

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

CARBYNE BIOMETRICS, LLC,
Patent Owner.

IPR2024-00334
Patent 11,514,138 B1

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

LEE, *Administrative Patent Judge*.

DECISION
Granting 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 1–3, 5, 7, 8, 10–15, 17, 19, and 22–25 (“challenged claims”) of U.S. Patent No. 11,514,138 B1 (Ex. 1001, “the ’138 patent”). Paper 2 (“Pet.”). Carbyne Biometrics, LLC (“Patent Owner”) filed a Preliminary Response. Paper 7 (“Prelim. Resp.”). Petitioner filed an authorized Preliminary Reply. Paper 8 (“Prelim. Reply”). Patent Owner filed an authorized Preliminary Sur-reply. Paper 9 (“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) (2023). 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 before us, we conclude Petitioner has shown a reasonable likelihood that it would prevail in establishing the unpatentability of at least one challenged claim of the ’138 patent.

Accordingly, we institute an *inter partes* review of all challenged claims of the ’138 patent on all grounds set forth in the Petition.

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 '138 patent (Pet. 1; Paper 4, 2): *Carbyne Biometrics, LLC v. Apple Inc.*, 1:23-cv-00324 (W.D. Tex.).

Petitioner identifies *Samsung Electronics Co., Ltd. v. RightQuestion, LLC*, IPR2022-00244 (PTAB) (Terminated July 26, 2022 subsequent to institution), which involved an ancestral patent of the '138 patent, as related matter. Pet. 1–2.

Petitioner further identifies *Samsung Electronics Co., Ltd. v. RightQuestion, LLC*, IPR2022-00251 (PTAB) (Non-instituted June 9, 2022), which involved an ancestral patent of the '138 patent. Pet. 9.

C. The '138 Patent

The '138 patent is directed to authentication techniques to provide credentials to a service. Ex. 1001, 1:37–46. The goal is to reduce practices such as password re-use and/or selection of poor quality passwords. *Id.* Specifically, the '138 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 '138 patent is reproduced below:

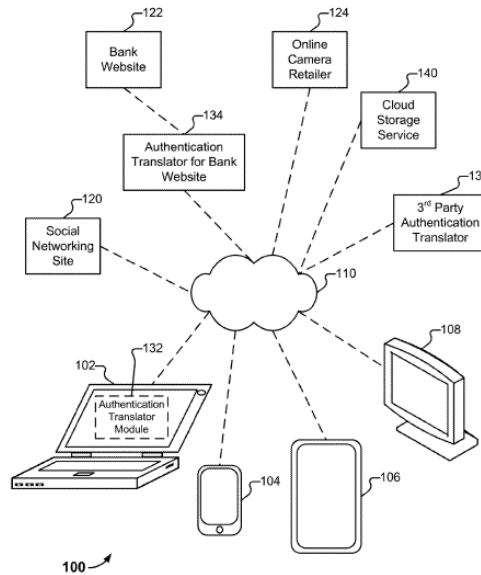


FIG. 1

Figure 1 illustrates an embodiment of an environment in which authentication translation is provided. Ex. 1001, 2:40–41. 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 2:41–45.

Client device 102 is a notebook computer owned by user Alice and includes a camera, a microphone, and a fingerprint sensor. Ex. 1001, 2:45–48. Client device 104 is a smartphone owned by user Alice and includes a camera. *Id.* at 2:48–49. 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 2:50–52. Client device 108 is a kiosk located in the lobby of a hotel and it includes a camera and a microphone. *Id.* at 2:52–54.

Service 120 is a social networking site; service 122 is a website of a bank; and service 124 is the online store of a boutique camera retailer; and 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, 2:60–65. 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 2:65–3:4.

For example, notebook computer 102 includes authentication translator module 132 that provides authentication translation services. *Id.* at 3:7–9. Devices 104–108 can also include, but need not include, their own respective authentication translator modules. *Id.* at 3:9–11. The owner of bank website 122 operates authentication translator 134 associated with the bank. *Id.* at 3:11–13. Authentication translator 136 provides authentication services to a variety of businesses, including online camera retailer 124. *Id.* at 3:13–15.

Figure 2 of the ’138 patent is reproduced below:

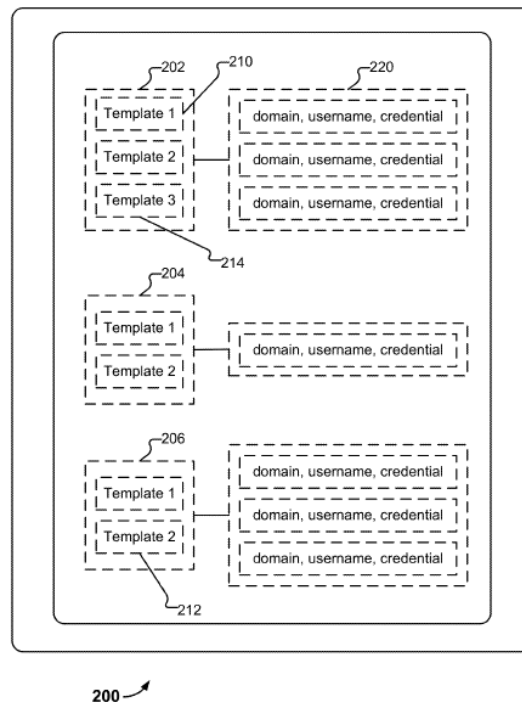


FIG. 2

Figure 2 shows an embodiment of credential information stored on device 200. Ex. 1001, 3:17–18. 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 3:18–21. A template is a collection of biometric features, where a fingerprint is an example of a biometric feature. *Id.* at 3:21–23. 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 3:27–31. When other biometrics are employed, for example facial recognition, voice print, or retina scan, corresponding features are included in the template. *Id.* at 3:32–35.

Policies can be included in a profile that govern how matches are to be performed. Ex. 1001, 3:50–51. 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 3:51–55. A profile is associated with a vault, for example vault 220. *Id.* at 3:56. A vault, in turn, contains triples specifying a service provider/domain, a username, and a credential. *Id.* at 3:56–58.

The credential for a service provider or domain can be a password or a cryptographic key. Ex. 1001, 3:61–64. The '138 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 3:65–4:3. 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 4:24–28. Figure 3 is reproduced below:

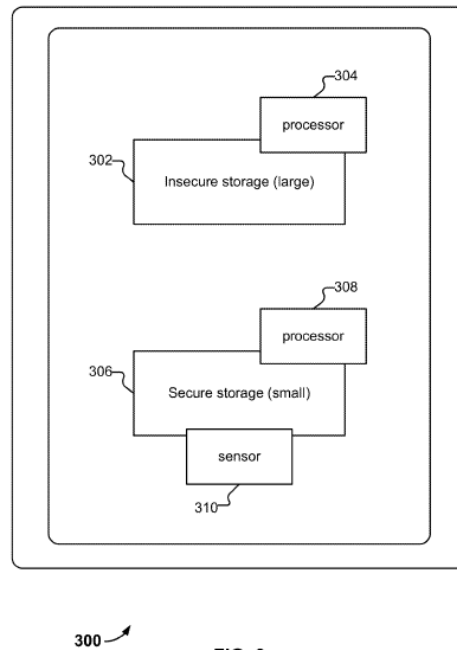


Figure 3 shows an embodiment using secured storage to hold authentication information. *Id.* at 4:1–5.

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 4:5–9. “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 4:9–13.

D. Illustrative Claim

Claims 1, 13, and 25 are independent. All other challenged claims depend, directly or indirectly, from claim 1 or claim 13. Claim 1 is reproduced below:

1. [1.0] A device, comprising:
 - [1.1] a processor on the device;
 - [1.2] a storage on the device that is accessible by the processor on the device via an interface that facilitates communication between the storage on the device and the processor on the device,
 - [1.3] wherein the processor on the device is configured to:
 - based at least in part on a request from a user to access an external resource, facilitate, using the interface, access of at least one record stored at least in part in the storage on the device;
 - [1.4] wherein the at least one record is associated at least with the external resource, and wherein the at least one record comprises:
 - a biometric template; and
 - a credential comprising a cryptographic key;
 - [1.5A] in response to determining a match between a biometric input and the biometric template,
 - retrieve, from the at least one record, the credential, wherein the biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voiceprint, a feature usable for a retina scan, or a typing feature,
 - [1.5B] wherein the biometric input is received subsequent to presenting of a prompt, wherein the prompt comprises a prompt to provide biometric information, and wherein the prompt is visually presented;
 - [1.6] establish a connection with the external resource;
 - [1.7] facilitate a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the credential retrieved from the at least one record, and wherein the user is logged in to the external resource based at least in part on the output; and

[1.8] facilitate wiping of both the biometric template and the credential comprising the cryptographic key of the at least one record stored at least in part in the storage on the device; and

[1.9] a memory coupled to the processor and configured to provide the processor with instructions.

Ex. 1001, 11:17–56.¹

E. Prior Art and Declaration Evidence Relied on by Petitioner

Petitioner relies on the following evidence:²

Name	Patent Document	Exhibit
Challener ³	US Patent 8,099,789 B2	1007
Brown ⁴	US Patent 9,652,629 B2	1009
Headley ⁵	US Patent 8,185,646 B2	1010
Kesanupalli ⁶	US Patent 8,799,666 B2	1006
Cheng ⁷	US Pub. App. 2004/0117636 A1	1008

¹ The bracketed heading labels correspond to those used by Petitioner to reference the claim elements. *See* Pet. 20–44. We use the same labels here for ease of reference, understanding, and consistency.

² The '138 patent issued from Application No. 17/027,481, filed Sept. 21, 2020, which claims priority to a long chain of ancestral applications including Application No. 3/706,254, filed Dec. 5, 2012, now Patent 9,294,452, and Provisional Application 61/569,112, filed Dec. 9, 2011. Ex. 1001, codes (21), (22), (60), (63).

³ Issued Jan. 17, 2012 from Application No. 11/529,795, filed Sept. 29, 2006. Ex. 1007, codes (21), (22), (45).

⁴ Issued May 16, 2017 from Application No. 14/816,271, filed Aug. 3, 2015, which is a continuation of Application No. 13/245,061, filed Sept. 26, 2011, which is a continuation of Application No. 12/016,723, filed Jan. 18, 2008. Ex. 1009, codes (21), (22), (45), (63).

⁵ Issued May 22, 2012, from Application No. 12/608,190, filed Oct. 29, 2009. Ex. 1010, codes (21), (22), (45).

⁶ Issued Aug. 5, 2014, from Application No. 12/731,050, filed Mar. 24, 2010. Ex. 1006, codes (21), (22), (45).

⁷ Published June 17, 2004. Ex. 1008, code (43).

Petitioner also relies on the Declaration of Patrick McDaniel, Ph.D. (Ex. 1003). Patent Owner has not submitted any declaration testimony of an expert in support of its Preliminary Response and Preliminary Sur-reply.

