engineer at a repair plant. *Id.* Thereafter, the registered authentication information of the user is used when backing up the data recorded in the HDD to the online backup service system, and the second authentication information is used when restoring the data already backed up to the online backup service system. *Id.* The user also receives an email from the online backup system regarding who restored what data at what time, so that the user can audit the data restoration process independently of the person recovering the backup data. *Id.*

Kodama describes that, previously, if an HDD recorder malfunctions and is then repaired, the recorder is returned to the user “in a status where only the hardware is repaired, and in most cases the data that was stored in the HDD recorder is lost.” Ex. 1010 ¶4. Kodama describes that its invention relates to a service of backing up data recorded in an electronic appliance such as an HDD recorder, and if the HDD recorder malfunctions, “recovering the data recorded in the HDD recorder using the data backed up to the online backup service system in addition to repairing the HDD recorder at a repair plant.” *Id.* ¶2.

Kodama describes that although the user may acquire backup data from an online storage, “there are users who are unfamiliar with the handling of electronic appliances.” Ex. 1010 ¶4. Kodama states: “[I]t would be much more convenient for the user if the data recovery process of HDD recorders is performed by an engineer of the repair plant together with the repair of the HDD recorder.” *Id.*

Figure 1 of Kodama is reproduced below:

FIG.1

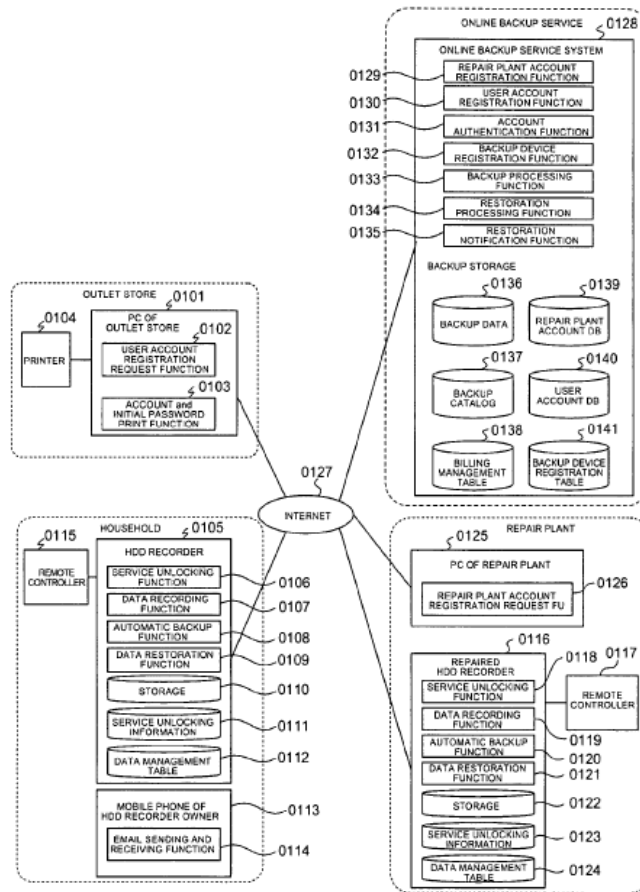


Figure 1 is a system configuration diagram showing an embodiment of Kodama. Ex. 1010 ¶ 10. HDD recorder 0105 in user's household, PC 0125 at a repair plant, PC 0101 at an outlet store, and online backup service system 0128 are all interconnected through Internet 0127. Kodama states the following regarding the service provided by its system:

The service provided by this service system includes backing up the data recorded in an HDD recorder used by a user subscribing to the service to an online backup service system via a network, and, if the HDD recorder malfunctions, repairing the HDD recorder at a repair plant and thereafter restoring the data recorded in the HDD recorded from the online backup service system to the repaired HDD recorder at the repair plant, and then returning the HDD recorder to the user. This service may also

include the service of copying or migrating the data recorded in an old HDD recorder installed at home to a new HDD recorder purchased at an outlet store.

Ex. 1010 ¶ 34.

Kodama further describes:

The backup target appliance is not limited to an HDD recorder, and the present invention can be applied to any electronic appliance such as a mobile phone, a PDA or a PC that is capable of loading the foregoing functions (i.e., any electronic appliance including a communication function and a function for recording information).

Ex. 1010 ¶ 40. Kodama states: “Moreover, there is no particular limitation in the backup target data upon applying the present invention and, in addition to TV programs, the backup target data may be music or emails, address books, files or the like.” *Id.* ¶ 41.

The online backup service system 0128 comprises a repair plant account registration function 0129, a user account registration function 0130, an account authentication function 0131, a backup device registration function 0132, a backup processing function 0133, a restoration processing function 0134, and a restoration notification function 0135. Ex. 1010 ¶ 43. The online backup service system 0128 includes storage 0136 for storing backup data and management information, and is configured from an online backup server and a storage system. *Id.* ¶ 45.

Kodama describes another embodiment where “data is restored to a new HDD recorder by the repair plant at the point in time that it is discovered that the HDD recorder 0105 may malfunction, and replacing the HDD recorder 0105 with the new HDD recorder before or immediately after the malfunction of the HDD recorder 0105.” Ex. 1010 ¶ 160. Kodama describes:

When it is determined that a malfunction has occurred, *data backed up by the user is restored in the same model as the HDD recorder owned by the user*. If the HDD recorder 0105 owned by the user malfunctions, after confirming that all backup data has been restored to the new HDD recorder by comparing the data management table 0112 of the HDD recorder 0105 and the backup management table of the online backup service system 0128, the new HDD recorder is sent to the user, and the user returns [] the failed HDD recorder.

Id. ¶ 161 (emphasis added).

4. *Claim 1 (base claim for claims 2, 4, 12, and 15)*

a. *Preamble recitation [1.0]*

The preamble recites: “A system, comprising:.” Ex. 1001, 24:47. Petitioner asserts that Kesanupalli discloses a system, i.e., system 200. Pet. 20–21 (citing Ex. 1003 ¶¶ 91–93, Ex. 1006, 2:1–2, code (57), Figs. 11–12). Petitioner’s assertions are supported by the cited evidence and not disputed by Patent Owner. We need not determine whether the preamble is limiting. Petitioner sufficiently establishes that Kesanupalli discloses a system.

b. *Limitation [1.1]*

Limitation [1.1] recites: “one or more processors configured to:.” Ex. 1001, 24:48. Petitioner explains:

Kesanupalli describes what POSITA would readily recognize—namely that functions of authentication translation and communication with external resources such as discussed in Section IX.A.1 and detailed below are performed by *one or more processors*. *Id.*; APPL-1006, 9:58–10:1. The processor functions of authentication (*e.g.*, those of sensor 204 such as matching) and the processor functions of communicating with an external resource (*e.g.*, those of HOST PC 202) together provide *one or more processors*. *See id.*, APPL-1006, 5:62–6:31, 6:40–49.

Pet. 21–22.

Petitioner's assertions are supported by the cited evidence and not disputed by Patent Owner. Petitioner sufficiently establishes that Kesanupalli discloses limitation [1.1].

c. Limitation [1.2]

Limitation [1.2] recites: “receive, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;.” Ex. 1001, 24:49–51.

