Trials@uspto.gov
571-272-7822

Paper : 21
Date: October 14, 2025

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
VERIZON CORP. SERVS. GRP. INC., T-MOBILE USA, INC.,
AT&T SERVS., INC., AT&T MOBILITY LLC, and AT&T CORP.,
Petitioner,

v.

HEADWATER PARTNERS I LLC,
Patent Owner.

IPR2024-00809
Patent 9,198,042 B2

Before HYUN J. JUNG, STEPHEN E. BELISLE, and RUSSELL E. CASS, *Administrative Patent Judges.*

JUNG, *Administrative Patent Judge*.

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

AMAZON-1010
Amazon.com Services LLC v. Headwater Research LLC, IPR2027-00015

I. INTRODUCTION

We have jurisdiction under 35 U.S.C. § 6 (2024). This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73 (2023). For the reasons that follow, we determine that Cellco Partnership d/b/a Verizon Wireless, Verizon Corp. Servs. Grp. Inc., T-Mobile USA, Inc., AT&T Servs., Inc., AT&T Mobility LLC, and AT&T Corp. (collectively, "Petitioner") have shown by a preponderance of the evidence that claims 1–18 of U.S. Patent No. 9,198,042 B2 (Ex. 1001, "the '042 patent") are unpatentable.

A. Background and Summary

Petitioner filed a Petition (Paper 4, "Pet.") requesting institution of an *inter partes* review of claims 1–18 of the '042 patent. Headwater Partners I LLC ("Patent Owner") filed a Preliminary Response. Paper 8. With our authorization, the parties filed papers directed only to our discretion under 35 U.S.C. § 314(a). Papers 9, 10. Pursuant to 35 U.S.C. § 314, we instituted an *inter partes* review of claims 1–18 of the '042 patent on all presented challenges. Paper 11 ("Inst. Dec."), 2, 30–31.

After institution, Patent Owner filed a Response (Paper 14, "PO Resp."), and Petitioner filed a Reply (Paper 17, "Pet. Reply"). Patent Owner did not file a sur-reply.

B. Real Parties in Interest

Petitioner identifies as real parties in interest Cellco Partnership d/b/a Verizon Wireless, Verizon Corp. Servs. Grp. Inc., T-Mobile USA, Inc., AT&T Servs., Inc., AT&T Mobility LLC, and AT&T Corp. Pet. 81. Petitioner also names all current defendants in related litigation as potential real parties in interest. *Id.* at 81 n.4. Patent Owner identifies itself as a real party in interest. Paper 6, 1.

C. Related Matters

The parties identify *Headwater Research LLC v. Verizon Commc'ns Inc.*, 2:23-cv-00352-JRG-RSP (E.D. Tex.), *Headwater Research LLC v. AT&T Inc.*, 2:23-cv-00398-JRG-RSP (E.D. Tex.), and *Headwater Research LLC v. T-Mobile US, Inc.*, 2:23-cv-00379-JRG-RSP (E.D. Tex.) as related matters. Pet. 82; Paper 6, 1.

D. The '042 Patent (Ex. 1001)

The '042 patent issued on November 24, 2015, from an application filed on January 9, 2013 that is a continuation of two previously filed applications, the earliest of which was filed on March 2, 2009. Ex. 1001, codes (22), (45), (63), 1:7–16. The '042 patent also claims priority to several provisional applications, the earliest of which was filed on January 28, 2009. *Id.* at code (60), 1:16–43.

Figure 1 of the '042 patent is below reproduced.