F. The Asserted Grounds of Unpatentability

Petitioner asserts that the challenged claims of the '138 patent are unpatentable based on the following grounds (Pet. 11, 54, 62, 70):

Claims Challenged	35 U.S.C. §	References/Basis
1–3, 7, 8, 12–15, 19, 24, 25	103(a) ⁸	Kesanupalli, Brown
10, 22	103(a)	Kesanupalli, Brown, Cheng
11, 23	103(a)	Kesanupalli, Brown, Challener
5, 17	103(a)	Kesanupalli, Brown, Headley

III. ANALYSIS

A. Legal Standards

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *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

⁸ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112–29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C. §§ 102 and 103. Because the '138 patent claims priority to an application filed before March 16, 2013 (the effective date of the amendments), the pre-AIA version of § 103 applies.

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. 6 (citing Ex. 1003 ¶¶ 18–21).

At this preliminary stage and on this record, we adopt Petitioner’s statement of the level of ordinary skill in the art, except for the qualifier “at least” which would make the stated scope without an upper bound and thus potentially cover the level of skill of an expert. It is supported by the testimony of Dr. McDaniel (Ex. 1003 ¶¶ 18–21) and not disputed by Patent Owner (Prelim. Resp. 10–11). 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).

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

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

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) (2022). 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))).

1. “processor”

Petitioner states:

Each independent claim recites generally “a processor;” and the ’138 patent states “[a]s used herein, the term ‘processor’ refers to one or more devices, circuits, and/or processing cores configured to process data, such as computer program instructions.” APPL-1001, 2:21–23. POSITA would understand that the plain and ordinary meaning of the term “processor” may include “one or more devices, circuits, and/or processing cores,” which includes a plurality of separate devices, circuits, and/or processing cores functioning together to provide a processor. APPL-1003, ¶56.

Pet. 7. Patent Owner has not proposed a construction for “processor” and states that “it does not address these positions [of Petitioner]” because its Response “does not depend on these definitions.” Prelim. Resp. 11.

Based on the description in the specification of the ’138 patent, as cited by Petitioner, we determine, preliminarily, that a “processor,” in the context of the ’138 patent, may include a plurality of separate devices, circuits, and/or processing cores functioning together to provide a processor.

2. “restricted interface”

The term “restricted interface” is recited in dependent claims 11 and 23. Ex. 1001, 12:16–17, 13:13–14.

Petitioner asserts that the plain and ordinary meaning of a “restricted interface” is “an interface that limits accessibility.” Pet. 9 (citing Ex. 1003 ¶¶ 57–60). Petitioner explains:

In the ’138 patent specification, disclosure of such an interface is sparse. For an example device that “includes a large and insecure storage 302 attached to a fast processor 304, and a smaller but secure storage 306 attached to a dedicated processor 308 and a sensor 310 (e.g., a camera or a fingerprint reader),” the specification refers to access limitations in connection with an application programming interface (API). APPL-1001, 4:9–13 (“users cannot access the secure storage area, and the fast processor can only communicate with the dedicated processor/sensor via a restricted API”). Thus, POSITA would understand *restricted interface* to at least include an API that limits accessibility to secure storage, fingerprint sensor, or dedicated processor. APPL-1003, ¶57.

Pet. 7–8. Patent Owner has not proposed a construction for “restricted interface” and states that “it does not address these positions [of Petitioner]” because its Response “does not depend on these definitions.” Prelim. Resp. 11.

Based on Petitioner’s explanations, which are supported by the cited evidence including the example given in the specification of the ’138 patent, we determine, preliminarily, that a “restricted interface” is an interface that limits accessibility and includes within its scope a restricted API.

D. Patent Owner’s Argument That Petitioner’s Expert Declaration Should Be Accorded No Weight

Patent Owner asserts that “Petitioner’s expert declaration should be given no weight as to the reasonable expectation of success analysis [in the context of combining teachings from prior art references].” Prelim. Resp. 39.

Citing Board decisions, Patent Owner contends that if an expert's declaration merely repeats or contains arguments that are identical to arguments set forth in the petition, then the declaration adds little probative value to the attorney arguments in the petition. Prelim. Resp. 39–40. Patent Owner then compares the statements in the Petition on pages 19–20 with the testimony of Dr. Patrick McDaniel in paragraphs 81–82 of his declaration (Ex. 1003), regarding reasonable expectation of success in adding Brown's wiping feature to the system of Kesanupalli, and asserts that they are "nearly identical." *Id.* at 40–43. Patent Owner notes: "This Board has previously held in situations like this when an expert adds nothing beyond what is already found in the Petition, that the expert testimony should be given little to no weight." *Id.* at 42.

Patent Owner's contentions are misplaced. It is an oversimplification to say that if the expert testimony is the same as statements in the Petition, then the testimony should be accorded no weight. The issue is not whether the two are the same or nearly identical. Rather, the issue is whether the testimony refers to supporting evidence or contains technical reasoning. *See Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9 at 15–17 (PTAB Aug. 24, 2022) (precedential) (accorded "little weight" to declaration testimony that contains a *verbatim* restatement of a petition's conclusory assertions without additional supporting evidence or reasoning). This is consistent with 37 C.F.R. § 42.65(a), which states: "Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight." We do not accord expert testimony little or no weight simply because it is verbatim to what Petitioner states in the Petition.

Patent Owner has not even attempted to show that Dr. McDaniel's testimony is without citation to underlying evidence and lacks technical reasoning. Further, Dr. McDaniel's testimony regarding motivation to combine the teachings of Kesanupalli and Brown includes numerous other paragraphs, e.g., paragraphs 75–79, and Dr. McDaniel also has testified to the technical content of Kesanupalli, e.g., paragraphs 65–70. All of that testimony should be read together in determining whether Dr. McDaniel's testimony regarding combining the teachings of Kesanupalli and Brown is wholly conclusory, i.e., without any evidentiary support or technical reasoning. Patent Owner has not shown that it is.

Thus, Patent Owner's argument that Dr. McDaniel's testimony should be accorded no weight as to the reasonable expectation of success analysis lacks merit. We decline to accord Dr. McDaniel's testimony no weight.

E. Alleged Obviousness of Claims 1–3, 7, 8, 12–15, 19, 24, and 25 over Kesanupalli and Brown

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:

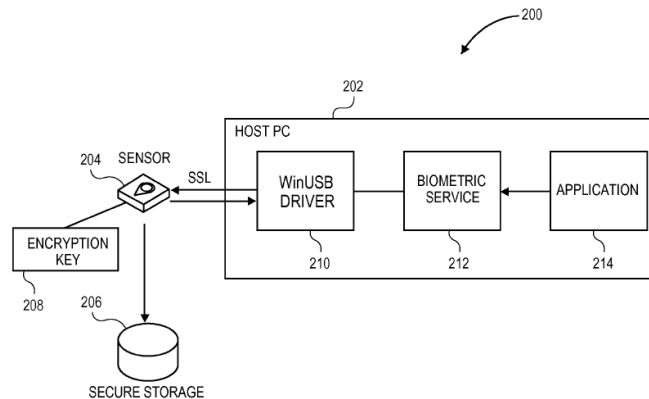


FIG. 2

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 released from the secure storage device until a matching fingerprint template is confirmed. *Id.* at 3:59–61.

Figure 9 is reproduced below:

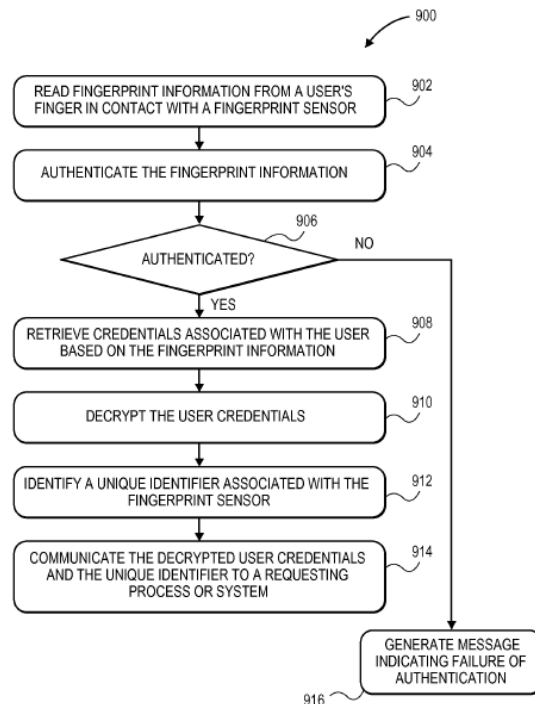


FIG. 9

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 Brown (Ex. 1005)*

Brown discloses a system and method for selectively securing data from unauthorized access on a client device. Ex. 1009, code (57). The data may be secured by encrypting and/or deleting. *Id.* Brown describes:

While data may be protected by requiring the user to enter a valid password in order to access applications or data on the device, or by encrypting data stored on the device such that access to the data requires decryption by a valid decryption key, there are instances when the device may be compromised, decommissioned, or redeployed, making it desirable to delete or “wipe” data, including applications, on the communication device so that it cannot be accessed by unauthorized or malicious

users. However, it may not always be necessary or desirable to wipe all data and applications from a device.

Therefore, it is desirable to provide a system and method for selectively wiping data at a communication device.

Ex. 1009, 2:7–19.

Brown further describes:

Occasionally, it may be desirable to delete data at the client device 10, 100 to prevent its access by an unauthorized party. This deletion, which may comprise either the overwriting of all or substantially all memory addresses in the data store 300, for example all but the addresses used to store the operating system 301 and PIM/messaging applications 305, may be accomplished through the invocation of a “wipe” command.

Ex. 1009, 11:57–64.

Brown’s client devices may be “laptop and notebook computers, PDAs,” and smartphones. *Id.* at 5:8–10. Figure 6 of Brown is reproduced below:

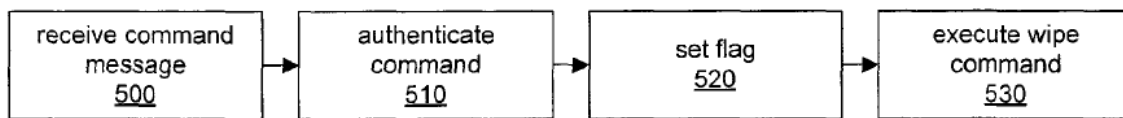


Figure 6

Figure 6 is a flowchart of a method for processing a wipe command at a communication device. *Id.* at 1:62–63. In its simplest, step 520 sets a flag of a single bit indicating whether a wipe is in progress. *Id.* at 14:3–5. Alternatively, the flag comprises a multi-bit value corresponding to the authorization level indicated in an indicator accompanying the wipe command. *Id.* at 14:5–7. Different authorization levels correspond to types of data which may be wiped. *Id.* at 14:9–38. “The types of data to be wiped are indicated in the flag.” *Id.* at 14:38–39.

3. *Independent Claim 1*

a. *Preamble recitation [1.0]*

The preamble recites: “A device, comprising:” Ex. 1001, 11:17. Referring to Kesanupalli’s Figure 2, Petitioner asserts: “Biometric sensor 204, its secure storage 206, and Host PC 202 (including web browser application and biometric services executing thereon) constitute a device that provides authentication translation and ultimately communicate user credentials to web servers.” Pet. 20–21 (emphasis omitted) (citing Ex. 1006, code (57), 2:54–3:3, 4:3–11, 4:36–50, 6:11–49). Petitioner notes that Kesanupalli describes: (1) “In particular embodiments, the biometric sensor is physically attached (or manufactured into) a client device such as a computer, cellular phone, and so forth,” and (2) “In one embodiment the secure voltage 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.” *Id.* at 21 (emphasis omitted) (citing Ex. 1006, 2:48–50, 3:46–51).

