Trials@uspto.gov
571-272-7822

Paper 26
Date: May 22, 2025

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*.

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

I. INTRODUCTION

We instituted 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") owned by Carbyne Biometrics, LLC ("Patent Owner"). Paper 10 ("Decision to Institute"). We have authority to conduct this *inter partes* review under 35 U.S.C. § 6. This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. We determine that Apple Inc. ("Petitioner") has proved by a preponderance of the evidence that claims 1–3, 5, 7, 8, 10–15, 17, 19, and 22–25 of the '138 patent are unpatentable.

A. Background

Petitioner filed a Petition requesting an *inter partes* review of the challenged claims pursuant to 35 U.S.C. §§ 311–319. Paper 2 ("Pet."). Patent Owner filed a Preliminary Response. Paper 7. Petitioner filed an authorized Preliminary Reply. Paper 8. Patent Owner filed an authorized Preliminary Sur-reply. Paper 9. The Decision to Institute was entered on July 16, 2024. Paper 10. Thereafter, Patent Owner filed a Response (Paper 13, "PO Resp."), Petitioner filed a Reply. Paper 16. Patent Owner filed a Sur-reply. Paper 17.

A consolidated oral hearing was held on April 16, 2025, for this proceeding and related proceeding IPR2024-00332. The hearing transcript has been entered into the record as Paper 25.

B. Real Parties-in-Interest

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

C. Related Matters

The parties 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 a related matter. Pet. 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.

D. The ’138 Patent (Ex. 1001) [1]

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:

[1] The ’138 patent issued from Application No. 17/027,481, filed Sept. 21, 2020, which claims priority to a chain of ancestral applications including Application No. 13/706,254, 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).

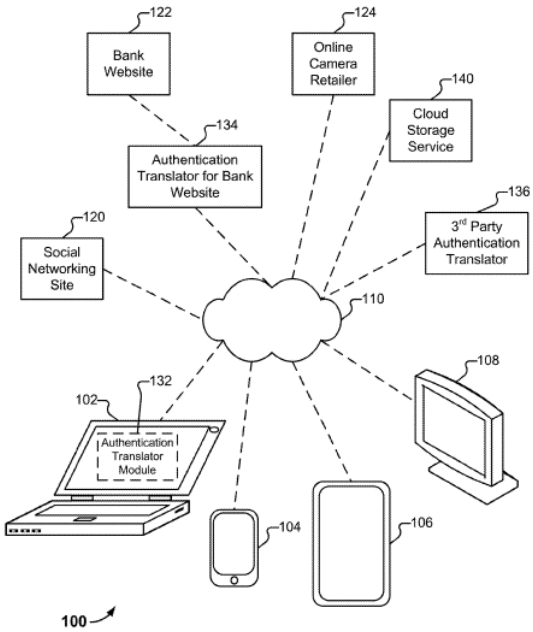


FIG. 1

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:

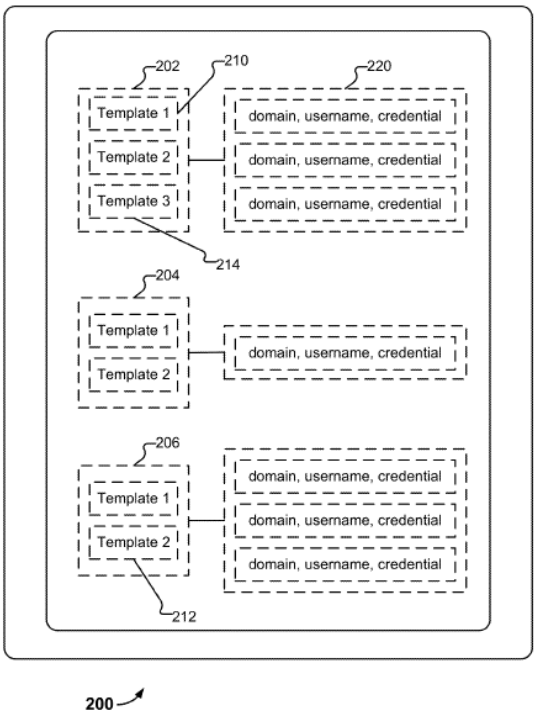


FIG. 2

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 governs 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:

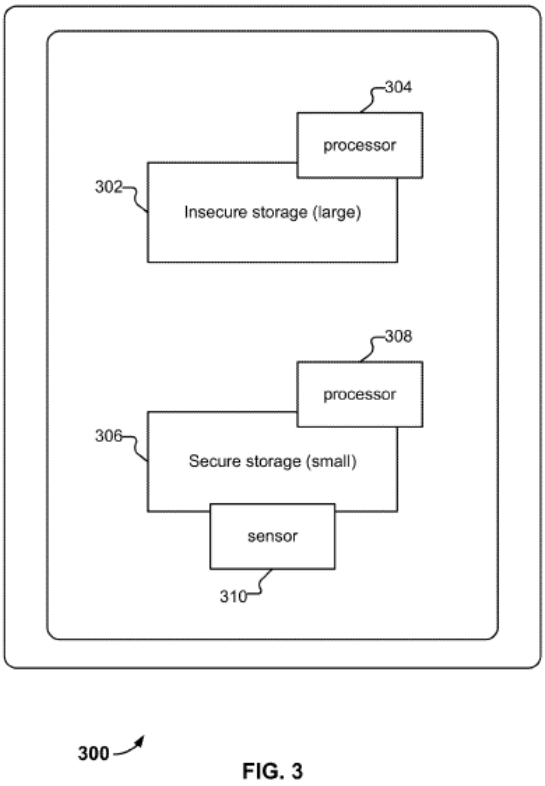


FIG. 3

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.