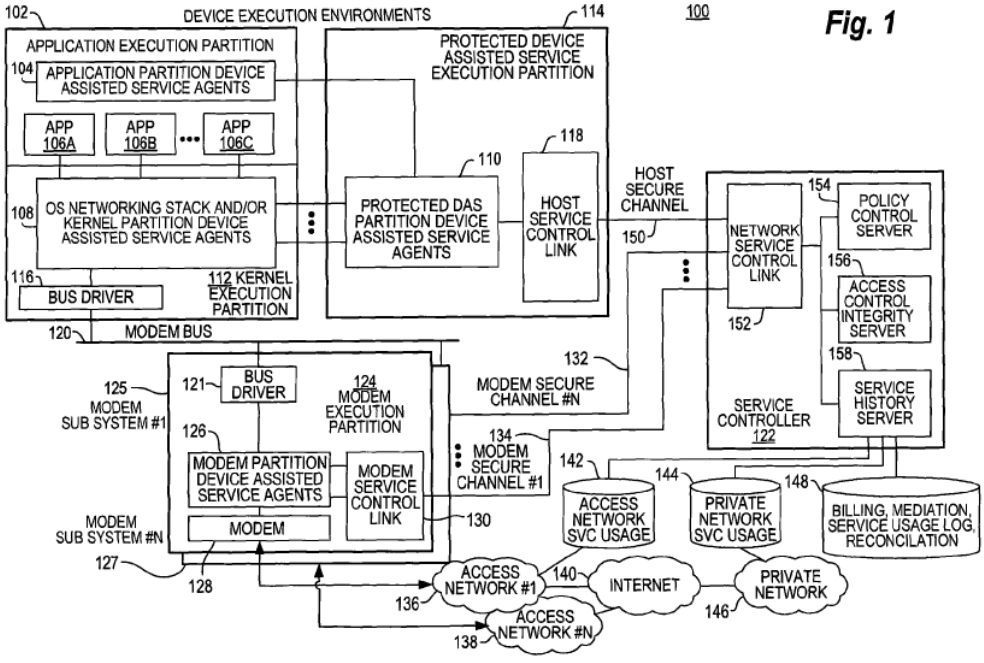


Figure 1 shows "a secure execution environment for device assisted services." Ex. 1001, 2:10–11. "[T]he device execution environments

include program/functional elements for," as an example, a "mobile communications device, such as a mobile phone" that uses modem subsystems 125, 127 to connect to access networks 136 and 138. *Id.* at 5:40–52.

Secure execution environment 100 has application execution partition 102, kernel execution partition 112, protected device assisted service ("DAS") execution partition 114, and modem execution partition 124. Ex. 1001, 5:54–65. Application programs execute in application execution partition 102, and low-level drivers and OS programs execute in kernel execution partition 112. *Id.* at 5:54–58. DAS agents and functions execute in DAS execution partition 114, and modem program elements execute in modem execution partition 124. *Id.* at 5:58–65.

"[P]rotected DAS partition 114 can make it more difficult for a hacker, malware or system errors to compromise, attack or modify the device assisted service measurements, service policy implementation or service usage control operations on the device (e.g., communications device)." Ex. 1001, 6:32–37. "[S]ervice control link (e.g., host service control link 118 via host secure channel 150 to network service control link 152) is used for communication between the device assisted service agents and a service controller 122." *Id.* at 7:28–32.

Service controller 122 can include access control integrity server 156 and policy control server 154. Ex. 1001, 8:8–9, 8:26–27. "Access control integrity server 156 is used to compare various access control verification checks to ensure that the device assisted service agents have not been compromised." *Id.* at 8:8–11. "[P]olicy control server 154 stores policy settings for the various service plans that can be implemented on the device, and communicates the appropriate policy settings to the appropriate device

DAS agents." *Id.* at 8:26–30. "[S]ervice controller 122 has secure access to service measures, service control settings, software images, software security state(s), and/or other settings/functions, for example, by virtue of the hardware enhanced execution partition and the secure channel into the protected DAS partition 114." *Id.* at 8:31–36.

E. Illustrative Claim

The '042 patent includes 18 claims, all of which Petitioner challenges. Claim 1, reproduced below, is the only independent claim.

> 1. A method comprising:
>
> receiving, over a service control link, a report from a wireless end-user device, the report comprising information about a device service state;
>
> determining, based on the report, that a particular service policy setting of the wireless end-user device needs to be modified, the particular service policy setting being stored in a protected partition of the wireless end-user device, the protected partition configured to deter or prevent unauthorized modifications to the particular service policy setting, the particular service policy setting being associated with a service profile that provides for access by the wireless end-user device to a network data service over a wireless access network, the particular service policy setting configured to assist in controlling one or more communications associated with the wireless end-user device over the wireless access network; and
>
> is in response to determining that the particular service policy setting needs to be modified, sending configuration information to the wireless end-user device over the service control link, the configuration information configured to assist in modifying or allowing modifications to the particular service policy setting.