Petitioner’s assertions about “device” are supported by the cited evidence and not disputed by Patent Owner. Because Petitioner sufficiently establishes that Kesanupalli discloses a “device,” by mapping it to what are shown in Figure 2 as “HOST PC 202,” “sensor 204,” and “secure storage 206,” collectively labeled as element 200, we need not determine whether this preamble is limiting. *Realtime Data*, 912 F.3d at 1375.

Petitioner sufficiently persuades us that Kesanupalli discloses preamble recitation [1.0].

b. *Limitation [1.1]*

Limitation [1.1] recites “a processor on the device.” Ex. 1001, 11:18.

First, Petitioner refers to the following description in Kesanupalli: “The invention may also involve a number of functions to be performed by a computer processor, such as a microprocessor. The microprocessor may be a specialized or dedicated microprocessor that is configured to perform particular tasks according to the invention.” Ex. 1006, 9:58–62 (cited at Pet. 22). Then, Petitioner explains: a “POSITA [person with ordinary skill in the art] would understand Kesanupalli to describe implementations in which its biometric authentication techniques are provided using specialized processor circuitry executing the authentication functions (those of sensor 204 such as matching) and general processor circuitry executing the function of communicating with an external resource (those of HOST PC 202).” Pet. 22 (citing Ex. 1003 ¶ 91; Ex. 1006, 5:62–6:31, 6:40–49).

Thus, Petitioner concludes: “The processor circuitry executing functions of sensor 204 and the processor circuitry executing functions of PC 202 provide *a processor on the device*.” Pet. 22 (emphasis added). In that regard, Petitioner also cites to the following definition of “processor” expressly provided in the ’138 patent: “As used herein, the term ‘processor’ refers to one or more devices, circuits, and/or processing cores configured to process data, such as computer program instructions.” Ex. 1001, 2:21–23 (cited at Pet. 22).

Patent Owner does not present counter-argument for the above-noted assertions of Petitioner. We find Petitioner’s assertions to be supported by the cited evidence.

Petitioner sufficiently establishes that Kesanupalli’s device 200 includes a processor on the device and thus teaches limitation [1.1]. Specifically, this processor includes two parts: (1) processing circuitry

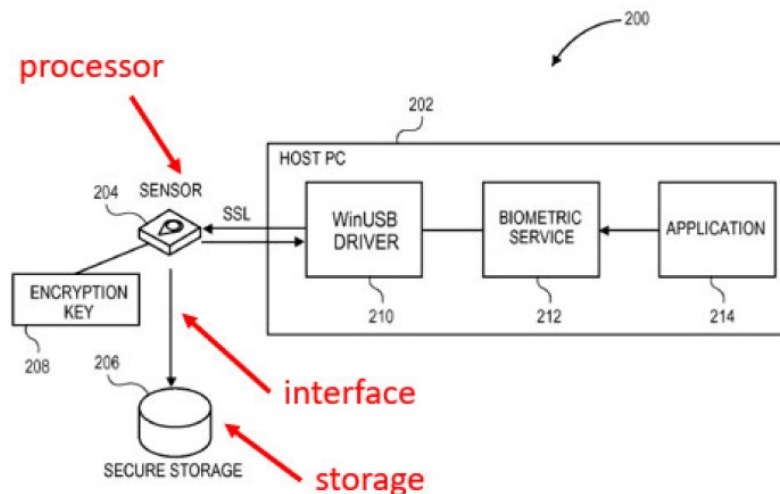
executing functions of sensor 204; and (2) processing circuitry executing functions of Host PC 202.

c. Limitation [1.2]

Limitation [1.2] recites “a storage on the device that is accessible by the processor on the device via an interface that facilitates communication between the storage on the device and the processor on the device.”

Ex. 1001, 11:19–22.

Petitioner identifies Kesanupalli’s secure storage 26 as the claimed storage on the device. Pet. 23 (citing Ex. 1006, 2:48–50, 3:46–51, 6:45–47, Fig. 2). Petitioner explains that secure storage 206 is accessible by the processor circuitry executing sensor 204. Pet. 24 (citing Ex. 1003 ¶¶ 95–96, Fig. 2). On page 24 of the Petition, Petitioner produces the following annotated version of Kesanupalli’s Figure 2:



APPL-1006, FIG. 2, annotated

Figure 2 depicts an embodiment of Kesanupalli’s system. Ex. 1001, 2:1–2. Petitioner has added red highlighted annotations which point to processing circuitry which implement sensor 204, secure storage 206, and the interface

therebetween. Pet. 24. Petitioner states: “As illustrated in FIG. 2 above, secure storage 206 is accessible by processor circuitry executing sensor 204 as shown by the vertical arrow extending from sensor 204 to storage 206.”

Id. (citing Ex. 1003 ¶¶ 95–96).

Petitioner further explains:

As discussed in limitation [1.1], POSITA would understand Kesanupalli to provide a processor on its device that executes its functions, including those described in association with sensor 204. As such, Kesanupalli describes the devices, circuits and/or processing cores that constitute or render obvious the processor, as claimed, and which access the secure storage 206.

Pet. 24–25 (citing Ex. 1003 ¶¶ 89–92). Petitioner also explains: “Each time the processor accesses secure storage 206, it does so via the interface, which is software and/or hardware framework by which the processor exchanges information with its storage; the interface (*see* annotated FIG. 2 above) is the only disclosed connection to secure storage 206.” *Id.* at 25 (citing Ex. 1003 ¶ 99).

Patent Owner does not present counter-argument against the above-noted assertions of Petitioner. Petitioner’s assertions are supported by the cited evidence. Petitioner sufficiently establishes that Kesanupalli teaches limitation [1.2].

d. Limitation [1.3]

Limitation [1.3] recites “wherein the processor on the device is configured to: based at least in part on a request from a user to access an external resource, facilitate, using the interface, access of at least one record stored at least in part in the storage on the device.” Ex. 1001, 11:22–27.

Petitioner explains that “Kesanupalli describes a user’s enrollment process for an external resource such as a website where the user’s credential and biometric template are stored in secure storage.” Pet. 26 (citing Ex. 1006, 3:15–51). Petitioner asserts that “[t]he user’s credential (*e.g.*, cryptographic key) and biometric template, which are bound and stored in secure storage 206,” constitute the claimed at least one record. *Id.* (citing Ex. 1003 ¶¶ 104–105). Petitioner notes that Kesanupalli’s Figure 7 describes this enrollment process. *Id.* at 26–27 (citing Ex. 1006, 8:29–53).

Petitioner further explains:

After enrollment including creation and storage of the record, subsequent visits by the user to the external resource initiate an authentication translation procedure. APPL-1006, 5:9–14 (“After a user has enrolled with a particular Web site that supports biometric authentication, subsequent visits cause . . . the Web site [to] prompt the user to perform user authentication.”) This authentication process is *based at least in part on a request from a user to access an external resource (i.e., the visit to the website for which the user has previously enrolled)* and includes the processor accessing the record in storage to perform the authentication. APPL-1003, ¶¶ 106–107; *see also*, APPL-1006, FIGS. 8, 9, 3:52–4:1, 8:54–9:24, FIGS. 8, 9, 12.

Pet. 27. In summary, Petitioner states:

In particular with respect to the device illustrated in Kesanupalli’s FIG. 2, in the authentication process, the *processor* (including circuits of sensor 204) *facilitates access* to storage 206 using its *interface* to storage 206 to obtain the biometric template of the record stored there so the processor can perform a matching of biometric input to said template, and again *facilitates access* to storage 206 to access the user credential of the record to release the credential to the external resource (using application 214) on a successful match as discussed above. *See* APPL-1003, ¶¶ 106–108; APPL-1006, FIG. 2, 3:44–51, 6:42–49, FIG. 12.

Id. at 28.

Patent Owner does not present counter-argument against the above-noted assertions of Petitioner. Petitioner's assertions are supported by the cited evidence. Petitioner sufficiently establishes that Kesanupalli teaches limitation [1.3].

e. Limitation [1.4]

Limitation [1.4] recites “wherein the at least one record is associated at least with the external resource, and wherein the at least one record comprises: a biometric template; and a credential comprising a cryptographic key.” Ex. 1001, 11:28–32.

Petitioner explains:

In particular, Kesanupalli describes that in its enrollment, “a user swipes their finger across the fingerprint sensor several times to create a **fingerprint template** . . . After creating a fingerprint template, the user (or a web server or other system) provides **user credentials**, such as a password, **cryptographic key**, random seed, and the like. The systems and procedures described herein **bind the user's fingerprint template with the user credentials**. The fingerprint template and user credentials are then **stored in a secure storage device**.” APPL-1006, 3:32–51. The fingerprint template is one type of “biometric template” suggested by Kesanupalli. APPL-1006, 3:15–18 (“a user enrolls...by binding their user credentials with the user's **biometric template (a ‘fingerprint template’ in specific implementations.**”[)]) A fingerprint template is a biometric template. APPL-1003, ¶113.

Pet. 29–30. Petitioner states that Kesanupalli's user credential and bound biometric template is the at least one record associated with the external resource as it is specific to the external resource such as a website. *Id.* at 30 (citing Ex. 1003 ¶¶ 112–114; Ex. 1006, 5:33–43). Further, Petitioner notes

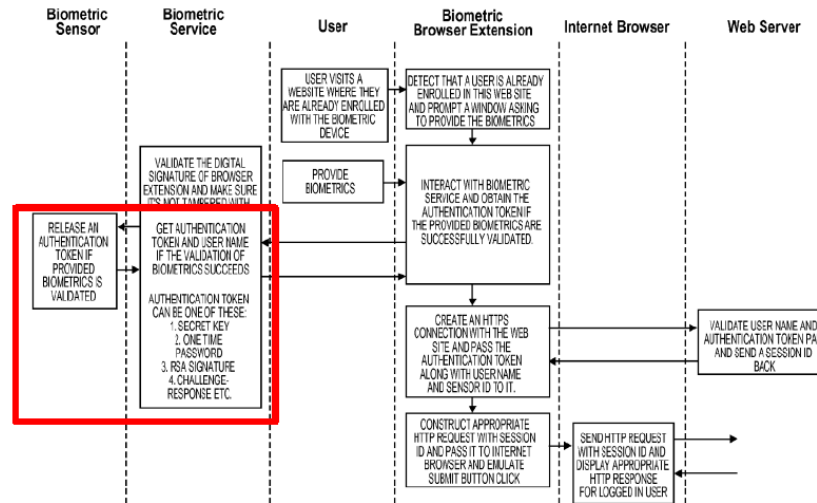
that Kesanupalli describes one type of user credential is a cryptographic key. *Id.* (citing Ex. 1006, 3:32–51, 8:6–22).