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.[2]

E. Prior Art and Declaration Evidence

Petitioner relies on the following evidence:

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

Petitioner also relies on the Declaration (Ex. 1003) and Reply Declaration (Ex. 1036) of Patrick McDaniel, Ph.D. Patent Owner relies on the Declaration of Michael T. Goodrich, Ph.D. (Ex. 2037).

---

[2] 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.
[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). We alternatively also refer to Kesanupalli as "the Kesanupalli reference."
[7] Published June 17, 2004. Ex. 1008, code (43).

F. Asserted Grounds of Unpatentability

Petitioner asserts that the challenged claims of the ’138 patent are unpatentable based on the following grounds (Pet. 10, 54, 62, 70):

Claim(s) Challenged	35 U.S.C. §	Reference(s)/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

II. ANALYSIS

A. Burden of Proof

The Petitioner has the burden of proving unpatentability by a preponderance of the evidence. 35 U.S.C. § 316(e) (2024). That burden only shifts to Patent Owner in limited circumstances not present here. *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1375 (Fed. Cir. 2016). “Preponderance of the evidence means the greater weight of evidence, evidence which is, more convincing than the evidence which is offered in opposition to it.” *United States v. C.H. Robinson Co.*, 760 F.3d 1376, 1383 (Fed. Cir. 2014) (internal quotations omitted).

[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.

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).

Patent Owner states in its Response that "Patent Owner has applied Petitioner's POSITA [person of ordinary skill in the art] for the sake of this Response." PO Resp. 12. 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. Petitioner's proposed level of ordinary skill is supported by the testimony of Dr. McDaniel (Ex. 1003 ¶¶ 18–21) and not disputed by Patent Owner (PO. Resp. 12). 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 Construction

We use the same claim construction standard that would be used to construe a claim in a civil action under 35 U.S.C. § 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. 37 C.F.R. § 42.100(b)

(2024). 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. *Phillips*, 415 F.3d at 1316. If an inventor acts as his or her own lexicographer, the definition must be set forth in the specification with reasonable clarity, deliberateness, and precision. *Renishaw PLC v. Marposs Societa' per Azioni*, 158 F.3d 1243, 1249 (Fed. Cir. 1998). 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" and "restricted interface"

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.

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 either "processor" or "restricted interface," and states that because the Response does not depend on the meaning of those terms construed by Petitioner, "Patent Owner does not address these positions." PO Resp. 12.

The issues in this case do not require a construction of "processor." 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 that a "restricted interface" is an interface that limits accessibility and includes within its scope a restricted API.

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

1. The Law on Obviousness

A claim is unpatentable if the differences between the subject matter sought to be patented 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. 35 U.S.C. § 103(a); *see KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) where in evidence, so-called secondary considerations, including commercial success, long-felt but unsolved needs, failure of others, and unexpected results. *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17–18 (1966).

When evaluating a combination of teachings, we must also "determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR*, 550 U.S. at 418 (citing *In re*

Kahn, 441 F.3d 977, 988 (Fed. Cir. 2006)). "[T]here must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *In re Kahn*, 441 F.3d at 988.

2. Overview of Kesanupalli (Ex. 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:

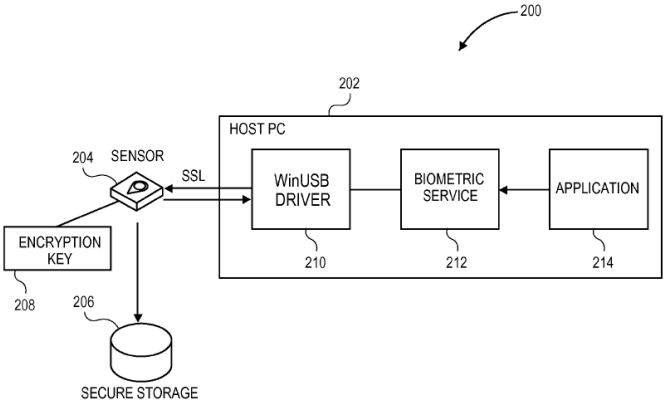


FIG. 2

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:

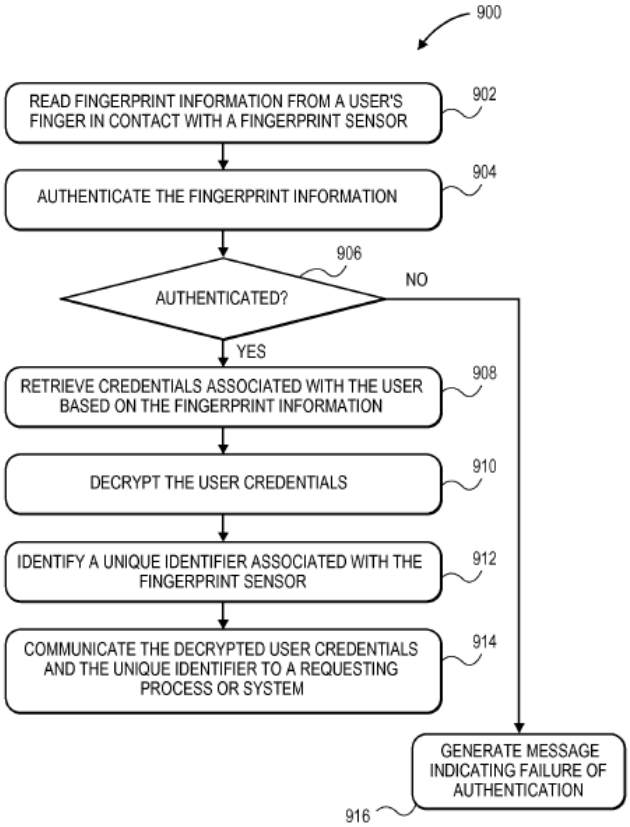


FIG. 9

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 credentials. 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.