Ex. 1001, 19:22–45.

F. Asserted Prior Art and Proffered Testimonial Evidence

Petitioner identifies the following references as prior art in the asserted grounds of unpatentability:

Name	Reference	Exhibit
Wright	US 2004/0123153 A1, published June 24, 2004	1005
Limont	US 2007/0006289 A1, published Jan. 4, 2007	1004
Xu	US 2007/0061535 A1, published Mar. 15, 2007	1016
Polson	US 2007/0104169 A1, published May 10, 2007	1008

Petitioner contends that the above references are prior art under § 102(a), (b), (e), and (g).[1] Pet. 10–11. Petitioner also provides a Declaration of Henry Houh, Ph.D. (Ex. 1003) and a Declaration of Henry Houh, Ph.D., under 37 C.F.R. § 1.68 in support of Petitioner's Reply to Patent Owner's Response (Ex. 1028).

Patent Owner provides Declarations of Erik De La Iglesia (Exs. 2001, 2032). No deposition transcripts were filed.

G. Asserted Grounds

Petitioner asserts that claims 1–18 are unpatentable on the following grounds:

Claims Challenged	35 U.S.C. §	References/Basis
1, 2, 6–18	103(a)	Limont, Wright, Xu
3–5	103(a)	Limont, Wright, Xu, Polson

Pet. 10.

[1] The relevant sections of the Leahy-Smith America Invents Act ("AIA"), Pub. L. No. 112–29, 125 Stat. 284 (Sept. 16, 2011), took effect on March 16, 2013. Because the '042 patent issued from an application filed before that date, our citations to 35 U.S.C. §§ 102 and 103 in this Decision are to their pre-AIA versions. *See also* Pet. 7 (noting that "[t]he '042 Patent's application claims priority to various applications, the earliest of which was filed January 28, 2009").

II. ANALYSIS

A. Legal Standards

"In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent [claim] it challenges is unpatentable." *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016). This burden of persuasion never shifts to Patent Owner. *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). To prevail in an *inter partes* review, the petitioner must support its challenges by a preponderance of the evidence. 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d).

Petitioner contends that the challenged claims of the '042 patent are unpatentable under § 103. Pet. 10. A claim is unpatentable under § 103 if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) where in evidence, so-called secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). When evaluating a combination of teachings, we must also "determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)). Whether a combination of elements produces a predictable result weighs in the ultimate determination of obviousness. *Id.* at 416–417.

B. Level of Ordinary Skill in the Art

Petitioner argues that a person of ordinary skill in the art "would have been familiar with the changing of configuration settings of end-user devices to control access of the device to network data services, and storing those configuration settings in a protected partition" and "would have gained this knowledge through a mixture of training and work experience, such as by having a Bachelor's degree in computer science and two years of experience." Pet. 7–8 (citing Ex. 1003 ¶¶ 41–43).

For institution, we adopted Petitioner's proposed level of ordinary skill. Inst. Dec. 15. Patent Owner does not challenge Petitioner's proposal. PO Resp. 6–7 (citing Pet. 7–8).

Based on the full record, we maintain and affirm that one of ordinary skill in the art "would have been familiar with the changing of configuration settings of end-user devices to control access of the device to network data services, and storing those configuration settings in a protected partition" and "would have gained this knowledge through a mixture of training and work experience, such as by having a Bachelor's degree in computer science and two years of experience." Pet. 7–8 (citing Ex. 1003 ¶¶ 41–43). We find that Petitioner's proposed level of ordinary skill in the art is consistent with the '042 patent and the asserted prior art.

C. Claim Construction

In an *inter partes* review, the claims are construed

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

37 C.F.R. § 42.100(b); *see Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc).

Petitioner proposes that claim terms be given their plain and ordinary meaning "because the prior art relied on in this Petition meets each claim term under any reasonable construction." Pet. 7. For institution, we preliminarily adopted Patent Owner's proposed interpretation of "network data service" to mean "a service that provides network data." Inst. Dec. 17 (citing Ex. 1001, 1:48–49; Ex. 2001 ¶ 30).