Patent Owner does not present counter-argument against the above-noted assertions of Petitioner. Petitioner’s assertions are supported by the cited evidence. Petitioner sufficiently establishes that Kesanupalli teaches limitation [1.4].

f. Limitation [1.5A]

Limitation [1.5A] recites: “[wherein the processor on the device is configured to:] in response to determining a match between a biometric input and the biometric template, retrieve, from the at least one record, the credential, wherein the biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voice print, a feature usable for a retina scan, or a typing feature.” Ex. 1001, 11:33–39.

Petitioner explains that, in one example, Kesanupalli describes that sensor 204 receives a biometric input of a fingerprint from a fingerprint sensor. Pet. 31 (citing Ex. 1006, 6:31–37, 9:10–24). Petitioner then asserts: “Kesanupalli’s authentication process includes *determining a match between a biometric input (e.g., fingerprint information) and the biometric template (e.g., fingerprint template) and if there is a match, in response retriev[ing], from the at least one record, the credential.*” Pet. 31 (alteration by Petitioner) (citing Ex. 1006, 9:14–20). Petitioner presents, on page 33 of the Petition, an annotated version of Kesanupalli’s Figure 12 to illustrate the actions performed to authenticate a user, reproduced below:



APPL-1006, FIG. 12, annotated

Figure 12 depicts an embodiment of a procedure for identifying and authenticating a user. Ex. 1006, 2:22–24. Petitioner has enclosed certain pertinent steps in a red square. Referring to the emphasized steps, Petitioner explains:

Kesanupalli describes the *processor on the device* performs the steps above of retrieving the credential as sensor 204 is accessing storage 206, performing the matching of the input and template and, if a match is found, releasing the credential for transfer to a requesting processor system by the application of PC 202.

Pet. 33 (citing Ex. 1006, 6:11–49, 9:10–24, FIG. 2).

Patent Owner does not present counter-argument against the above-noted assertions of Petitioner. Petitioner’s assertions are supported by the cited evidence. Petitioner sufficiently establishes that Kesanupalli teaches limitation [1.5A].

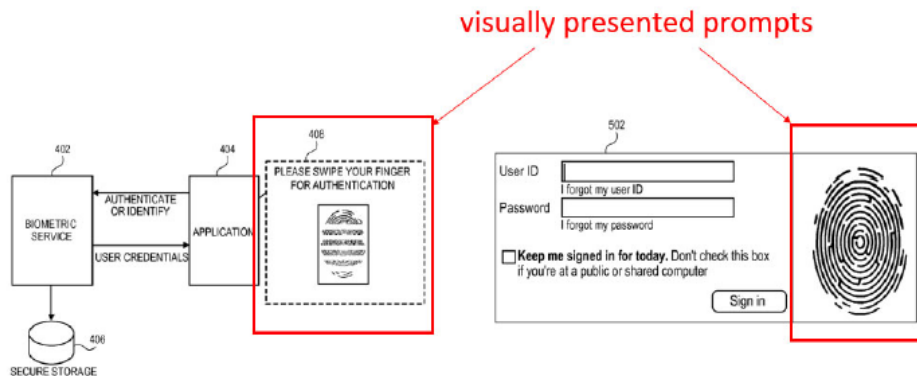
g. *Limitation [1.5B]*

Limitation [1.5B] recites: “wherein the biometric input is received subsequent to presenting of a prompt, wherein the prompt comprises a

prompt to provide biometric information, and wherein the prompt is visually presented.” Ex. 1001, 11:39–43.

Petitioner asserts that Kesanupalli discloses the biometric input, e.g., fingerprint information, is received subsequent to presenting of a prompt, wherein the prompt comprises a prompt to provide biometric information, noting that Kesanupalli describes: “the Web site **prompts the user** to perform user authentication (e.g., using the biometric device).” Pet. 34 (citing Ex. 1006, 5:9–14) (emphasis by Petitioner). Petitioner also notes that in Figure 12, Kesanupalli discloses a procedure of authentication which includes the operation of “prompt a window asking to provide the biometrics.” *Id.* (citing Ex. 1006, Fig. 12).

Petitioner further asserts that Kesanupalli describes this prompt can be visually presented. Pet. 34 (citing Ex. 1006, 7:1–24, Figs. 4 and 5). On page 34 of the Petition, Petitioner also presents an annotated version of Kesanupalli’s Figures 4 and 5, to illustrate the visual prompt:



APPL-1006, FIGS. 4 and 5, annotated

Figure 4 depicts an example of user authentication process, and Figure 5 depicts an example of a user login interface. Ex. 1006, 2:4–5. Petitioner

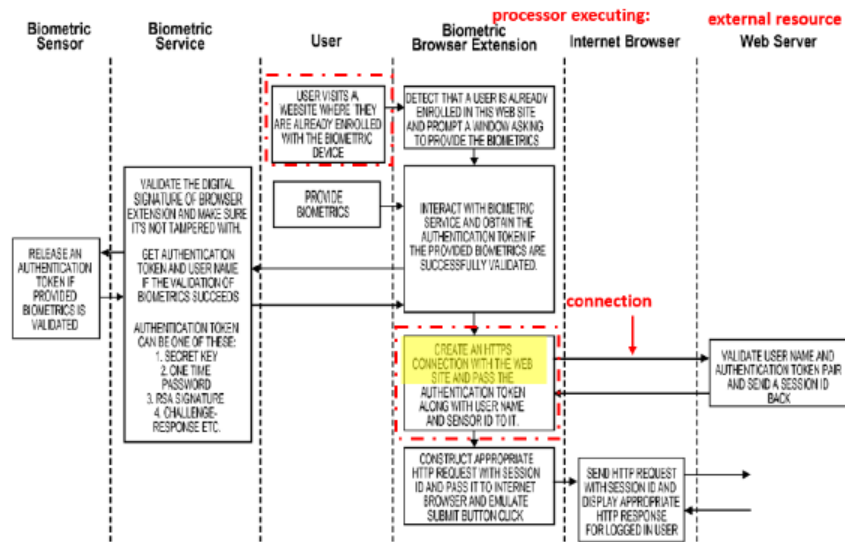
has inserted the annotation “visually presented prompts” with arrows pointing to the visual prompts.

Patent Owner does not present counter-argument against the above-noted assertions of Petitioner. Petitioner’s assertions are supported by the cited evidence. Petitioner sufficiently establishes that Kesanupalli teaches limitation [1.5B].

h. Limitation [1.6]

Limitation [1.6] recites “[wherein the processor on the device is configured to:] establish a connection with the external resource.” Ex. 1001, 11:44.

Petitioner asserts: “In Kesanupalli, the processor on the device *establishes a connection with the external resource* (e.g., connects to the website). In particular, a connection is provided between the application executing on the processor circuitry and the web server of the website.” Pet. 35 (citing Ex. 1006, 2:54–3:3, 4:36–5:63, 6:11–49, 7:67–8:4, 9:58–10:1). Petitioner explains: “In particular in the device of FIG. 2, based on the user’s request to access the website, application 214 establishes a *connection*, via the Internet, with a web server of the website. *Id.* (citing Ex. 1003 ¶¶ 130–131; Ex. 1006, 6:11–31, FIG. 9, block 914.). On page 36 of the Petition, Petitioner presents an annotated version of Kesanupalli’s Figure 12 to illustrate the information provided on the connection between the processor and the web server providing the external resource, reproduced below:



APPL-1006, FIG. 12, annotated

Figure 12 depicts an embodiment of a procedure for identifying and authenticating a user. Ex. 1006, 2:22–24. Petitioner has labeled and highlighted the connection between the user and the external resource.

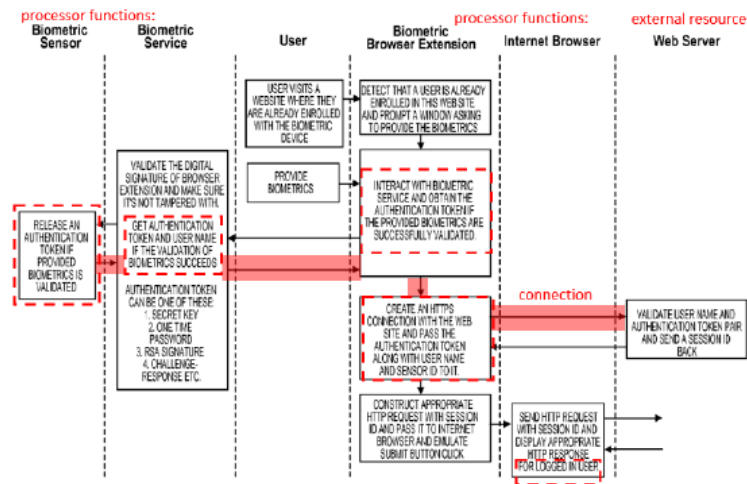
Patent Owner does not present counter-argument against the above-noted assertions of Petitioner. Petitioner’s assertions are supported by the cited evidence. Petitioner sufficiently establishes that Kesanupalli teaches limitation [1.6].

i. Limitation [1.7]

Limitation [1.7] recites “[wherein the processor on the device is configured to:] facilitate a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the credential retrieved from the at least one record, and wherein the user is logged in to the external resource based at least in part on the output.” Ex. 1001, 11:45–50.

Petitioner asserts that Kesanupalli describes its processor performs transmitting output, the user credential, to the external resource, the website.

Pet. 37 (citing Ex. 1006, 9:4–24). Petitioner asserts that in the device of Kesanupalli’s Figure 2, “the user credential (*e.g.*, cryptographic key) is retrieved from the secure storage 206 and provided to application 214 for communication to the external resource.” *Id.* at 38 (citing Ex. 1006, 6:11–49). Petitioner asserts that the application of PC 202 communicates a decrypted credential to the website via the established connection between the device and the external resource. *Id.* (citing Ex. 1006, 4:1–11, 5:51–63, 5:59–6:25). On page 39 of the Petition, Petitioner presents an annotated version of Kesanupalli’s Figure 12 to illustrate transmission of user credential to the external resource, reproduced below:



APPL-1006, FIG. 12, annotated

Figure 12 depicts an embodiment of a procedure for identifying and authenticating a user. Ex. 1006, 2:22–24. Petitioner has labeled and highlighted the transmission path.

Petitioner explains that Kesanupalli’s transmission of the decrypted user credential meets the transmission part of limitation [1.7]. Pet. 39. Petitioner further explains:

The output of the user credential to the external resource facilitates a login of the user to the external resource because, based at least in part on the output of the user credential, the user is logged in to the external resource. POSITA would understand when Kesanupalli communicates the credentials “to the Web site to complete the user authentication process,” the user login has occurred.

Id. at 39–40 (emphases omitted).

Patent Owner does not present counter-argument against the above-noted assertions of Petitioner. Petitioner’s assertions are supported by the cited evidence. Petitioner sufficiently establishes that Kesanupalli teaches limitation [1.7].

j. Limitation [1.8]

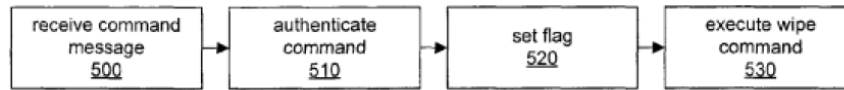
Limitation [1.8] recites “[wherein the processor on the device is configured to:] facilitate wiping of both the biometric template and the credential comprising the cryptographic key of the at least one record stored at least in part in the storage on the device; and” Ex. 1001, 11:51–54.