Petitioner refers to Kesanupalli's Figure 2 as illustrating biometric sensor 204, secure storage 206, and Host PC 202 including web browser application executing thereon as together constituting a first device that provides authentication translation and ultimately communicates user credentials to web servers. Pet. 22–23 (citing Ex. 1003 ¶¶ 100–102, Ex. 1006, code (57), 2:54–3:3, 4:3–11, 4:36–50, 6:11–49). Petitioner further asserts that if Patent Owner argues that the claimed device has to be integrally-formed, a POSITA would understand Kesanupalli as disclosing integrally-formed realizations of such a device. *Id.* at 23 (citing Ex. 1003 ¶ 102, Ex. 1006, 2:48–50, 3:48–51). Kesanupalli states: “In particular embodiments, the biometric sensor is physically attached (or manufactured into) a client device such as a computer, cellular phone, and so forth.” Ex. 1006, 2:48–50. Kesanupalli also states: “In one embodiment, the secure storage device is contained within the fingerprint sensor hardware. In other embodiments, the secure storage device is contained in a device that utilizes the fingerprint sensor.” Ex. 1006, 3:48–51.

Petitioner further explains:

Kesanupalli describes processor(s) *receiv[ing]*, at Host PC 202 of the first device, a *request* (visit to a website by user of PC 202) *to access a resource* (website) *external to the first device*.

APPL-1006, 5:9–14 (“. . . **subsequent visits to the same Web site** cause the Web browser plug-in to detect that the user has already enrolled . . . , the Web site prompts the user to perform user authentication (*e.g.*, using the biometric device).”) *See also*, APPL-1006, 2:54–3:3, FIGS. 10–11. A user accessing/visiting a website in which she has enrolled means the user has made a *request* to access the site. APPL-1003, ¶¶ 103-105.

Pet. 23 (alterations in original). Petitioner asserts that the request to access the resource is received by the processor of PC 202. *Id.* at 24 (citing Ex. 1006, 6:11–31, Fig. 2). Petitioner also asserts that the website visited by the user is a resource external to the first device “as it is provided on a web server external to the first device.” *Id.* (citing Ex. 1006, 6:11–15, Fig. 12). Petitioner further asserts that the website is a resource associated with a user “as the user has visited the resource and previously enrolled.” *Id.* (citing Ex. 1006, 3:32–51, Figs. 7, 11).

Petitioner’s assertions are supported by the cited evidence and not disputed by Patent Owner. Petitioner sufficiently establishes that Kesanupalli discloses limitation [1.2].

d. Limitation [1.3a]

Limitation [1.3a] recites: “access at least one record stored in the first device, the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access,.” Ex. 1001, 24:52–56.

Petitioner asserts that Kesanupalli describes a user’s enrollment process in an external resource such as a website where the user’s credential (key) and biometric template (fingerprint template) associated with the user and the website are stored in secure storage 206 of the first device. Pet. 25

(citing Ex. 1006, 3:32–51, 8:29–53, Fig. 7). Petitioner explains that the user’s credential bound with a biometric template is a record in secure storage 206 of the first device, that Kesanupalli’s user credential is credential information associated with the external resource (website) to which the user has requested access, and that Kesanupalli’s biometric template (fingerprint template) is authentication information associated with the user as it is the user’s personal biometric data. Pet. 25 (citing Ex. 1003 ¶¶ 110–112, Ex. 1006, 4:36–5:43, Ex. 1019).

Petitioner explains that after enrollment including creating and storing the record, a user’s subsequent visits to the external resource initiate an authentication procedure, and that this authentication procedure includes the processor(s) accessing the record in storage to perform the authentication and accessing the record in storage to release the credential of the record to the requesting resource upon a successful match. Pet. 25–26 (citing Ex. 1006, 3:51–4:1, 5:9–14, 8:54–9:24, Figs. 9, 12).

Petitioner asserts that Kesanupalli’s one or more processors access secure storage 206 to obtain the biometric template of the record so the processor can determine if there is a match of biometric input to the template, and again access secure storage 206 to release the credential and communicate it to the external resource using application 214 on a successful match. *Id.* at 26–27 (citing Ex. 1006, 3:44–51, 6:42–49, Figs. 2, 12).

Petitioner’s assertions are supported by the cited evidence and not disputed by Patent Owner. Petitioner sufficiently establishes that Kesanupalli discloses limitation [1.3a].

e. Limitation [1.3b]

Limitation [1.3b] recites: “wherein the credential information comprises a cryptographic key;” Ex. 1001, 24:56–57. Petitioner asserts that Kesanupalli describes “credential information,” which it describes as “user credentials,” exemplified by a “*cryptographic key*.” Pet. 27 (citing Ex. 1003 ¶¶ 46–54, Ex. 1006, 3:32, 3:65–4:1, 8:6–22, Fig. 12). Petitioner’s assertions are supported by the cited evidence and not disputed by Patent Owner. Petitioner sufficiently establishes that Kesanupalli discloses limitation [1.3b].

f. Limitation [1.4]

Limitation [1.4] recites: “receive authentication input from the user;” Ex. 1001, 24:58.

Petitioner explains:

Kesanupalli describes one or more processors *receive an authentication input (e.g., biometric input) from the user*. Kesanupalli describes sensor (204) circuitry receives an authentication input of a fingerprint. APPL-1006, 6:31–34 (“a **fingerprint swipe or fingerprint scan** (using a placement style fingerprint sensor”), 9:10–14 (“**. . . procedure 900 reads fingerprint information from a user’s finger in contact with a fingerprint sensor (902)**.”), 8:54–9:3, FIG. 12 “provide[s] biometrics.”). Kesanupalli also describes other types of authentication input from the user. APPL-1006, 2:30–38.

Pet. 27–28 (alterations in original).

Petitioner’s assertions are supported by the cited evidence and not disputed by Patent Owner. Petitioner sufficiently establishes that Kesanupalli discloses limitation [1.4].

g. Limitation [1.5]

Limitation [1.5] recites: “determine that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;.” Ex. 1001, 24:59–62.

Petitioner asserts that Kesanupalli’s one or more processors (executing functions of sensor 204) determine the authentication input from the user, such as fingerprint, and match the authentication information associated with the user (fingerprint template) included in the at least one record (bound template and credential) stored in secure storage 206 on the first device. Pet. 28 (citing Ex. 1003 ¶ 124; Ex. 1006, 3:32–51). Petitioner further explains that Kesanupalli describes the processor executing functions of sensor 204 when performing the matching. *Id.* (citing Ex. 1006, 3:52–4:2, 5:9–24, 6:31–49, 8:59–9:24, Figs. 2, 12).

Petitioner’s assertions are supported by the cited evidence and not disputed by Patent Owner. Petitioner sufficiently establishes that Kesanupalli discloses limitation [1.5].

h. Limitation [1.6]

Limitation [1.6] recites: “retrieve at least a portion of the credential information from the at least one record stored on the first device;.” Ex. 1001, 24:63–64.

Petitioner explains that processor circuitry of sensor 204 retrieves the credentials from the record in storage so that the credential can be transmitted to a requesting resource such as the website. Pet. 29 (citing Ex. 1006, 9:14–20). Petitioner also notes that in Kesanupalli’s Figure 2, it is shown that processor circuitry of sensor 204 retrieves the credential from

record in storage 206 and provides the credential to PC 202, which in turn sends the credential to the requesting service. *Id.* (citing Ex. 1006, 3:52–4:11, 5:17–32, 6:42–45, 8:59–9:24, Figs. 2, 8–9). Petitioner asserts that retrieving the credential is retrieving at least a portion of the credential information. *Id.*

Petitioner’s assertions are supported by the cited evidence and not disputed by Patent Owner. We are sufficiently persuaded that Kesanupalli discloses limitation [1.6].

i. Limitation [1.7]

Limitation [1.7] recites “facilitate access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and.” Ex. 1001, 24:65–25:6.