Patent Owner responds "that 'network data service' is a term of art, and refers to a service in which access to network data is provided." PO Resp. 7 (citing Ex. 2032 ¶¶ 33–51, 56–59). Patent Owner argues that "data" refers to "data accessibility (i.e., a data plan or data connectivity), as opposed to other types of network services (such as network SMS service or network voice service)" and, therefore, "'network data service' refers to connectivity to an access network such that data service can be used (i.e., network data provided by a network data service provider), rather than specific services that might make use of such network data services (such as a content service provider like a webpage provider)." *Id.* (citing Ex. 2032 ¶ 34). Patent Owner also argues with citations to the record that its proposed interpretation is consistent with intrinsic and extrinsic evidence, including patents assigned to Petitioner. *Id.* at 9–18.

Petitioner replies that Patent Owner's "new restrictive, exclusionary" interpretation should be rejected because it lacks support in the record, and that one of ordinary skill in the art would not have understood the term to be so restricted. Pet. Reply 1–2 (citing Ex. 1001, 5:4–20; Ex. 1028 ¶¶ 39–42, 44–49), 5, 12–14 (citing PO Resp. 13; Ex. 1001, 5:4–20), 17–18 (citing PO Resp. 15–18; Ex. 1028 ¶¶ 71–77; Ex. 2033; Ex. 2037, 1:66–2:5). Petitioner

argues that one of ordinary skill in the art would have understood "that this type of service provides for specific network data service to a particular 'destinations, URLs or addresses on a network.'" *Id.* at 7 (citing Ex. 1028 ¶ 50). Petitioner also argues that Patent Owner fails to provide analysis for adopting its new proposed interpretation, the asserted prior art still meets the interpretation, and there is no lexicography or scope disavowal. *Id.* at 2, 11–12 (citing PO Resp. 7, 10–13; Ex. 1001, 5:11–20), 15 (citing Ex. 1028 ¶¶ 63–69), 14 (citing PO Resp. 3–4, 11–12). Petitioner further addresses Patent Owner's asserted extrinsic evidence. *Id.* at 17–18 (citing PO Resp. 15–18; Ex. 1028 ¶¶ 71–77; Ex. 2033; Ex. 2037, 1:66–2:5).

Petitioner also replies that Patent Owner could have, but did not, amend the claims to recite its proposed interpretation and the claims should not be effectively amended by adopting the proposed interpretation. Pet. Reply 17. Petitioner further replies that Patent Owner does not mention nor address the proposed construction of the same term in the Preliminary Response that was adopted. *Id.* at 1–2, 3–4 (citing Inst. Dec. 15–17; PO Resp. 1, 7).

Based on the full record, we do not need to interpret expressly "network data service," or any other term, to resolve the parties' dispute, because, for the reasons below, Petitioner shows that the challenged claims are unpatentable even under Patent Owner's newly proposed interpretation. *Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) ("The Board is required to construe 'only those terms that . . . are in controversy, and only to the extent necessary to resolve the controversy.'") (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

D. Asserted Obviousness Based on Limont, Wright, and Xu

1. Limont (Ex. 1004)

Limont is "directed towards methods . . . for enforcing device settings for mobile devices." Ex. 1004 ¶ 16. Figure 3 of Limont is below reproduced.