Petitioner asserts that in light of the teachings of Brown, it would have been obvious for the processor in Kesanupalli to perform this added wiping feature of limitation [1.8]. Pet. 40. Petitioner first notes that as discussed previously in connection with the storing of a record, Kesanupalli discloses storing at least one record, the biometric template bound with the user credential (e.g., cryptographic key), in the storage on the device. *Id.*

Petitioner explains:

Brown discloses a system and method for deleting or wiping data, including personal data, from a user’s electronic device. APPL-1003, ¶¶143–145; APPL-1009, Abstract. *See also*, APPL-1009, 1:15–18, 2:7–15, 11:65–13:14 (describing the method of FIG. 6). FIG. 6 of Brown is illustrative of executing

its wipe command at the user's device such as a personal computer, mobile device or the like:



APPL-1009, FIG. 6

APPL-1009, 4:64–5:11, 11:65–66 (FIG. 6 is a flowchart of “execution of the wipe command on the client device[]”). Brown describes that it may be desirable to delete all data on a user’s device. APPL-1009, 11:56–64 (“Occasionally, it may be desirable to delete data at the client device 10, 100 to prevent its access by an unauthorized party. This deletion, which may comprise either the overwriting of all or substantially all memory addresses . . . through the invocation of a “wipe” command.”). Brown’s “overwriting” data is deleting or wiping data. APPL-1003, ¶144; APPL-1009, 13:12–14 (“The wiping process may also include repeated overwriting of ones, zeros, or a random arrangement of ones and zeros over the data to be wiped.”) Teaching of overwriting all data of a client device is a teaching of overwriting the data including a biometric template and user credential in the client device of Kesanupalli. APPL-1003, ¶144. Benefits of wiping all data are readily recognizable for protection of all data for example when repurposing the client device. APPL-1003, ¶144.

Pet. 41–42.

Petitioner further contends that to the extent Patent Owner argues that wiping must be particularized to the recited elements to wipe, and not met by deleting all data, Brown still describes selective wiping of data, and that one of ordinary skill in the art would have recognized that the biometric template and the credential comprising the cryptographic key of Kesanupalli are just the type of personal data Brown suggests for selective wiping. Pet. 42–43. We need not engage in this alternative analysis, because Patent Owner does not dispute that wiping all data in Kesanupalli meets the

requirement of wiping the biometric template and the credential comprising the cryptographic key and also because we agree with Petitioner that wiping all data satisfies wiping the biometric template and the credential comprising the cryptographic key.

Petitioner further explains:

Further, Brown discloses a *processor* of the client device facilitates the wiping. *See* APPL-1009, 4:7–44 (“a mobile client device for selectively securing data from unauthorized access of the client device . . . the device comprising a processor . . . the processor may be configured to secure the data by deleting the data corresponding to each of the plurality of data types thus determined in the memory. . .”), 9:12–38, 21:1–48, FIG. 2, 7:47–55. Therefore, it would have been obvious for Kesanupalli’s *processor*, which has the same relevant functions and capabilities, to facilitate wiping of both the biometric template and the credential comprising the cryptographic key of the at least one record stored at least in part in the storage on the device. Kesanupalli’s processor executing the functions of sensor 204 has access to the record in the storage on the device to facilitate the wiping of Brown; and the processor circuitry (*e.g.*, executing application 214) receives communication. APPL-1003, ¶147.

Pet. 43.

Regarding motivation to combine the teachings of Brown and Kesanupalli, Petitioner provides rational reasoning:

POSITA would have been motivated to apply Brown’s teachings of wiping sensitive data from storage of a device to Kesanupalli’s device, which is used to store data of biometric information associated with a user and credentials for user authentication to resources such as websites. APPL-1003, ¶¶71–82. Kesanupalli’s stored biometric information and credentials are sensitive data and applying Brown’s wiping teachings would produce the obvious, beneficial, and predictable results of reducing the risk of unauthorized or malicious user access to that sensitive data should Kesanupalli’s device be out of user’s control, such as if lost or stolen. *Id.*

Pet. 15. Petitioner notes that Kesanupalli is directed to secure storage of the personal data required for biometric authentication and associated user credentials, and “Brown is similarly directed to systems for securing client devices that include data of a sensitive nature such as the user’s personal files and implements its system in the context of authentication services.”

Id. at 17. Petitioner explains:

POSITA would have been motivated to employ Brown’s wiping technique in connection with Kesanupalli’s secure user authentication methods because Kesanupalli’s stored biometric information and credential are sensitive data. APPL-1003, ¶¶79–80. POSITA would have readily understood the stored biometric information and credentials would be at risk if Kesanupalli’s device were lost or stolen. *Id.*

Id. at 17–18. Petitioner also notes that “Brown itself teaches ‘there are instances when the device may be compromised, decommissioned, or redeployed, making it desirable to delete or “wipe” data.’” *Id.* at 18 (citing APPL-1009, 2:6–15).

Petitioner further explains:

Brown recognizes that while data may be protected by authentication procedures and encryption, additional protection is desired and achieved by wiping techniques. *See* APPL-1009, 1:28–35, 2:6–17. POSITA would have readily recognized that Brown’s system and method for wiping data at a communication device including according to a predefined rule would provide an advantage for client devices like those of Kesanupalli—namely, that of protecting data on the client device from unauthorized use by wiping it from the device. APPL-1003, ¶80.

Pet. 18–19.

Petitioner also explains why one of ordinary skill in the art would have had a reasonable expectation of success in adding Brown’s wiping technique to Kesanupalli’s system:

Adding a wiping feature would merely have been applying a known technique to a known device (method, or product) that was ready for improvement to yield predictable results. Indeed, the wiping technique of Brown is implemented by routine software executed on generic processing components, which would have been a predictable application relative to Kesanupalli's system and devices. APPL-1003, ¶81. Brown discloses that a processor facilitates its wiping techniques. *See* APPL-1009, 4:9–50 (“a mobile client device for selectively securing data from unauthorized access of the client device. . . the device comprising a processor . . . the processor may be configured to a secure the data by deleting the data corresponding to each of the plurality of data types thus determined in the memory . . .”), 9:12–38, 21:1–48; FIG. 2, 7:48–55. Kesanupalli's processor (including circuits, processor cores and devices thereof) would have been operable to execute instructions that implement wiping functions such as performed by Brown's processor, and wiping is a predictable data management task that would have been easily accomplished in Kesanupalli device. APPL-1003, ¶82.

Pet. 19–20.

Petitioner's above-noted assertions and explanations are rational and supported by the cited evidence. Notwithstanding Patent Owner's arguments that Petitioner has not shown a reasonable expectation of success in combining the teachings of Kesanupalli and Brown, discussed below, we are sufficiently persuaded that Petitioner has sufficiently shown both a reasonable motivation to combine the teachings of Kesanupalli and Brown and a reasonable expectation of success in adding Brown's wiping technique to Kesanupalli's system.

Patent Owner argues:

Petitioner [1] has failed to articulate why a POSITA would have believed it would have had a reasonable expectation of success implementing a system using Brown's “routine” wiping software to wipe Kesanupalli's “secure storage.” Further, [2]

given that Petitioner's expert has failed to support the Petition, Petitioner is left with a naked assertion that a POSITA would have reasonably believed this combination would have succeeded—when there are many unanswered questions.

Pet. 43–44. Neither of Patent Owner's broadly stated arguments has merit. We have quoted above Petitioner's explanation of how a POSITA would have had a reasonable expectation of success implementing a system adding Brown's wiping technique to Kesanupalli's system, and that explanation cites to the supporting testimony of Dr. McDaniel (Ex. 1003 ¶¶ 81–82).

Patent Owner also more specifically explains its arguments. Patent Owner on page 45 of the Preliminary Response produces an annotated version of Brown's Figure 2, reproduced below:

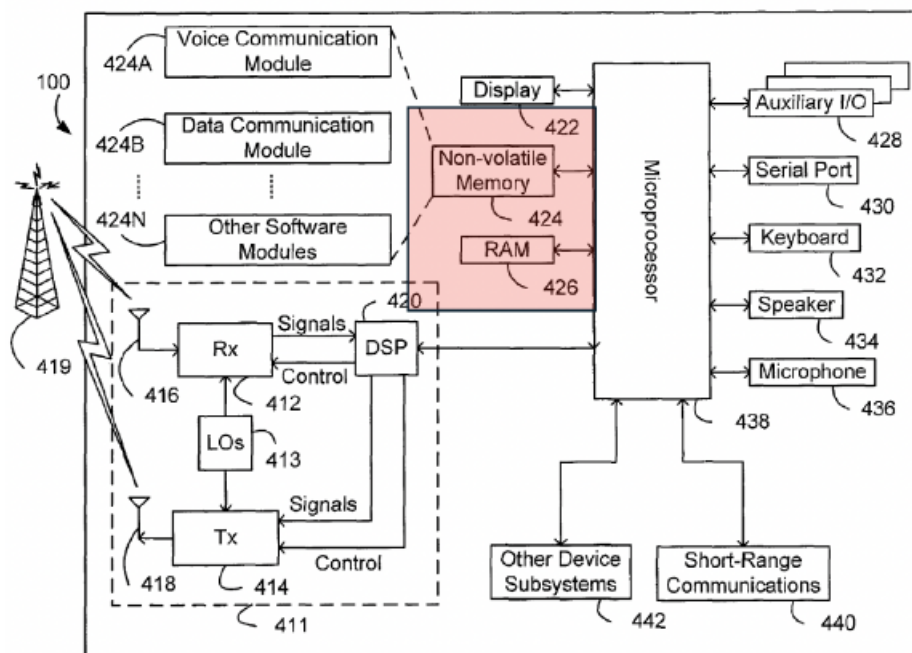
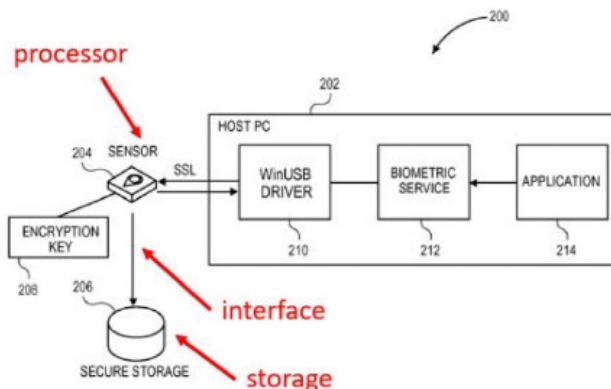


Figure 2

Figure 2 is a block diagram of Brown's mobile communication device. Ex. 1009, 1:52–53. Patent Owner has colored red non-volatile memory 424 and RAM 426.

