

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

**PETITION FOR *INTER PARTES* REVIEW
UNDER 35 U.S.C. § 312 AND 37 C.F.R. § 42.104**

I.	INTRODUCTION	1
II.	MANDATORY NOTICES	1
	A. Real Party-in-Interest	1
	B. Related Matters.....	1
	C. Lead and Back-up Counsel and Service Information	2
III.	GROUND FOR STANDING	2
IV.	THE '138 PATENT	3
	A. Summary of the '138 patent	3
	B. Prosecution History	5
V.	LEVEL OF ORDINARY SKILL IN THE ART	6
VI.	CLAIM CONSTRUCTION	7
	A. “processor”	7
	B. “restricted interface” (Claims 11, 23).....	7
VII.	REQUESTED RELIEF	9
VIII.	OVERVIEW OF CHALLENGES	9
	A. Challenged Claims	9
	B. Statutory Grounds for Challenges	10
IX.	IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE..	11
	A. Ground 1: Claims 1-3, 7-8, 12-15, 19 and 24-25 are obvious under 35 U.S.C. §103(a) over Kesanupalli and Brown.....	11
	1. Kesanupalli.....	11
	2. Brown.....	13
	3. Combination of Kesanupalli and Brown	15
	4. Claim 1	20
	5. Claim 2	44
	6. Claim 3	45
	7. Claim 7	45
	8. Claim 8	47
	9. Claim 12.....	48

10.	Claims 13–15, 19 and 24	49
11.	Claim 25	51
B.	Ground 2: Claims 10 and 22 are obvious under 35 U.S.C. §103(a) over Kesanupalli and Brown further in view of Cheng.	54
1.	Cheng	54
2.	Reasons to Combine Kesanupalli, Brown and Cheng	57
3.	Claim 10	60
4.	Claim 22	61
C.	Ground 3: Claims 11 and 23 are obvious under 35 U.S.C. §103(a) over Kesanupalli and Brown further in view of Challenger.	62
1.	Challenger	62
2.	Reasons to Combine Kesanupalli, Brown and Challenger	64
3.	Claim 11	66
4.	Claim 23	70
D.	Ground 4: Claims 5 and 17 are obvious under 35 U.S.C. §103(a) over Kesanupalli and Brown further in view of Headley.	70
1.	Headley	70
2.	Reasons to Combine Kesanupalli, Brown and Headley	71
3.	Claim 5	73
4.	Claim 17	74
X.	DISCRETIONARY DENIAL IS NOT WARRANTED	74
A.	The <i>Fintiv</i> factors favor institution.	75
B.	The Board should not deny under <i>General Plastic</i>	77
C.	<i>Advanced Bionics</i> Test Favors Institution.	77
XI.	CONCLUSION	78
XII.	CERTIFICATE OF WORD COUNT	79
	CERTIFICATE OF SERVICE	80

PETITIONER’S EXHIBIT LIST

JANUARY 19, 2023

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-

	Commands_v1.2_rev116_01032011.pdf (retrieved Dec. 12, 2023)
APPL-1018	Introduction to Programmable Systems on a Chip, Bob Zeidman, 07.27.2005 at https://www.eetimes.com/introduction-to-programmable-systems-on-a-chip/ (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 https://www.popularmechanics.com/technology/gadgets/how-to/a6819/how-to-restore-your-data-after-a-hard-drive-crash/ (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 https://trustedcomputinggroup.org/wp-content/uploads/TPM-Applications-Whitepaper.pdf (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), https://www.uscourts.gov/statistics/table/na/federal-court-management-statistics/2023/09/30 (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)
--	-----------------------

I. INTRODUCTION

U.S. Patent No. 11,514,138 (the “’138 patent”) relates to “Authentication Translation” where a request to access a resource and an authentication input is received, and in response, “a previously stored credential associated with the resource is accessed” and provided to the resource. APPL-1001, Title, Abstract. Apple Inc. (“Petitioner” or “Apple”) respectfully requests that the Board review and cancel as unpatentable under (pre-AIA) 35 U.S.C. §103(a) claims 1-3, 5, 7-8, 10-15, 17, 19 and 22-25 (“Challenged Claims”) of the ’138 patent.

II. MANDATORY NOTICES

A. Real Party-in-Interest

Pursuant to 37 C.F.R. §42.8(b)(1), Petitioner certifies that the real party-in-interest is Apple Inc.

B. Related Matters

Pursuant to 37 C.F.R. §42.8(b)(2), the ’138 patent is or was involved in the following matters, which may affect, or be affected by, this proceeding:

- *Carbyne Biometrics, LLC v. Apple Inc.*, 1:23-cv-00324 (WDTX), filed March 24, 2023 (Pending) (“Parallel District Court Proceeding”)

Apple is not aware of any disclaimers, reexamination certificates or other IPR petitions addressing the ’138 patent; however, the following matter involved a related application and may affect this proceeding:

- *Samsung Electronics Co., Ltd. et al v. RightQuestion, LLC*, IPR2022-00244 (PTAB), filed December 1, 2021 (Terminated July 26, 2022) (“Samsung ’696 Patent IPR”)

C. Lead and Back-up Counsel and Service Information

Lead Counsel

David W. O’Brien
HAYNES AND BOONE, LLP
2801 N. Harwood St., Suite 2300
Dallas, TX 75201

Phone: (512) 867-8457
Fax: (214) 200-0853
david.obrien.ipr@haynesboone.com
USPTO Reg. No. 40,107

Back-up Counsel

Kelly Lyle
HAYNES AND BOONE, LLP
2801 N. Harwood St., Suite 2300
Dallas, TX 75201

Phone: (512) 867-8528
Fax: (214) 200-0853
kelly.lyle@haynesboone.com
USPTO Reg. No. 62,332

Hong Shi
HAYNES AND BOONE, LLP
2801 N. Harwood St., Suite 2300
Dallas, TX 75201

Phone: (512) 867-8440
Fax: (214) 200-0853
hong.shi.ipr@haynesboone.com
USPTO Reg. No. 69,009

Please address all correspondence to lead and back-up counsel. Petitioner consents to electronic service and asks Patent Owner to do the same.

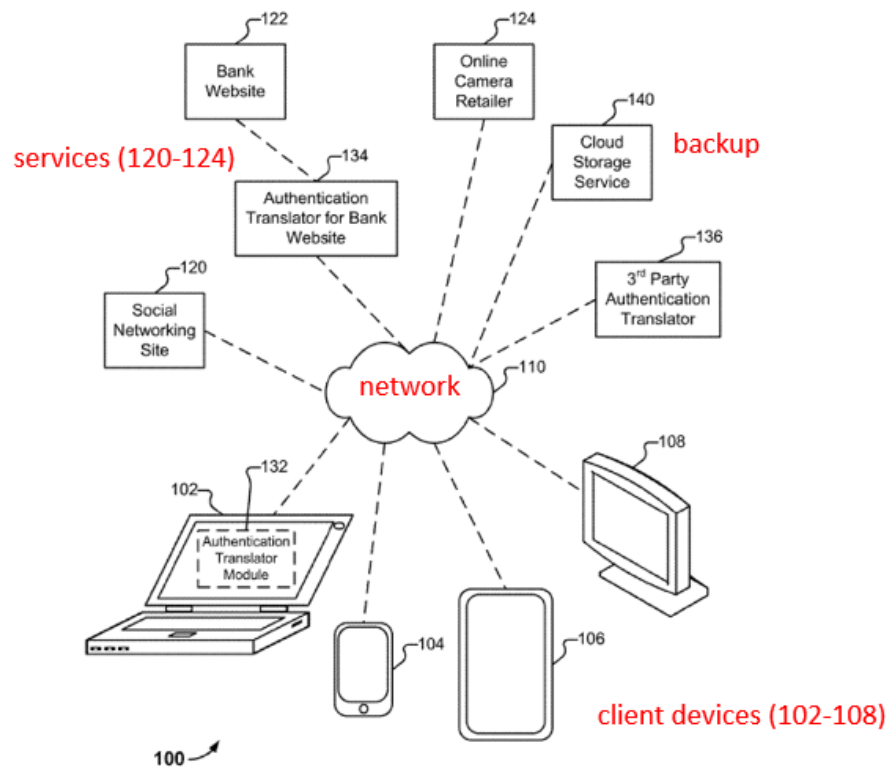
III. GROUNDS FOR STANDING

Petitioner certifies that the ’138 patent is eligible for IPR and that Petitioner is not barred or estopped from requesting IPR challenging the patent claims. 37 C.F.R. §42.104(a).

IV. THE '138 PATENT

A. Summary of the '138 patent

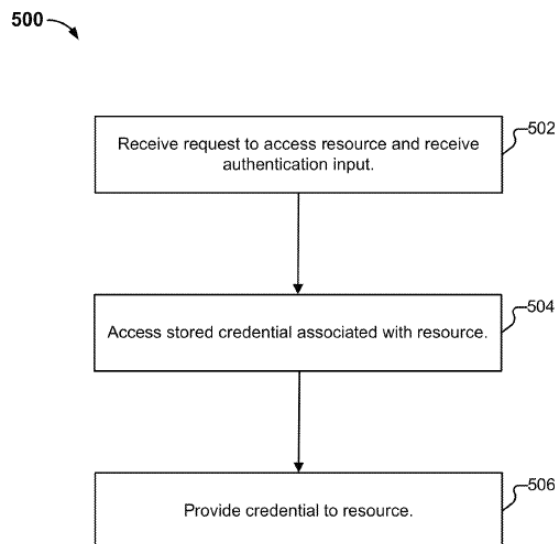
The '138 patent is directed to an environment including a client device, such as a computer or smartphone, which is connected via a network to a service such as a website. APPL-1001, 2:40-659. FIG. 1 is illustrative:



APPL-1001, FIG. 1, annotated

The '138 patent describes authentication techniques to provide user credentials (*e.g.*, a password) from a client device to a service with a goal of avoiding reliance on a user's input of the credential, which is tedious for the user and leads to poor security practices. APPL-1001, 1:37-46. The '138 patent states

users “need not type such usernames and passwords into their devices whenever required by a service. Instead, users can authenticate themselves to an ‘authentication translator’...and the authentication translator will provide the appropriate credentials to the implicated service on the user’s behalf.” APPL-1001, 2:65-3:4. FIG. 5 illustrates a process for performing this authentication translation. APPL-1001, 1:60-61.



APPL-1001, FIG. 5

The '138 patent describes an example of FIG. 5 where a user, Alice, wishes to sign onto a resource (*e.g.*, social networking website 120). Alice is prompted by her client device, in this example her laptop, to provide biometric information using an “integrated fingerprint reader on her laptop.” APPL-1001, 6:33-42. Alice provides her biometric information in response to the prompt. *Id.* A translation module such as provided in her laptop compares her provided biometric

information with a template stored on the computer. APPL-1001, 6:50-56. If a match is found, a previously stored credential associated with the resource is provided to the resource. APPL-1001, 6:57-63.

However, as discussed below, these techniques for authentication translation were well-known at the time of the claimed invention. APPL-1003, ¶¶28-54.

B. Prosecution History

After an initial indication of allowability of the claims, the applicant replaced the “system” preamble of its as-filed claim 1 to recite a “device,” and removed a recitation of a “restricted interface” to read simply “interface” in each independent claim. APPL-1002, 153-158, 170, 178-184. The Examiner subsequently withdrew the indication of allowance rejecting then-pending claims as obvious over a combination of prior art from an Applicant submitted IDS; the Applicant responded with claim amendments that included further defining the storage on the device and its accessibility and wiping to be of **both** the biometric template and the credential comprising the cryptographic key. APPL-1002, 117-136, 105-113. The Examiner rejected the amended claims. APPL-1002, 54-75. And in response, the Applicant amended its claims to include the recitation of “the prompt is visually presented,” as shown in exemplary claim 1:

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, [[and]] 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;

APPL-1002, 41. A notice of allowance issued with no additional reasons for allowance given. APPL-1002, 8-15.

V. LEVEL OF ORDINARY SKILL IN THE ART

The level of ordinary skill in the art may be reflected by the prior art of record. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). Here, Persons of Ordinary Skill in the Art (“POSITA”) at the time of the claimed invention would have had a bachelor’s degree in an 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. APPL-1003, ¶¶18-21. Furthermore, a person with less formal education but more experience, or more formal education but less experience, could have also met the relevant standard for POSITA. *Id.* However, Petitioner does not imply that a person having an extraordinary level of skill should be regarded as POSITA.

VI. CLAIM CONSTRUCTION

During IPR, claims are construed according to the standard as set forth in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (*en banc*). 37 C.F.R. §42.100(b) (Nov. 13, 2018). The claims are construed to the extent necessary to resolve the underlying controversy. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). Petitioner submits that for purposes of this proceeding, and as set forth below, the terms of the challenged claims should be given their plain and ordinary meaning. *Phillips*, 415 F.3d at 1314-17; APPL-1003, ¶¶55-60.

A. “processor”

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 to a processor. APPL-1003, ¶56.

B. “restricted interface” (Claims 11, 23)

A “restricted interface” is an interface that limits accessibility. APPL-1003, ¶57. 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.