Petitioner cites to Kesanupalli’s column 9, lines 4–24, which states:

If the fingerprint information read by the fingerprint sensor matches the information stored in the fingerprint template, the biometric authentication system retrieves the credentials associated with the user (block 810). The user credentials are then communicated to a requesting process or system (block 812).

FIG. 9 is a flow diagram depicting another embodiment of a procedure 900 for authenticating a user of a biometric authentication system. Initially procedure 900 reads fingerprint information from a user’s finger in contact with a fingerprint sensor (902). The procedure then authenticates the fingerprint information (block 904). If the fingerprint information is not authenticated, a message is generated indicating an

authentication failure (block 906). If the fingerprint information is authenticated, the procedure retrieves credentials associated with the user based on the fingerprint information (block 908). The procedure then decrypts the user credentials (block 910) and identifies a unique identifier associated with the fingerprint sensor (block 912). The decrypted credentials and the unique identifier are communicated to a requesting process or system (block 914).

Ex. 1006, 9:4–24 (cited at Pet. 30).

Petitioner explains: “In FIG. 2, the user credential (*e.g.*, cryptographic key) is retrieved from secure storage 206 and PC 202 communicates it to the external resource. APPL-1006, 6:11–49.” Pet. 30. Petitioner also reproduces the following annotated version of Kesanupalli’s Figure 12, on page 30 of the Petition:

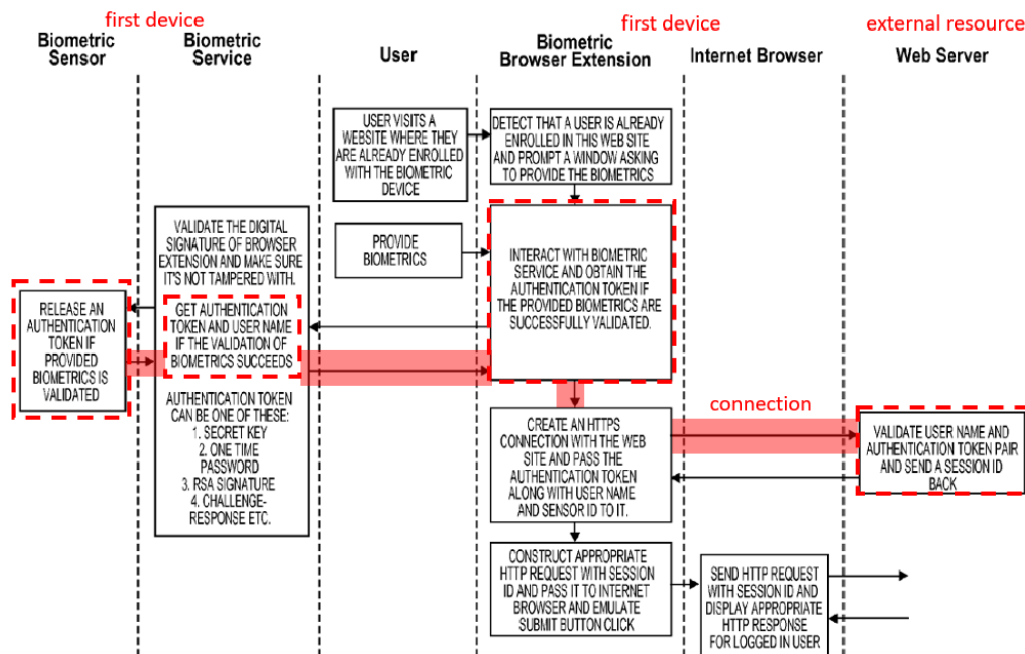


Figure 12 depicts a procedure for identifying and authenticating a user of a biometric authentication system. Ex. 1006, 2:22–23. Petitioner has highlighted in red a path through this procedure from validating user

biometrics to making a connection with the external resource and providing authentication to the external resource.

Petitioner explains:

When Kesanupalli transmits the user credential to the requesting website as discussed, it does so on *behalf of the user* as its the **user’s** credential, which is transmitted **in response to the user’s request** to access the website. The user credential is *output based at least in part on the at least portion of the credential information* as the output is the user credential itself—*e.g., the cryptographic key. The user of the first device is granted access to the external resource (website) based at least in part on the output (user credential)* because the credential is used to login the user to the external resource. APPL-1003, ¶¶135–136, APPL-1006, FIG. 12 (“logged in user”), 5:22–24 (“to the Web site to complete the user authentication process”). Processing circuitry of sensor 204 facilitates this by transmitting the credential to the processor (PC 202 and application 214), which in turn transmits the credential to the web server of the resource. Thus, sensor 204 and PC 202 provide *one or more processors that facilitate access of the user to the external resource by transmitting the credential information.*

Pet. 30–31 (alteration by Petitioner).

Petitioner’s assertions are supported by the cited evidence and not disputed by Patent Owner. We are sufficiently persuaded that Kesanupalli discloses limitation [1.7].

j. Limitation [1.8]

Limitation [1.8] recites “based at least in part on the first device being a same brand as a second device, initiate a backup, to the second device, of at least a portion of the at least one record.” Ex. 1001, 25:7–10.

Petitioner asserts that in light of the teachings of Cheng, it would have been obvious for one or more processors of Kesanupalli to initiate a backup to a second device of at least a portion of the at least one record of

Kesanupalli's device. Pet. 32 (citing Ex. 1003 ¶¶ 141–144). Petitioner explains:

In particular, Cheng teaches initiating *a backup* of data of a first device to a *second device* by registering a first device with a storage location, such as a user service bureau, generating a “backup file(s)” of the device's data, and providing the backup file from the first device to the user service bureau (storage). *See* APPL-1008, Abstract, [0002], [0007]–[0008], [0023]–[0030], FIGS. 3A–3B. Cheng describes exemplary data for backup includes user authentication information, such as key and biometric data, which is the same type of data as in Kesanupalli's *record* (user credential and biometric template). APPL-1003, ¶142; APPL-1008 [0007]–[0008], [0030], FIGS. 3A–3B.

Pet. 32 (emphasis in original). The above-quoted explanation appears to be based on rational reasoning and supported by the cited evidence, so long as the referenced “second device” is at the user service bureau. However, Petitioner continues with the following further explanation which we find problematic and misplaced:

Cheng's backup procedure provides the backup data from the storage location (user service bureau) to a *second device*, which in some implementations is a new device replacing the user's first device. APPL-1008, FIGS. 4A, 5, [0009], [0045]—[0050]. Cheng describes “[t]he **new** biometrics-based authentication **device** establishes a secure connection with a user service bureau, begins the restore process and **downloads backup data from storage.**” APPL-1008, [0048]. *See also*, APPL-1008, FIGS. 4A–4C, [0009], [0031]–[0039] (restoration). As discussed above, POSITA would recognize applying Cheng's teachings to Kesanupalli's device to backup its *record* would provide a benefit allowing the user to save resources (*e.g.*, time) in recreating the data in the record (*e.g.*, biometric template and/or user credential) on the second device. APPL-1003, ¶144, 85–89. Thus, it would have been obvious to backup to the second device *at least a portion* of Kesanupalli's *record* in light of Cheng.

