

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner

v.

CARBYNE BIOMETRICS, LLC,

Patent Owner

IPR2024-00334

U.S. Patent No. 11,514,138

**PETITIONER'S REPLY TO
PATENT OWNER'S RESPONSE**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	LEVEL OF ORDINARY SKILL IN THE ART.....	1
III.	GROUND 1: KESANUPALLI AND BROWN RENDER THE CHALLENGED CLAIMS OBVIOUS.....	2
A.	PO misapplies the framework of obviousness analysis with respect to a POSITA.	3
B.	PO mischaracterizes Kesanupalli’s goals.....	6
C.	PO misapplies the obviousness framework with respect to combining prior art teachings.....	11
D.	PO disregards the record illustrating the motivation to combine Kesanupalli and Brown for Ground 1	13
IV.	GROUND 3: KESANUPALLI, BROWN AND CHALLENGER RENDER THE CHALLENGED CLAIMS OBVIOUS.	14
A.	PO relies upon arguments for Ground 1 that are unpersuasive	14
B.	Kesanupalli is ready for improvement based on Challenger’s restricted interface	15
C.	Tradeoffs or adoption of TPM do not preclude Challenger’s combination with Kesanupalli.....	18
V.	GROUPS 2, 4, 5	20
VI.	CONCLUSION.....	21
	CERTIFICATE OF WORD COUNT	23
	CERTIFICATE OF SERVICE	24

PETITIONER'S EXHIBIT LIST

Updated: January 16, 2026

APPL-1001	U.S. Patent No. 11,514,138 (“the ’138 patent”)
APPL-1002	Prosecution History of the ’138 patent
APPL-1003	Declaration of Dr. Patrick McDaniel
APPL-1004	<i>Curriculum Vitae</i> of Dr. Patrick McDaniel
APPL-1005	Reserved
APPL-1006	U.S. Patent No. 8,799,666 (“Kesanupalli”)
APPL-1007	U.S. Patent No. 8,099,789 (“Challener”)
APPL-1008	U.S. Patent Publication No. 2004/0117636 (“Cheng”)
APPL-1009	U.S. Patent No. 9,652,629 (“Brown”)
APPL-1010	U.S. Patent No. 8,185,646 (“Headley”)
APPL-1011	Reserved
APPL-1012	Patrick McDaniel, <i>Authentication</i> , Handbook of Computer Networks, Volume 3, Part 2, pp. 570-580, John Wiley and Sons, 2008. Ed. Hossein Bidgoli
APPL-1013	IBM Introducing Fingerprint Reader Into Laptop. Jack Germain. 2004 at https://www.technewsworld.com/story/ibm-introducing-fingerprint-reader-into-laptop-37017.html (retrieved Dec. 12, 2023)
APPL-1014	U.S. Patent Publication 2008/0059804 to Shah et al.
APPL-1015	Kerberos: An Authentication Service for Computer Networks. B. Clifford Neuman et al. 1994 at https://gost.isi.edu/publications/kerberos-neuman-tso.html (retrieved Dec. 12, 2023)
APPL-1016	ISO/IEC 11889-1:2009 Information technology Trusted Platform Module Part 1: Overview at https://www.iso.org/standard/50970.html (retrieved Dec. 12, 2023)
APPL-1017	TPM Main Part 3 Commands Specification Version 1.2 1 March 2011 at https://trustedcomputinggroup.org/wp-content/uploads/TPM-Main-Part-3-