The Board has addressed this term, *restricted interface*, in a third-party IPR challenging US 10,824,696 (“the ’696 patent,” to which the ’138 patent claims priority as a continuation), in which the Board found “[t]he specification of the ’696 describes only an ‘API’ (Application Programming Interface) as an example of a restricted interface between two processors.” IPR2022-00244, (Institution), Paper 17, 31 (PTAB 2002). In IPR2022-00244, the Board referenced (in its description of the ’696 patent) the very same description noted above (from the ’138 patent). *See* IPR2022-00244, Paper 17, 8. In IPR2022-00244, the Board was persuaded that a trusted platform module (TPM) architecture sufficiently disclosed the restricted interface. IPR2022-00244 Paper 17, 40 (relying on a TPM API stack depicted in Figure 7 of U.S. Pub. App. 2008/0059804 naming Shah).

In the Parallel District Court Proceeding, Patent Owner proposed (and the court issued a preliminary construction) that the term *restricted interface* is to be understood in accord with plain and ordinary meaning. APPL-1026, 1. Nonetheless, Petitioner is mindful that (in IPR2022-00251 of US Patent 10,929,512 patent, to which the '138 patent claims priority as a continuation) the term *restricted interface* was central to a non-institution decision that found the petitioner in that proceeding and its expert failed to explain how prior art teachings disclosed a “restricted interface” in part because no express construction was offered. *See* IPR2022-00251, Paper 17, at 23, 25 (PTAB 2002).

Plain and ordinary meaning of “*restricted interface*” is an interface that limits accessibility. APPL-1003, ¶¶57-60. Petitioner also demonstrates in the analysis that follows that the prior art renders obvious a *restricted interface* including an API that limits accessibility to secure storage, a fingerprint sensor, or a dedicated processor, which is included within the meaning of the term regardless of how it is construed.

VII. REQUESTED RELIEF

Petitioner asks the Board to institute trial and cancel the Challenged Claims.

VIII. OVERVIEW OF CHALLENGES

A. Challenged Claims

Claims 1-3, 5, 7-8, 10-15, 17, 19 and 22-25 (“Challenged Claims”) of the '138 patent are challenged.

B. Statutory Grounds¹ for Challenges

Grounds	Claim(s)	Basis
#1	1-3, 7-8, 12-15, 19, and 24-25	§103(a) over Kesanupalli and Brown
#2	10, 22	§103(a) over Kesanupalli and Brown further in view of Cheng
#3	11, 23	§103(a) over Kesanupalli and Brown further in view of Challener
#4	5, 17	§103(a) over Kesanupalli and Brown further in view of Headley

Kesanupalli was filed March 24, 2010, published April 7, 2011, and issued August 5, 2014. Brown was filed August 3, 2015 and claims priority through a chain of continuations to an application filed on January 18, 2008. Challener was filed September 29, 2006, published May 1, 2008, and issued January 17, 2012. Cheng was filed September 24, 2003 and published June 17, 2004. Headley was filed October 29, 2009 and published May 22, 2012. Kesanupalli and Challener are prior art under at least §§102(e) and 102(a), Brown and Headley at least under §102(e); Cheng under §102(b). Challener's PG-PUB (APPL-1022) is also prior art under §102(b). *See* APPL-1003, ¶¶61-64.

¹ Pre-AIA §§102, 103(a) apply.

IX. IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE

A. Ground 1: Claims 1-3, 7-8, 12-15, 19 and 24-25 are obvious under 35 U.S.C. §103(a) over Kesanupalli and Brown.

1. Kesanupalli

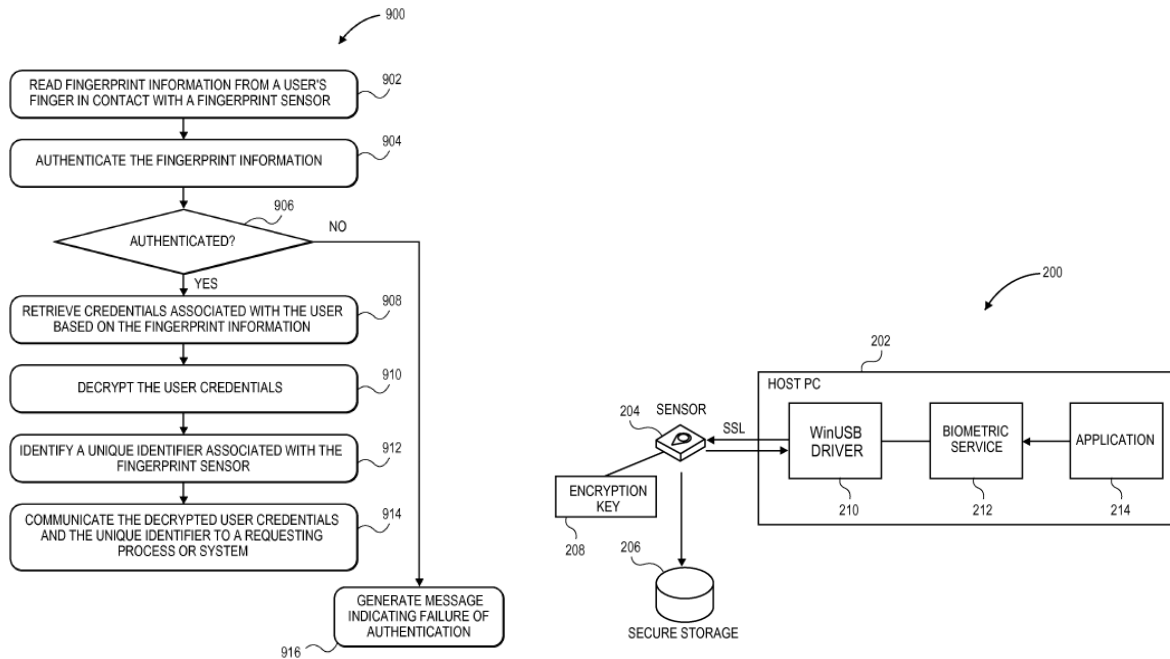
Kesanupalli is entitled “Secure User Authentication Using Biometric Information” and is directed to a secure authentication system that uses biometric information to “provide[] a more secure authentication of the user than commonly used password-based methods and systems.” APPL-1006, (54), 1:59-62. *See* APPL-1003, ¶¶65-70. For example, based on a match between a fingerprint template stored for a particular user and fingerprint information read from a finger presented at a fingerprint reader, Kesanupalli’s methods retrieve credentials associated with the user and communicate those credentials to an external system or process. APPL-1006, FIGS. 8-9, 3:14-4:11.

During an enrollment process with a resource such as a website, “a user swipes [or places] their finger [on] a fingerprint sensor several times to create [the] fingerprint template. The fingerprint template allows the user’s fingerprint to be distinguished from fingerprints associated with other users.” APPL-1006, 3:33-41. The user (or system) also “provides user credentials, such as a password, cryptographic key...or the like,” and the systems and methods described in Kesanupalli “bind the user’s fingerprint template with the user credentials.” APPL-1006, 3:15-18, 3:41-46. To protect user credentials, “[t]he fingerprint

template and user credentials are then stored in a secure storage of the user's device." APPL-1006, 3:46-47, *see also*, 5:61-6:49, 8:29-53.

During a subsequent user identification or verification for the website, a user presents her biometric information (*e.g.*, places a finger on a fingerprint sensor) and if the presented fingerprint "matches a fingerprint template, the user's credentials are released to the user and/or [the] service or process requesting the user verification." APPL-1006, 3:52-61. "[T]he user credentials released after finding a matching fingerprint template may include an OTP (One Time Password) token, RSA signature and the like," such as a "cryptographic key." APPL-1006, 3:65-4:1, 3:41-44, FIG. 12.

FIG. 9 of Kesanupalli illustrates these steps of authenticating a user in the context of an embodiment in which user credentials are cryptographically secured in storage; FIG. 2 illustrates an example system 200 in which user enrollment and authentication processes are performed using a biometric sensor 204, secure storage 206 and a Host PC 202. APPL-1006, 6:26-49, 9:10-24.



APPL-1006, FIGS. 9 and 2

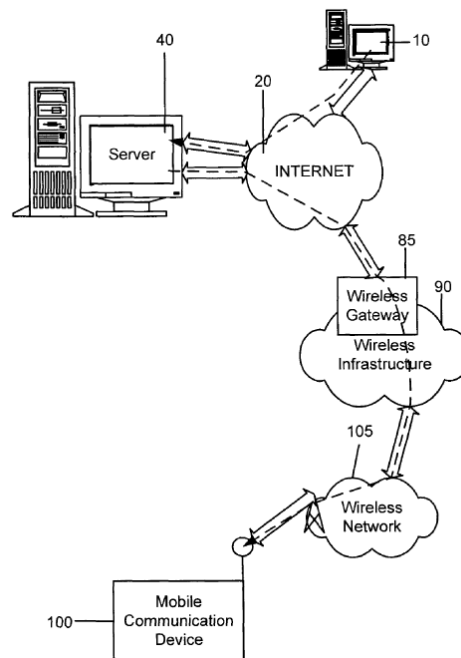
In an authentication process such as discussed above, the sensor 204 receives a biometric input from a user and releases the user's credentials from secure storage 206 upon a successful match of the input with the user's stored biometric template. APPL-1006, 6:31-45. The released credentials are then communicated to the external resource by an application 214 of the Host PC 202. APPL-1006, 5:9-58, 6:11-31.

2. Brown

Brown is entitled "Selectively Wiping a Remote Device" and "relates generally to the field of computer and network security, and more particularly, to wiping data stored on a remote device such as a mobile communication device."

APPL-1009, (54), 1:15-18. *See* APPL-1003, ¶¶71-74.

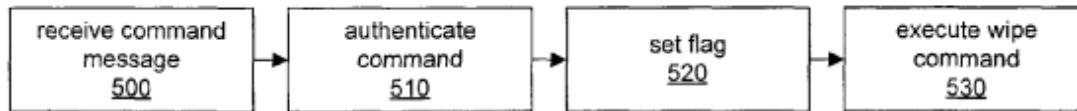
FIG. 1 of Brown “shows a first communication device, here a client personal computer 10, a network, herein the Internet 20...and a second communication device, here a client mobile communication device 100.” APPL-1009, 4:60-64. The client devices may be personal computers, mobile devices, mobile communication devices, communication devices, computing devices, or data storage devices” such as “laptop and notebook computers, PDAs, smartphones, and the like.” APPL-1009, 4:64-65.



APPL-1009, FIG. 1

Brown recognizes client devices include “data of a sensitive or critical nature” desired to be protected from “unauthorized or malicious users” should the

client's device be "compromised, decommissioned, or redeployed." APPL-1009, 1:15-45, 2:8-17. Brown provides for protecting the data in such instances by wiping the data from the client device so it is deleted from the device and cannot be retrieved. Brown illustrates in its FIG. 6 "a flowchart depicting a sequence of steps in the execution of the wipe command on the client device 10, 100." APPL-1009, 11:65-13:14.



APPL-1009, FIG. 6

3. Combination of Kesanupalli and Brown

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.*

First, Kesanupalli, Brown and the '138 patent are analogous art and are all in the same field of endeavor—information security, and more particularly, security arrangements for protecting computers or other electronic devices, components thereof, programs or data against unauthorized activity. APPL-1003, ¶¶76-78, *see, e.g.*, APPL-1006, 2:30-38 (“[S]ystems and methods described herein relate to biometric authentication of users...[B]iometric information provides an additional level of security when used in systems and procedures related to authentication of a user.”), 2:48-50 (“client device, such as a computer, cellular phone, and so forth”); APPL-1009, 1:15-25 (“[D]isclosure relates generally to the field of computer and network security [including] [d]ata stored in the memory of a communication and/or computing device, such as a mobile communication device, personal digital assistant (PDA), smartphone, laptop computer, and the like, [that] may include data of a sensitive or critical nature that is accessible only by authorized users.”); APPL-1001, 1:35-44 (“Providing credentials to a service, whether via a mobile or other device, is often a tedious experience for a user...users will often engage in practices...which render their credentials less secure against attacks. Accordingly, improvements in authentication techniques would be desirable.”), FIG. 1.

Moreover, as evidenced on the front page of Kesanupalli, Brown and the '138 patent, the international classification (IPC), U.S. classifications (CPC) and/or

the field of search classification consulted by the Office during examination for each patent include the same subclass, namely CPC/IPC G06F 21 (security arrangements for protecting computers, components thereof, programs or data against unauthorized activity). *See* APPL-1001, (51), (52); APPL-1006, (51) (58); APPL-1009, (51), (52).²

Further, both Kesanupalli and the '138 patent are directed to biometric authentication including the secure storage of the personal data required to perform this authentication and associated user credentials. *See, e.g.*, APPL-1006, FIG. 9; APPL-1001, FIG. 5. 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. APPL-1003, ¶78; APPL-1009, 1:15-2:8, 6:4-31.

Second, 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 credentials are sensitive

² *See also*, [www.uspto.gov/web/patents/classification/cpc/html/cpc-](http://www.uspto.gov/web/patents/classification/cpc/html/cpc-G06F.html#G06F)

[G06F.html#G06F](http://www.uspto.gov/web/patents/classification/cpc/html/cpc-G06F.html#G06F) (subclass definitions);

www.uspto.gov/web/patents/classification/cpc/html/cpc-G06F.html#G06F (CPC to IPC concordance).