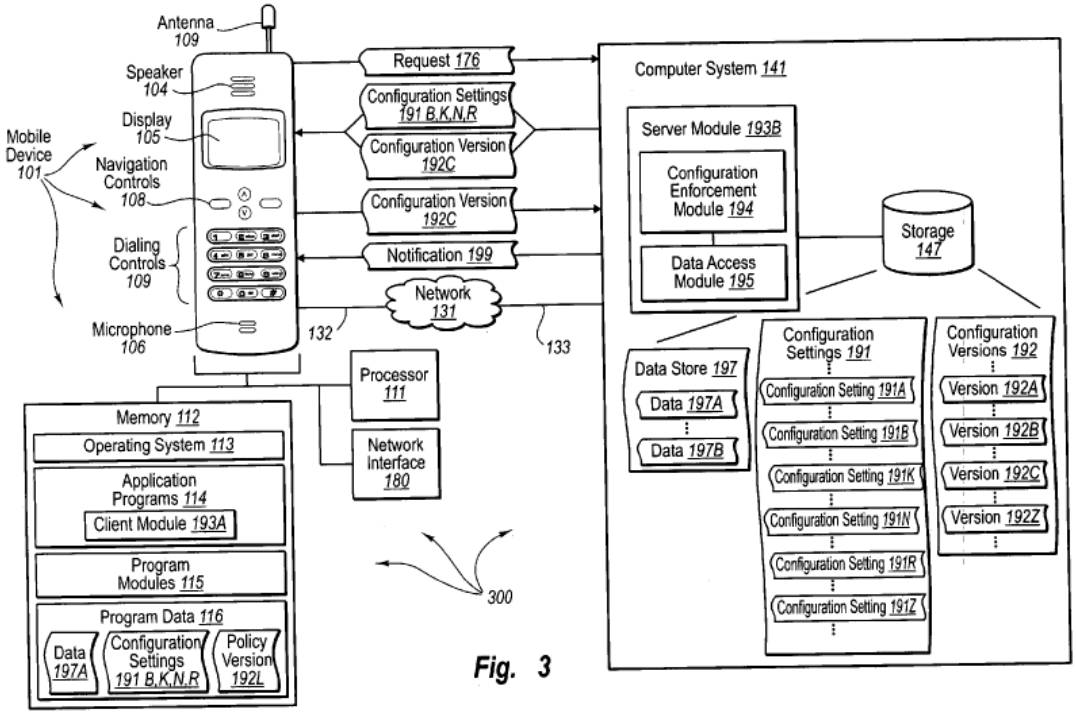


Fig. 3

Figure 3 shows a "computer architecture that facilitates enforcing configuration settings of mobile devices," in particular, computer architecture 300. Ex. 1004 ¶ 25. In computer architecture 300, "mobile device 101 includes client module 193A (e.g., a Web browser)" that can be utilized "to access data maintained by a server." *Id.* ¶ 72.

"Computer system 141 includes server module 193B (e.g., a Web server)" that "includes policy enforcement module 194 and data access module 195." Ex. 1004 ¶ 73. Computer system 141 also includes configuration settings 191 that include policy settings 191A, 191B, 191Z, and possibly more. *Id.* "Configuration settings can include: operating

system settings, application program settings, hardware settings, allocated resource settings, network interface settings, wireless protocol settings, etc." *Id.* Computer system 141 further includes configuration versions 192A, 192B, 192C, and possibly others. *Id.* ¶ 75. "A configuration version is a reduced set of data . . . that represents one or more configuration settings." *Id.*

"Server module 193B can interoperate with client side programs (e.g., client module 193A) to transfer data (e.g., Web pages) to a mobile device," and "in response to a mobile device data request, policy enforcement module 194 can determine if a requesting mobile device's policy settings are appropriate for accessing data." Ex. 1004 ¶ 77.

"Configuration enforcement module 193 can interoperate with one or more of an authentication module, authorization modules, and policy enforcement module of server module 193B (not shown) to reduce the likelihood of inappropriate data access." Ex. 1004 ¶ 78. "When configuration settings are appropriate (and, for example, a user is authenticated and authorized and policy settings are appropriate), data access module 195 accesses requested data and transfers requested data to the requesting mobile device." *Id.* "[W]hen configuration settings are inappropriate (and even if a user is authenticated and authorized and policy requirements are appropriate), configuration enforcement module 194 can access appropriate configuration settings and transfer the appropriate configuration settings to the requesting mobile device." *Id.*

Limont also describes "method 400 for enforcing an appropriate mobile device configuration prior to permitting a mobile device to access maintained data." Ex. 1004 ¶¶ 79–91, Fig. 4.

2. Wright (Ex. 1005)

Wright's "protection of data is administered through one or more security policies" that can "determin[e] accessibility of data for the mobile device," for example, "as required or recommended by a security policy." Ex. 1005 ¶ 14. The "security policy may not allow a particular network service or application or both to be used based upon either or both of a particular detected location or the activity status of a security feature." *Id.*

Wright describes "system 200 for administering protection of data accessible by a mobile device." Ex. 1005 ¶ 47. System 200 can include authorization module 232, policy distribution module 234, policy management module 236, policy setting module 238, and policy enforcement module 244. *Id.* ¶¶ 47, 48, Fig. 2A. System 200 can protect data resident in the mobile device or "data 242 that is accessible by the mobile device over a network 204." *Id.* ¶ 47.