	<u>Commands_v1.2_rev116_01032011.pdf</u> (retrieved Dec. 12, 2023)
APPL-1018	Introduction to Programmable Systems on a Chip, Bob Zeidman, 07.27.2005 at <u>https://www.eetimes.com/introduction-to-programmable-systems-on-a-chip/</u> (retrieved Dec. 12, 2023)
APPL-1019	Computer Dictionary, Second Edition, entry “data record” (1994)
APPL-1020	How to Restore Your Data After a Hard Drive Crash, Glenn Derene, Aug 4, 2011 at <u>https://www.popularmechanics.com/technology/gadgets/how-to/a6819/how-to-restore-your-data-after-a-hard-drive-crash/</u> (retrieved Dec. 12, 2023)
APPL-1021	Reserved
APPL-1022	U.S. Patent Application No. 2008/0104416 to Challenger et al. (“Challenger’s PG-PUB”)
APPL-1023	RFC2818, HTTP Over TLS (May 2000)
APPL-1024	Trusted Computing Group, <i>Enterprise Security: Putting the TPM to Work</i> , 2008 at <u>https://trustedcomputinggroup.org/wp-content/uploads/TPM-Applications-Whitepaper.pdf</u> (retrieved Jan. 2, 2024)
APPL-1025	Director Memorandum, Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (June 21, 2022)
APPL-1026	Preliminary Constructions, <i>Carbyne Biometrics v. Apple, Inc.</i> , 1:23-cv-00324 (December 11, 2023)
APPL-1027	United States District Courts—National Judicial Caseload Profile (September 30, 2023), <u>https://www.uscourts.gov/statistics/table/na/federal-court-management-statistics/2023/09/30</u> (retrieved Dec. 14, 2023)
APPL-1028	Scheduling Order, <i>Carbyne Biometrics, LLC v. Apple Inc.</i> , WDTX-1:23-cv-00324 (July 14, 2023)

APPL-1029	Plaintiff Carbyne Biometrics, LLC's Preliminary Infringement Contentions, <i>Carbyne Biometrics v. Apple, Inc.</i> , 1:23-cv-00324 (June 21, 2023)
APPL-1030	Sotera Stipulation dated April 17, 2024
(New) APPL-1031	Deposition transcript of Dr. Michael Goodrich (January 8, 2025)
(New) APPL-1032	<i>Introduction to Computer Security</i> , Michael T. Goodrich and Roberto Tamassia, Table of Contents, 2011
(New) APPL-1033	Techradar, Lenovo ThinkPad T60p review, Tech staff, May 4, 2008 (https://www.techradar.com/reviews/pc-mac/laptops-portable-pcs/laptops-and-netbooks/lenovo-thinkpad-t60p-305039/review), retrieved January 16, 2025 from archive.org, October 8, 2009 capture
(New) APPL-1034	Laptop Mag, Lenovo ThinkPad R500 Review, Jamie Bsales, August 20, 2008 (https://www.laptopmag.com/reviews/laptops/lenovo-thinkpad-r500), retrieved January 8, 2025
(New) APPL-1035	Intel Integrated TPM (Trusted Platform Module) for Windows XP (SP2) - ThinkPad R400, R500, T400, T400s, T500, W500, W700, W700ds, X2[], X200a, X200 Tablet, X301 (https://pcsupport.lenovo.com/us/en/downloads/ds001667), retrieved January 8, 2025
(New) APPL-1036	Supplemental Declaration of Dr. Patrick McDaniel ("McDaniel Suppl. Decl.")

I. INTRODUCTION

Carbyne Biometrics (“PO”), in its Patent Owner’s Response (“POR”), cannot dispute that the claims are rendered obvious by the prior art. So, to avoid a clear finding of unpatentability, PO attempts to limit the motivation of a person of ordinary skill in the art (“POSITA”) and the prior art references themselves to a narrow purpose that misapplies fact and the law. The Board should disregard these arguments and find the challenged claims unpatentable as shown in this Petitioner Reply and the accompanying declaratory evidence from Dr. McDaniel. APPL-1036, ¶¶1-9.

II. LEVEL OF ORDINARY SKILL IN THE ART

In the Institution Decision, the Board adopted Petitioner’s POSITA standard “except for the language ‘at least’ that qualifies the experience level and allows the experience level to encompass an expert’s level of skill.” Paper 10, p. 11. Petitioner applies the standard as clarified by the Board. The analysis of the Petition remains the same, applying this clarified level of skill for a POSITA. APPL-1036, ¶9 (Dr. McDaniel explaining that his analysis in the original declaration APPL-1003 remains the same).

III. GROUND 1: KESANUPALLI AND BROWN RENDER THE CHALLENGED CLAIMS OBVIOUS.

Claims 1-3, 7-8, 12-15, 19 and 24-25 are rendered obvious by Kesanupalli in view of Brown. In particular, Ground 1 shows that Brown's teachings of facilitating wiping of sensitive data from storage applied to Kesanupalli's device renders obvious the claims. As the Petition explained, "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. 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." Petition, p. 15; *see also* Petition, pp. 16-20.