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.* Such a problem would have also been reasonably pertinent to the inventor of the challenged patent. *See* APPL-1001, 8:30-35 (noting that “criminals with physical component access to lost devices [could] gain access” to sensitive information). Indeed, Brown itself teaches “there are instances when the device may be compromised, decommissioned, or redeployed, making it desirable to delete or ‘wipe’ data.” APPL-1009, 2:6-15. Thus, not only were Kesanupalli, Brown and the '138 patent in the same field of endeavor, but Brown would have been reasonably pertinent to a problem faced by the inventor of the '138 patent and pertinent to known risks of theft and loss that POSITA would have been motivated to address through the Kesanupalli-Brown combination. APPL-1003, ¶¶79-80.

POSITA would readily recognize a personal electronic device can be compromised such as when a component is lost, damaged, or otherwise requires replacement, and a typical practice in the industry to address these concerns by wiping data long before the '138 patent. APPL-1003, ¶80. 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.

Finally, POSITA would have had reasonable expectations of success in adding a wiping technique of Brown in a biometric authentication system such as taught by Kesanupalli as Brown is similarly directed to improving security of personal information in a substantially similar device. APPL-1003, ¶¶81-82. Adding a wipe 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

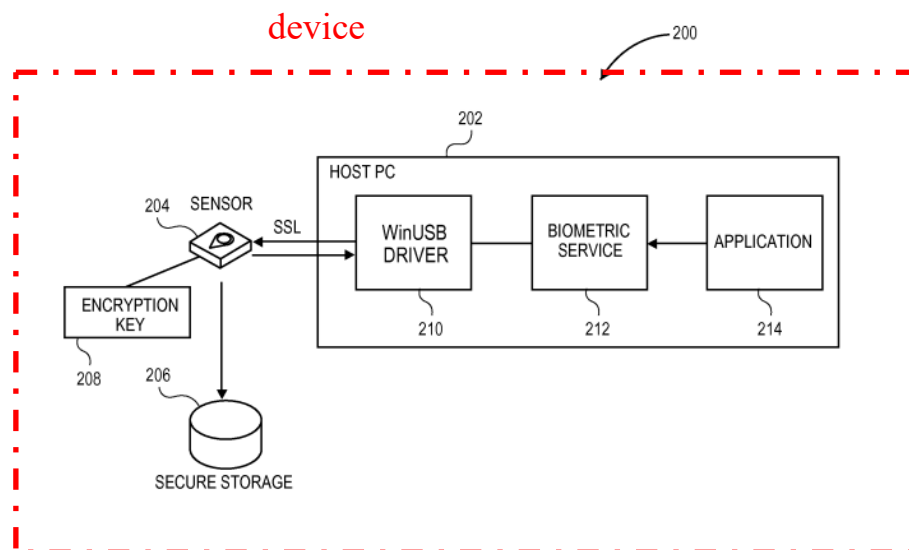
Brown's processor, and wiping is a predictable data management task that would have been easily accomplished in Kesanupalli device. APPL-1003, ¶¶82.

4. Claim 1

[1.0] *A device, comprising:*

Kesanupalli teaches the preamble to the extent it's limiting. APPL-1003, ¶¶83-87.

Kesanupalli describes a device exemplified in FIG. 2 "capable of performing biometric user enrollment and authentication." APPL-1006, 2:1-2.



APPL-1006, FIG. 2, annotated

Biometric sensor 204, its secure storage 206, and Host PC 202 (including web browser application and biometric services executing thereon) constitute *a device* that provides authentication translation and ultimately communicate user

credentials to web servers. APPL-1006, Abstract, 2:54-3:3, 4:3-11, 4:36-50, 6:11-49. POSITA would appreciate Kesanupalli's embodiments (e.g., FIG. 2) constitute a *device*, generically defined in claim 1 and the '138 patent. APPL-1003, ¶¶84-86; APPL-1001, 2:21-23. To the extent that Patent Owner imparts some more integrally-formed meaning to the term, POSITA would also understand Kesanupalli to disclose integrally-formed realizations of a *device* which also includes sensor 204. APPL-1003, ¶86; APPL-1006, 2:48-50 ("In particular embodiments, the biometric sensor is **physically attached (or manufactured into) a client device** such as a computer, cellular phone, and so forth."), 3:46-51 ("In one embodiment the secure storage device is contained within the fingerprint sensor hardware. In other embodiments, the secure storage device is contained in a device that utilizes the fingerprint sensor.")

Therefore, Kesanupalli discloses a *device*, as claimed.

[1.1] *a processor on the device;*

Kesanupalli discloses or renders obvious this limitation. APPL-1003, ¶¶88-93.

As explained in Section VI.A, POSITA would understand *processor* to encompass circuits, processor cores and devices that process data such as computer instructions within the construct of the larger device in (or on) which they reside. Kesanupalli includes a *processor on the device* that includes processor circuitry

executing sensor 204 and processor circuitry executing PC 202. APPL-1006, FIG. 2, 6:26-49. Kesanupalli describes what POSITA would readily recognize—namely that its functions of authentication translation including accessing data in a secure storage and communication with external resources are performed by a *processor*. APPL-1003, ¶¶89-90; APPL-1006, 9:58-10:1 including “[t]he invention may also involve a number of functions to be **performed by a computer processor**, such as a microprocessor. The microprocessor may be a specialized or dedicated microprocessor that is configured to perform particular tasks according to the invention[.]”).

Kesanupalli suggests both specialized and generalized processors may be used to effectuate its biometric authentication techniques, and POSITA would understand Kesanupalli to describe implementations in which its biometric authentication techniques are provided using specialized processor circuitry executing the authentication functions (those of sensor 204 such as matching) and general processor circuitry executing the functions of communicating with an external resource (those of HOST PC 202). *See* APPL-1003, ¶91; APPL-1006, 5:62-6:31, 6:40-49. The processor circuitry executing functions of sensor 204 and the processor circuitry executing functions of PC 202 provide a *processor on the device*. The ’138 patent expressly states a processor can encompass multiple devices (APPL-1001, 2:21-23); however, to the extent the Patent Owner argues it’s

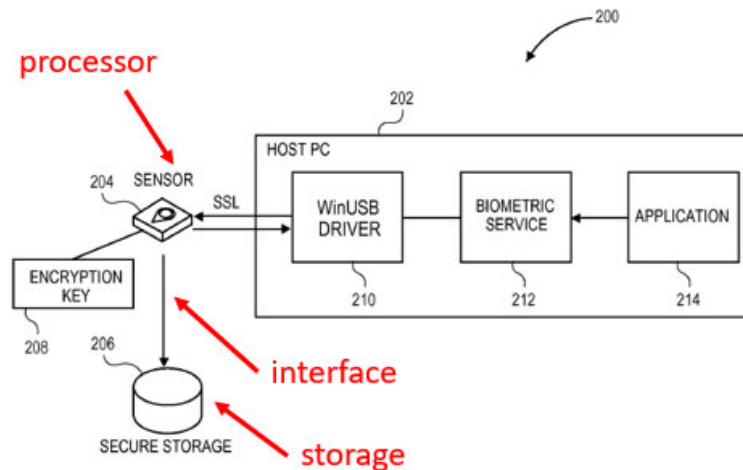
so required, POSITA would readily recognize implementations of Kesanupalli's processing circuitry as a single chip processor. APPL-1003, ¶92 (discussing system on a chip (SoC), APPL-1018).

Thus, Kesanupalli discloses and renders obvious *a processor on the device*, as claimed.

[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,*

Kesanupalli discloses or renders obvious this limitation. APPL-1003, ¶¶94-100.

Kesanupalli illustrates a **secure storage 206**, which provides a *storage on the device*. See APPL-1006, 2:48-50, 3:46-51, 6:45-47, FIG. 2. Kesanupalli's storage 206 is *accessible by the processor on the device via an interface that facilitates communication between the storage on the device (secure storage 206) and the processor (processor circuitry executing functions of sensor 204) on the device*.



APPL-1006, FIG. 2, annotated

As illustrated in FIG. 2 above, secure storage 206 is accessible by the processor circuitry executing sensor 204 as shown by the vertical arrow extending from sensor 204 to storage 206. APPL-1003, ¶¶95-96. This is confirmed by Kesanupalli's disclosure which, as discussed in detail below in limitations [1.3] and [1.7] respectively, describes that processor circuitry executing sensor 204 *access[es]* and *communicat[es]* with storage 206 in order to perform authentication, which includes matching a user's biometric input with a biometric template in storage 206 and releasing user credentials from storage 206 on a successful match. See APPL-1003, ¶¶98-100, 106-107; APPL-1006, 3:52-4:12, 5:17-32, 9:4-24, FIGS. 9, 12.

As discussed in limitation [1.1], POSITA would understand Kesanupalli to

provide a processor on its device that executes its functions, including those described in association with sensor 204. As such, Kesanupalli describes the devices, circuits and/or processing cores that constitute or render obvious the *processor*, as claimed, and which access secure storage 206. APPL-1003, ¶¶89-92; APPL-1006, 9:58-10:1. Each time the processor accesses secure storage 206, it does so via the *interface*, which is software and/or hardware framework by which the processor exchanges information with its storage; the interface (*see* annotated FIG. 2 above) is the only disclosed connection to secure storage 206. APPL-1003, ¶99.

Thus, Kesanupalli discloses or renders obvious “*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;*

Kesanupalli discloses or renders obvious this limitation. APPL-1003, ¶¶101-110.

As described above with reference to limitation [1.1] and in view of the ’138 patent specification’s use of the term *processor* in a generic manner, POSITA would understand Kesanupalli to describe the devices, circuits and/or processing

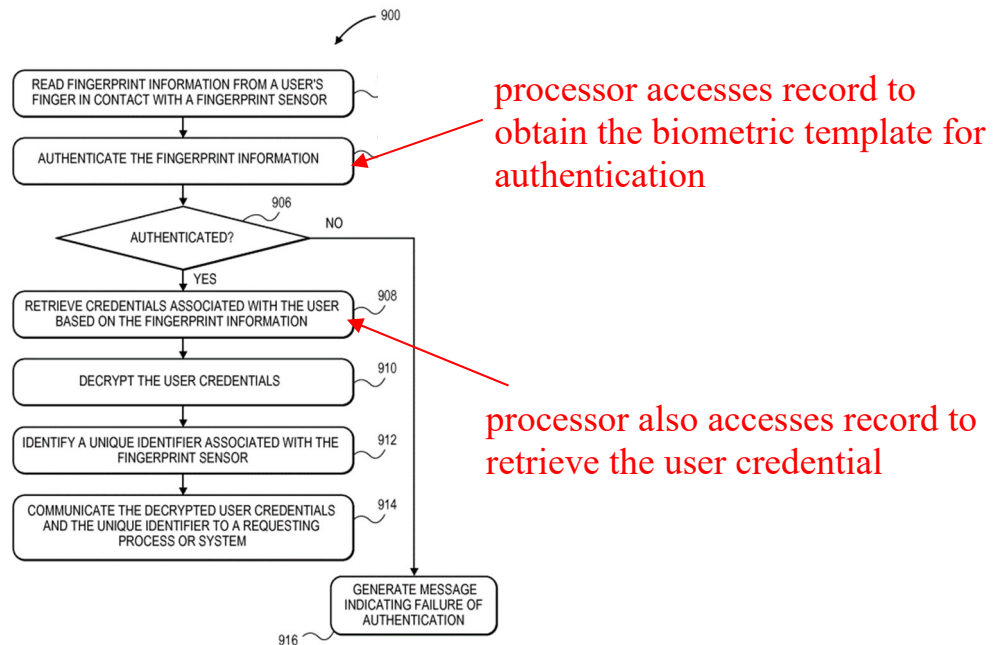
cores that constitute or render obvious the *processor on the device*. Kesanupalli and, in combination, Brown disclose the functionality, *i.e.*, the processing, that the *processor on the device* is *configured to perform*, and that functionality is described with reference limitations [1.3]-[1.8].

With respect to limitation [1.3], Kesanupalli describes a user's enrollment process for an external resource such as a website where the user's credential and biometric template are stored in secure storage. APPL-1006, 3:15-51 ("Initially, a user enrolls with the biometric user authentication system by **binding their user credentials with the user's biometric template (a 'fingerprint template' in specific implementations)**...During an example enrollment process that uses a fingerprint sensor as the biometric sensor, a user swipes their finger across the fingerprint sensor several times to create a fingerprint template...After creating a fingerprint template, the user (or a web server or other system) provides **user credentials**, such as a password, cryptographic key, random seed, and the like. The systems and procedures described herein **bind the user's fingerprint template with the user credentials**. The fingerprint template and user credentials are then stored in a **secure storage device**.")

The user's credential (*e.g.*, cryptographic key) and biometric template, which are bound and stored in secure storage 206, constitute *at least one record*, as claimed. APPL-1003, ¶¶104-105 (citing APPL-1019 definition of "record").

Kesanupalli in FIG. 7 walks through this enrollment process. APPL-1006, 8:29-53 (describing block 710 where “the procedure binds the user credentials with the fingerprint template[], then stores the user credentials and the fingerprint template [] in a secure storage.”). Kesanupalli describes its record—the bound credentials and template—is associated with a particular external resource (*e.g.*, website). APPL-1006, 4:36-5:43.