Patent Owner explains that because non-volatile memory 424 and RAM 426 are the only storage locations disclosed in Brown, they are the storage locations being wiped by Brown. Prelim. Resp. 46. Also, Patent Owner notes that in Brown these two storage locations are directly accessible by Brown’s microprocessor. *Id.* According to Patent Owner, “this presents a problem for the Petition because that is not where Kesanupalli stores its credentials.” *Id.*

Patent Owner asserts: “Kesanupalli discloses an architecture with a completely different type of memory for storing the credentials. In Kesanupalli, the Host PC 202 is like Brown’s device 100 and is a generic computer running the Windows operating system (*see* WinUSB Driver 210) with applications like an internet browser installed.” Prelim. Resp. 46. In that regard, Patent Owner produces a Petitioner-annotated version of Kesanupalli’s Figure 2 (from page 24 of the Petition), on page 46 of the Preliminary Response, reproduced below:



APPL-1006, FIG. 2, annotated

Figure 2 is an illustration of a sample system of Kesanupalli. Ex. 1006, 2:1–2. In this annotated version, Petitioner has placed red arrows, labelled as “processor,” “interface,” and “storage.”

Patent Owner explains that although Host PC 202 of Kesanupalli, shown in blue, is where Brown wiping method would be running (in application 214), there is no explanation how a POSITA would make the Brown system wipe data in Kesanupalli's secure storage shown in red, "which is not akin to anything disclosed in Brown and only has one accessible interface which is not accessible by the Host PC—only the sensor 204." Prelim. Resp. 47–48. Patent Owner reiterates the same, in different words:

Under Petitioner's combination, Brown's generic software would be an application 214 running on Host PC 202 (blue above) and it would not have direct access to the secure storage (red above). Petitioner has not explained how Brown could wipe the secure storage of Kesanupalli without having direct access to it. Brown discloses no such mechanism. To the contrary, Brown's wiping is of RAM and non-volatile storage directly accessible to the processor.

Id. at 49. Patent Owner further asserts:

The Petition has no support at all for the proposition that a POSITA would have had a reasonable expectation of success wiping Kesanupalli's secure storage with Brown's generic disclosures. Brown does not disclose wiping storage it does not have access to and Brown does not disclose wiping of secure storage (or non-generic storage). A POSITA would be in the dark about how to implement Brown's generic disclosures within Kesanupalli's architecture and Petitioner nor Petitioner's expert shed any light on this issue.

Id.

These arguments of Patent Owner are misplaced.

Patent Owner overlooks that what Petitioner proposes to do simply is to incorporate into the system of Kesanupalli the wiping feature disclosed by Brown, i.e., the ability to wipe stored sensitive data, nothing more.

Petitioner has not proposed to wipe Kesanupalli's secure memory, where the sensitive data is stored, the way Brown wipes its unprotected memory. In characterizing Petitioner's theory as the latter, Patent Owner creates a problem where there is none.

Kesanupalli's system uses a secure memory, and Brown's system does not. That does not mean Petitioner has proposed to access Kesanupalli's secure memory the way Brown accesses its unprotected memory, which neither Kesanupalli nor Brown teaches how to do. Petitioner's expert, Dr. McDaniel, also has not explained how to do so. But that is a non-issue, because it is not Petitioner's theory to access Kesanupalli's secure memory to wipe the sensitive data contained therein the exact same way Brown accesses its unprotected memory to wipe the sensitive data therein.

As discussed above in the context of limitation [1.3], biometric templates and user credential comprising cryptographic key are stored in Kesanupalli's secure memory 206. *See* Ex. 1003 ¶¶ 104–105; Ex. 1006, 3:15–51. Whichever circuit would perform the wiping in Kesanupalli to implement the wiping feature of Brown must have access to that secure memory. Petitioner has indicated clearly how that would be done.

Petitioner explains: “Kesanupalli's processor circuitry executing the functions of sensor 204 has access to the record in the storage on the device to facilitate the wiping of Brown; and the processor circuitry (e.g., executing application 214) receives communication.” Pet. 43 (citing Ex. 1003 ¶ 147). Thus, as has been explained by Petitioner, a portion of the processor circuitry, e.g., executing application 214, is responsible for communication and does not access the secure memory, and a portion of the processor

circuitry interacting with sensor 204 has access to the secure memory and does the actual wiping.

In the context of limitation [1.1], Petitioner has mapped the claimed processor to include both circuitry which executes the function of sensor 204 and circuitry which executes functions of PC 202. Pet. 22. Specifically, Petitioner states: “The processor circuitry executing functions of sensor 204 and the processor circuitry executing functions of PC 202 provide a processor on the device.” *Id.* It is unavailing for Patent Owner to point out that Kesanupalli’s Host PC 202 does not have direct access to secure memory 206 as Brown’s processor does to its non-volatile memory and RAM. That argument insists that wiping be performed for Kesanupalli’s secure memory in the same way it is performed for unprotected memory in Brown. That is not Petitioner’s theory of combination for Kesanupalli and Brown. Patent Owner has not explained any proper basis for such a requirement, and we see none.

For the foregoing reasons, we find Petitioner sufficiently establishes that limitation [1.8] is met by the combined teachings of Kesanupalli and Brown.

k. Limitation [1.9]

Limitation [1.9] recites “a memory coupled to the processor and configured to provide the processor with instructions.” Ex. 1001, 11:55–56.

Petitioner asserts that Kesanupalli’s system includes a main memory. Pet. 44 (citing Ex. 1006, 9:58–10:46). Petitioner explains that a “POSITA would understand that the main memory of Kesanupalli’s system is coupled to the processor and configured to provide the processor with instructions

including at least those that execute the functions of the Host PC 202.” *Id.* (emphases omitted) (citing Ex. 1003 ¶ 151).

Patent Owner does not present counter-argument against the above-noted assertions of Petitioner. Petitioner’s assertions are supported by the cited evidence. Petitioner sufficiently establishes that Kesanupalli teaches limitation [1.9].

l. Conclusion for Claim 1

For the foregoing reasons, Petitioner has shown a reasonable likelihood that it would prevail in establishing the obviousness of claim 1 over Kesanupalli and Brown.

4. Independent Claims 13 and 25

Claim 13 recites similar subject matter as claim 1, but in method form. Ex. 1001, 12:20–56. The various functionalities recited in claim 1 are recited as method steps in claim 13. *Id.* Petitioner presents the same arguments for claim 13 as it does for claim 1. Pet. 49–50. Patent Owner does not present arguments for claim 13 separate from or additional to its arguments for claim 1. For substantially the same reasons as we explained above in the context of claim 1, we find that Petitioner has shown a reasonable likelihood that it would prevail in establishing the obviousness of claim 13 over Kesanupalli and Brown.

Claim 25 recites similar subject matter as claim 1, but in the form of a computer program product embodied in a non-transitory computer readable storage medium and comprising computer instructions. Ex. 1001, 13:17–14:26. The various functionalities recited in claim 1 are recited as what are achieved by computer instructions. *Id.* Petitioner presents substantially the same arguments for claim 25 as it does for claim 1. Pet. 51–54.

Additionally, Petitioner asserts:

The citations to Kesanupalli and Brown above apply to a device as in claim 1, and also to a computer program product embodied in a non-transitory computer readable storage medium. Kesanupalli discloses a computer program product can comprise instructions for the processes including those executed by its sensor 204 and a computing host (PC) 202 discussed above. *See* APPL-1006, 9:58–10:12 (“configured to perform particular tasks according to the invention, by executing machine-readable software code that defines the particular tasks embodied by the invention.”), 13:8–39. *See also*, APPL-1009, 19:49–56 (“The systems and methods data may be stored in one or more data stores. . . It is noted that data structures describe formats for use in organizing and storing data in databases, programs, memory, or other computer-readable media for use by a computer program.”)

Pet. 53 (emphases omitted).

Patent Owner does not present arguments for claim 25 separate from or additional to its arguments for claim 1. For substantially the same reasons as we explained above in the context of claim 1, and also based on Petitioner’s accounting, quoted above, for a computer program product embodied in a non-transitory computer storage medium, we find that Petitioner has shown a reasonable likelihood that it would prevail in establishing the obviousness of claim 25 over Kesanupalli and Brown.

5. *Dependent Claims 2, 3, 7, 8, 12, 14, 15, 19, and 24*

Claims 2, 3, 7, 8, and 12 each depend, directly or indirectly, from claim 1. Ex. 1001, 11:57–60, 12:1–7, 12:18–19. Claims 14, 15, 19, and 24 each depend, directly or indirectly, from claim 13. *Id.* at 12:57–60, 13:1–4, 13:15–16.

Petitioner addresses these dependent claims and explains how they are met by the combined teachings of Kesanupalli and Brown. Pet. 44–48, 51.

Petitioner's assertions are supported by the cited evidence and not disputed by Patent Owner.¹⁰

On this record, Petitioner has shown a reasonable likelihood that it would prevail in establishing the obviousness of claims 2, 3, 7, 8, 12, 14, 15, 19, and 24 over Kesanupalli and Brown.

F. Alleged Obviousness of Claims 10 and 22 over Kesanupalli, Brown, and Cheng

1. Overview of Cheng (Exhibit 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:

¹⁰ For claim 7, Petitioner presents an alternative argument premised on Patent Owner possibly arguing that “remote wiping” is “self-wiping.” Pet. 46. We need not and do not express any view in that regard. Patent Owner has not asserted that “remote wiping” is “self-wiping,” and we have no reason to so hold.

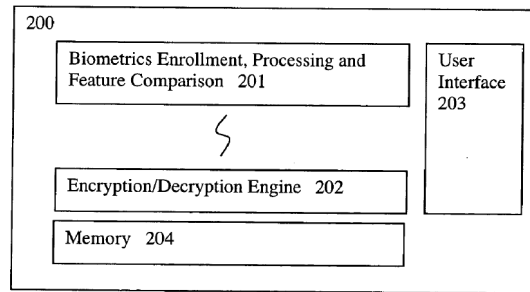


FIG. 2

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.

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 ¶¶ 8–9.

2. *Claims 10 and 22*

Claim 10 depends from claim 1 and claim 22 depends from claim 13, and each of claims 10 and 22 further recites: “wherein the at least portion of the at least one record is backed up to a remote entity.” Ex. 1001, 12:12–14, 13:11–12. Petitioner explains how the added limitation of claims 10 and 22 is taught by Cheng and how one of ordinary skill in the art would have been motivated to incorporate that feature of Cheng into the system of claim 1 and the method of claim 13 which, as discussed above, is taught by the combined teachings of Kesanupalli and Brown. Pet. 57–62 (citing Ex. 1003 ¶¶ 189–193; Ex. 1008 ¶¶ 6, 8, 23–28, 30, Figs. 3A–3B).

Regarding motivation to combine the teachings of Cheng with those of the combination of Kesanupalli and Brown, Petitioner asserts that a “POSITA would have been motivated to apply Cheng’s teachings of backing

up data from storage of an electronic device to a remote entity to the device of Kesanupalli as modified by Brown.” Pet. 57 (citing Ex. 1003 ¶¶ 184–188). Petitioner notes that like Kesanupalli and Brown, “Cheng is also similarly directed to protection of a user’s authentication data in particular.” *Id.* at 57–58 (citing Ex. 1008 ¶¶ 4, 7; Ex. 1006, Fig. 2, code (57); Ex. 1009, 1:15–2:8). Petitioner explains that applying Cheng’s backup teachings to Kesanupalli “would produce the obvious, beneficial, and predictable results of reducing the need to recreate the user’s personal data when using a new device, such as on replacing a lost or stolen device.” *Id.* at 57 (citing Ex. 1003 ¶¶ 184–188).