PO presents arguments regarding a supposed lack of motivation to combine teachings of the Brown and Kesanupalli references; these arguments fail because they rely on irrelevant speculation as to the decisions of one person—Mr. Ramesh Kesanupalli—regarding what to include in a patent disclosure and ignore the motivation to combine offered in the Petition by focusing on a legally irrelevant mischaracterization that Kesanupalli's "concerns" were limited to a social engineering problem.

A. PO misapplies the framework of obviousness analysis with respect to a POSITA.

The Petition and accompanying declaratory evidence provided by Dr. McDaniel (APPL-1003) set forth the requisite factors for obviousness including the level of a POSITA and the reasons why a POSITA, at the time of the invention, would have been motivated to combine Brown's teaching of a wiping technique with Kesanupalli's device/method providing authentication using biometric information.¹ The Board agreed that the Petition's reasons for the combination were "rational and supported by the cited evidence." Paper 10, p. 37. PO does not rebut the legal or technological sufficiency of this evidence. Rather, PO conjures reasons that Mr. Ramesh Kesanupalli²—the individual—did not include "wiping" (and a trusted platform module (TPM)) within the text of Kesanupalli—the patent—and argues

¹ Tellingly, despite Ground 1 being based on a combination of Brown's wiping technique, PO's arguments rest nearly exclusively on the bodily incorporation of a trusted platform module (TPM), related to Challener's *restricted interface* teachings, which are relevant to Ground 3.

² Mr. Ramesh Kesanupalli is listed as one of five inventors of the Kesanupalli patent. APPL-1006, (75).

that its conjured reasoning is determinative of non-obviousness. PO's reasoning is neither factually supported, nor legally relevant.

First, (pre-AIA) 35 U.S.C. §103(c) provides the statutory framework by which obviousness is to be determined and makes clear that obviousness is an inquiry from the perspective of a POSITA. A POSITA is an imaginary person(s), a hypothetical legal construct. The 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.

Second, PO's argument invites the Board to eviscerate the obviousness doctrine. PO attempts to disguise its over-reach by presenting its argument as "a unique opportunity" involving "unique facts." *See* POR, pp. 16-17. This is a mischaracterization. There is nothing "unique" about a patentability challenge involving "review [of] a reference from a contemporary POSITA." *See* POR, p. 16. Technical papers and patents are commonly, if not prevalently, attributed to authors or inventors having credentials that meet or exceed those of a POSITA. Should patentability be concluded based on what that author or inventor subjectively chose to include within his article or patent, only anticipatory challenges to patentability would remain. Statutory law and case law demand that is incorrect. "[I]n many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 420 (2007).

Third, *why* Mr. Ramesh Kesanupalli or the other named inventors chose not to include a discussion of wiping (or of TPM) within their patent application is unknown. PO's assertions are simply unsupported conjecture.³ There may be any number of reasons that wiping, or a TPM, or numerous other well-known features of information security and security arrangements for protecting computers or other electronic devices are not expressly called out in the text of Kesanupalli.⁴ Not the least of these reasons is that Kesanupalli stems from a U.S. Patent application (Appl. 12/731,505). An inventor has reason and motivation to ensure that his patent application meets the enablement and written description requirements of U.S. patent law with respect to his claimed invention. There is no reason, no necessity, and no expectation that a patent survey all available related features or describe further combinations beyond the invention claimed therein.

³ Despite PO's expert Dr. Goodrich's declaratory statements as to the motivation and choices of Mr. Ramesh Kesanupalli, his deposition shows he does not personally know Mr. Ramesh Kesanupalli (nor Inventor David Challener) or speak to anyone outside of counsel to form these declaratory statements. APPL-1031, pp. 7, 68-69 discussing inventors Kesanupalli and Challener.

⁴ See APPL-1036, ¶¶10-13 discussing reasons why a standards-based TPM may not be detailed.

The Board need not make “assumptions” (*see* POR, p. 16) as to what a POSITA would have done; the Petition and accompanying declaration testimony of Dr. McDaniel (APPL-1003) provided reasoned analysis and evidentiary support showing that a POSITA would have had reason and motivation to combine Brown's wiping technique (and Challenger's restricted interface in Ground 3) to Kesanupalli's device with a reasonable expectation of success.