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



APPL-1006, FIG. 9, annotated

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

Thus, Kesanupalli discloses or renders obvious “*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;*

Kesanupalli discloses or renders obvious this limitation. APPL-1003,

¶¶111-115.

Continuing from limitation [1.3] above, Kesanupalli discloses a *record*—e.g., biometric (e.g., fingerprint) template and user credential bound and stored in the secure storage 206—according to the aspects of this limitation. In particular, Kesanupalli describes that in its enrollment, “a user swipes their finger across the fingerprint sensor several times to create a **fingerprint template**...After creating a fingerprint template, the user (or a web server or other system) provides **user credentials**, such as a password, **cryptographic key**, random seed, and the like. The systems and procedures described herein **bind the user’s fingerprint template with the user credentials**. The fingerprint template and user credentials are then **stored in a secure storage device**.” APPL-1006, 3:32-51. The fingerprint template is one type of “biometric template” suggested by Kesanupalli. APPL-1006, 3:15-18 (“a user enrolls...by binding their user credentials with the user’s **biometric template (a ‘fingerprint template’** in specific implementations.”) A fingerprint template is a biometric template. APPL-1003,

¶113.

Kesanupalli's user credential and bound biometric template is *the at least one record associated at least with the external resource* as it is specific to the particular external resource such as a website. APPL-1003, ¶¶112-114; APPL-1006, 5:33-43 (“different user credentials are associated with each Web site with which the user enrolls”). Kesanupalli also describes one type of user credential is a *cryptographic key* as the user credentials may be a “password, cryptographic key, random seed, and the like.” APPL-1006, 3:32-51, *see also*, 3:41-44, FIG. 12, 8:6-22.

Thus, Kesanupalli discloses or renders obvious “*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] [*wherein the processor on the device is configured to:*] *in response to determining a match between a biometric input and the biometric template, retrieve, from the at least one record, the credential, wherein the biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voiceprint, a feature usable for a retina scan, or a typing feature,*

Kesanupalli discloses or renders obvious this limitation. APPL-1003,

¶¶116-123.

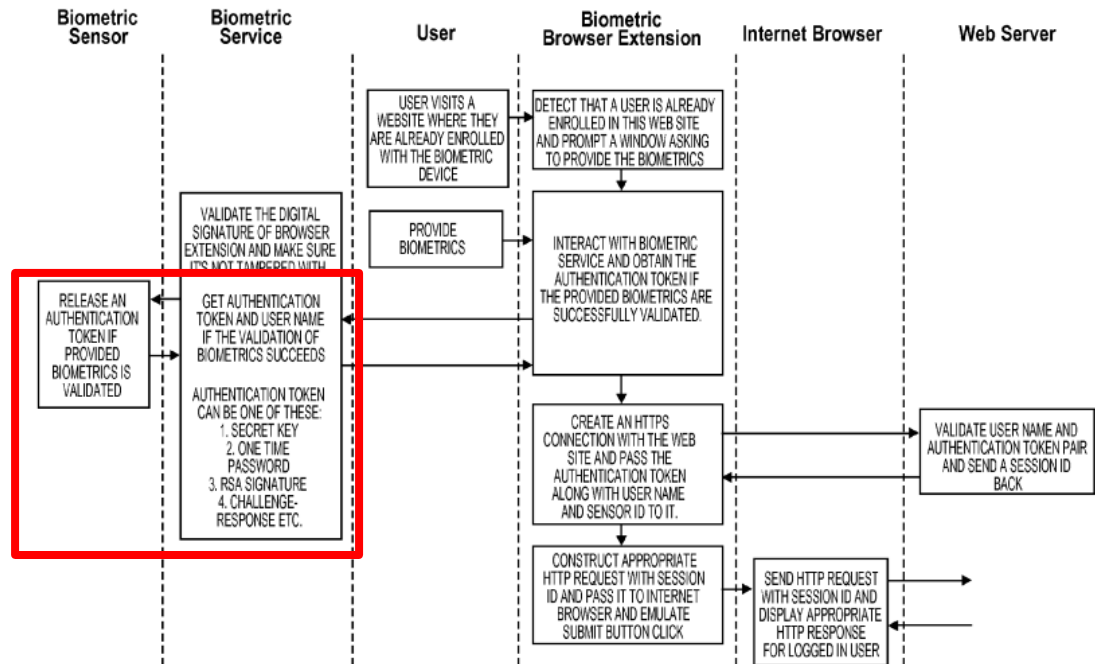
As described above with reference to limitation [1.1], POSITA would understand Kesanupalli to describe the devices, circuits and/or processing cores

that constitute or render obvious the *processor on the device*. Kesanupalli also discloses and renders obvious the functionality, *i.e.*, the processing, that the *processor* is configured to perform, and that functionality is now described relative to the limitations of limitation [1.5A].

First, Kesanupalli describes a *biometric input*. In one example, Kesanupalli describes that the sensor (sensor 204) receives a biometric input of a “fingerprint” from a “fingerprint sensor.” APPL-1006, 6:31-37, 9:10-24 (“procedure 900 reads **fingerprint information** from a user's finger in contact with a fingerprint sensor (902).”), FIGS. 8, 9, 8:54-9:3. Kesanupalli not only describes that *biometric input corresponds to at least one of a fingerprint* but also that suggests other biometric information including those further recited in the recited group. APPL-1006, 6:31-36 (“‘Biometrics’ and ‘biometric information’ refers to measurable biological characteristics of a user, such as a **fingerprint, facial characteristics, eye characteristics**, voice characteristics (also referred to as a ‘voiceprint’) and the like.”).

Kesanupalli's authentication process includes *determining a match between a biometric input (e.g., fingerprint information) and the biometric template (e.g., fingerprint template)* and if there is a match, *in response retriev[ing], from the at least one record, the credential*. APPL-1006, 9:14-20 (“The procedure then **authenticates the fingerprint information** (block 904)...If the fingerprint

information is authenticated, the procedure **retrieves credentials** associated with the user based on the fingerprint information (block 908).”), 6:31-49 (“For example, in a successful fingerprint swipe, **the swiped fingerprint information matches a fingerprint template** associated with the fingerprint sensor...**biometric sensor 204 includes a ‘match on chip’ functionality that releases a user’s credentials only upon a successful** fingerprint swipe or other biometric reading...”), 3:52-56 (“During an example user identification process (also referred to as a user verification process), a user swipes their finger across a fingerprint sensor. The process then **determines whether the user’s fingerprint information matches a fingerprint template** associated with the fingerprint sensor.”) *See also*, APPL-1006, 5:17-32, 8:54-9:25, FIGS. 8, 9. Kesanupalli’s FIG. 12 illustrates actions for authenticating a user, including those performed by a “user,” by the processor of the user’s device (*e.g.*, by circuitry of the sensor and applications on the Host PC (*e.g.*, biometric service, browser extension, browser applications), and by an external resource’s web server.



APPL-1006, FIG. 12, annotated

Kesanupalli describes the *processor on the device* performs the steps above of retrieving the credential as sensor 204 is accessing storage 206, performing the matching of the input and template and, if a match is found, releasing the credential for transfer to a requesting processor system by the application of PC 202. See APPL-1006, 6:11-49, 9:10-24, FIG. 2.

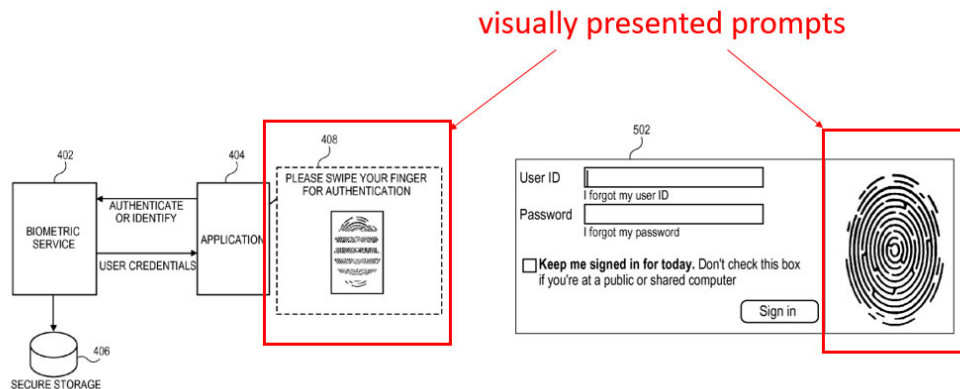
Thus, Kesanupalli discloses or renders obvious a processor configured to “*in response to determining a match between a biometric input and the biometric template, retrieve, from the at least one record, the credential, wherein the biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a 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;*

Kesanupalli discloses this limitation. APPL-1003, ¶¶124-127.

First, Kesanupalli discloses the *biometric input* (e.g., fingerprint information) *is received subsequent to presenting of a prompt, wherein the prompt comprises a prompt to provide biometric information.* APPL-1006, 5:9-14 (“the Web site **prompts the user** to perform user authentication (e.g., using the biometric device).”), FIG. 12 (“prompt a window asking to provide the biometrics”).



APPL-1006, FIGS. 4 and 5, annotated

Second, Kesanupalli also describes that this prompt can be *visually presented* as illustrated in FIGS. 4 and 5 (annotated above) and the accompanying descriptions. APPL-1006, 7:1-16 (discussing FIG. 4 including “Application 404 initiates the

user authentication process by **displaying** a request 408 for the user to provide their fingerprint (in the case of a fingerprint sensor).”); 7:17-24 (discussing FIG. 5 including “example user login interface 502 **displayed**...”). POSITA would understand prompts that are “displayed” are *visually presented*. APPL-1003, ¶126.

Thus, Kesanupalli discloses “*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.*”

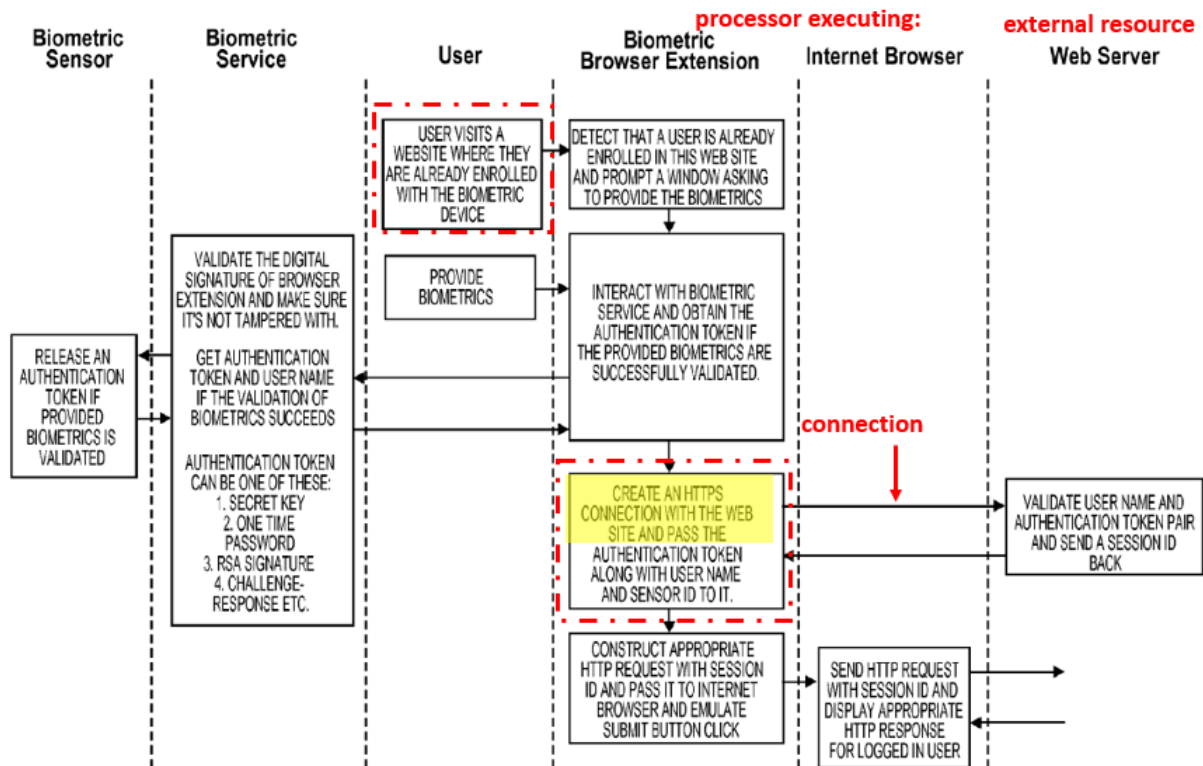
[1.6] [wherein the processor on the device is configured to:] establish a connection with the external resource;

Kesanupalli discloses or renders obvious this limitation. APPL-1003, ¶¶128-132.

As described above with reference to limitation [1.1], POSITA would understand Kesanupalli to describe the devices, circuits and/or processing cores that constitute or render obvious the *processor on the device* including the functionality that the processor is configured to perform. That functionality described relative to limitation [1.6].