Pet. 32–33 (alterations and emphasis in original).

Petitioner mistakenly treats subsequent use of already backed-up data, stored at the user service bureau, to download into a new device, as a part of the act of backing up the data in the first instance. Cheng clearly distinguishes data backup from data restoration using already backed-up data. Ex. 1008 ¶¶ 8–9.

Cheng describes the following regarding backing up a device:

In an embodiment, the encryption keys for both the upper and lower tiers are separately generated within the device. In a preferred embodiment, the device obtains a first encryption key from a first user service bureau. The lower tier data is encrypted with this encryption key. Then, the device obtains a second encryption key from a second user service bureau, which may or may not be the same as the first user service bureau, and the upper tier data are further encrypted using the second encryption key, generating a multiple-encrypted backup file. *The multiple-encrypted backup file is then copied to a storage medium of user's choice.*

Ex. 1008 ¶ 8 (emphasis added). Cheng describes that the user service bureau could provide that backup storage service. *Id.* ¶ 29.

To place already backed-up data onto a new device, Cheng describes:

To *restore* the multiple-encrypted backup data onto a new biometrics-based authentication device, the user first needs to enroll the relevant biometrics in the new device and upload the multiple-encrypted backup data onto the device, then contact the corresponding user service bureau to obtain an access clearance to the encrypted lower and upper tier encryption keys. The access clearance enables the device to establish a secure connection with the user service bureau service. Upon establishing the secure connection, the restore process begins automatically. The device first requests the upper tier data decryption key from the user service bureau server to decipher the encrypted upper tier data. The device then compares the decrypted backup biometrics data with the newly enrolled

biometrics data. If they match, then the newly enrolled biometrics data are replaced with the decrypted backup biometrics data. Only then, will the system confirm the match to the user service bureau server and request the lower tier decryption key. Once the lower tier decryption key is received, the lower tier data is deciphered and stored in the device. *This completes the restore process.* If they do not match, the restore process is terminated. When the restore process is complete or otherwise terminated, the device automatically disconnects from the user service bureau and communicates the results to the user.

Ex. 1008 ¶ 9 (emphasis added).

Petitioner points to nothing in the specification of the '105 patent to indicate that the '105 patent treats subsequent restoration of data from backup storage onto a new device as backing up the original data from the device which had sent that data to backup storage, and we can find none. Petitioner does not assert that the inventor of the '105 patent is his own lexicographer and provided a special definition for “backup.” Petitioner also does not explain why the plain and ordinary meaning of “backup” would include subsequent download of already backed-up data onto a new device if and when the need for such restoration arises such as when the original device is lost or stolen. As noted above in Section III.D.2, Cheng also distinguishes “backup” from “restore.” The two operations are separate, occur at different times, and are not different parts of one backup operation. Petitioner cites to no testimony of its expert, Dr. McDaniel, which explains why subsequent data restoration from already backed-up data to a newly acquired device is a part of the initial data backup operation.

Citing paragraph 147 of Dr. McDaniel’s declaration, Petitioner asserts that “restoration” only to the same manufacturer/model means “initiating backup” to the second device is based at least in part on the manufacturer

being the same. Pet. 34. We have reviewed paragraph 147 of Dr. McDaniel's declaration and can find only a conclusory suggestion, without any explanation, that because already backed-up data from a first device is restored only to a second device of the same brand, Kodama discloses initiating backup to a second device only if the brand of the second device is the same as the brand of the first device. Ex. 1003 ¶ 147. The suggestion lacks persuasion because it is illogical, conclusory, and also contrary to the disclosures of Cheng, discussed above, which distinguish data backup and data restoration.

Accordingly, Petitioner has improperly mixed data backup with data restoration using already backed-up data. Petitioner has not sufficiently shown that the "new" device of Cheng is a second device to which data from Cheng's first device is backed up.

Petitioner's additional reliance on Kodama does not cure this deficiency. Kodama is merely relied on by Petitioner to account for the first and second devices being of the same brand. Pet. 33 ("Second, it would have been obvious to *initiate* Cheng's backup to a second device *based at least in part on the first device being a same brand as a second device* as taught by Kodama."). Like Cheng, Kodama also distinguishes data backup from data restoration. Kodama states the following:

The service provided by this service system includes *backing up the data* recorded in an HDD recorder used by a user subscribing to the service *to an online backup service system* via a network, and, if the HDD recorder malfunctions, repairing the HDD recorder at a repair plant and *thereafter restoring the data recorded in the HDD recorded from the online backup service system to the repaired HDD recorder at the repair plant*, and then returning the HDD recorder to the user.

Ex. 1010 ¶ 34 (emphasis added). Kodama describes another embodiment where “data is restored to a new HDD recorder by the repair plant at the point in time that it is discovered that the HDD recorder 0105 may malfunction, and replacing the HDD recorder 0105 with the new HDD recorder before or immediately after the malfunction of the HDD recorder 0105.” *Id.* ¶ 160. Kodama describes:

When it is determined that a malfunction has occurred, *data backed up by the user is restored in the same model as the HDD recorder owned by the user.* If the HDD recorder 0105 owned by the user malfunctions, after confirming that all backup data has been restored to the new HDD recorder by comparing the data management table 0112 of the HDD recorder 0105 and the backup management table of the online backup service system 0128, the new HDD recorder is sent to the user, and the user returns [] the failed HDD recorder.

Id. ¶ 161 (emphasis added). Consequently, Kodama as applied by Petitioner does not cure the deficiency of Petitioner’s reliance on Cheng.

Furthermore, even disregarding the above-noted deficiency of Cheng and assuming that Cheng discloses backing up of data from a first user device to a second, new user device, without any user service bureau in between, Petitioner has not shown sufficient motivation to combine the teachings of Kodama with the teachings of Kesanupalli and Cheng to account for the remainder of limitation [1.8], i.e., initiate the backup “based at least in part on the first device being a same brand as a second device.”

Ex. 1001, 25:7–10.

Petitioner explains:

Kodama continues its backup procedure by providing a *second device* associated with the user, which is registered with the backup service. In an example, the second device is a user’s “new” device. APPL-1010, [0160]. . . . Kodama again expands

on this registration by providing “[second] device information including the **manufacture name**” to the backup service. APPL-1010, [0135]–[0136]. The backup service then “**checks** whether there is an entry where the user account name, device name and **device information coincides.**” APPL-1010, [0137]. Kodama describes “[t]he **restoration is permitted when the manufacturer name and the model number of the restoration target appliance coincide.** This embodiment explains a case where restoration is **permitted only** with the same model of the **same manufacturer.**” APPL-1010 [0138].

Pet. 34–35 (emphasis in original). Kodama’s same-brand requirement is applicable only to a restoration operation, not a backup operation.

Even Kodama itself expressly distinguishes “automatic backup processing” from “data restoration processing” by stating the following:

The processing flow for realizing the HDD recorder repair service system with data restoration is now explained by being dividing into (A) repair plant account registration processing, (B) service registration processing, (C) automatic backup processing, and (D) data restoration processing.”

Ex. 1010 ¶ 67.

Also, Kodama is concerned with security in restoration for a reason. In that regard, Kodama states: “an object of the present invention is to provide an electronic appliance service system capable of mitigating the risk of third party referring to or using backup data without authorization upon restoring such backup data in an electronic appliance.” Ex. 1010 ¶ 7.