3. 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:

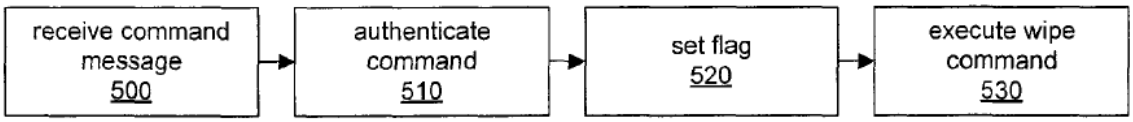


Figure 6

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.

4. Independent Claim 1

a) The Preamble and Limitations [1.1] to [1.7] and [1.9]

Petitioner provides accounting for the preamble recitation [1pre] on pages 20–21 of the Petition, for limitation [1.1] regarding a processor on the device on pages 21–23 of the Petition, and for limitation [1.2] regarding a storage on the device on pages 23–24 of the Petition. According to Petitioner, Kesanupalli discloses each of preamble [1pre], limitation [1.1] and limitation [1.2]. *Id.* at 20–24. Patent Owner has not presented a counter-argument or disputed Petitioner's assertions in this regard. We have reviewed the evidence cited by Petitioner, and find that Kesanupalli discloses each of the preamble [1pre], limitation [1.1] and limitation [1.2].

Petitioner provides accounting for the processor function limitation [1.3] on pages 25–29 of the Petition. According to Petitioner, Kesanupalli discloses limitation [1.3]. Pet. 25–29. Patent Owner has not presented a counter-argument or disputed Petitioner's assertions in this regard. We have

reviewed the evidence cited by Petitioner, and find that Kesanupalli discloses limitation [1.3].

Petitioner provides accounting for the wherein clause limitation [1.4] regarding a stored record on pages 29–34 of the Petition. According to Petitioner, Kesanupalli discloses limitation [1.4]. Pet. 29–34. Patent Owner has not presented a counter-argument or disputed Petitioner's assertions in this regard. We have reviewed the evidence cited by Petitioner, and find that Kesanupalli discloses limitation [1.4].

Petitioner provides accounting for the processor function limitation [1.5A] regarding matching a biometric input with a biometric template on pages 30–34 of the Petition. According to Petitioner, Kesanupalli discloses limitation [1.5A]. Pet. 30–34. Patent Owner has not presented a counter-argument or disputed Petitioner's assertions in this regard. We have reviewed the evidence cited by Petitioner, and find that Kesanupalli discloses limitation [1.5A].

Petitioner provides accounting for the wherein clause of limitation [1.5B] regarding receiving biometric input subsequent to presentation of a prompt on pages 34–35 of the Petition. According to Petitioner, Kesanupalli discloses limitation [1.5A]. Pet. 34–35. Patent Owner has not presented a counter-argument or disputed Petitioner's assertions in this regard. We have reviewed the evidence cited by Petitioner, and find that Kesanupalli discloses limitation [1.5B].

Petitioner provides accounting for limitation [1.6] relating to establishing a connection with an external resource on pages 35–37 of the Petition. According to Petitioner, Kesanupalli discloses limitation [1.6]. Pet. 35–37. Patent Owner has not presented a counter-argument or disputed

Petitioner's assertions in this regard. We have reviewed the evidence cited by Petitioner, and find that Kesanupalli discloses limitation [1.6].

Petitioner provides accounting for the processor function required by limitation [1.7] on pages 37–40 of the Petition. According to Petitioner, Kesanupalli discloses limitation [1.7]. Pet. 37–40. Patent Owner has not presented a counter-argument or disputed Petitioner's assertions in this regard. We have reviewed the evidence cited by Petitioner, and find that Kesanupalli discloses limitation [1.7].

Petitioner provides accounting for the memory required by limitation [1.9] on pages 44–45 of the Petition. According to Petitioner, Kesanupalli discloses limitation [1.9]. Pet. 44–45. Patent Owner has not presented a counter-argument or disputed Petitioner's assertions in this regard. We have reviewed the evidence cited by Petitioner, and find that Kesanupalli discloses limitation [1.9].

b) Limitation [1.8]

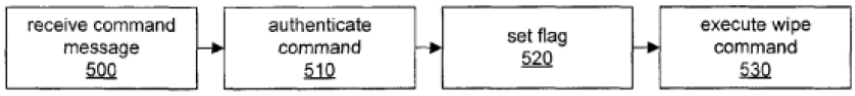
Limitation [1.8] recites "[wherein the processor on the device is configured to:] facilitate wiping of both the biometric template and the credential comprising the cryptographic key of the at least one record stored at least in part in the storage on the device." Ex. 1001, 11:51–54.

(1) Petitioner's Assertions

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 <u>all</u> 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 (emphases omitted).

Petitioner also 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 similarly is directed to systems for securing client devices that include data of a sensitive nature such as the user’s personal files and implements its systems 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 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 (emphasis omitted).