In Kesanupalli, the processor on the device *establishes a connection with the external resource* (e.g., connects to the website). In particular, a connection is provided between the application executing on the processor circuitry and the web server of the website. APPL-1006, 2:54-3:3 (an application is “capable of communicating with one or more web servers or similar devices via the Internet or

other data communication network”), 4:36-5:63, 6:11-49, 7:67-8:4, 9:58–10:1. In particular in the device of FIG. 2, based on the user’s request to access the website, application 214 establishes a *connection*, via the Internet, with a web server of the website. APPL-1003, ¶¶130-131; APPL-1006, 6:11-31, FIG. 9, block 914. FIG. 12 is illustrative of the information provided on the connection between the processor and the web server providing the *external resource*. APPL-1003, ¶130.



APPL-1006, FIG. 12, annotated

Kesanupalli describes the connection between the PC and the web server as a “secure communication link,” which is a *connection*. APPL-1006, 7:54-8:5, 12:62-67. *See also*, APPL-1003, ¶131 (discussing SSL/HTTP connections).

Thus, Kesanupalli discloses or renders obvious a processor configured to
“*establish a connection with the external resource.*”

[1.7] “[*wherein the processor on the device is configured to:*] *facilitate a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the credential retrieved from the at least one record, and wherein the user is logged in to the external resource based at least in part on the output; and*

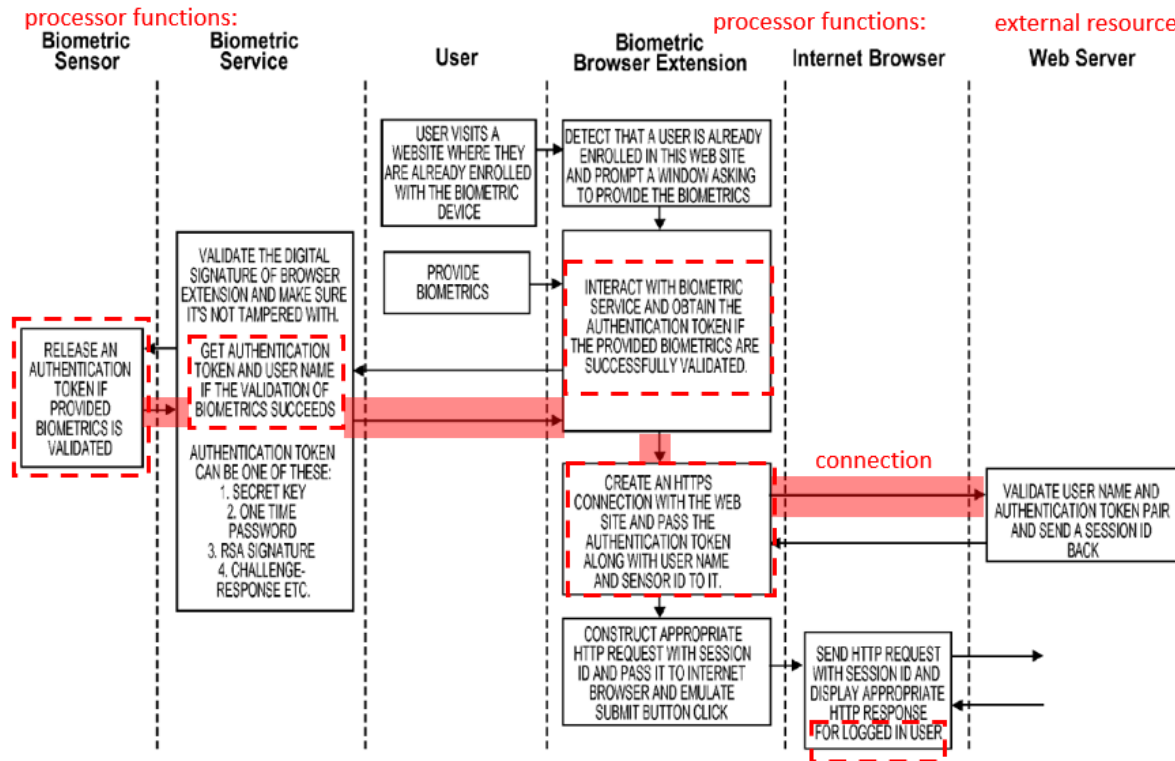
Kesanupalli discloses or renders obvious this limitation. APPL-1003,
¶¶133-138.

As described above with reference to limitation [1.1], POSITA would understand Kesanupalli to describe the devices, circuits and/or processing cores that constitute or render obvious the *processor on the device*. Kesanupalli also discloses and renders obvious the functionality, *i.e.*, the processing, that the *processor* is configured to perform, and that functionality is now described relative to limitation [1.7].

In Kesanupalli’s device, the processor *facilitates a login of the user to the external resource (e.g., website) at least in part by transmitting, via the established connection (e.g., connection between PC 202 (application 214) with the web server), output (e.g., the user credential) based at least in part on the credential retrieved from the at least one record*. First, Kesanupalli describes its processor performs *transmitting output* (the user credential itself) to the external resource (website). APPL-1006, 9:10-24 (“If the fingerprint information is authenticated,

the procedure **retrieves credentials** associated with the user based on the fingerprint information (block 908)...The decrypted credentials...are **communicated to a requesting process or system** (block 914).” *See also*, APPL-1006, 9:4-9. In particular, in the device of FIG. 2, the user credential (*e.g.*, cryptographic key) is retrieved from the secure storage 206 and provided to application 214 for communication to the external resource. APPL-1006, 6:11-49. As discussed in limitation [1.6], a *connection* is established between the device (application of PC 202) and the external resource. The application of PC 202 communicates the decrypted credential to the website via this *established connection*. *See* APPL-1006, 4:1-11, 4:51-63, 5:59-6:25 discussing application 112 which is substantially the same as application 214 of FIG. 2.

FIG. 12 annotated below illustrates transmitting user credentials to an external resource. APPL-1003, ¶135.



APPL-1006, FIG. 12, annotated

Kesanupalli's transmitting the decrypted user credential is *transmitting...output based at least in part on the at least one the password or the cryptographic key retrieved from the record* as Kesanupalli transmits output of the (decrypted) user credential (cryptographic key).

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

1003, ¶137 (citing APPL-1006, 5:22-24, FIG. 12 (“logged in user”)).

Thus, Kesanupalli discloses or renders obvious a processor configured to *“facilitate a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the credential retrieved from the at least one record, and wherein the user is logged in to the external resource based at least in part on the output.”*

[1.8] *[wherein the processor on the device is configured to:] facilitate wiping of both the biometric template and the credential comprising the cryptographic key of the at least one record stored at least in part in the storage on the device; and*

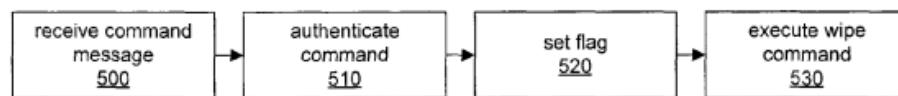
Kesanupalli and Brown render obvious this limitation. APPL-1003, ¶¶139-148.

As described above with reference to limitation [1.1], POSITA would understand Kesanupalli to describe the devices, circuits and/or processing cores that constitute or render obvious the *processor on the device*. Kesanupalli also discloses and renders obvious the functionality, *i.e.*, the processing, that the *processor* is configured to perform includes that of limitation [1.8]. *See also*, the discussion below regarding the applied teachings of Brown.

As discussed above, 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. It would have been obvious for the processor 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 in light of the teachings of Brown.

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 a 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, zeroes, or a random arrangement of ones and zeros over the data to be wiped.”) Teaching of overwriting all data of a client device is a teaching

of overwriting the data including a biometric template and user credential in the client device of Kesanupalli. APPL-1003, ¶144. Benefits of wiping all data are readily recognizable for protection of all data for example when repurposing the client device. APPL-1003, ¶144.

To the extent the Patent Owner argues the wiping must be particularized to the recited elements, in addition to examples in Brown deleting all data from the device, Brown describes selective wiping of data. APPL-1009, Abstract, 2:18-35, 13:15-24. POSITA would recognize that *the biometric template and the credential comprising the cryptographic key* of Kesanupalli are just the type of personal data Brown suggests identifying for selectively wiping. APPL-1003, ¶¶145. This is because the biometric template and credential are stored personal data related to the security functions of the device and Brown suggest its procedure applies to personal data such as security functions and encryption keys of a user's device. *Id.*; APPL-1009, 3:12-18 (“The data types may comprise at least one of an operating system, **encryption and decryption keys...**”), 1:20-34 (“The data may further include applications, or data files created at the device or received by an authorized user at the device that are **personal to the user**, or that are used by the device for the management of data and/or **security functions on the communication device.**”) Thus, POSITA would have had reason to apply Brown's teachings to selectively wipe the user's biometric template and credential

comprising the cryptographic key as Brown has a recognized desire to keep such personal data protected from access by unauthorized or malicious users. APPL-1003, ¶¶146, 75, 79-81.

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 circuitry executing the functions of sensor 204 has access to the record in the storage on the device to facilitate the wiping of Brown; and the processor circuitry (*e.g.*, executing application 214) receives communication. APPL-1003, ¶147.

Thus, Kesanupalli in view of Brown renders obvious “[*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.*”

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

Kesanupalli discloses this limitation. APPL-1003, ¶¶149-152.

Kesanupalli's system includes a main memory, a *memory*. APPL-1006, 9:58-10:46 ("Main **memory** is also usually included for storing and retrieving larger amounts of information such as data and software applications configured to perform functions according to the invention when executed by the central processing unit."). POSITA would understand that the main memory of Kesanupalli's system is coupled to the *processor* and configured to provide the processor with *instructions* including at least those that execute the functions of Host PC 202. APPL-1003, ¶151.

Thus, Kesanupalli discloses "*a memory coupled to the processor and configured to provide the processor with instructions.*"

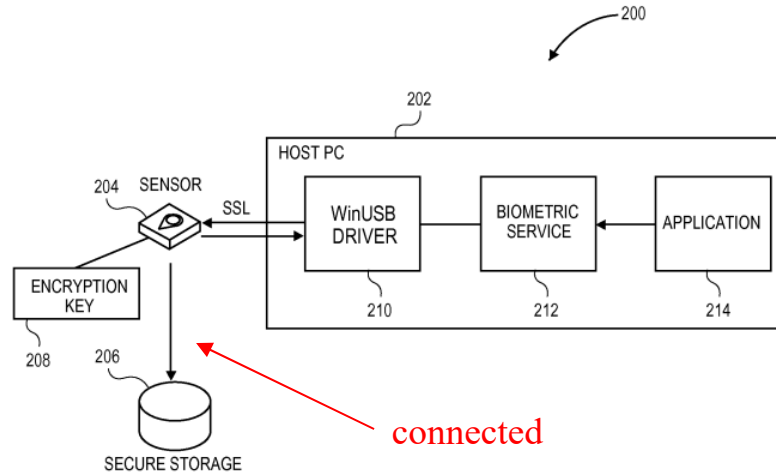
Therefore, claim 1 is obvious over Kesanupalli and Brown. APPL-1003, ¶153.

5. Claim 2

[2.0] *The device recited in claim 1 wherein the storage is connected to a sensor.*

As explained above, Kesanupalli and Brown render obvious claim 1. Kesanupalli discloses the further limitation of claim 2. APPL-1003, ¶¶154-156.

Kesanupalli's secure storage 206 is connected to sensor 204. *See* APPL-1006, FIG. 2, 6:42-47.



APPL-1006, FIG. 2, annotated

Therefore, claim 2 is obvious over Kesanupalli and Brown.

6. Claim 3

[3.0] *The device recited in claim 2 wherein the sensor comprises at least one of a camera and a fingerprint reader.*

As explained at [2.0], Kesanupalli and Brown render obvious claim 2.

Kesanupalli discloses the further limitations of claim 3. APPL-1003, ¶¶157-159.

Kesanupalli describes, in an example, the biometric input of a fingerprint is provided by a fingerprint sensor, which is a *fingerprint reader*. APPL-1003, ¶158; APPL-1006, 2:39-53.

Therefore, claim 3 is obvious over Kesanupalli and Brown.

7. Claim 7

[7.0] *The device recited in claim 1 wherein facilitating wiping of the at least portion of the at least one record comprises facilitating remote wiping of the at least portion of the at least one record*

As explained above, Kesanupalli and Brown render obvious claim 1.

Kesanupalli and Brown also render obvious the further limitation of claim 7. APPL-1003, ¶¶160-163.

Continuing with the discussion of the teachings of Brown as applied to Kesanupalli above in claim 1, Brown describes facilitating the wiping of the record by facilitating a *remote wiping*. Brown discloses that its command to wipe a device “may be received over the air.” APPL-1009, 2:63-3:6. For example, the “wipe command may be carried out at the server” (server 40), which is remote from the client device (10, 100) and sends the command “over the air.” APPL-1009, 11:65-12:21, FIG. 1, 12:28-35 including (“If the **command is received from the server 40, in one embodiment it is received over the air**; for example, a mobile communication device 100 may receive via the transceiver 411 (shown in FIG. 2) an incoming message from **a remote location** comprising a command at step 500...”)

The ’138 patent does not define “remote wiping;” however, under the heading of “Remote wiping,” the ’138 patent provides an example of “self-wipes” of a device. APPL-1001, 8:35-38. To the extent Patent Owner argues remote wiping is self-wiping, Brown similarly discloses this describing when a user enters a password incorrectly a predetermined number of times, the wiping command self-executes at the device. APPL-1003, ¶162; APPL-1009, 12:6-15.