"[P]olicy distribution module 234 distributes security information to the one or more client mobile devices" and "has a communication interface or is communicatively coupled to the policy management module 236 for receiving notifications of updated security information." Ex. 1005 ¶ 51. "Examples of security information are versions of existing policies, policies, or software." *Id.* "[P]olicy management module 236 determines 309 whether the security information is to be encrypted." *Id.* ¶ 104.

Wright also describes "system 201 for protecting data accessible by a mobile device based on a location associated with a network environment in which the mobile device is operating." Ex. 1005 ¶ 58, Fig. 2B. System 201 "determin[es] and enforc[es] security policies based upon the activity status of a security feature in a communication session between the mobile device and another computer" and includes location detection module 208, policy

setting module 212, security features determination module 210, policy enforcement control module 214, memory location(s) 216, authorization module 245, and client diagnostics module 246. *Id.*

3. Xu (Ex. 1016)

Xu's "processing unit with embedded system functions provides a secure base for enforcing security and/or operating policies" for "an electronic device such as a computer, cellular telephone, personal digital assistant, media player, etc." Ex. 1016 ¶ 3. "The processing unit may include features and functional support found in most or all modern microprocessors and also support additional functions providing . . . secure storage." *Id.*

Xu describes that "secure memory 318 may store, in a tamper resistant manner, code and data related to the secure operation of the computer 302." Ex. 1016 ¶ 23, Fig. 3. "Data in the secure memory 318 may include . . . policy data 322 that may specify policy related operational directives such as metering, reporting, update requirements, etc." *Id.* ¶ 23. Cryptography function 334 may also be used. *Id.* ¶ 25. Xu further describes how computer 300 is configured according to policy data 322 and when non-compliance to a policy is discovered. *See id.* ¶¶ 29–32.

4. Claim 1

Petitioner notes that it primarily relies on description related to the embodiment shown in Figures 3 and 4 of Limont, and that the description for Figures 1 and 2 "contain parallel invalidating disclosure" that are relied upon for corresponding disclosures. Pet. 26 (citing Ex. 1003 ¶¶ 304–307).

a) "A method comprising:"

Petitioner argues that Limont discloses the preamble. Pet. 24–26 (citing Ex. 1003 ¶¶ 300–303; Ex. 1004, Figs. 1–4).

The cited portions of Limont show "an example flow chart of a method for enforcing an appropriate mobile device configuration prior to permitting a mobile device to access maintained data." Ex. 1004 ¶ 26, Figs. 3, 4. We credit Petitioner's testimonial evidence regarding the preamble, because the cited portions of the record support it. Ex. 1003 ¶¶ 300–303; Ex. 1004 ¶ 26, Figs. 3, 4. Patent Owner does not present an argument for the preamble. *See* PO Resp.

Based on the full record, Petitioner persuades us, and we find, that Limont teaches or suggests the preamble of claim 1.

b) "receiving, over a service control link, a report from a wireless end-user device, the report comprising information about a device service state"

Petitioner argues that Limont teaches the above-quoted step. Pet. 26–28 (citing Ex. 1003 ¶¶ 309–341; Ex. 1004 ¶¶ 38, 43, 47, 56, 73, 80–81, Figs. 1, 3, 4). Petitioner also points to data command, data request 164, and policy version 118. *Id.* at 27 (citing Ex. 1003 ¶¶ 314–327; Ex. 1004 ¶¶ 30, 55, 58, 59, 67–69, Fig. 2).