B. PO mischaracterizes Kesanupalli's goals

As the Petition explained, “Kesanupalli...is directed to a secure authentication *system* that uses biometric information to ‘provide[] a more secure authentication of the user than commonly used password-based methods and systems.’” Petition, p. 11 citing APPL-1006, (54), 1:59-62, APPL-1003, ¶¶65-70 (emphasis added). To protect the user's sensitive information, “[t]he fingerprint template and user credentials are then stored in a secure storage of the user's device.” Petition, pp. 11-12 citing APPL-1006, 3:46-47, 5:61-6:49, 8:29-53; Petition, p. 13 citing APPL-1006, Fig. 2 (“secure storage”).

In contrast, PO argues that Kesanupalli—the patent—is concerned *only* with a problem of social engineering attacks and posits that because Brown's wiping technique (or a TPM as to Ground 3) is not narrowly targeted to that same problem,

the combination fails.⁵ First, this is a mischaracterization of Kesanupalli, and second, as discussed in Section III.C, this is not the proper framework in which to determine obviousness of USP 11,514,138 (“the ’138 patent”) claims.

Kesanupalli's teachings are not constrained to *only* mitigating social engineering attacks. Kesanupalli begins by recognizing that typical authentication systems use passwords, which are at risk for attacks “including ‘phishing attacks’ and ‘social engineering attacks.’” POR, p. 4 citing APPL-1006, 1:27-37. However, these risks—phishing and social engineering attacks—to which PO attempts to constrain all of Kesanupalli's teachings appear in only in one sentence of its

⁵ PO's distinction between an attacker's *initial* strategy in exploiting a security risk—tricking human users in a social engineering attack and breaching the actual device—is untenable as these attacks are often interrelated. Social engineering attacks are often used as a precursor other exploits or intrusions of the targeted device or its resources, services or data (e.g., to deploy malware). APPL-1036, ¶21. This is one reason why a POSITA does not approach information security and security arrangements with a goal of mitigating only one type of attack and why Kesanupalli addresses device security features in implementing its authentication techniques. APPL-1036, ¶¶22, 32 (explaining CIA and defense in depth and citing APPL-1032).

background discussion of use of passwords as a means for authentication. And even there, consideration of the entirety of the cited sentence shows that Kesanupalli's teachings are not so limited: "Although passwords are commonly used to authenticate users, **passwords** are subject to **various attacks, such as** phishing attacks, social engineering attacks, dictionary attacks and the like." APPL-1006, 1:35-38 (emphasis added); POR, p. 4.⁶ There is no requirement (explicit or implicit) in Kesanupalli that its authentication systems and methods only address social engineering attacks. APPL-1036, ¶¶10-23 (discussing a POSITA's understanding of Kesanupalli and Kesanupalli's broad-based security teachings). Rather, Kesanupalli's specification broadly discusses authentication systems and methods without constraining their purpose and claims these systems and methods without such a limitation. *See* APPL-1006, 10:47-54, 11:5-38. Kesanupalli discloses numerous security features not driven solely by a concern for social engineering attacks. APPL-1036, ¶¶14-23 (Dr. McDaniel describing Kesanupalli's use of

⁶ Notably, the explicitly mentioned "dictionary attacks," omitted by the POR's quotation and are not social engineering attacks that trick a user, but a different security risk mitigated by strong passwords. APPL-1031, p. 26 ("Q: So does dictionary attacks trick people as social engineering did? A: No, not usually..."). *See also*, APPL-1036, ¶19.

cryptographically secured communications, secure storage, digitally-signed code, etc.).

While Kesanupalli facilitates the use of secure, complex passwords by freeing a user from the difficult task of remembering those complex passwords—or worse remembering and typing a complex and unique password for each site and only for the right site, it does so by storing a copy of the passwords (or other credentials) and biometric information (which, unlike passwords, cannot be easily changed). In doing so, Kesanupalli mitigates one set of risks—weak passwords. But another risk comes to the fore—breach of the device with the password biometric information store(s). *See* APPL-1036, ¶15.

This is one reason Kesanupalli describes numerous specific security features that are not 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, 4:64-5:33.⁷ 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, 6:39-42.⁸ 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.

⁷ *See also*, APPL-1031, pp. 40-42 discussing cryptographic hash functions are for “confidentiality” (one facet of security), use of digital signatures (keys) are for another facet (“integrity”), which confirms the discussion of APPL-1003, ¶¶45-47 describing cryptography, including encryption and hash functions, being “for a goal of protecting confidentiality and/or integrity (protecting against corruption) of data.”