However, unlike the circumstance in Kodama, where a third-party repair shop technician would have possession of the new replacement device as well as access to the user’s already backed-up data, there is no such third party in the described environment of Cheng. In Cheng, there is no broken device of a user being repaired by a third party, no new device in possession

by a third party to replace any broken device of the user, and no third party with access to already backed-up data from a first device of the user.

Requiring brand identity between the user's first device and a new device of the user does not mitigate the risks of any third-party misappropriation of sensitive data at issue and discussed in Kodama. The third-party misappropriation risks expressed in Kodama have little or no application in the context of Cheng.

Petitioner additionally asserts:

Considering Kesanupalli's device having Cheng's backup technique, POSITA would have had reason to employ Kodama's technique of controlling backup processes such that the first device and the second device (the source and target devices) are compatible. APPL, 1003, ¶89. Kodama recognizes "if data restoration is to be performed to a different product or a different manufacturer, the format and product proprietary information of the data between the products will differ." APPL-1010, [0157], [0158]. POSITA would recognize benefits of transfer of data between like brands, including ensuring different security protections for receipt and storage of personal data without introducing risk of compatibility issues. APPL-1003, ¶89.

Pet. 19. But the same brand requirement of Kodama is not provided to solve any problem with differing formats. Kodama states:

At Step 1313 of the restoration processing, if data restoration is to be performed to a different product of a different manufacturer, the format and product proprietary information of data between the products will differ. Thus, before the restoration processing function of the online backup service system 0128 sends the data read at Step 1318 to the HDD recorder 0116, the data format is converted into the file format of the HDD recorder 0116 of the restoration destination.

Ex. 1010 ¶ 157. Kodama does not describe format compatibility as presenting any problem but simply notes that there should and would be

format conversion during the data restoration operation if the brands of the first and second devices are different. In this context, requiring brand identity between the user's first device and second device to perform data backup from the first device to the second device is not an advantage. Rather, it appears to be a hindrance and disadvantage for the user, and an application of improper hindsight in light of the '105 patent's disclosure.

For the foregoing reasons, Petitioner has not sufficiently shown that limitation [1.8] would have been suggested by the combined teachings of Kesanupalli, Cheng, and Kodama.

5. *Claim 18 (base claim for claims 21, 23, 31, and 34)*

Claim 18 recites similar subject matter as claim 1, but in method form. Ex. 1001, 26:4–32. The various functionalities recited in claim 1 are recited as method steps in claim 18. *Id.* Petitioner presents essentially the same arguments to claim 18 as it does for claim 1. Pet. 40–42. For substantially the same reasons as we explained above in the context of limitation [1.8] of claim 1, Petitioner has not sufficiently shown that the corresponding limitation in claim 18 would have been suggested by the combined teachings of Kesanupalli, Cheng, and Kodama.

6. *Dependent Claims 2, 4, 12, 15, 21, 23, 31, and 34*

Claims 2, 4, 12, and 15 each depend directly from claim 1. Ex. 1001, 25:14–16, 25:22–24, 25:56–57, 25:63–64. Claims 21, 23, 31, and 34 each depend directly from claim 18. *Id.* at 26:39–41, 26:46–48, 27:11–12, 27:18–20. The deficiency of Petitioner's accounting for claim 1 equally applies to claims 2, 4, 12, and 15. The deficiency of Petitioner's accounting for claim 18 equally applies to claims 21, 23, 31, and 34.

Petitioner has not shown a reasonable likelihood that it would prevail in establishing obviousness of claims 2, 4, 12, 15, 21, 23, 31, and 34 over Kesanupalli, Cheng, and Kodama.

E. Alleged Obviousness of Claims 5, 6, 24, and 25 over Kesanupalli, Cheng, Kodama, and Hubner

1. Overview of Hubner (Exhibit 1030)

Hubner describes an approach for enabling execution of data backup and restoration among a group of user devices. Ex. 1030, code (57). Specifically, Hubner states:

A data management platform detects at a source device, one or more peer devices capable of wireless communication with the source device. It then determines one or more of the peer devices as belonging to a backup device group according to a predetermined criterion. The data management platform 103 then designates data resident within the source device for backup and initiates transfer within the source device for backup and initiates transfer of the backup data to the backup device group over a wireless communication session.

Id. Figure 1 of Hubner is reproduced below:

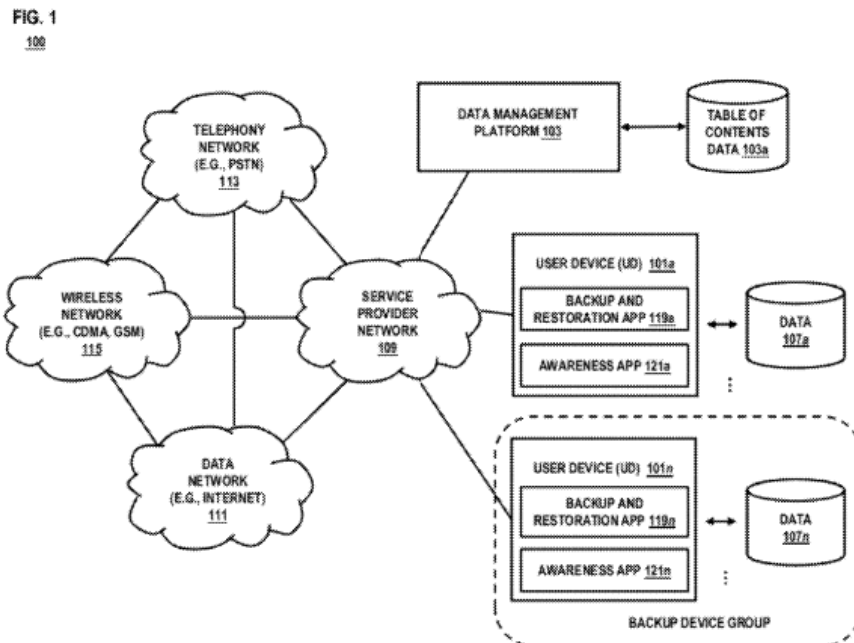


Figure 1 is a diagram of a system for enabling execution of data backup and restoration among a group of user devices. Hubner states:

[S]ystem 100 is shown to [include] one or more user devices (UD) 101a-101n (e.g., mobile device, smart phone, etc.), which are configured to communicate with each other to share data on a peer-to-peer basis and to coordinate such transfer with a data management platform 103. The platform 103 in essence provides backup and restoration services to these devices 101a-101n. The data management platform 103 can facilitate peer-distributed, network controlled data backup and restoration. In certain embodiments, “backup” of data pertains to the process [of] generating copies of data, such as maintained by a computing device, so that additional copies of data may be used when a restoration of data is required. Data backup and subsequent restoration may be required for various reasons, including data loss, file corruption or even computing system failure. . . . the backup device group can include one or more peer user devices configured to participate in the service.

Ex. 1030 ¶ 12.

According to Hubner, “[i]nformation acquired or generated by user devices 101a-101n is initially stored to internal memory 107a-107n.”

Ex. 1030 ¶ 14. Hubner explains:

[T]he data management platform 103 is configured to enable a group of peer devices 101a-101n belonging to a backup device group to regulate and manage the execution of the backup process. By way of these approaches, a source device (e.g., a requesting device of the backup device group) is able to ensure regular and timely performance of backups and/or restorations based in part on the detection of associated peer devices.

Id. ¶ 15.