Therefore, claim 7 is obvious in view of Kesanupalli and Brown.

8. Claim 8

[8.0] *The device recited in claim 1 wherein the at least portion of the at least one record is automatically wiped based at least in part on a policy.*

As explained above, Kesanupalli and Brown render obvious claim 1. Kesanupalli and Brown also render obvious the further limitation of claim 8. APPL-1003, ¶¶164-167.

Brown provides a *policy*, which is stored in the client device and defines rules for wiping. APPL-1009, Abstract (“**Based on at least one predefined rule, which may be implemented in an IT policy stored at the client device**, each of the plurality of data types to be secured is determined, and then the data corresponding to those types is secured. The **data may be secured by** encrypting and/or **deleting the data** at the client device.”) *See also*, APPL-1009, 16:40-45, 1:56-59, 11:22-31, FIG. 3 including IT policies 315, FIG. 4a, FIG. 4b. The policy may include various predefined rules related to a wipe including which data is *automatically* wiped on receipt of the wipe command. APPL-1003, ¶165, APPL-1009, 14:20-28. *See also*, APPL-1009, 15:46-49, 16:40-45, FIGS. 8a, 8b.

Brown also describes predefined rules for predetermined actions, which are themselves a *policy*, that trigger execution automatic wiping of the client device. In an example, Brown describes implementing a policy of an automatic wiping if a predetermined action of entering a password incorrectly too many times occurs “The wipe command may alternatively be invoked by...engaging in a

predetermined action at the client device 10, 100, such as entering a password incorrectly for a predetermined number of times.” APPL-1009, 12:6-15.

Therefore, claim 8 is obvious in view of Kesanupalli and Brown.

9. Claim 12

[12.0] *The device recited in claim 1, wherein the storage comprises a secure storage.*

As explained above, Kesanupalli and Brown render obvious claim 1. Kesanupalli also discloses the further limitation of claim 12. APPL-1003, ¶¶168-171.

As shown in limitation [1.2] above, Kesanupalli provides the recited storage, which is a *secure storage*, in its secure storage 206. *See* APPL-1006, FIG. 2, 6:45-49. A *secure storage* is storage protected from unauthorized use. APPL-1003, ¶170. By describing its storage as “secure storage,” POSITA would understand Kesanupalli to be providing storage protected from unauthorized use. APPL-1003, ¶170. As illustrated by Kesanupalli’s FIG. 2, use of secure storage 206 is controlled by sensor 204, and the secure storage is not directly accessible by others (*e.g.*, application 214 executing on Host PC 202); for example, the user credential in the storage cannot be accessed except by sensor 204 when verifying a match of biometric input as discussed in limitation [1.5A]. Therefore, secure storage 206 is *secure storage*. APPL-1003, ¶170.

Thus, claim 12 is obvious over Kesanupalli and Brown.

10. Claims 13–15, 19 and 24

Claims 13-15, 19 and 24 are obvious over Kesanupalli and Brown. APPL-1003, ¶¶172-175. The limitations of independent claim 13, except its preamble, are substantively identical to limitations already addressed above, as correlated in the table below.

Claim 13 Limitation	Corresponding Claim Limitation of Claim 1 illustrating that the limitation is disclosed in Kesanupalli and/or Brown
[13.1a] <i>based at least in part on a request from a user to access an external resource, using a processor on a device to facilitate access of at least one record stored at least in part in a storage on the device, wherein the storage on the device 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;</i>	[1.1], [1.2], [1.3]
[13.2] <i>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;</i>	[1.4]
[13.3a] <i>in response to determining a match between a biometric input and the biometric template, retrieving, 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,</i>	[1.5A]

[13.3b] <i>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;</i>	[1.5B]
[13.4] <i>establishing a connection with the external resource;</i>	[1.6]
[13.5] <i>facilitating 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</i>	[1.7]
[13.6] <i>facilitating, by the processor on the device, 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.</i>	[1.8]

[13.0] *A method, comprising:*

To the extent the preamble is limiting, Kesanupalli and Brown disclose it. APPL-1003, ¶173. The citations to Kesanupalli and Brown above apply to a *device* as in claim 1 and also to a *method*. APPL-1006, 2:30-38 (“The systems and methods described herein relate to biometric authentication of users...”); APPL-1009, Abstract (“method for selectively securing data from unauthorized access on a client device storing a plurality of data types...”), 2:18-35, FIG. 6.

Thus, claim 13 is obvious in view of Kesanupalli and Brown.

Dependent claims 14–15, 19, 22, and 24 are substantively identical

limitations to claims already addressed above but depend from method claim 13, as correlated in the table below. The combination of Kesanupalli and Brown renders obvious these claims for the same reasons discussed above with respect to claim 13 and the corresponding claims in of the table.

Claim	Corresponding Claim analyzed above illustrating the limitations are disclosed in Kesanupalli and/or Brown
[14]	[2]
[15]	[3]
[19] ³	[7]
[24]	[12]

11. Claim 25

Claim 25 is obvious over Kesanupalli and Brown. APPL-1003, ¶¶176-179. The limitations of claim 25, except its preamble, are substantively identical to limitations already addressed above, as correlated in the table below:

³ Claim 19 has a preamble of a “method” but purports to depend from Claim 12, which is a device claim. Whether Claim 19 is directed to a method, or a device, it is obvious over Kesanupalli and Brown for the reasons discussed in the analysis for Claim7.

Claim 25 Limitation	Corresponding Claim Limitation illustrating Claim 25 is disclosed in Kesanupalli and/or Brown
[25.1] <i>based at least in part on a request from a user to access an external resource, using a processor on a device to facilitate access of at least one record stored at least in part in a storage on the device, wherein the storage on the device 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;</i>	[1.1], [1.2], [1.3]
[25.2] <i>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;</i>	[1.4]
[25.3a] <i>in response to determining a match between a biometric input and the biometric template, retrieving, 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,</i>	[1.5A]
[23.3b] <i>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;</i>	[1.5B]
[24.4] <i>establishing a connection with the external resource;</i>	[1.6]
[25.5] <i>facilitating 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</i>	[1.7]

<i>at least one record, and wherein the user is logged in to the external resource based at least in part on the output; and</i>	
<i>[25.6] facilitating, by the processor on the device, 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.</i>	[1.8]

[25.0] *A computer program product embodied in a non-transitory computer readable storage medium and comprising computer instructions for:*

To the extent this preamble is limiting, Kesanupalli discloses it. APPL-1003, ¶¶177-178.

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.”)

Thus, claim 25 is obvious over Kesanupalli and Brown.

B. Ground 2: Claims 10 and 22 are obvious under 35 U.S.C. §103(a) over Kesanupalli and Brown further in view of Cheng.

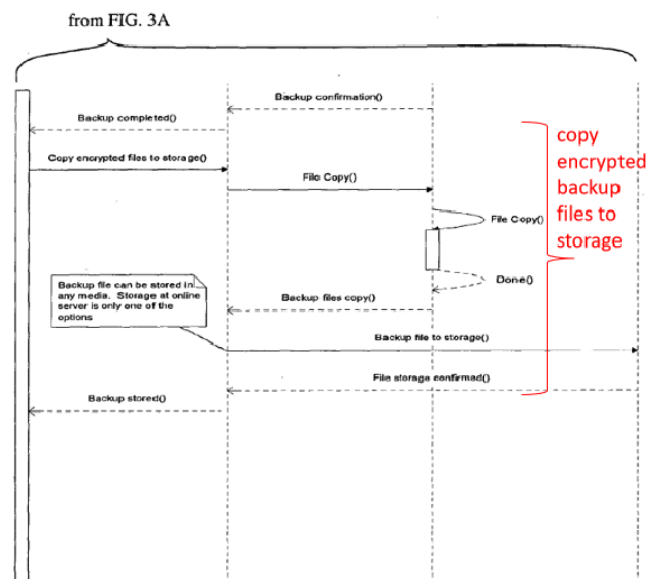
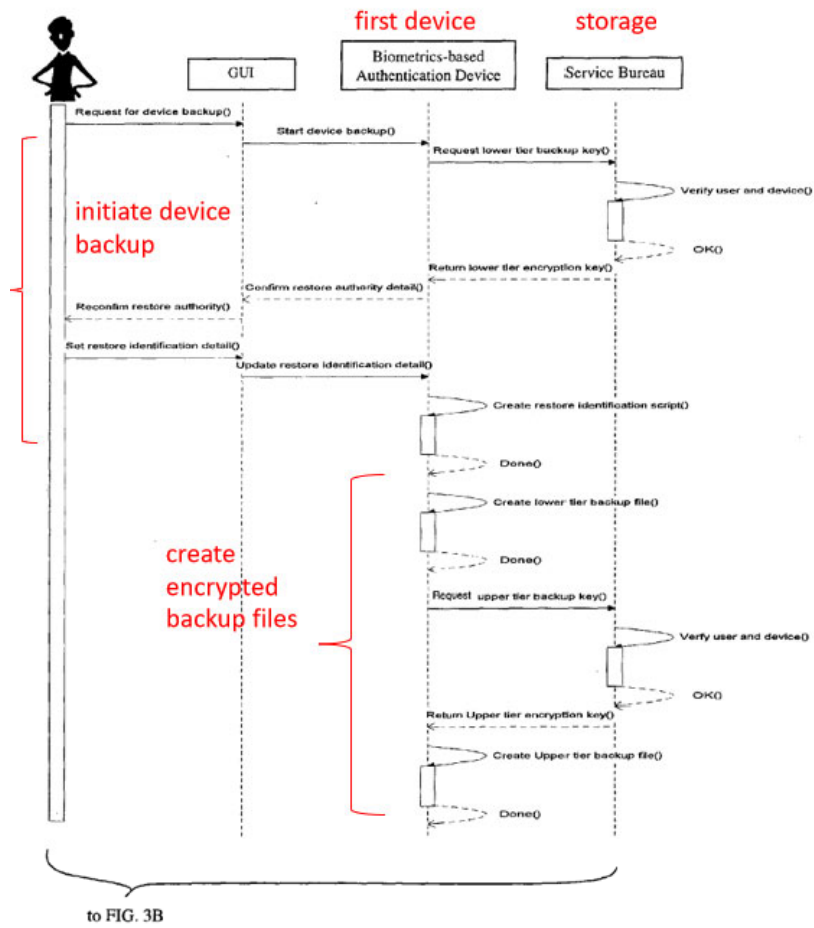
1. Cheng

Cheng is entitled “System, Method and Apparatus for Secure Two-Tier Backup and Retrieval of Authentication Information” and provides ways to “securely backup and restore” a user’s authentication-based device without compromising the security thereof. APPL-1008, (54), Abstract. *See* APPL-1003, ¶¶180-183.

Cheng recognizes “[w]ith the rapid growth of computers, electronics, communications, networks, and the Internet, access control in general and network security in particular have become increasingly important for obvious reasons.” APPL-1008, [0003]. “Data, property interests, personal identity as well as personal safety could be at risk if security is breached” and to satisfy security needs, authentication systems, methods, and devices are needed to “certify the validity of an identity, account, object, and so on.” *Id.* According to Cheng, “[b]iometrics-based authentication” is commonly implemented, which leads to portable devices that include “user’s authentication information, electronic identity and any data associated therewith.” APPL-1008, [0004], [0006].

Cheng performs a secure backup of this data to avoid costs of registering a new device from scratch should a first device containing the data be lost or stolen.

See APPL-1008, Abstract, [0006]. An exemplary backup process is illustrated in Cheng's FIGS. 3A-3B where a backup of data of a first user's device is performed through secure communication between a user service bureau and the device. APPL-1008, [0029]-[0030]. Cheng's backup process includes a two-tier encryption of the backed-up data. APPL-1008, [0031]-[0039].



APPL-1008, FIG. 3A – 3B, annotated

2. Reasons to Combine Kesanupalli, Brown and Cheng

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. APPL-1003, ¶¶184-188. Kesanupalli’s device having stored biometric information and credentials, which are a user’s personal data, with Cheng’s back-up teachings applied 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.*

First, like Kesanupalli, Brown and the ’138 patent as discussed above, Cheng is also analogous art and in the same field of endeavor—namely, security arrangements and procedures for protecting data in computer systems. *See supra* Section IX.A.3 (Combination of Kesanupalli and Brown); APPL-1008, [0002], [0003]. Cheng is directed to handling of personal data of a computer system in a secure manner that protects the data from trespassers and security attacks. APPL-1008, [0003], [0004] (“Data, property interests, personal identity as well as personal safety could be at risk if security is breached. To satisfy different security needs, various authentication systems, methods, and devices exist today and new ones are continually being developed.”). Like Kesanupalli, Brown, and the ’138 patent, Cheng is also similarly directed to protection of a user’s authentication data

in particular. APPL-1008, [0004], [0007] (“The present invention provides new ways to **securely backup** and restore a user’s **authentication information**, electronic identity and any data associated therewith, without comprising the security thereof.”); APPL-1006, FIG. 2, Abstract; APPL-1009, 1:15-2:8; APPL-1001, 2:40-59. And Cheng relies on “enabling technologies” that are just like those of Kesanupalli, Brown and the ’138 Patent. APPL-1008, [0007] (“Enabling technologies include biometrics, authentication, cryptography, and encryption/decryption.”) APPL-1003, ¶185.