⁸ *See also*, APPL-1036, ¶18 discussing Kesanupalli's security feature of digitally signing and checking credentials and biometric component and citing APPL-1006, APPL-1006, 8:23-28.

C. PO misapplies the obviousness framework with respect to combining prior art teachings

PO argues extensively against the combination of Kesanupalli with Brown (or with Challener as to Ground 3) on the theory that Brown and Challener, and their respective *wiping* and *restricted interface* techniques, are not improvements that address social engineering attacks. PO provides no indication as to how this, even if true (which it is not as discussed above in Section I.B), would save its claims from being unpatentable.

First, the Petition shows Kesanupalli, Brown, and Challener are all analogous art to the '138 patent as they are in the same field of endeavor. Petition, pp. 16-17, 64-65. PO does not dispute this. Further, when more than one prior art reference is used as the basis of an obviousness rejection, it is not required that the references be analogous art to each other, much less share a common singular problem. *See Sanofi-Aventis Deutschland GmbH v. Mylan Pharms. Inc.*, 66 F.4th 1373, 1380 (Fed. Cir. 2023) and *Corephotonics, Ltd. v. Apple Inc.*, 84 F.4th 990, 1007, (Fed. Cir. 2023).

Second, Kesanupalli's teachings are neither limited to the problem of social engineering attacks as discussed above, nor would any recognition of a particular problem by Kesanupalli constrain the obviousness inquiry to solving just that particular problem. Rather, the inquiry is from the perspective of a POSITA with all his relevant knowledge as "a person of ordinary creativity, not an automaton." *KSR*, 550 U.S. at 421 (discussing exemplary motivations). PO's attempt to confine an

obviousness inquiry to a particular problem has been squarely rejected by the Supreme Court. *KSR*, 550 U.S. at 404.

Third, social engineering attacks are but one type of security threat related to the information security and access controls that are used to protect computers or other electronic devices. They do not exist in a vacuum. A POSITA would have recognized that social engineering is often an attack vector for intrusions that seek sensitive personal information such as passwords and security keys. APPL-1036, ¶22. Moreover, a POSITA would have readily recognized that addressing system vulnerabilities cannot be constrained to just one type, or stage, of attack and still provide a secure system. *See* APPL-1036, ¶¶10-13, 21-23, 32 (discussing a POSITA's approach to security enhancements, CIA framework, multiple and multifaceted security threats, defense in depth); APPL-1031, pp. 37-38 (discussing "the concept of computer security is wrapped up into a number of other sub-concepts" including "confidentiality, integrity, and availability" and "assurance, authenticity, and anonymity"), pp. 13-14, 71-72 (where Dr. Goodrich also identifies framework of security in his textbook taught to early undergraduate students); APPL-1032 (Table of Contents of Dr. Goodrich's book illustrating the same sub-concepts). This is exactly the sort of flexible analysis required under *KSR*. *KSR*, 550 U.S. at 424 ("The proper question to have asked was whether a [person] of ordinary skill, facing the wide range of needs created by developments in the field of

endeavor, would have seen a benefit to upgrading [the primary reference] with a [particular feature].”)

PO's attempt to limit a POSITA's perspective to only one type of attack is specious on its face. It is akin to arguing that daily transport of cash to the bank by armored car after verifying the identity of the driver would preclude any motivation to use a safe on premise or that anti-lock brakes obviate and render non-obvious the use of seatbelts and airbags.

D. PO disregards the record illustrating the motivation to combine Kesanupalli and Brown for Ground 1

The Petition provided a reasoned analysis with accompanying evidence showing that a POSITA would have readily understood that a personal electronic device such as Kesanupalli's may be lost, damaged or otherwise require replacement, and had reason to combine Brown's technique for wiping data to prevent unauthorized use in those situations. *See* Petition, pp. 17-18; APPL-1003, ¶¶79-80. Brown itself teaches that “there are instances when the device may be compromised, decommissioned, or redeployed, making it desirable to delete or ‘wipe’ data.” Petition, p. 18 citing APPL-1009, 2:6-15. PO did not dispute this.