The cited portions of Limont disclose computer system 141 receiving request 176 from mobile device 101 over communication links 132, 133 that connect mobile device 101 to computer system 141 using wireless protocols. Ex. 1004 ¶ 38 ("Mobile device 101 is connected to network 131 . . . via communication link 132. Similarly, computer system 141 [is] connected to network 131 via communication link 133."), ¶ 43 (communication link 132 "can include wireless communication using wireless protocols (e.g., GPRS, GSM, etc. to a mobile telephone server provider"), ¶ 56 (communication link 133 "can include wireless communication using wireless protocols"), ¶ 80 ("Computer system 141 can receive request 176 from mobile device

101."), ¶ 81, Figs. 1, 3, 4 (showing, as step 401, "Receiving A Request From A Mobile Device, The Request Requesting That The Mobile Device Be Permitted To Access Data Maintained By The Computer System, The Request Indicating A Current Mobile Device Configuration Of The Mobile Device").

The cited portions of the record support Petitioner's testimonial evidence that Limont teaches receiving a report from a wireless end-user device. Ex. 1003 ¶¶ 309–313; Ex. 1004, Figs. 3, 4. We agree with Petitioner's declarant that request 176 teaches the recited "report." Ex. 1003 ¶ 311. The cited portions of the record support that Limont's request 176 includes different pieces of data, including "configuration version" that would teach or suggest "information about a device service state." Ex. 1003 ¶¶ 314–315; Ex. 1004 ¶ 80 ("Request 176 can indicate configuration version representing the one or more of the current configuration settings of mobile de[v]ice 101."), ¶ 81 ("A request may or may not expressly include a configuration version."); *see also* Ex. 1003 ¶¶ 316–324 (opining about similar disclosures in Limont's Figures 1, 2) (citing Ex. 1004 ¶¶ 58–59, 67–69, Figs. 1, 2, claim 9).

Petitioner also cites portions of Limont that disclose "configuration settings" can include "policy settings." Ex. 1004 ¶ 73 (describing that "configuration settings 191 includes . . . policy setting 191A, policy setting 191B, and policy setting 191Z"), ¶ 47 (listing what "[p]olicy settings can include"). We agree with Petitioner that Limont's disclosure of "configuration settings" and "policy settings" is consistent with the '042 patent's disclosure of "device service state includ[ing] current service usage policy settings, current DAS settings, device status information, application status information, or other state and/or settings information." Pet. 27

(citing Ex. 1001, 17:46–18:11; Ex. 1003 ¶¶ 315–327); Ex. 1001, 17:46–18:11 ("device service control state (e.g., . . . current service usage policy settings, . . . current DAS settings, . . . device status information, application status information, . . . and/or other state and/or settings information)."); Ex. 1003 ¶¶ 324–331.

Patent Owner does not present an argument for the recited "receiving" step. *See* PO Resp. Based on the full record, Petitioner persuades us, and we find, that Limont teaches or suggests "receiving, over a service control link, a report from a wireless end-user device, the report comprising information about a device service state."

c) "determining, based on the report, that a particular service policy setting of the wireless end-user device needs to be modified"

Petitioner argues that Limont discloses the above-quoted step. Pet. 28–30 (citing Ex. 1003 ¶¶ 343–375; Ex. 1004 ¶¶ 45–53, 60–65, 80–83, Fig. 2 (steps 202, 205), Fig. 4 (step 402)). Petitioner also argues that Limont's mobile device seeks access to data on a server that can only be accessed with appropriate configuration settings. *Id.* at 30 (citing Ex. 1003 ¶¶ 354–360, 374; Ex. 1004 ¶¶ 60–64, 73, 79, 84–89, Fig. 4 (step 405)). Petitioner notes that Limont uses "configuration setting" and "policy setting" interchangeably. *Id.* (citing Ex. 1003 ¶¶ 362–369; Ex. 1004 ¶¶ 45, 55, 77–78, 83). Petitioner further argues that Limont's configuration settings are sent from computer system 141. *Id.* at 30–31 (citing Ex. 1003 ¶¶ 370–374; Ex. 1004 ¶¶ 65, 85, 89).

The cited portions of Limont describe mobile device 101 seeking to access maintained data that require appropriate configuration settings and that "[m]ethod 400 includes an act of determining that current mobile device

configuration is not appropriate for accessing the maintained data (act 402)," for example, "determin[ing] that the configuration settings of mobile device 101 are inappropriate for accessing data maintained by server module 193B." Ex. 1004 ¶ 82; *see also id.* ¶¶ 60–64, 73, 79, 84–89, Fig. 2 (steps 202, 205), Fig. 4 (steps 402, 405).