(2) Patent Owner’s Assertions

Patent Owner argues that Petitioner’s proposed combination of Kesanupalli and Brown “fails to consider that Kesanupalli’s *main goal* was to thwart social engineering attacks,” and that Brown’s teachings about wiping “would not further Kesanupalli’s goals.” PO Resp. 15 (emphasis added). Patent Owner also argues that “Kesanupalli is only concerned with social engineering and not breaches to the actual device,” noting that the user’s biometrics and cryptographic key are provided to the browser extension in the general processor. *Id.* at 27, 29–30.

According to Patent Owner, we must also consider what Ramesh Kesanupalli, a coinventor of the Kesanupalli reference and purportedly a person of ordinary skill in the art, actually did, i.e., not describing wiping in the disclosure of the Kesanupalli reference. PO Resp. 15–16.

Patent Owner asserts that Mr. Kesanupalli was a leader in the computer security field, was aware of existing wiping functionality, and “made a conscious decision to not use [wiping] in his patented system.” PO Resp. 16. According to Patent Owner, Mr. Kesanupalli’s decision not to include wiping reflects “common sense and real world indicators” which

must not be ignored. *Id.* at 17. Patent Owner asserts that Kesanupalli's focus on preventing social engineering attacks would not be furthered by adding a wiping feature, and that the concerns of the Kesanupalli reference are not addressed by adding a wiping feature. *Id.*

Patent Owner asserts that Kesanupalli's disclosure is interested in curbing social engineering attacks such as phishing and spoofed websites, and that the goal of curbing social engineering attacks would not have benefitted from inclusion of a wiping feature. PO Resp. 18. Patent Owner's expert, Dr. Goodrich, testifies that social engineering attacks rely on tricking the user to release credentials to imposters or bad actors. Ex. 2037 ¶ 50 (cited at PO Resp. 18). Patent Owner further explains:

> Tricking the user to release their credentials is typically done through email or text messages containing a link to a fake website that looks legitimate to convince the victim to enter their sensitive information. Ex. 2037 (Goodrich Decl.) at ¶¶50-53. For example, someone could trick a user by pretending to [be] Netflix and telling the user that they must log in and provide updated payment details to get their account off hold. If the user selects the update account button, they will be redirected to a spoofed version of Netflix where the bad actor will collect the user's credentials.

PO Resp. 18–19.

Dr. Goodrich testifies: "[W]iping a device would have no impact on deterring a social engineering attack. Once the attacker has tricked a user to release their credentials, wiping the device will not bring those credentials back or benefit the user in any way." Ex. 2037 ¶ 69.

Patent Owner asserts that social engineering attacks do not require a device to be breached, and argues that there is no reason for one of ordinary skill in the art to combine "Brown's wiping with Kesanupalli's social engineering protections." PO Resp. 26–27. Further, Patent Owner notes

that one actual person of ordinary skill in the art, Ramesh Kesanupalli, made a conscious decision to not use wiping in the disclosed system of Kesanupalli because it "would have no impact on curbing social engineering attacks." *Id.* at 31 (citing Ex. 2037 ¶ 64). Patent Owner further asserts: "Kesanupalli decided to confront social engineering attacks with his system and a POSITA given the disclosures of the reference would not have been motivated to add [wiping] as it would not have added any additional benefit to the user." *Id.* (citing Ex. 2037 ¶ 64).

(3) Discussion

Patent Owner's arguments are unpersuasive for two reasons.

First, assuming that Kesanupalli's main goal or focus is on thwarting social engineering attacks and that Kesanupalli's disclosure is "interested in curbing social engineering attacks" as Patent Owner asserts, it does not mean Kesanupalli's "only" goal or interest is on thwarting social engineering attacks to the exclusion of everything else. Kesanupalli reveals an interest and concern in areas outside of thwarting social engineering attacks, (1) by noting that "any person can access the user's Web-based accounts and information if they gain knowledge of the user's password and username" (Ex. 1006, 1:44–46), (2) by identifying malware attacks in the form of "Man in the Browser" as a potential threat associated with user passwords (Ex. 1006, 1:47–58), and (3) by encrypting user credentials and storing the encrypted credentials in a secure storage (Ex.. 1006, 6:6–8). We agree with Petitioner's reasoning as reproduced below:

> [Risk of device breach] is one reason Kesanupalli describes <u>numerous</u> specific security features that are <u>not</u> focused exclusively on social engineering attacks or on promoting stronger passwords. Rather, these security features focus on protecting passwords, other credentials such as cryptographic

> keys, and biometric information from compromise while held in its device and during communication. For example, Kesanupalli discusses using secure socket layer (SSL) protocol for encrypted transmission of data including between its sensor and general processor, implementing strong cryptographic algorithms in its hardware and/or software, strengthening security by biometric sensor unique identifiers (ID), using cryptography features of secure keys and hashes, and so on. APPL-1036, ¶¶17-18 citing APPL-1006, 1:28-30, 6:39-42, 4:12-23, 4:64-5:33. Further, Kesanupalli generally discusses providing "secure transactions," "secure application," and "secure communication," with no implication that these are "secure" only with respect to social engineering attacks. APPL-1036, ¶17 citing APPL-1006, 5:53-58, 6:15-17, 6:39-42. In perhaps a plainest example, Kesanupalli provides that its storage for biometric data and credentials be in "a **secure** storage device." APPL-1006, 3:46-51, 6:6-10; *see also*, APPL-1036, ¶16. Thus, Kesanupalli is certainly concerned with breaches to its device—why else place the credentials in a "**secure** storage" of its architecture. *See* POR, p. 27. Any one of these features shows that Kesanupalli is concerned with security as a whole, including device security. APPL-1036, ¶¶14-23.