Petitioner further explains that a “POSITA would recognize that while Kesanupalli-Brown has a benefit of wiping data to preserve security, wiping data risks losing the deleted data.” Pet. 58 (citing Ex. 1003 ¶¶ 186–187; Ex. 1008 ¶ 6). Petitioner further asserts: a “POSITA would have understood this deletion of the user’s personal data raises cost and inconvenience to the user.” *Id.* Petitioner states: a “POSITA would benefit from providing Cheng’s teachings to Kesanupalli-Brown in order to avoid the ‘cost and inconvenience’ of recreating the record wiped as a user would desire such data on a new or replacement device to continue to access the enrolled websites.” *Id.* at 59 (citing Ex. 1003 ¶ 187; Ex. 1008 ¶¶ 6–7). Petitioner further states that a POSITA “would have been motivated to address the preservation of data in the Kesanupalli-Brown combination by implementing the teachings of Cheng. *Id.* (citing Ex. 1003 ¶ 187).

Regarding a reasonable expectation of success in implementing Cheng’s backup technique in Kesanupalli as modified by Brown, Petitioner explains:

Adding [Cheng's] backup procedure would merely have been applying a known technique to a known device (method, or product) ready for improvement to yield predictable results. APPL-1003, ¶188. Indeed, the backup technique is implemented by routine software executed on generic processing components, which would have been a predictable application relative to Kesanupalli's system and devices as in particular as enhanced by the teachings of Brown. *Id.*

Pet. 59–60.

Petitioner's reasoning and assertions are supported by the cited evidence. Patent Owner does not present arguments separate from or additional to those it presents for independent claims 1 and 13, which we have already discussed and rejected in the context of claims 1 and 13.

Petitioner has shown a reasonable likelihood that it would prevail in establishing the obviousness of claims 10 and 22 over Kesanupalli, Brown, and Cheng.

G. Alleged Obviousness of Claims 11 and 23 over Kesanupalli, Brown, and Challenger

1. Overview of Challenger (Exhibit 1007)

Challenger relates to security processors provided in computer systems to implement security features. Ex. 1007, 3:24–26. It discloses a security processor apparatus including a processor and a memory coupled to the processor and operative to store a secure table. *Id.* at 2:23–25. The secure table stores a plurality of different certified endorsement keys and a plurality of different values each associated with one of the endorsement keys. *Id.* at 2:25–28. Figure 1 of Challenger is reproduced below:

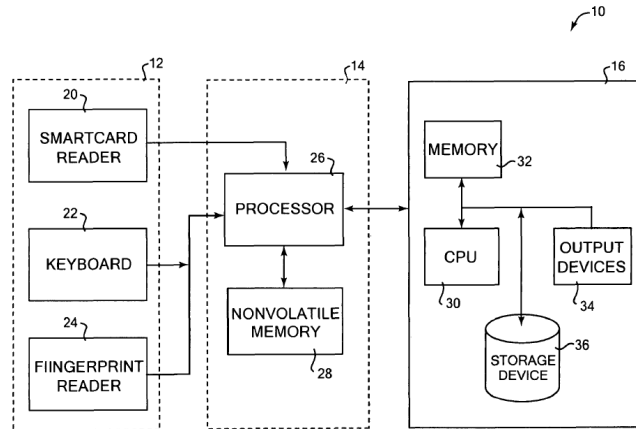


FIG. 1

Figure 1 illustrates computer system 10. Ex. 1007, 3:7–8.

Challenger describes: “System 10 includes security architecture such as a Trusted Platform Module (TPM) from the Trusted Computing Group (TCG),” for “securing data and functions of the system 10 from unauthorized access and manipulation.” Ex. 1007, 3:51–56. Challenger states:

In [the TPM] specification, a standard chipset including a programmable microcontroller is provided on a computer’s circuit board during manufacturing, and is used to store and secure information of the computer system that is desired to be protected, i.e., enable effective trusted computing features. The security architecture (i.e., the functions and the application program interface (API) that runs on the microcontroller, can be referred to as a TPM. A TPM can offer a variety of features, including a random number generator, facilities for secure generation of cryptographic keys, and ability to limit the use of keys, e.g., to signing and verification, and/or encryption and decryption.

Ex. 1007, 1:18–31.

System 10 includes input portion 12, security portion 14, and standard portion 16. Ex. 1007, 3:56–57. Input portion 12 includes a variety of different input devices which allow a user to input data to system 10 and

authenticate the user's identity to the system. *Id.* at 3:58–60. These input devices allow access to secured data of system 10 to authorized users. *Id.* at 4:1–3. Security portion 14 of system 10 is used to secure the data and application of the system for access and use only by authorized users. *Id.* at 4:9–11. In one embodiment, security processor 26 is dedicated to security functions. *Id.* at 4:11–13. Security processor 26 typically implements a “security architecture” which refers to the particular security features and functions (e.g., API functions, algorithms) implemented for system 10 as determined by a security architecture application loaded on security processor 26. *Id.* at 4:15–20. Challenger describes:

For example, processor 26 can implement a TPM security architecture, which is a well-known standard for securing computer data. A TPM architecture is implemented on a secure, dedicated chipset incorporated into a motherboard or other circuitry of a computer by the manufacturer. In other embodiments, the TPM architecture can be implemented in another existing chip of the computer system 10.

Ex. 1007, 4:24–30.

Nonvolatile memory 28 is included in security portion 14 and is connected to security processor 26. Ex. 1007, 4:57–58. “[M]emory 28 is a secure memory which cannot be easily tampered with to read its data contents.” *Id.* at 4:61–63. Memory 28 can be incorporated on the same integrated circuit chip as security processor 26. *Id.* at 4:63–65. Challenger describes: “[N]onvolatile memory 28 stores a secure table of hash values and endorsement keys which are used to determine whether applications to be loaded on the processor 26 are authorized, and enables flexible and secure support of various different security architectures and programs on processor 26.” *Id.* at 4:66–5:4.

2. *Claims 11 and 23*

Claim 11 depends from claim 1 and claim 23 depends from claim 13, and each of claims 11 and 23 further recites: “wherein the interface comprises a restricted interface.” Ex. 1001, 12:15–16, 13:13–14.

Petitioner adequately accounts for this additional limitation, on pages 62–70 of the Petition, relying on the combined teachings of Kesanupalli, Brown, and Challenger, including reasoning on why the teachings of Kesanupalli and Brown are properly combinable with the teachings from Challenger about having a restricted interface. Pet. 62–70 (citing Ex. 1003 ¶¶ 51–54, 57–60, 195–197, 198–202, 203–211; Ex. 1006, 1:25–27; Ex. 1007, 1:7–9, 1:18–31, 3:24–26, 3:37–56, 3:46–57, 3:51–56, 3:67–4:23, 4:9–65, 4:57–5:9, 5:15–25, Fig. 1, code (51); Ex. 1017; Ex. 1024).

Regarding motivation to combine the teachings of Challenger with those of the combination of Kesanupalli and Brown, Petitioner asserts that the combination would have produced the obvious, beneficial, and predictable results of a standardized and widely-deployed security architecture for implementation of Kesanupalli and Brown’s techniques.” Pet. 64 (citing Ex. 1003 ¶¶ 198–202). Petitioner explains:

POSITA would have been motivated to apply Challenger’s teachings of a standard-based TPM architecture as an implementation framework for Kesanupalli’s biometric security techniques given the support that a TPM implementation provides for many of the underlying cryptographic security services (encryption/decryption) and secure storage facilities provided. APPL-1003, ¶¶200–201; APPL-1007, 1:18–31 (summarizing typical TPM functions and APIs). Indeed, Challenger’s description of its TPM-based security architecture includes *both* secure storage (nonvolatile memory 28) for secure data, *e.g.*, “secure hash values and . . . keys,” *and* fingerprint reader 24 behind a security processor 26 that “implements the

particular security features and functions (e.g., API functions, algorithms)” in a system that includes secure and non-secure portions. APPL-1007, 4:57–5:9, 3:67–4:23. These are precisely the security architecture features POSITA having Kesanupalli before them would be motivated to implement in a standards-based security architecture that would engender trust amongst users and customers. APPL-1003, ¶¶200–202.

Pet. 65–66 (alteration by Petitioner). Regarding expectations of success, Petitioner asserts: a “POSITA would have had reasonable expectations of success in implementing Kesanupalli’s biometric authentication techniques and in applying Brown’s wipe features to a sensitive data in secure storage given that Challener’s architecture applies TPM techniques, which were well-known, standard, and widely-deployed in the industry.” Pet. 66 (citing Ex. 1003 ¶ 202; Ex. 1007, 1:18–31).

Petitioner’s reasoning and assertions are supported by the cited evidence. Patent Owner does not present arguments separate from or additional to those it presents for independent claims 1 and 13, which we have already discussed and rejected in the context of claims 1 and 13.

Petitioner has shown a reasonable likelihood that it would prevail in establishing the obviousness of claims 11 and 23 over Kesanupalli, Brown, and Challener.

H. Alleged Obviousness of Claims 5 and 17 over Kesanupalli, Brown, and Headley

1. Overview of Headley (Exhibit 1010)

Headley is titled “USER AUTHENTICATION FOR SOCIAL NETWORKS.” Ex. 1010, code (54). It discloses verification, by biometric templates, of users logging into a social network, to prevent user impersonation. *Id.* at code (57). “Verification can be performed, for example, by reference to biometric templates stored during the user

enrollment process.” *Id.* Biometric data can be that of user’s fingerprint, voice, eyes, face, genetic material, scent, and signature. *Id.* at 3:58–62.

Headley describes:

The methods described herein comprise an initial enrollment and subsequent authorizations. In the initial enrollment process, an enrollee user is associated with a user ID and that user ID is further associated with the address of a communication device for the user. The user is also asked to provide biometric samples in response to a plurality of different prompts. The prompts and responses are also associated with the user ID. After enrollment, a person seeking to be authenticated, termed a claimant herein, first submits a claimant target which can be the user ID or some other unique identifier from which the authentication system can infer the particular identity sought to be authenticated. One of the prompts associated with the user ID is then provided to the claimant, the claimant provides a biometric response to the prompt, and that response is compared to the biometric sample previously associated with that prompt. Within this simple framework a variety of security features can be effectively employed.

Ex. 1010, 3:41–57. Headley further describes that a prompt can be provided to the user’s device visually or aurally, e.g., by text message, verbal command or cue, audio clip, or video clip. *Id.* at 7:39–52.

2. *Claims 5 and 17*

Claim 5 depends from claim 1 and claim 17 depends from claim 13, and each of claims 5 and 17 further recites: “wherein the prompt is aurally presented.” Ex. 1001, 11:63–64, 12:63–64. Petitioner adequately accounts for this additional limitation, on pages 71–74 of the Petition, relying on the combined teachings of Kesanupalli, Brown, and Headley, including reasoning on why the teachings of Kesanupalli and Brown are properly combinable with the teachings from Headley about presenting a prompt aurally. Pet. 71–74.