2. *Claims 5, 6, 24, and 25*

Claim 5 depends from claim 1, and claim 24 depends from claim 18.

Each of claims 5 and 24 further recites: “wherein the first device and the

second device are configured to complete a pairing process.” Ex. 1001, 25:25–26, 26:49–51.

Claim 6 depends from claim 5, and claim 25 depends from claim 24. Each of claims 6 and 25 further recites: “wherein the pairing process comprises a comparison of data generated from one or more authentication inputs.” Ex. 1001, 25:27–29, 26:52–54.

Petitioner asserts that each of claims 5 and 6 would have been obvious over the combined teachings of Kesanupalli, Cheng and Kodama, and, alternatively, would have been obvious over the combined teachings of Kesanupalli, Cheng, Kodama, and Hubner. Pet. 49, 52. In either case, however, Petitioner’s assertions and reasoning based on Hubner do not relate to and do not cure the deficiency of Petitioner’s accounting for limitation [1.8] as discussed above in Section III.D.4.j, pertaining to insufficient motivation to combine Kodama’s same-brand teachings of a user’s first and second devices to the first and second devices of Kesanupalli as modified by Cheng.

Petitioner makes essentially the same arguments for claims 24 and 25 as Petitioner does for claims 5 and 6, respectively. Pet. 55. Petitioner’s assertions and reasoning based on Hubner do not relate to and do not cure the deficiency of Petitioner’s accounting for claim 18 with regard to requirements corresponding to limitation [1.8] as discussed above in Section III.D.4.j and Section III.D.5, pertaining to insufficient motivation to combine Kodama’s same-brand teachings of a user’s first and second devices to the first and second devices of Kesanupalli as modified by Cheng.

For the foregoing reasons, Petitioner has not shown a reasonable likelihood that it would prevail in establishing obviousness of claims 5, 6, 24, and 25 over Kesanupalli, Cheng, Kodama, and Hubner.

F. Alleged Obviousness of Claims 2, 4, 12, 15, 21, 23, 31, and 34 over Jakobsson '351 and Kodama

1. Overview of Jakobsson '351 (Exhibit 1011)

Jakobsson '351 is a patent that issued from an ancestral application of the '105 patent, i.e., Application No. 15/042,636. Ex. 1001, code (63). Petitioner expressly acknowledges that Jakobsson '351 lacks a teaching of “based at least in part on the first device being a same brand as a second device, initiat[e/ing] a backup, to the second device,” which is a limitation of each of the challenged claims of the '105 patent. Pet. 55.

Petitioner relies primarily on claims 1 and 16 of Jakobsson '351, in combination with Kodama, to render obvious claim 1 of the '105 patent. Pet. 57–63. Claims 1 and 16 of Jakobsson '351 are reproduced below:¹⁰

1. [1.0] A system, comprising:
 - [1.1] one or more processors configured to:
 - [1.2] receive, at an authentic translator at a device, an authentication input and an indication of a request, by a user of the device, to access a resource external to the device;
 - [1.3] in response to determining, by the authentication translator at the device, a match using the received authentication input, obtain access to a record stored on the device, wherein the record is associated at least with the external resource;
 - [1.4] retrieve, from the stored record accessed at least in part by determining, by the authentication translator at the device, the

¹⁰ We added the bracketed heading labels to each claim element to provide ease of reference.

match using the received authentication input, a previously stored credential associated with the external resource, wherein the previously stored credential is different from the received authentication input, and wherein the previously stored credential retrieved from the record stored on the device comprises at least one of a cryptographic key and a cookie;

[1.5] establish a connection between the device and the external resource to which the user requested access; and

[1.6] facilitate a login of the user to the external resource at least in part by transmitting, on behalf of the user, from the device and via the established connection, output based at least in part on the at least one of the cryptographic key and the cookie retrieved from the record accessed at least in part by determining, by the authentication translator at the device, the matching using the retrieved authentication input, wherein the user of the device is logged into the external resource based at least in part on the output transmitted from the device on behalf of the user; and

[1.7] a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.

Ex. 1011, 10:50–11:21.

16. [16.0] The system of claim 1, wherein the one or more processors are further configured to:

[16.1] encrypt and authenticate at least a portion of the record;
and

[16.2] perform a backup of the encrypted and authenticated record to a remote storage entity, wherein the remote storage entity is configured to synchronize records between at least two devices associated with the user.

Id. at 12:13–20.

2. *Claim 1 (base claim for claims 2, 4, 12, and 15)*

Petitioner asserts that Jakobsson '351's claim 1 preamble [1.0] teaches preamble [1.0] of claim 1 of the '105 patent. Pet. 57 (citing Ex. 1003 ¶¶ 199–200, Ex. 1011, 10:50). Patent Owner does not argue otherwise.

Petitioner asserts that Jakobsson '351's claim 1 limitation [1.1] teaches limitation [1.1] of claim 1 of the '105 patent. Pet. 58 (citing Ex. 1011, 10:51). Patent Owner does not argue otherwise.

Petitioner asserts that Jakobsson '351's claim 1 limitation [1.2] teaches limitation [1.2] of claim 1 of the '105 patent. Pet. 58 (citing Ex. 1003 ¶¶ 203–204). Patent Owner does not argue otherwise.

Petitioner asserts that Jakobsson '351's claim 1 limitations [1.3] and [1.4] together with Jakobsson '351's corresponding description that a stored template is used for matching authentication input and that the template comprises at least one of a fingerprint feature, a voice biometric feature, a facial recognition feature, an iris detection feature, and a retina scan feature, teach limitations [1.3a] and [1.3b] of claim 1 of the '105 patent. Pet. 58–59 (citing Ex. 1003 ¶¶ 205–208). Patent Owner does not argue otherwise.

Petitioner asserts that Jakobsson '351's claim 1 limitations [1.2] and [1.3], together with recognizing that a stored template is “authentication information associated with the user included in the at least one record on the first device and is used for the matching,” teach limitations [1.4] and [1.5] of claim 1 of the '105 patent. Pet. 59–60 (citing Ex. 1003 ¶¶ 209–212, Ex. 1011, 4:55–68, 11:45–50, Fig. 2). Patent Owner does not argue otherwise.

Petitioner asserts that Jakobsson '351's claim 1 limitation [1.4] teaches limitation [1.6] of claim 1 of the '105 patent. Pet. 60 (citing Ex. 1011, 10:61–11:[3], 12:4–7). Patent Owner does not argue otherwise.

Petitioner asserts that Jakobsson '351's claim 1 limitations [1.5] and [1.6] together teach limitation [1.7] of the '105 patent. Pet. 60–61 (citing Ex. 1003 ¶¶ 215–216). Patent Owner does not argue otherwise.

Limitation [1.8] of claim 1 of the '105 patent reads as follows: “based at least in part on the first device being a same brand as a second device, initiate a backup, to the second device, of at least a portion of the at least one record.” Ex. 1001, 25:7–10. Petitioner asserts that this feature is suggested by the combined teachings of Jakobsson '351 and Kodama. Pet. 61.