Reply 9–10 (footnote omitted).

Dr. McDaniel testifies:

> Kesanupalli is concerned with protection of user credentials (e.g., passwords and cryptographic keys) and biometric information in secure storage. For example, Kesanupalli describes that all user data is securely stored outside of the browser in a secure storage device: "The enrolled credentials of a user are encrypted with the encryption key and stored in a storage device. Such as secure storage 106.

Ex. 1036 ¶ 16.

> Kesanupalli addresses numerous security features not constrained to a social engineering purpose. Kesanupalli generally discusses providing "secure transactions," "secure application," and "secure communication," with no implication that these are "secure" *only* with respect to social engineering attacks. APPL-1006, 5:53-58, 6:15-17, 6:39-42. As one

> example, Kesanupalli discloses using secure socket layer (SSL) protocol for encrypted transmission of data including between its sensor and general processor. *See* APPL-1006, 1:28-30, 6:39-42. This addresses attacks in which the communication between process (programs) in an operating system can be compromised (addressing IPC eavesdropping attacks). Further, Kesanupalli discloses implementing strong cryptographic algorithms in its hardware and/or software which prevent compromise of data when stored (sometimes called offline or data-store attacks) or communicated between hosts and system components (eavesdropping attacks). *See* APPL-1006, 4:12-23. Further cryptographic examples include using cryptography features of secure keys and hashes of the secure key, random challenge sensor ID, and the like. *See* APPL-1006, 4:64-5:33.

Id. ¶ 17.

> As another example, Kesanupalli uses digitally signed code and runtime checks for protection against man-in-the-browser attacks and malware. This prevents adversaries from replacing or corrupting the authentication service of Kesanupalli either before or during use. APPL-1006, 8:23-28. These protections are essential in modern systems to prevent attacks against the storage and runtime of running services.

Id. ¶ 18.

We credit the above-quoted testimony of Dr. McDaniel as it is based on the disclosure of Kesanupalli when considered in its entirety. That in Kesanupalli's system, user biometrics and other credentials, such as a cryptographic key, may be sent to the browser extension in the general processor does not sufficiently undermine Dr. McDaniel's testimony. Kesanupalli does not have to be free of all vulnerabilities to be regarded as having an interest in device security. Further, Dr. McDaniel has testified that Kesanupalli "uses digitally signed code and runtime checks for protection against man-in-the-browser attacks and malware." Ex. 1036 ¶ 18 (citing Ex. 1006, 8:23–28). We credit this testimony.

Second, even assuming that Kesanupalli's only goal and interest are to thwart social engineering attacks, Patent Owner incorrectly limits the usefulness of a prior art reference to just the problem addressed, solutions proposed, and the goals achieved by the reference's disclosures. Such a reading of Kesanupalli is misplaced and inappropriate.

A prior art reference must be considered for everything it teaches by way of technology and is not limited to the particular invention it is describing and attempting to protect. *EWP Corp. v. Reliance Universal Inc.*, 755 F.2d 898, 907 (Fed. Cir. 1985). Similarly, "[t]he use of patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned. They are part of the literature of the art, relevant for all they contain." *In re Heck*, 699 F.2d 1331, 1333 (Fed. Cir. 1983) (citing *In re Lemelson*, 397 F.2d 1006, 1009 (CCPA 1968)). We have reviewed all of the cases cited by Patent Owner regarding determination of obviousness. None of them is at odds with the principle as stated in *EWP* or *Heck*.

A determination of obviousness requires "articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *Kahn*, 441 F.3d at 988. We are not aware of authority that requires the articulated reasoning with rational underpinning to be addressing the same problem as that addressed by the prior art reference whose teachings are modified on the basis of the articulated reasoning with rational underpinning. When evaluating a combination of teachings, we "determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR*, 550 U.S. at 418.

Although it does not appear that Brown's wiping feature would have provided any benefit for thwarting social engineering attacks, Petitioner has not proposed to incorporate Brown's wiping feature in Kesanupalli to thwart social engineering attacks. Instead, Petitioner explains:

> 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.

For the reason explained by Petitioner, Kesanupalli's disclosed system still would benefit from inclusion of Brown's wiping feature, i.e., reducing the risk of unauthorized or malicious access of sensitive data in case the device is lost or stolen. We see nothing wrong with Petitioner's articulated reasoning for a proper motivation to combine teachings, as it has a rational underpinning. Patent Owner does not explain why the disclosed system of Kesanupalli would not benefit in the way as explained by Petitioner, by inclusion of Brown's wiping feature.

Patent Owner's reliance on what Ramesh Kesanupalli, the individual, allegedly chose not to include in the disclosure of the Kesanupalli reference is misplaced. The obviousness question is determined from the perspective of a *hypothetical* person of ordinary skill in the art, not of any actual person who purportedly possesses ordinary skill in the art. That distinction is underscored by the fact that Ramesh Kesanupalli is a named coinventor on

the Kesanupalli reference. Patent Owner's position constitutes another attempt to limit the contents of the Kesanupalli reference to just the problems addressed, solutions proposed, and goals achieved by the Kesanupalli reference, which restriction we already determined above as incorrect.