PO argues that one would not combine Brown with Kesanupalli as “[o]nce 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.” POR, p. 23. As discussed above, constraining the inquiry to the social engineering attacker is

factually and legally incorrect. Security threats are multiple and multifaceted. APPL-1036, ¶¶21-23, 32. Wiping is directed to security threats to a device and device data no longer under the user's control irrespective of previous attacks on access to that data, or portions of that data. The benefits of wiping are shown by Brown itself and by Dr. McDaniel's reasoning and evidence supporting the benefits of combining Brown's wiping technique with Kesanupalli. APPL-1036, ¶23; Petition, pp. 16-43 discussing Brown, APPL-1003, ¶80 citing APPL-1008 (Cheng), APPL-1009 (Brown).

IV. GROUND 3: KESANUPALLI, BROWN AND CHALLENGER RENDER THE CHALLENGED CLAIMS OBVIOUS.

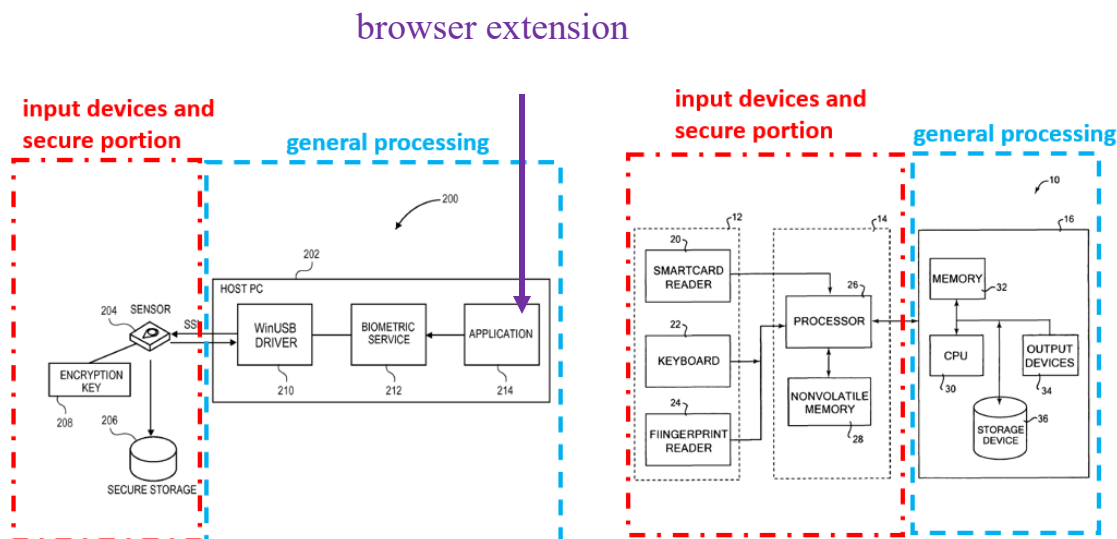
Ground 3 of the Petition demonstrated that dependent claims 11 and 23 of the '138 patent are rendered obvious by Kesanupalli and Brown combined with the teachings of a *restricted interface* of Challenger. Petition, pp. 62-70.

A. PO relies upon arguments for Ground 1 that are unpersuasive

PO argues that a POSITA would not combine Challenger's restricted interface teachings with Kesanupalli-Brown because Mr. Ramesh Kesanupalli did not disclose a TPM in his patent and a TPM does not itself mitigate social engineering attacks. *See* APPL-1013, ¶¶10-23. These arguments are factually unsupported and legally unpersuasive as discussed above in Sections III.A – III.C.

B. Kesanupalli is ready for improvement based on Challenger's restricted interface

The Petition, with reasoned analysis supported by evidence, showed that a POSITA would have been motivated to apply Challenger's teachings of a TPM-type security architecture (with API-mediated interfaces to secure functions and data) in implementations of Kesanupalli's authentication techniques (with Brown's wiping). Petition, pp. 62-70 citing APPL-1003, ¶¶198-212. In particular, the security functions of Kesanupalli's sensor 204 are beneficially implemented using Challenger's specialized security processing circuitry such as illustrated by Challenger's security processor (26) and its restricted interfaces (including to its storage (28) and general processing (16)). This is because a standards-based TPM architecture would provide support for many underlying cryptographic security services and secure storage facilities and because using standards-based TPM architecture would have engendered trust among users and customers. Petition, pp. 65-66 citing APPL-1003, ¶¶200-202, APPL-1007, 1:18-31 (summarizing typical TPM functions and APIs). That is, it would have been obvious to implement the functions of the red-delineated portion of Kesanupalli using the processing, interfaces and storage elements of the red-delineated portion of Challenger's TPM-based architecture, which includes Challenger's API-mediated connections such as between the security processor and its storage, *i.e.*, a *restricted interface*. See also, APPL-1036, ¶¶24-36 discussing Challenger's TPM-based architecture.