First, Petitioner cites to claim 16 of Jakobsson '351, which depends from claim 1 of Jakobsson '351 and reads as follows:

16. The system of claim 1, wherein the one or more processors are further configured to:

encrypt and authenticate at least a portion of the record; and

perform a backup of the encrypted and authenticated record to a remote storage entity, *wherein the remote storage entity is configured to synchronize records between at least two devices associated with the user.*

Ex. 1011, 12:13–20 (emphasis added). Thus, Petitioner regards the synchronization of data being backed up from a user device to a remote storage facility among different devices of the user as backing up the same data to the other devices of the user. Without deciding whether such a position is likely correct, we continue with the analysis of the remainder of limitation [1.8] of claim 1 of the '105 patent, which requires the backup to be initiated from the record stored in the first device to a second device “based at least in part on the first device being a same brand as a second

device.” Ex. 1001, 25:7–10. For that aspect of limitation [1.8], Petitioner relies on Kodama. Pet. 61–63.

Petitioner explains:

Kodama teaches registering a first device with a backup service [and] explaining this registration includes device information of a *brand* (e.g., manufacture name). See APPL-1010, [0101], [0103]; APPL-1003, ¶¶221-222. See also, APPL-1010 [0078]–[0104], FIG. 4, [0054], FIG. 6, [0061]. Kodama then continues the backup process by sending a copy of the data of the first device to the backup service. APPL-1010 [0106]–[0107]. See also, APPL-1010 [0108]–[0118]. Thus Kodama teaches providing a *brand* of the first device to the backup service.

Kodama further registers a *second device* (e.g., a “new” device) associated with the backup service. APPL-1010, [0160], [0157], [0137]. The registration includes providing “[*second*] device information including the manufacturer name, model name and product serial number.” APPL-1010, [0135]–[0136]. The backup service system “checks whether there is an entry where the user account name, device name and **device information coincides**.” APPL-1010 [0137]. “[T]he restoration is permitted when the **manufacturer name** and the model number of the restoration target appliance **coincide**. This embodiment explains a case where **restoration is permitted only with the same model of the same manufacturer**.” APPL-1010, [0138]. Permitting restoration only when the manufacturer and model are the same means *initiating* of backup to the second device is based on the manufacturer being the same—*i.e.*, brand is the same. See also, APPL-1010 [0143]–[0144]. Therefore, Kodama discloses *initiating a backup* to a second device based *at least in part on* the brand (e.g., manufacturer name) of the first device being the same as the second device.

Pet. 61–62 (alterations and emphasis in original). Regarding motivation to combine teachings of Jakobsson ’351 and Kodama, Petitioner asserts:

[A] POSITA would have found it predictable to apply Kodama’s teachings to Jakobsson ’351’s backup process. APPL-1003, ¶197. Jakobsson ’351 describes the desire to back up or

synchronize data across a user's devices. APPL-1011, 7:37-41. Kodama recognizes "if data restoration is to be performed to a different product or a different manufacturer, the format and product proprietary information of data between the products will differ." APPL-1010, [0157]. POSITA would recognize this differing format can create compatibility issues and thus would recognize an advantage of, and reason for, basing the initiation of data transfer to the second device on brand and thereby avoiding these compatibility issues as taught by Kodama. APPL-1003, ¶197. Kodama also describes its system "mitigat[es] the risk of a third party referring to or using backup data without authorization upon restoring such backup data in an electronic appliance." APPL-1010, [0007]. One way it provides this benefit is by ensuring the source and target devices are the same brand and therefore have similar safeguards.

Pet. 56–57.

For reasons discussed below, Petitioner's assertions and reasoning are misplaced and not sufficiently persuasive even for institution purposes.

First, as in the case of analyzing limitation [1.8] in the ground of unpatentability based on Kesanupalli, Cheng, and Kodama, discussed above in Section III.D.4.j, Petitioner has improperly mixed data backup with data restoration using already backed-up data. The so-called "new" device in Kodama, which Petitioner regards as the claimed "second device" of limitation [1.8], is a device onto which already backed-up data from the user's first device is restored and not a device onto which data from the user's first device is backed up.

As Petitioner recognizes, Kodama teaches registering a first device with a backup service and then sending a copy of the registered first device's data to a backup service. Pet. 61–62 (citing Ex. 1003 ¶¶ 221–222, Ex. 1010 ¶¶ 101, 106–107). This is the backup process described by Kodama, and

Petitioner's identified second device is not any portion of this backup service for backing up data.

As Petitioner also recognizes, Kodama describes that subsequent to backing up data from a user device to the backup service, and if and when a new device of the same brand for the user is obtained, the already backed-up data in the backup service will be restored to the new device. Pet. 62 (citing Ex. 1010 ¶¶ 135–138, 143–144, 157, 160). Petitioner has not provided a claim construction for the term “backup,” and we have no reason to regard the data restoration process which loads already backed-up data from a backup service to the user's new device as a part of the initial data backup process from the first device to the backup service. Even Kodama itself expressly distinguishes “automatic backup processing” from “data restoration processing” by stating the following:

The processing flow for realizing the HDD recorder repair service system with data restoration is now explained by being dividing into (A) repair plant account registration processing, (B) service registration processing, (C) automatic backup processing, and (D) data restoration processing.”

Ex. 1010 ¶ 67.

Thus, Petitioner incorrectly asserts that Kodama discloses initiating a backup to a second device based at least in part on the brand of the first device being the same as the second device. The assertion is not supported by the cited evidence. In the absence of this teaching, and assuming in Jakobsson '351's system data from a user's first device is backed up to the user's other devices by synchronization of all of the user's devices, the same brand requirement of Kodama has not been adequately shown by Petitioner as applicable to the user's devices in Jakobsson '351.

Second, there are deficiencies in Petitioner's stated reasoning for the motivation to combine the teachings of Jakobsson '351 and Kodama.

Petitioner asserts:

Kodama recognizes "if data restoration is to be performed to a different product or a different manufacturer, the format and product proprietary information of data between the products will differ." APPL-1010, [0157]. POSITA would recognize this differing format can create compatibility issues and thus would recognize an advantage of, and reason for, basing the initiation of data transfer to the second device on brand and thereby avoiding these compatibility issues as taught by Kodama. APPL-1003, ¶197.

Pet. 56–57. But the same brand requirement of Kodama is not provided to solve any problem with differing formats. Kodama states:

At Step 1313 of the restoration processing, if data restoration is to be performed to a different product of a different manufacturer, the format and product proprietary information of data between the products will differ. Thus, before the restoration processing function of the online backup service system 0128 sends the data read at Step 1318 to the HDD recorder 0116, the data format is converted into the file format of the HDD recorder 0116 of the restoration destination.

Ex. 1010 ¶ 157. Kodama does not describe format compatibility as presenting any problem. Kodama merely indicates that format conversion would be performed prior to restoration of data onto a product which requires a different data format.

Requiring brand identity between the first device and the other devices of the user in Jakobsson '351 to synchronize data among all of the user's devices is also not an advantage. The devices of the user in Jakobsson '351 are devices the user already owns, possesses, and uses. They are not a new device as in the case of Kodama, where a broken device may be

expected to lead to the user acquiring a new device of the same brand as a replacement. Petitioner provides no explanation as to why one would expect all of the user's devices in Jakobsson '351 would be of the same brand. Applying a same-brand requirement would substantially undermine Jakobsson '351's feature of synchronizing user data among all of the user's devices. We do not see this result as either an advantage or an improvement.

Petitioner additionally explains:

Kodama also describes its system "mitigat[es] the risk of a third party referring to or using backup data without authorization upon restoring such backup data in an electronic appliance." APPL-1010, [0007]. One way it provides this benefit is by ensuring the source and target devices are the same brand and therefore have similar safeguards.

Pet. 57 (alterations in original).