We agree with Petitioner that "[t]he subjective decisions of Mr. Ramesh Kesanupalli, even if demonstrated unambiguously (and they are not), are not a stand-in for the legal construct of a POSITA." Reply 4.[9] In any event, the record does not establish (1) why the inventors of the Kesanupalli reference chose not to discuss wiping, and (2) what they would have decided if there is also a goal to protect sensitive data if and when the device containing the sensitive data is lost or stolen. There is no requirement that inventors describe features which are not claimed and not necessary to provide an enabling disclosure of what is claimed. We do not see the absence of a description about a wiping feature in the Kesanupalli reference as somehow undermining Petitioner's reasoning that in light of the disclosure of Brown, one of ordinary skill in the art would have wanted to include a wiping feature in Kesanupalli's disclosed system.

(4) Conclusion for Limitation [1.8]

Petitioner's assertions are amply supported by the cited evidence, and Patent Owner's arguments are misplaced and unpersuasive. We determine that the combined teachings of Kesanupalli and Brown, as proposed by Petitioner, disclose limitation [1.8].

[9] We note that there is no testimony in the record from Mr. Kesanuppalli.

c) Conclusion for Claim 1

Petitioner has set forth persuasive reasoning why one of ordinary skill in the art would have combined the teachings of Kesanupalli and Brown in the manner proposed by Petitioner to yield the subject matter of claim 1, and would have had a reasonable expectation of success in doing the same. Petitioner has shown by a preponderance of the evidence that claim 1 would have been obvious over the combination of Kesanupalli and Brown.

5. 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 proved by a preponderance of the evidence that claim 13 would have been obvious 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 proved by a preponderance of the evidence that claim 25 would have been obvious over Kesanupalli and Brown.

6. 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. Patent Owner does not present arguments for these claims separate or additional to those it presents for independent claims 1 and 13, already discussed and rejected above.[10]

---

[10] For claim 7, Petitioner presents an alternative argument premised on Patent Owner possibly arguing that "remote wiping" is "self-wiping."

We have reviewed the arguments and evidence presented by Petitioner, and determine that Petitioner has proved by a preponderance of the evidence that each of claims 2, 3, 7, 8, 12, 14, 15, 19, and 24 would have been obvious over Kesanupalli and Brown.

E. 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 secrecy thereof." Ex. 1008, code (57). The method has a two-tier backup encryption structure which allows decryption of lower-tier data only when upper-tier data has been decrypted and validated. *Id.* The lower-tier data contain encrypted electronic identity of a user and authentication information associated therewith such as private keys and corresponding certificates. *Id.* The upper-tier data contain the encrypted lower-tier data and the user's biometrics information. *Id.* Figure 2 of Cheng is reproduced below:

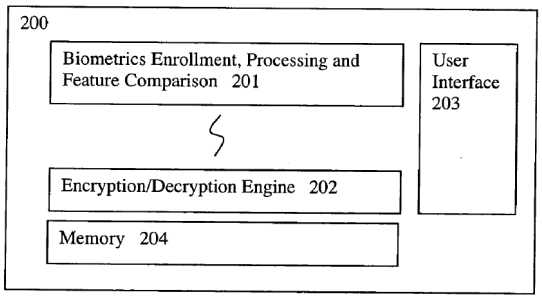


FIG. 2

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.

Figure 2 shows a sample portable biometrics-based authentication device 200 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 serv[er]. 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, are 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, already discussed and rejected in the context of claims 1 and 13.

Petitioner has proved by a preponderance of the evidence that claims 10 and 22 would have been obvious over Kesanupalli, Brown, and Cheng.

F. Alleged Obviousness of Claims 11 and 23 over Kesanupalli, Brown, and Challener

1. Overview of Challener (Exhibit 1007)

Challener 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 Challener is reproduced below:

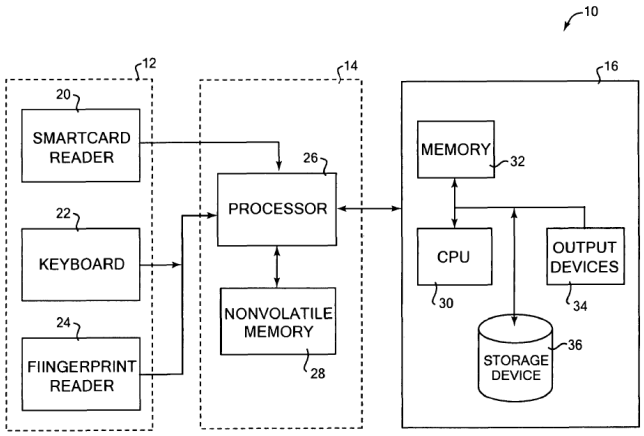


FIG. 1

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

Challener 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. Challener 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. Challener 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. Challener 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.

a) Petitioner's Assertions

Petitioner accounts for this additional limitation on pages 62–70 of the Petition, relying on the combined teachings of Kesanupalli, Brown, and Challener, including reasoning on why the teachings of Kesanupalli and Brown are properly combinable with Challener's teachings of 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 Challener with those of the combination of Kesanupalli and Brown, Petitioner asserts that "[t]he 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 Challener'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, Challener'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).

b) Patent Owner's Assertions

Patent Owner's arguments are largely in common with the arguments it presents with respect to alleged obviousness of claims 1 and 13 over the combined teachings of Kesanupalli and Brown. We first identify these arguments, which are already addressed and discussed above in the context of alleged obviousness of claims 1 and 13 over Kesanupalli and Brown.

Patent Owner argues that Petitioner's proposed combination of Kesanupalli and Challener "fails to consider that Kesanupalli's *main goal* was to thwart social engineering attacks," and that Challener's teachings about using a TPM restricted interface "would not further Kesanupalli's goals." PO Resp. 15 (emphasis added). Patent Owner also argues that "Kesanupalli is only concerned with social engineering and not breaches to the actual device," noting that the user's biometrics and cryptographic key are provided to the browser extension in the general processor. *Id.* at 27, 29–30.