Regarding motivation to combine teachings, Petitioner explains:

POSITA would have been motivated to apply Headley's teachings of providing a prompt aurally to elicit a user's biometric input in Kesanupalli's device. APPL-1003, ¶¶213–216. Kesanupalli discloses a visual prompt for biometric input, and Headley's teachings that such a prompt may be provided aurally as well as visually would produce the obvious, beneficial, and predictable results of increasing the robustness of the prompt to the user. *Id.*

Pet. 71–72. Petitioner further explains:

POSITA would have been motivated to employ Headley's presentation of a prompt visually and aurally in connection with Kesanupalli's secure authorization system and methods including Brown's wiping technique because POSITA would recognize that while Kesanupalli-Brown describes a *visual* prompt to provide biometric data additionally introducing a different type of prompt reaches more users and/or increases convenience to a user in recognizing a prompt. APPL-1003, ¶215.

Id. at 72.

Regarding reasonable expectation of success, Petitioner asserts:

POSITA would have had reasonable expectation of success in adding an aural presentation of Kesanupalli-Brown's prompt, as Headley is similarly directed to improving security of a user's data through biometric authentication procedures. APPL-1003, ¶216. Indeed, an aural prompt is implemented by routine software executed on generic processing components, which would have been a predictable application to Kesanupalli's devices as enhanced by Brown's teachings. *Id.*

Id. at 73.

Petitioner's reasoning and assertions are supported by the cited evidence. Patent Owner does not present arguments separate from or additional to those it presents for independent claims 1 and 13, which we have already discussed and rejected in the context of claims 1 and 13.

We determine that Petitioner has shown a reasonable likelihood that it would prevail in establishing the obviousness of claims 5 and 17 over Kesanupalli, Brown, and Headley.

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

Under 35 U.S.C. § 314(a) and applying factors set forth 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.

On April 29, 2024, prior to filing of Patent Owner’s Preliminary Response, Petitioner filed Exhibit 1030, which is an email letter from Petitioner’s counsel to Patent Owner’s counsel. Ex. 1030. The letter states, *inter alia*:

Petitioner Apple Inc. (“Apple”) hereby stipulates that if the Patent Trial and Appeal Board (PTAB) institutes the IPR based on the grounds identified below, then it (i) will not pursue the grounds identified below in the Parallel District Court Litigation and (ii) *will not pursue any other ground that reasonably could have been raised during the IPR* (should it be instituted) in the Parallel District Court Litigation.

Ex. 1030, 1 (emphasis added). The letter then produces a table identifying the four grounds of unpatentability matching the grounds of unpatentability specifically identified in the Petition in this proceeding and as noted in Section II.F above. *Id.*

We determine Petitioner’s stipulation possesses attributes sufficient to meet the requirements of *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020) (precedential as to § II.A). Office policy provides that, “[c]onsistent with *Sotera Wireless, Inc.*, the PTAB will not discretionarily deny institution in view of parallel district court litigation

where a petitioner presents a stipulation not to pursue in a parallel proceeding the same grounds or any grounds that could have reasonably been raised before the PTAB.” *Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation*, Memorandum, June 21, 2022, 3, 7–8 (available at https://www.uspto.gov/sites/default/files/documents/interim_proc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621_.pdf).

Patent Owner characterizes Petitioner’s latest “*Sotera* style” stipulation as “not being added to simplify the proceedings” but “a last gasp effort to have these proceedings instituted prior to the upcoming Western District of Texas trial scheduled for December 2024 that Petitioner was not expecting when it filed its original stipulations.” Prelim. Resp. 22. This argument is unavailing, because Petitioner nonetheless still filed a qualifying *Sotera* stipulation prior to the Board’s decision to institute review. We do not regard the filing as belated.

Further, Patent Owner asserts:

Regardless of Petitioner’s actions, Petitioner’s stipulation does not in fact guarantee the reduction of any duplicate effort. Petitioner has already positioned itself to combine the petitioned art with art that Petitioner will argue it “could **not** have reasonably been raised” in the IPR petitions, such as system art, in the district court in order to avoid the consequences of its stipulation. For example, Petitioner could allege in the district court a combination of a system art reference such as the “UPEK system” in combination with the exact the grounds—Kesanupalli and Brown—in this Petition.

Prelim. Resp. 23. This argument also is unavailing, because Petitioner’s stipulation nonetheless still satisfies the requirements of *Sotera*. Patent

Owner does not explain how the requirements of a “*Sotera* style” stipulation have not been met.

Further, Patent Owner notes that Petitioner has filed seven petitions to institute *inter partes* reviews when all issues could instead 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.* But *General Plastic* relates to the filing of multiple follow-on petitions by the same party against the same patent. Patent Owner has not identified any other petition for *inter partes* review filed by Petitioner against the ’138 patent.

Consequently, we do not exercise our discretion to deny institution based on the parallel district court litigation or based on *General Plastic* under 35 U.S.C. § 314(a).

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

Patent Owner contends 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). Prelim. Resp. 25–38. In *Advanced Bionics*, the Board applied a two-part framework in considering whether to exercise discretion to deny institution under 35 U.S.C. § 325(d):

- (1) whether the same or substantially the same art previously was presented to the Office or whether the same or substantially the same arguments previously were presented to the Office; and (2)
- if either condition of first part of the framework is satisfied,

whether the petitioner has demonstrated that the Office erred in a manner material to the patentability of challenged claims.

Advanced Bionics at 8 (footnote omitted).

Within this two-part framework, the Board considers a number of non-exclusive factors in evaluating whether to exercise its discretion under § 325(d). *See Becton, Dickinson & Co. v. B. Braun Melsungen AG*, IPR2017-01586, Paper 8 (PTAB Dec. 15, 2017) (precedential as to § III.C.5, first para.); *see also Advanced Bionics* at 9–11. The factors set forth in *Becton, Dickinson* are as follows:

(a) the similarities and material differences between the asserted art and the prior art involved during examination; (b) the cumulative nature of the asserted art and the prior art evaluated during examination; (c) the extent to which the asserted art was evaluated during examination, including whether the prior art was the basis for rejection; (d) the extent of the overlap between the arguments made during examination and the manner in which Petitioner relies on the prior art or Patent Owner distinguishes the prior art; (e) whether Petitioner has pointed out sufficiently how the Examiner erred in its evaluation of the asserted prior art; and (f) the extent to which additional evidence and facts presented in the Petition warrant reconsideration of the prior art or arguments.

Becton, Dickinson at 17–18 (footnote omitted).

Becton, Dickinson factors (a), (b), and (d) relate to whether the art or arguments presented in the Petition are the same or substantially the same as those previously presented to the Office. *Advanced Bionics* at 10. Factors (c), (e), and (f) “relate to whether the petitioner has demonstrated a material error by the Office” in its prior consideration of that art or arguments. *Id.* Only if the same or substantially the same art or arguments were previously presented to the Office do we then consider whether petitioner has demonstrated a material error by the Office. *Id.* “At bottom, this framework

reflects a commitment to defer to previous Office evaluations of the evidence of record unless material error is shown.” *Id.* at 9.

Regarding prong (1) of *Advanced Bionics*, i.e., factors (a), (b), and (d), Patent Owner asserts that although Kesanupalli was not before the Examiner during prosecution of the ’138 patent, another Kesanupalli reference, i.e., U.S. Pat. Pub. No. 2011/0138450 (“Kesanupalli ’450” (Ex. 2030)), which has similar subject matter, was before the Examiner and that Petitioner is relying on portions of Kesanupalli which are also in Kesanupalli ’450. Prelim. Resp. 29–31. The parties dispute whether the claimed feature of “prompt is visually presented,” for which Petitioner relies on Kesanupalli, is disclosed in Kesanupalli ’450. Pet. 78; Prelim. Resp. 32–34.

Patent Owner also notes that Kesanupalli ’450 was an applied reference in the Petition filed in *Samsung Electronics Co., Ltd. v. RightQuestion, LLC*, IPR2022-00251, which involved a patent of Patent Owner that is related to the ’138 patent, and that institution was denied there. Prelim. Resp. 8, 26–27, 29.

Patent Owner does not dispute that Brown was not previously before the Office during prosecution of the ’138 patent. Prelim. Resp. 34. However, Patent Owner asserts that Brown’s disclosure of wiping is cumulative of a reference that was used by the Examiner to reject some claims, i.e., U.S. Patent No. 7,780,080 B2 (“Owen” (Ex. 2031)). *Id.* Specifically, Patent Owner points to where and how the Examiner identified portions of Owen for its teachings about wiping. *Id.* at 34–36 (citing Ex. 1002, 126–127 (citing Ex. 2031, 27:35–37, 27:56–66, 30:21–39)).

Even assuming that both Kesanupalli and Brown or their equivalents were previously cited to and considered by the Examiner during prosecution

of the '138 patent, that still would not lead to a satisfaction of prong 1 of *Advanced Bionics*. That is because the Petition includes additional grounds of alleged unpatentability, and those additional grounds rely on Cheng, Challenger, and Headley, none of which appears to have been previously presented to the Examiner or the Office during prosecution of the '138 patent. Patent Owner does not contend that any of Cheng, Challenger, and Headley was previously presented before the Office, and Petitioner expressly states that neither Challenger nor Cheng was before the Office during prosecution. Pet. 78.

As for the Petition in IPR2022-00251 which relied on Kesanupalli '450, it did not apply Kesanupalli '450 in combination with any of Brown, Challenger, Cheng, and Headley, or each's equivalent. "[T]he petitioner's petition, not the Director's discretion, is supposed to guide the life of the litigation." *SAS Inst., Inc. v. Iancu*, 138 S. Ct. 1348, 1356 (2018); *see also Sirona Dental Sys. GmbH v. Institut Straumann AG*, 892 F.3d 1349, 1356 (Fed. Cir. 2018) ("It would . . . not be proper for the Board to deviate from the grounds in the petition and raise its own obviousness theory.").

Petitioner is master of its Petition, and IPR2022-00251 is no exception. Further, Patent Owner has not shown that the subject matter claimed in the patent challenged in IPR2022-00251 is the same as that of the challenged claims in this proceeding.

For the foregoing reasons, we determine that prong 1 of *Advanced Bionics* is not met. Consequently, we do not exercise our discretion to deny institution based on 35 U.S.C. § 325(d).

IV. CONCLUSION

For the foregoing reasons, we determine that Petitioner has shown a reasonable likelihood that it would prevail in establishing that at least one of claims 1–3, 5, 7, 8, 10–15, 17, 19, and 22–25 of the '138 patent is unpatentable.

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that *inter partes* review of all challenged claims, i.e., claims 1–3, 5, 7, 8, 10–15, 17, 19, and 22–25 of the '138 patent, is hereby instituted on all grounds stated in the Petition; and

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial; the trial will commence on the entry date of this decision.

IPR2024-00334
Patent 11,514,138 B1

For PETITIONER:

David W. O'Brien
Kelley 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