However, unlike the circumstance in Kodama, where a third-party repair shop technician would have possession of the new replacement device as well as access to the user's backup data, there is no such third party in the described environment of Jakobsson '351. In Jakobsson '351, there is no broken first user device being repaired by anyone, no new device to replace any broken device, and no third party in possession of any replacement device of the user together with access to already backed-up data of the user. In Jakobsson '351, the user is in possession of all of his or her devices, none of which is broken, and there simply is a synchronization operation to make the data on all of the devices of the user the same.

Requiring brand identity between the user's first device and all of the user's other devices prior to data synchronization does not mitigate the risk of any third-party misappropriation of sensitive data at issue and discussed in Kodama. A same-brand requirement would likely preclude or nullify

Jakobsson '351's feature of automatic data synchronization among all of the user's devices. Petitioner has shown no reasonable expectation that all of the user's existing devices, to which the same data must be synchronized, are of the same brand. The third-party misappropriation risks expressed in Kodama have little or no application in the context of automatic synchronization of data among all of a user's devices in Jakobsson '351.

For the foregoing reasons, Petitioner has not sufficiently shown that limitation [1.8] reasonably would have been suggested by the combined teachings of Jakobsson '351 and Kodama.

3. *Claim 18 (base claims for claims 21, 23, 31, and 34)*

Claim 18 recites similar subject matter as claim 1, but in method form. Ex. 1001, 26:4–32. The various functionalities recited in claim 1 are recited as method steps in claim 18. *Id.* Petitioner presents essentially the same arguments to claim 18 as it does for claim 1. Pet. 66–67. For substantially the same reasons as we explained above in the context of limitation [1.8] of claim 1, Petitioner has not sufficiently shown that the corresponding limitation in claim 18 would have been suggested by the combined teachings of Jakobsson '351 and Kodama.

4. *Dependent Claims 2, 4, 12, 15, 21, 23, 31, and 34*

Claims 2, 4, 12, and 15 each depend directly from claim 1. Ex. 1001, 25:14–16, 25:22–24, 25:56–57, 25:63–64. Claims 21, 23, 31, and 34 each depend directly from claim 18. *Id.* at 26:39–41, 26:46–48, 27:11–12, 27:18–20. The deficiency of Petitioner's accounting for claim 1 equally applies to claims 2, 4, 12, and 15. The deficiency of Petitioner's accounting for claim 18 equally applies to claims 21, 23, 31, and 34.

Petitioner has not shown a reasonable likelihood that it would prevail in establishing obviousness of claims 2, 4, 12, 15, 21, 23, 31, and 34 over Jakobsson '351 and Kodama.

G. Alleged Obviousness of Claims 5, 6, 24, and 25 over Jakobsson '351, Kodama, and Hubner

Claim 5 depends from claim 1, and claim 24 depends from claim 18. Each of claims 5 and 24 further recites: “wherein the first device and the second device are configured to complete a pairing process.” Ex. 1001, 25:25–26, 26:49–51.

Claim 6 depends from claim 5, and claim 25 depends from claim 24. Each of claims 6 and 25 further recites: “wherein the pairing process comprises a comparison of data generated from one or more authentication inputs.” Ex. 1001, 25:27–29, 26:52–54.

Petitioner asserts that each of claims 5 and 6 would have been obvious over the combined teachings of Jakobsson '351, Kodama, and Hubner. Pet. 72–73. Petitioner states that “Hubner describes a system that provides for a first device and a second device to be configured to complete a *pairing process*.” *Id.* at 72. Petitioner also states: “Hubner describes its peer-to-peer backup process (a *pairing process*) requires each device register with data management platform 103 that operates the backup process; it would have been obvious for the registration to be compared in the authentication process.” *Id.* at 72–73.

Petitioner’s assertions and reasoning based on Hubner, however, do not relate to and do not cure the deficiency of Petitioner’s accounting for limitation [1.8] as discussed above in Section III.F.2, pertaining to insufficient motivation to combine Kodama’s same-brand teachings of a

user's first and second devices to the first and second devices of Jakobsson '351.

Petitioner makes essentially the same arguments for claims 24 and 25 as Petitioner does for claims 5 and 6, respectively. Pet. 73. Petitioner's assertions and reasoning based on Hubner do not relate to and do not cure the deficiency of Petitioner's accounting for claim 18 with regard to requirements corresponding to limitation [1.8] as discussed above in Section III.F.2 and Section III.F.3, pertaining to insufficient motivation to combine Kodama's same-brand teachings of a user's first and second devices to the first and second devices of Jakobsson '351.

For the foregoing reasons, Petitioner has not shown a reasonable likelihood that it would prevail in establishing obviousness of claims 5, 6, 24, and 25 over Jakobsson '351, Kodama, and Hubner.

H. Discretionary Denial Under 35 U.S.C. § 314(a)

Under 35 U.S.C. § 314(a) and applying factors articulated in *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential) ("*Fintiv*"), Patent Owner asserts that the Board should discretionarily deny this Petition. Prelim. Resp. 13–26.

Further, Patent Owner notes that Petitioner has filed seven petitions to institute *inter partes* reviews, when all issues could be resolved in a single district court proceeding. Prelim. Resp. 16. Citing *General Plastic Industrial Co., Ltd. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19 at 16–17 (PTAB Sept. 6, 2017) (precedential as to § II.B.4.i)), Patent Owner asserts that "the Board should deny institution to maintain the goals of efficiency and efficacy." *Id.*

Because we decline, based on the insufficient substantive merit of Petitioner's showings, to institute *inter partes* review, we do not reach the issue of discretionary denial based on the parallel district court litigation or based on *General Plastic* under 35 U.S.C. § 314(a).

I. Discretionary Denial Under 35 U.S.C. § 325(d)

The Preliminary Response does not make clear whether Patent Owner asserts that we should exercise discretion to deny institution under 35 U.S.C. § 325(d) based on the framework set forth in *Advanced Bionics, LLC v. Med-El Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6 (PTAB Feb. 13, 2020) (precedential). Patent Owner made no such assertion or request. However, Patent Owner does assert that Kesanupalli is cumulative of and nearly identical to another Kesanupalli reference that was previously considered by the Office. Prelim. Resp. 6–10. The allegedly near identical Kesanupalli reference is U.S. Pat. Pub. No. 2011/0138450 (“Kesanupalli ’450” (Ex. 2030)). Kesanupalli ’450 is cited on the face of the ’105 Patent.

Because we decline, based on the insufficient substantive merit of Petitioner's showings, to institute *inter partes* review, we do not reach the issue of discretionary denial under 35 U.S.C. § 325(d).

IV. CONCLUSION

Petitioner has not shown a reasonable likelihood that it would prevail in establishing that at least one of claims 2, 4–6, 12, 15, 21, 23–25, 31, and 34 of the ’105 patent is unpatentable.

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that no *inter partes* review is instituted in this proceeding.

IPR2024-00507
Patent 11,475,105 B2

For PETITIONER:

David W. O'Brien
Kelley Gehrke Lyle
Hong Shi
HAYNES AND BOONE, LLP
david.obrien@haynesboone.com
kelly.lyle@haynesboone.com
hong.shi@haynesboone.com

For PATENT OWNER:

Richard A Kamprath
George Fishback
MCKOOL SMITH P.C.
Rkamprath@mckoolsmith.com
gfishback@mckoolsmith.com
Carbyne_Apple@mckoolsmith.com