Second, POSITA would have been motivated to employ Cheng’s backup procedure in connection with Kesanupalli’s secure authorization system including Brown’s wiping technique because POSITA would recognize that while Kesanupalli-Brown has a benefit of wiping data to preserve security, wiping data risks losing the deleted data. APPL-1003, ¶¶186-187; APPL-1008, [0006]. POSITA would have understood this deletion of the user’s personal data raises cost and inconvenience to the user. *Id.* Such a problem would also have been reasonably pertinent to the inventors of the challenged patent. APPL-1001, 8:38-41 (“user data can be frequently backed up []and recovered from this...[and] inconvenience to the user will be minimized.”). After recognizing this same problem, Cheng provides a solution to backup data. APPL-1008, [0007]. Thus, not only were Kesanupalli, Brown, Cheng and the ’138 patent in the same field of

endeavor, but Cheng would have been reasonably pertinent to a problem faced by the inventors of the '138 patent and pertinent to known risks of loss of devices and data such that POSITA would have been motivated to address the preservation of data in the Kesanupalli-Brown combination by implementing the teachings of Cheng. APPL-1003, ¶187.

In particular, Cheng teaches backing up of biometric information and secret keys. APPL-1008, [0007]–[0009]. 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. *See* APPL-1008, [0006]–[0007]. Moreover, POSITA would have recognized a capability and desire for secure data to be capable of being backed-up long before the '138 patent. APPL-1003, ¶187.

Finally, POSITA would have had reasonable expectations of success in adding a backup procedure such as taught by Cheng in a biometric authentication system such as taught by Kesanupalli in view of Brown, as Cheng is similarly directed to improving security of personal information. APPL-1008, [0022]. Adding a 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.*

3. Claim 10

[10.0] *The device recited in claim 1 wherein the at least portion of the at least one record is backed up to a remote entity.*

As explained above, Kesanupalli and Brown render obvious claim 1. Kesanupalli, Brown and Cheng render obvious the further limitation of claim 10. APPL-1003, ¶¶189-193.

Cheng discloses data is *backed up to a remote entity* such as an internet-based storage service. APPL-1008, [0029] (“The **storage means could be, for instance, an online proprietary or Internet-based storage service, a remote server...capable of storing data.**”) *See also*, APPL-1008, FIGS. 3A, 3B, [0023]–[0028] (describing a method culminating in “(e) **storing** the encrypted [] backup file...on a **storage means.**”)

POSITA would have applied Cheng's teachings of its backup process to a remote entity to the data of Kesanupalli's device in general and in particular to backup Kesanupalli's *record*. APPL-1003, ¶¶191-192. This is because not only does Cheng generally suggest the back-up of data of an electronic device, but also provides specific examples of data that is backed-up including a private key and biometric data, which is just like the data of the record of Kesanupalli discussed

above. APPL-1003, ¶191; APPL-1008, [0030] (“In a preferred embodiment, the **lower tier authentication data include private keys, certificates, and other data held within the device.** In this embodiment, the upper tier authentication data include the user's **biometrics** information.” *See also*, APPL-1008, [0008] (“The lower tier data contain encrypted electronic identity such as private keys and associated certificates. The upper tier data contain the encrypted lower tier data, restore validation script, and biometrics data.”)).

Thus, POSITA would have been motivated to use Cheng’s method to back-up, to a remote entity, *the at least one record* of Kesanupalli as discussed in the reasons to combine above including to recognize the benefits of, “[i]n the event of loss, damage, or destruction of the device,” avoiding cost and inconvenience of the user to create and register new templates and keys when erased as taught by Brown’s security procedures applied to Kesanupalli. *See* APPL-1008, [0006]; APPL-1003, ¶192.

Thus, claim 10 is obvious over Kesanupalli, Brown and Cheng.

4. Claim 22

[22.0] *The method of claim 13 wherein the at least portion of the at least one record is backed up to a remote entity.*

As explained above, Kesanupalli and Brown render obvious claim 13; Kesanupalli, Brown and Cheng render obvious the further limitation of claim 22. APPL-1003, ¶194.

In particular, for the same reasons as discussed with respect to claims 10 and 13, claim 22 is rendered obvious by Kesanupalli in view of Brown and Cheng.

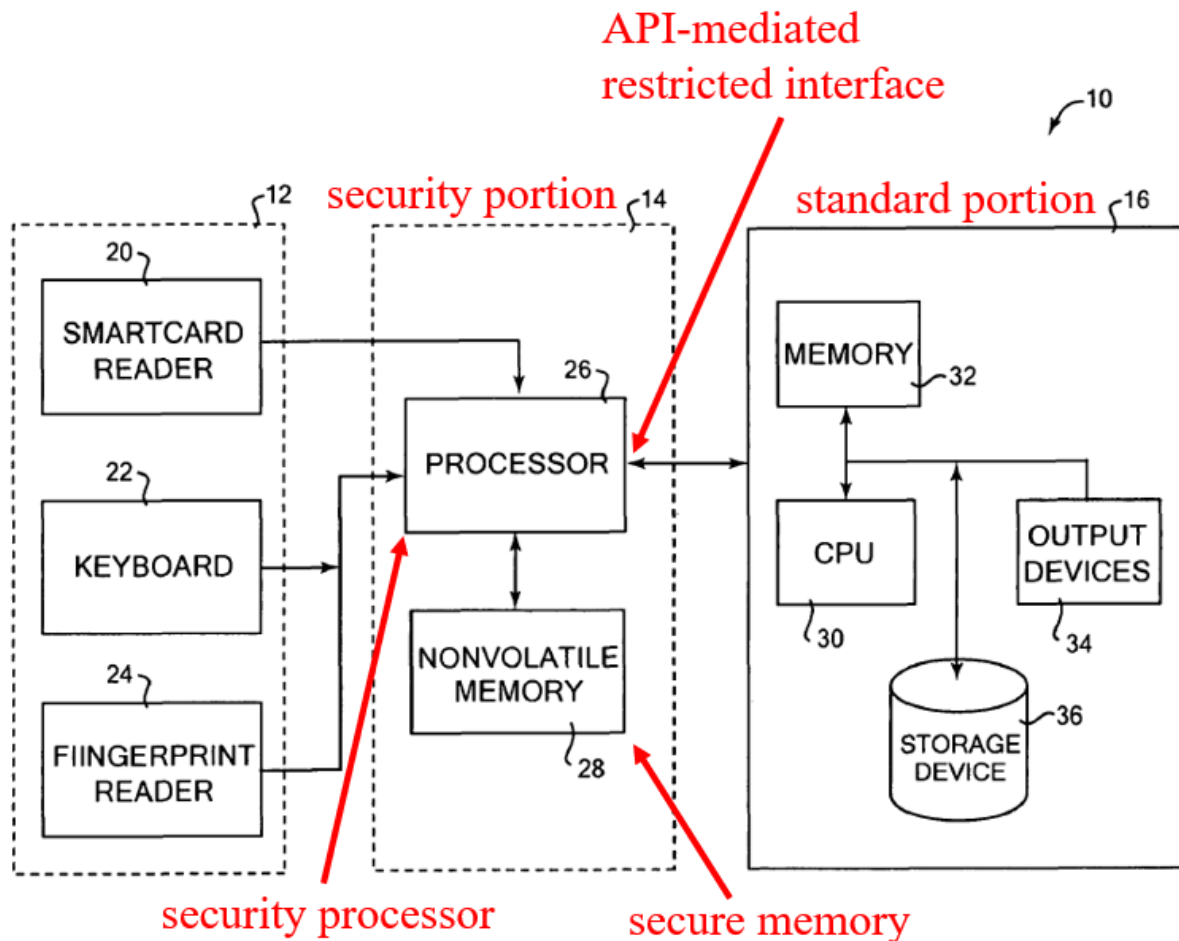
C. Ground 3: Claims 11 and 23 are obvious under 35 U.S.C. §103(a) over Kesanupalli and Brown further in view of Challenger.

1. Challenger

Challenger “relates to securely protecting computer data, and more particularly to security processors provided in computer systems to implement security features.” APPL-1007, 1:7-9, 3:24-26. Challenger illustrates a system 10 (*e.g.*, computer or electronic device) with a system architecture suitable for securing data and functions of system 10 from unauthorized access and manipulation. APPL-1007, 3:37-56. In particular, Challenger describes system implementations in accord with a well-known Trusted Platform Module (TPM) specification promulgated by a standards organization, the Trusted Computing Group (TCG). *See* APPL-1007, 3:51-56. As explained in Challenger, in accord with the TPM specification, a standard chipset including a programmable microcontroller can be provided and used to store and secure information of the system that is desired to be protected. APPL-1003, ¶¶195-197, 51-54.

Broadly speaking, TPMs provide a platform for effective trusted computing features by implementing an architecture where security functions are performed separately from general functions. APPL-1003, ¶196. The security portion of the architecture (*e.g.*, the processor “functions and the application program interface

(API”) that run on the processor) can be referred to as a TPM. *Id.*, APPL-1006, 1:25-27. A TPM provides security features including an API-mediated interface between secure and insecure components, random number and cryptographic key generation, and facilities to limit use of stored keys, *e.g.*, to signing and verification, and/or encryption and decryption. APPL-1007, 1:18-31; APPL-1003, ¶196; APPL-1017 (TPM standard describing API mediated restricted interface).



APPL-1007, FIG. 1, annotated

Challenger provides an implementation framework for systems, which may

be TPM-based, and including an input portion 12, a security portion 14, and a standard portion 16. *See* APPL-1007, 3:46-57. Security portion 14 includes a dedicated security processor 26 (implementing a TPM) and a memory 28 used to secure data and applications of the system for access and use only by authorized users. APPL-1007, 4:9-65. Memory 28 “is a secure memory which cannot be easily tampered with to read its data contents” and can be on the same chip or package as processor 26. *Id.* The standard portion 16 is connected to the security processor 26 (via an API-mediated interface) and includes a microprocessor 30 that controls general operation of the system including input/output functions. APPL-1007, 5:15-25.

2. Reasons to Combine Kesanupalli, Brown and Challener

POSITA would have been motivated to apply Challener’s teachings of a TPM-type security architecture (with API-mediated interfaces to secure functions and data) in implementations of Kesanupalli’s secure user authentication techniques with Brown’s selectively wiping of sensitive data teachings. APPL-1003, ¶¶198-202. The combination would have produced the obvious, beneficial, and predictable results of a standardized and widely-deployed security architecture for implementation of Kesanupalli and Brown’s techniques as discussed below. *Id.*

First, Challener, Kesanupalli, Brown and the ’138 patent are analogous art and are all in the same field of endeavor—namely, information security, and more

particularly, security arrangements for protecting computers, components thereof, programs or data against unauthorized activity. APPL-1007, 1:7-9 (“The present invention relates to securely protecting computer data, and more particularly to security processors provided in computer systems to implement security features.”), 3:52-56 (“Trusted Platform Module (TPM)...for securing data and functions of the system [] from unauthorized access and manipulation.”); *see also supra* Section IX.A.3 (reasons to combine Kesanupalli and Brown). Moreover, Challenger bears the very the IPC subclass—CPC/IPC G0F6 21 as discussed above relative to Kesanupalli, Brown and the ’138 patent. APPL-1007, (51); *see also, supra* Section IX.A.3.

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

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

Finally, 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. APPL-1003, ¶202. *See* APPL-1007, 1:18-31.

3. Claim 11

[11.0] *The device recited in claim 1, wherein the interface comprises a restricted interface.*

As explained above in Ground #1, Kesanupalli and Brown render obvious claim 1. Kesanupalli, Brown and Challener render obvious the further limitation of claim 11. APPL-1003, ¶¶203-210.

As explained above relative to limitation [1.2], Kesanupalli discloses an interface that facilitates communication between secure storage 206 and processor circuitry of sensor 204. In view of Challener, it would have been obvious to provide a restricted interface as *an interface that facilitates communication between the storage on the device and the processor on the device* (limitation

[1.2]).

As discussed above, POSITA deploying the security functions of Kesanupalli's sensor 204 would have been motivated to implement those functions on Challenger's TPM-based security architecture using specialized security processing circuitry such as illustrated by Challenger's security processor 26. APPL-1003, ¶¶200-205 (explaining the mapping of secure portion functions of Kesanupalli's system to a corresponding secure portion of the TPM framework implemented by Challenger); APPL-1007, 4:9-24, FIG. 1. As detailed below, Challenger's interfaces with and within the secure portion of its architecture are *restricted interface[s]*.

POSITA would have been motivated to implement the functionality of sensor 204 of Kesanupalli using Challenger's teachings of providing secure processor functions (26) and Kesanupalli's secure memory 206 using Challenger's corresponding secure memory, non-volatile memory 28. *See supra* Section IX.C.2.; APPL-1003, ¶¶200-202, 204-205; APPL-1007, 4:57-65 (“memory 28 is a secure memory which cannot be easily tampered with to read its data contents. In some embodiments, the nonvolatile memory 28 can be included on the same integrated circuit chip [] of the processor 26.”) As construed above (*see supra* Section VI.B), a “*restricted interface*” is an interface that limits accessibility. POSITA would have recognized that secure processor 26 communicates with its

on-chip secure memory 28 using a *restricted interface* because the interface therebetween limits secure storage access to just security processor 26—other components such as those of the standard portion do not access memory 28 except through processor 26. APPL-1003, ¶205; *see* APPL-1007, FIG. 1.