**Kesanupalli, FIG. 2 and Challener, FIG. 1
annotated and juxtaposed; APPL-1036, ¶35; see also, Petition, pp. 65-
66 citing APPL-1003, ¶201**

PO again applies flawed logic to suggest that Kesanupalli was not concerned with device security, but its arguments are legally flawed for the same reasons discussed above, and factually unsupported by the record. In particular, PO and its expert Dr. Goodrich each argue that Kesanupalli's architecture allows sensitive data in the form of biometric information and credentials to be handled by a browser extension (purple above), which is executing on Kesanupalli's general processor (*i.e.*, the blue-delineated portion above). *See* POR, p. 28; Ex. 2037, ¶61 (biometrics) POR, p. 30; Ex. 2037, ¶62 (credential). According to the POR, "[i]f the device was breached by a bad actor, this process [of Kesanupalli providing sensitive data in the

browser extension] would make the credentials available to the bad actor.” POR, p. 30; *see also*, POR, p. 28 discussing the bad actor of malware. The POR argues this security risk of its browser extension means Kesanupalli is concerned *only* with social engineering attacks, not attacks that breach the device. POR, pp. 27-30. This is flawed logic as Kesanupalli is, in fact, concerned with malware risk and digitally signs its browser extensions to mitigate this risk. APPL-1036, ¶¶18, 30-31. Moreover, as discussed above, neither Kesanupalli itself, nor a POSITA's motivations, nor the framework of an obviousness analysis are so limited as to consider attacks from only one style of attacker or vector. Further, a POSITA would recognize that an architecture with security risks invites combining additional security features.⁹ APPL-1036, ¶¶22-23, 32. Challenger's security architecture

⁹ The PO's theory of unmitigated risk is also unsupported attorney argument directly contradicted by PO's expert Dr. Goodrich. *See* Ex. 2037, ¶¶64, 61 (“Kesanupalli reference's system securely provides sensitive information to the application processor executing the biometric browser extension” that is “digitally signed and validated at runtime...so malware cannot compromise credential information.”) Security features of Kesanupalli's browser extension are directed to a different portion of the architecture than Challenger's teachings. APPL-1036, ¶¶29-36 (Dr. McDaniel explaining TPM is complementary with Kesanupalli's security features).

provide benefits to overall security by securing data and cryptographic services that underly the functionality performed by Kesanupalli.

C. Tradeoffs or adoption of TPM do not preclude Challenger's combination with Kesanupalli

PO agrees that TPMs were “well known” and covered by published, international industry standards years before the '138 patent. POR, pp. 10-11.¹⁰ PO however incorrectly argues that combining teachings related to TPMs would have been non-obvious because TPMs were not **required** in commercial products or “turned on **by default**.” POR, p. 32. Market adoption rate is not a factor of obviousness. There were certainly commercial products that implemented TPMs prior to the earliest effective filing date of the '138 patent (December 2011). APPL-1036, ¶¶24-28 (citing APPL-1033, Lenovo ThinkPad T60p review *circa* 2008, describing “biometric fingerprint scanner...linked to a Trusted Platform Module (TPM) chip.”; APPL-1034, APPL-1035).

And such security features are entirely consistent with a multi-faceted security approach.

¹⁰ Ex. 2051 is a 2009 standard for TPMs by International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

To the extent that PO alleges “compatibility issues” (*see* POR, p. 32) with respect to use of a TPM, the allegations are not supported by any reasoned compatibility analysis, rather they devolve to a slow market adoption argument discussed above. APPL-1036, ¶¶30-36 (Dr. McDaniel further explains TPM’s compatibility and strengthening of Kesanupalli and disagrees with supposed compatibility issues). That TPMs were covered by an adopted industry standard well before the ’138 patent effective filing date and, according to the PO itself, would be “required” shortly thereafter suggests a lack of compatibility hurdles. Ex. 2042, at 336, n. 3 (citing a Microsoft hardware certification requirements document from 2013 that announced the TPM requirement for future certifications); APPL-1036, ¶28 (Dr. McDaniel discussing that technology had to be well understood and widely used long before a company like Microsoft would require every one of their customers to implement one). At bottom, PO provides no evidence as to *why* a TPM, much less Challenger’s teachings, is incompatible with Kesanupalli’s system/method, their compatibility is set forth in Petition and accompanying declaration. Petition, pp. 62-70 (citing APPL-1003, ¶¶195-211 including discussing the correspondence of general and secure processor portions, secure storage, and fingerprint readers in the teachings).