According to Patent Owner, we must consider what Ramesh Kesanupalli, a coinventor of the Kesanupalli reference and purportedly a person of ordinary skill in the art, actually did, i.e., not describing using a TPM restricted interface in the disclosure of the Kesanupalli reference. PO Resp. 15–16. Also according to Patent Owner, Mr. Kesanupalli's decision not to include a TPM restricted interface reflects "common sense and real world indicators" which must not be ignored. *Id.* at 17. Patent Owner asserts that Kesanupalli's focus on preventing social engineering attacks would not be furthered by adding a TPM restricted interface, and that the

concerns of the Kesanupalli reference are not addressed by adding a TPM restricted interface. *Id.*

Patent Owner explains that Kesanupalli's disclosure is directed to curbing social engineering attacks such as phishing and spoofed websites, and that the goal of curbing social engineering attacks would not have benefitted from inclusion of a TPM restricted interface. PO Resp. 18. Patent Owner's expert, Dr. Goodrich, testifies that social engineering attacks rely on tricking the user to release credentials. Ex. 2037 ¶ 50 (cited at PO Resp. 18). Patent Owner further explains:

> Tricking the user to release their credentials is typically done through email or text messages containing a link to a fake website that looks legitimate to convince the victim to enter their sensitive information. Ex. 2037 (Goodrich Decl.) at ¶¶50-53. For example, someone could trick a user by pretending to [be] Netflix and telling the user that they must log in and provide updated payment details to get their account off hold. If the user selects the update account button, they will be redirected to a spoofed version of Netflix where the bad actor will collect the user's credentials.

PO Resp. 18–19. Patent Owner asserts that "[t]he integration of a TPM would not have helped avoid social engineering attacks." *Id.* at 21 (citing Ex. 2037 ¶ 64).

Dr. Goodrich testifies: "Adding a TPM [restricted interface] to the Kesanupalli reference would not aid in reducing such social engineering attacks because these social engineering attacks trick a user into providing their credentials to illegitimate sources or use prevalent techniques to breach common passwords." Ex. 2037 ¶ 59. Dr. Goodrich also testifies:

Patent Owner asserts that social engineering attacks do not require a device to be breached, and argues that there is no reason for one of ordinary skill in the art to combine Challener's TPM restricted interface with

Kesanupalli's social engineering protections. PO Resp. 26–27. Further, Patent Owner notes that one actual person of ordinary skill in the art, Ramesh Kesanupalli, made a conscious decision to not use a TPM restricted interface in the disclosed system of Kesanupalli because it "would have no impact on curbing social engineering attacks." *Id.* at 31 (citing Ex. 2037 ¶ 64). Patent Owner asserts: "Kesanupalli decided to confront social engineering attacks with his system and a POSITA given the disclosures of the reference would not have been motivated to add [TPM restricted interface] as it would not have added any additional benefit to the user." *Id.* (citing Ex. 2037 ¶ 64).

Patent Owner additionally presents two arguments which are not in common with the arguments it presents in the context of the combined teachings of Kesanupalli and Brown. First, Patent Owner argues that "utilizing a TPM would have introduced compatibility issues with existing systems and software that did not support TPMs." PO Resp. 32 (citing Ex. 2037 ¶ 66). Patent Owner states: "The Windows Biometric Framework did not require or even mention a TPM. *See generally* Ex. 2050; Ex. 2037 (Goodrich Decl.) at ¶67. This is likely because TPMs were not required by Windows in 2012 and TPMs were disabled by default. Ex. 2027 (Goodrich Decl.) at ¶67; *see* Section II.C, *supra*." *Id.* Patent Owner further argues:

> Second, since the TPM's were not turned on by default, utilizing TPMs would have required end users to make firmware changes to even enable the TPM to work. A POSITA (like Mr. Kesanupalli) aiming to address the risk of social engineering (which again would not have benefitted from a TPM) would not have wanted to further deter users from using the patented system by requiring them to set up and configure a TPM. Ex. 2037 (Goodrich Decl.) at ¶67.

Id.

An additional argument, not made in the Patent Owner Response, is present in paragraph 64 of Dr. Goodrich's declaration (Ex. 2037). Dr. Goodrich states: "Because the Kesanupalli reference's system securely provides sensitive information to the application processor executing the biometric browser extension and to web servers receiving credentials, adding a TPM to the Kesanupalli reference's system would not result in security benefits." Ex. 2037 ¶ 64.

c) Discussion

With respect to Patent Owner's arguments common with those Patent Owner makes in the context of the combination of Kesanupalli and Brown, we already addressed and rejected them above in Section II.D.4.b. These arguments are equally unavailing here for essentially the same reasons explained above and need not be discussed again.

Arguments not made in the Patent Owner Response, even if contained in the expert declaration in support of the Patent Owner Response, are not entitled to consideration. Thus, the argument in Dr. Goodrich's declaration that adding a TPM to the Kesanupalli reference's system would not result in security benefits is not entitled to consideration.

In any event, even if considered, the argument is misplaced. Petitioner has not argued that adding Challener's TPM restricted interface provides security improvements to Kesanupalli. Rather, it is Petitioner's position that a "POSITA would have been motivated to apply Challener'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." Pet. 65. In other words, Petitioner applies Challener

teachings to implement Kesanupalli's disclosed system, not necessarily to improve on it.