As also discussed in Section VI.B, *supra*, the '138 patent discusses the restricted interface only in terms of an API. To the extent that the Patent Owner argues the configuration above is insufficiently restricted, Challenger also teaches implementing API-mediated interfaces. Based on the '138 patent's limited description, POSITA would understand "*restricted interface*" to at least include an API that limits accessibility to a secure storage, a fingerprint sensor, or dedicated processor. *See supra* Section VI.B; APPL-1003, ¶¶206, 57-60. In particular, for the Kesanupalli and Brown combination (implemented using Challenger's TPM framework for secure systems), communication between the security portion (sensor 204 and memory 206) and the standard portion (PC 202) occurs through an API-mediated interface, a *restricted interface*, as detailed below. APPL-1003, ¶¶206-209.

TPM-based implementations, including Challenger's TPM-based implementation, are widely recognized examples of a security architecture that provides a *restricted interface* in the form of an access limiting API that restricts access to the TPM (secure processor circuitry) and its secure memory by programs

running on a general processor in a standard (non-secure) portion of a system such that the general processor programs are limited from access to the security-related operations and stored data, such as key and credential management, secure storage, encryption, decryption and digital signatures that are in a secure portion of the system. APPL-1003, ¶¶207, ¶¶51-54; APPL-1024 (widespread TPM adoption). *See also*, APPL-1007, 4:3-15 discussing controlling “access.” The Board has itself recognized, in the context of the related ’696 patent, that TPM implementations disclose a “*restricted interface*.” *See* (Samsung ’696 Patent IPR) IPR2022-00244, Paper 17, 40.

In particular, Challenger describes restricted interfaces (in the form of an API) in particular relative to secure processor 26, which implements a TPM-based security architecture that includes API mediated interfaces for its communication with other components—including the general processor circuitry 30. APPL-1003, ¶¶206-209; APPL-1007, 4:9-24 (“The **processor 26 typically implements a ‘security architecture’** which, as used herein, refers to the particular security features and functions (e.g. **API functions**, algorithms) implemented for the system 10 as determined by a security architecture application loaded on the processor 26.”), FIG. 1. As a general proposition, an API is an interface that defines how two or more components communicate with one another—here software of the secure processing and the software of the general processing

portions (in Challenger processors 26 and 30 respectively). APPL-1003, ¶208. Because the API implemented by secure processor circuitry under a TPM-based architecture is an access limiting interface through which general processor circuitry must interface, it also provides the interface—indeed the *restricted interface*—for any communications between functions executing on general processor circuitry and the secure storage. *Id.*

Thus, in each of the foregoing ways, claim 11 is also obvious over Kesanupalli and Brown further in view of Challenger.

4. Claim 23

[23.0] *The method of claim 13, wherein the interface comprises a restricted interface.*

As explained above in Ground #1, Kesanupalli and Brown render obvious claim 13. Kesanupalli, Brown and Challenger render obvious the further limitation of claim 23. APPL-1003, ¶211. In particular, for the same reasons as discussed with respect to claim 11, claim 23 is rendered obvious by Kesanupalli and Brown further in view of Challenger. *Id.*

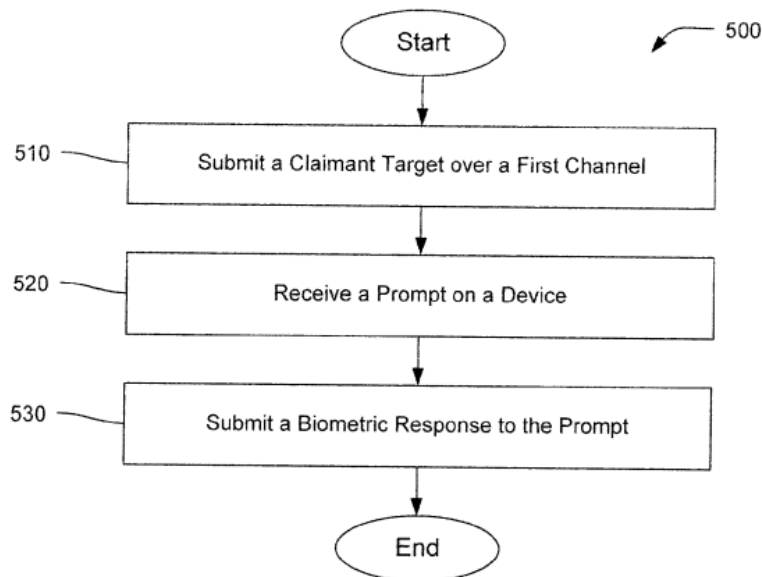
D. Ground 4: Claims 5 and 17 are obvious under 35 U.S.C. §103(a) over Kesanupalli and Brown further in view of Headley.

1. Headley

Headley is entitled “User authentication for social networks” and provides “[v]erification can be performed, for example, by reference to biometric templates stored during the user enrollment process. The biometric templates can also be

used to authenticate users logging into the social network to prevent user impersonation. APPL-1010, (54), Abstract. *See* APPL-1003, ¶212.

Headley discloses user enrollment with biometric samples (*e.g.*, fingerprint, voice, etc.). After enrollment, Headley's methods prompt a person seeking authentication to provide a biometric response. APPL-1010, 3:41-57, FIG. 5. Headley teaches that "[t]he prompt can be provided visually, **aurally** or in combination." APPL-1010, 7:48-50.



APPL-1010, FIG. 5

2. Reasons to Combine Kesanupalli, Brown and Headley

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.*

First, like Kesanupalli, Brown and the '138 patent as discussed above, Headley is analogous art and in the same field of endeavor—namely, security arrangements and procedures for protecting data in computer systems. *See supra* Section IX.A.3 (Combination of Kesanupalli and Brown); APPL-1010, 3:17-40. Headley also falls in the same class—CPC/IPC G0F6 21. APPL-1010, (51). Further, Headley describes analogous methods of initial enrollment and subsequent authentication of a user by matching a biometric input with a stored template. APPL-1003, ¶214, APPL-1010, (57); APPL-1001, 4:41-49, 5:10-19.

Second, 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.

Finally, 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.*

3. Claim 5

[5.0] *The device recited in claim 1 wherein the prompt is aurally presented.*

As explained above, Kesanupalli and Brown render obvious claim 1. Kesanupalli, Brown and Headley render obvious the further limitation of claim 5. APPL-1003, ¶¶217-218.

Headley describes providing a user's device, which may include a smart phone or PC, which presents a prompt for biometric input where the prompt is presented visually, aurally, or a combination of visually and aurally. APPL-1010, 7:39-58 ("...able to receive and render a prompt from the authentication system 110 and/or transmit a response thereto. The prompt can be provided by the second device 140 **visually, aurally, or in combination**, for example. For instance, the prompt can be displayed as a text message, a verbal command or cue, an audio clip, a video clip, etc. In some instances, the second device 140 can be used by the

claimant to provide the biometric response to the authentication system 110.”)

Headley’s suggested presentation of a visual and aural prompt for biometric input provides the benefits of presenting a prompt in more than one manner. APPL-1003, ¶¶213-218. If Patent Owner argues that the claim requires only aural presentation, Headley also teaches aural as an alternative to visual.

Thus, claim 5 is obvious over Kesanupalli, Brown and Headley.

4. Claim 17

[17.0] *The method of claim 13 wherein the prompt is aurally presented.*

As explained above, Kesanupalli and Brown render obvious claim 13. Kesanupalli, Brown and Headley render obvious the further limitation of claim 17. APPL-1003, ¶219. For the same reasons as discussed with respect to claims 5 and 13, claim 17 is rendered obvious by Kesanupalli, Brown and Headley.

X. DISCRETIONARY DENIAL IS NOT WARRANTED

The Board should not exercise its discretion under 35 U.S.C. §§314(a) or 325(d) to deny this Petition.

A. The *Fintiv*⁴ factors favor institution.

Denial would be improper based on factors in *Apple v. Fintiv*, IPR2020-00019, Paper 11 (P.T.A.B. Mar. 20, 2020) (precedential). Patent Owner asserted the '138 patent against Apple in WDTX-1-23-cv-00324 (“the Parallel District Court Proceeding”). *See supra* Section II.B.

First, this Petition presents compelling evidence of unpatentability of the Challenged Claims. *See supra* Section IX. Therefore, the Board should not deny institution based on parallel litigation. APPL-1025, 2, 4-5, 9 (Director Memo).

Second, the *Fintiv* factors weigh in favor of institution.

- Factor 1 is neutral. Apple has not yet requested a stay pending resolution of this IPR.
- Factors 2 and 5 favor institution. Although the current scheduling order projects a trial date of December 4, 2024 (APPL-1028, 4), median time-to-trial statistics for WDTX indicate 25.8 months (mid-June 2025, based on March 24, 2023 complaint). *See* APPL-1027, 8-

⁴ Apart from Apple’s showing that *Fintiv* favors institution, the *Fintiv* framework should not be followed because it is legally invalid. The framework (1) exceeds the Director’s authority, (2) is arbitrary and capricious, and (3) was adopted without notice-and-comment rulemaking.

9 (median time-to-trial, generally) APPL-1027, 37 (WDTX statistics).

Here, final written decision is due July 2025. Per the Director's Memo, PTAB will weigh factor 2 against exercise of discretion "if the median time-to-trial is around the same time or after the projected statutory deadline for the PTAB's final written decision." APPL-1025,

9. Inefficiency concerns are minimal.

- Factors 3 and 4 favor institution: The Parallel District Court Proceeding is in its early stages. Preliminary contentions have been served, a Markman hearing was held December 12, 2023, and fact discovery just opened. At the hearing, the Court indicated that it was adopting preliminary constructions and denied Apple's motion for transfer to NDCA, though no written order has issued. Preliminary constructions apply plain and ordinary meaning. APPL-1026, 1-2. This Petition is not duplicative because it challenges claims 2-3, 5, 14-15 and 17 which are not asserted in the Parallel District Court Proceeding. *See* APPL-1029, 2. Moreover, Apple stipulates that, if the Board institutes trial, it will not pursue the same grounds raised in this Petition in the Parallel District Court Litigation. *See Sand Revolution II, LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24 at 7 (June 16, 2020). The stipulation

reduces any overlap and mitigates concerns of duplicative efforts or potentially conflicting decisions.

- Factor 6 favors institution in view of compelling evidence of unpatentability of the Challenged Claims.

In short, *Fintiv* factors are either neutral or weigh in favor of institution.

B. The Board should not deny under *General Plastic*

The '138 patent has not been challenged in any prior IPR petition, so none of the *General Plastic* discretionary institution factors apply to this Petition. *See General Plastic Indus. Co., Ltd. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19 at 16 (PTAB Sept. 6, 2016) (Section II.B.4.i. precedential).

C. *Advanced Bionics* Test Favors Institution.

In determining whether to institute an IPR, the Board may consider whether “the same or substantially the same prior art or arguments previously were presented to the Office.” §325(d); *Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6, 7 (PTAB Feb. 13, 2020).

Relative to the first prong of *Advanced Bionics*, Petitioner acknowledges that *another* Kesanupalli reference was “previously presented to the Office.” More specifically, U.S. Patent Pub. 2011/0138450, naming Kesanupalli. The reference APPL-1006/Kesanupalli, relied upon herein is not the Kesanupalli '450 publication

(or counterpart thereof), although there is some overlapping disclosure. However, none of Brown, Challenger nor Cheng were before the Office during prosecution. Therefore, under the *first prong*, neither substantially the same art nor substantially the arguments were presented to the Office. *See Thorne Research, Inc. v. Trustees of Dartmouth College*, IPR2021-00491, Paper 18 at 7-9 (PTAB Aug. 12, 2021). Moreover, portions of APPL-1006/Kesanupalli, relied upon here to show the claimed recitation of the “prompt is visually presented” are not present in the Kesanupalli ’450 publication at (56) of the ’138 patent. *See* Section IX.A.4.[1.5B] discussing APPL-1006/Kesanupalli, FIGS. 4, 5. This limitation was added by amendment during prosecution, and in response the claims were allowed. *See* Section III.B.

XI. CONCLUSION

Petitioner has established a reasonable likelihood that Challenged Claims of the ’138 patent are unpatentable, and requests institution of *inter partes* review.

Respectfully submitted,

Dated: January 19, 2024

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

XII. CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. §42.24, the undersigned attorney for Petitioner declares that the argument section of this Petition (Sections I and III–XI) has 13,938 (less than 14,000) 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) and 37 C.F.R. § 42.105, service was made on Patent Owner as detailed below.

Date of service January 19, 2024

Manner of service FEDERAL EXPRESS

Documents served Petition for *Inter Partes* Review, including Exhibit List; Exhibits APPL-1001–APPL-1004, APPL-1006–APPL-1010, APPL-1012–APPL-1020, and APPL-1022–APPL-1029

Persons served VAN PELT, YI & JAMES LLP
1 1st ST, STE 12
LOS ALTOS, CA 94022
UNITED STATES

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