Further, PO’s arguments are again mischaracterizing what is required for obviousness. The Petition accompanied by Dr. McDaniel’s analysis showed that a

POSITA would have had reason and seen a benefit to applying Challenger's TPM-based architecture teachings to Kesanupalli (as enhanced by Brown) with a reasonable expectation of success. Petition, pp. 64-70 citing APPL-1003, ¶¶198-211. PO does not dispute the benefits of implementing a standards-based TPM architecture. Whether or not these benefits are tempered by a lack of industry-wide adoption, this allegation does not save the patent claims from obviousness. *See KSR*, 550 U.S. at 403 ("The proper question to have asked was whether a [person] of ordinary skill, facing the wide range of needs created by developments in the field of endeavor, would have seen a benefit to upgrading [the primary reference] with a [particular feature].")

V. GROUNDS 2, 4, 5

PO provides no additional arguments for these Grounds.

VI. CONCLUSION

PO analogizes combining a TPM or wiping to Kesanupalli as “‘gold plating a toothpick’—it can be done, but it doesn’t address the problem a toothpick was designed to address.” POR, p. 30. This analogy fails. An enhancement does not benefit *only* if it furthers a solution to one problem the original item was designed to address. While a toothpick is functional without gold plating, gold plating nonetheless can *benefit* the toothpick by providing a smooth coating, protecting underlying materials from wear, making the toothpick less vulnerable to damage, or enhancing aesthetics.

Petitioner concludes this Reply with a more relevant and appropriate analogy. While an attorney may maintain confidentiality by not discussing sensitive information in a public setting subject to eavesdropping, it would also have been desirable to securely maintain physical files and shred draft documents that contain the confidential information. Avoiding eavesdroppers, securing physical files and shredding drafts all contribute to a strategy to address multiple and multifaceted risks to confidential information and thus, enhance security.

The POR does not address the reasoned analysis and evidentiary support set forth in the Petition that showed all of the Challenged Claims to be obvious. Rather, relying on a mischaracterization of the art and a misapplication of the law, PO evades the clear obviousness showing by instead arguing that wiping and TPM-based

architecture do not address a social engineering issue. Wiping and a TPM-based architecture are beneficial features easily applied to Kesanupalli to enhance its overall defenses and improve security. Thus, a POSITA would have been motivated to make the combinations detailed in the Petition, and the Board should issue a final written decision holding all Challenged Claims unpatentable.

Respectfully submitted,

Dated: January 16, 2025
HAYNES AND BOONE PLLC
2801 N. Harwood Street, Suite 2300
Dallas, TX 75201

/David W. O'Brien/
David W. O'Brien
Lead Counsel for Petitioner
Registration No. 40,107

CERTIFICATE OF WORD COUNT

The undersigned attorney for Petitioner declares that the portions of this Reply subject to word count limitations of 37 C.F.R. §42.24(c)(1) have 4317 (less than 5,600) words, according to the word count tool in Microsoft Word™.

/David W. O'Brien/

David W. O'Brien
Lead Counsel for Petitioner
Registration No. 40,107

CERTIFICATE OF SERVICE

The undersigned certifies that, in accordance with 37 C.F.R. § 42.6(e), service was made on Patent Owner as detailed below.

Date of service: January 16, 2025

Manner of service: Electronic Mail: Rkamprath@mckoolsmith.com;
gfishback@mckoolsmith.com;
Carbyne_Apple@mckoolsmith.com

Documents served: **Petitioner's Reply to POR;
EXHIBITS APPL-1031 – APPL-1036.**

Persons served: Richard A. Kamprath
MCKOOL SMITH, P.C.
300 Crescent Court, Suite 1500
Dallas, Texas 75201

George Fishback
MCKOOL SMITH, P.C.
303 Colorado Street, Suite 2100
Austin, Texas 78701

/David W. O'Brien/
David W. O'Brien
Lead Counsel for Petitioner
Registration No. 40,107