Furthermore, Dr. McDaniel identifies and discusses additional security benefits to be achieved by including Challener's TPM restricted interface in Kesanupalli's system:

> **First**, the augmentation of Kesanupalli with a TPM follows the best practices of "defense in depth." Defense in depth is a security strategy that uses multiple independent layers of security apparatus to protect systems or programs at risk. This approach ensures that if one layer is breached, additional layers remain to counteract the threat, creating a more resilient overall defense. By multiple techniques, defense in depth minimizes vulnerabilities and increases the difficulty for attackers to compromise sensitive assets. This layers strategy acknowledges the complexity of modern threats, which are multifaceted themselves and the need for a multifaceted response to secure systems comprehensively.
>
> Adding Trusted Platform Modules (TPMs) to security-sensitive services like authentication strengthens the system against several classes of attacks. For example (and to name only a few), TPMs prevent keylogging attacks by securely generating and storing cryptographic keys within the hardware, making them inaccessible to malware. They also mitigate man-in-the-middle (MITM) attacks by enabling secure, hardware-based authentication protocols that verify both the user and the system. Additionally, TPMs resist offline attacks, such as brute force attempts to guess credentials, by requiring physical access to the device for key operations. By anchoring security in hardware, TPMs create a robust barrier that complements other security mechanisms.

Ex. 1036 ¶¶ 32–33 (footnote omitted).

We credit the above-quoted testimony of Dr. McDaniel. Patent Owner's argument against adding a TPM to Kesanupalli is unavailing.

We have considered Patent Owner's argument that "utilizing a TPM would have introduced compatibility issues with existing systems and software that did not support TPMs" (PO Resp. 32). We find it misplaced and without persuasion. Previous adoption in some commercial products of TPM is not a requirement for establishing obviousness of using TPMs, much less universal previous adoption of TPM in all commercial products. Dr. Goodrich, Patent Owner's expert, acknowledges that many prior systems had provided for use of TPMs but just optionally, not required or by default. Ex. 2037 ¶ 67. These facts support, not mitigate against, that one of ordinary skill in the art would have been motivated to incorporate Challener's TPM teachings in Kesanupalli's system.

We also have considered Patent Owner's argument that because preexisting systems provided TPM not by default but by user activation, one of ordinary skill in the art who is "aiming to address the risk of social engineering" would not have wanted to further deter users by requiring them to set up and configure a TPM. PO Resp. 32. This argument is unavailing for numerous reasons. First, as we have explained above, one of ordinary skill in the art is a hypothetical person who reads Kesanupalli for all of its technical disclosures and is not limited solely to the problems addressed, solutions provided, and the express goals of Kesanupalli. Second, as we also explained above, Kesanupalli is not solely interested in defending against social engineering attacks but is also concerned with device security. Third, Petitioner has not proposed to add TPM to Kesanupalli only as an optional feature that requires user activation via some complicated procedure. Fourth, even if user activation is required to configure TPM for use, that inconvenience does not sufficiently undermine Petitioner's articulated

reasons for incorporating into the disclosed system of Kesanupalli the teachings of Challener regarding the use of a TPM. "[A] given course of action often has simultaneous advantages and disadvantages, and this does not necessarily obviate motivation to combine." *Medichem, S.A. v. Rolabo, S.L.*, 437 F.3d 1157, 1165 (Fed. Cir. 2006).

d) Conclusion for Claims 11 and 23

For the foregoing reasons, Petitioner has proved by a preponderance of the evidence that claims 11 and 23 would have been obvious over Kesanupalli, Brown, and Challener.

G. Alleged Obviousness of Claims 5 and 7 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 a reasonable expectation of success, Petitioner asserts:

> POSITA would have had reasonable expectations 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, already discussed and rejected above in the context of claims 1 and 13.

Petitioner has proved by a preponderance of the evidence that claims 5 and 17 would have been obvious over Kesanupalli, Brown, and Headley.

III. CONCLUSION[11]

Petitioner has proved, by a preponderance of the evidence, that the subject matter of claims 1–3, 7, 8, 12–15, 19, 24, and 25 of the ’138 patent would have been obvious over Kesanupalli and Brown.

Petitioner has proved, by a preponderance of the evidence, that the subject matter of claims 10 and 22 of the ’138 patent would have been obvious over Kesanupalli, Brown, and Cheng.

Petitioner has proved, by a preponderance of the evidence, that the subject matter of claims 11 and 23 of the ’138 patent would have been obvious over Kesanupalli, Brown, and Challener.

Petitioner has proved, by a preponderance of the evidence, that the subject matter of claims 5 and 17 of the ’138 patent would have been obvious over Kesanupalli, Brown, and Headley.

---

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

In summary:

Claim(s)	35 U.S.C. §	Reference(s)/Basis	Claim(s) Shown Unpatentable	Claim(s) Not shown Unpatentable
1–3, 7, 8, 12–15, 19, 24, 25	103(a)	Kesanupalli, Brown	1–3, 7, 8, 12–15, 19, 24, 25	
10, 22	103(a)	Kesanupalli, Brown, Cheng	10, 22	
11, 23	103(a)	Kesanupalli, Brown, Challener	11, 23	
5, 17	103(a)	Kesanupalli, Brown, Headley	5, 17	
Overall Outcome			1–3, 5, 7, 8, 10–15, 17, 19, 22–25	

IV. ORDER

Accordingly, it is

ORDERED that claims 1–3, 5, 7, 8, 10–15, 17, 19, and 22–25 of the ’138 patent are unpatentable; and

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

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