Another cited portion describes that, "[i]n response to detection of an inappropriate configuration, configuration enforcement module 143 can identify configuration settings . . . that are appropriate for accessing data maintained by server module 193B." Ex. 1004 ¶ 83; *see also id.* ¶ 61 (describing similarly with respect to Figure 2). Other cited portions of Limont describe that "configuration settings" include policy settings and those settings can be sent from computer system 141 to permit access to the server data. *Id.* ¶¶ 45, 55, 65, 73, 77, 78, 83, 85, 89. We credit Petitioner's testimonial evidence that identifying correct settings is determining that Limont's mobile device's configuration settings need to be modified, because the cited portions of the record support it. Ex. 1003 ¶¶ 354–360, 374; Ex. 1004 ¶¶ 60–64, 84–89.

We also credit Petitioner's testimonial evidence regarding the above-quoted step generally, because the cited portions of Limont support it. Ex. 1003 ¶¶ 343–375; Ex. 1004 ¶¶ 45, 55, 60–65, 73, 77–83, 85, 88, 89, Figs. 1–4, claims 1, 9. Patent Owner does not present an argument for the recited "determining" step. *See* PO Resp.

Based on the full record, Petitioner persuades us, and we find, that Limont teaches or suggests "determining, based on the report, that a particular service policy setting of the wireless end-user device needs to be modified."

d) "the particular service policy setting being stored in a protected partition of the wireless end-user device, the protected partition configured to deter or prevent unauthorized modifications to the particular service policy setting"

Petitioner argues that Limont's mobile device 101 includes memory 112 for storing configuration settings 191B, 191K, 191N, 191R and configuration version 192L, but Limont does not teach that the configuration settings are secure. Pet. 31–32 (citing Ex. 1003 ¶¶ 378–386; Ex. 1004 ¶¶ 86, Figs. 1, 3). Petitioner also argues that Wright teaches encrypted security information, such as policy, and permissions for policies. *Id.* at 32–33 (citing Ex. 1003 ¶¶ 387–394; Ex. 1005 ¶¶ 14, 51, 61, 78–103, 262, 280–284). According to Petitioner, Wright's teachings regarding policies generally correspond to Limont's policy disclosures. *Id.* at 33 (citing Ex. 1003 ¶¶ 395–398; Ex. 1005 ¶¶ 48, 180–184, Figs. 5B–5F). Petitioner further argues that Wright teaches a "protected partition." *Id.* at 34 (citing Ex. 1003 ¶¶ 395–410; Ex. 1005 ¶¶ 47, 58–60, 176–177, 280, Fig. 2B).

If "protected partition" requires more than storing data, Petitioner argues that Wright's protected partition also encrypts and decrypts. Pet. 35–36 (citing Ex. 1003 ¶ 415; Ex. 1005 ¶¶ 47, 51, 62, 131, Figs. 2B, 3C). Petitioner also argues that Wright's protected partition prevents unauthorized users modifying policies stored in encrypted memory and, in view of Wright, Limont's data would likewise be protected. *Id.* at 36 (citing Ex. 1003 ¶¶ 416, 417; Ex. 1004 ¶ 71; Ex. 1005 ¶¶ 48, 78–104, 229–230, 259–264, 280–284).

Petitioner further argues that, to the extent "stored in a protected partition" requires a secure execution environment, as shown in Figure 4 of the '042 patent, then Xu teaches such an environment that Petitioner proposes to combine with Limont's memory 112 to execute Wright's

encryption protections. Pet. 36–40 (citing Ex. 1001, Fig. 1; Ex. 1003 ¶¶ 418–440; Ex. 1016 ¶¶ 3, 23, 25, 29–32, Fig. 3, claim 9).

The cited portions of Limont describe that mobile device 101 includes memory 112 with program data 116, configuration settings 191B, 191K, 191N, 191R, and configuration version 192L. Ex. 1004 ¶¶ 44–53, 86, Figs. 1, 3. The cited portions of Wright describe that "security information such as a policy or software being designated for encryption" and "permissions [that] typically relate to the allowable modification." Ex. 1005 ¶¶ 78–103, 280–284. Other cited portions of Wright describe storing encrypted policies and hiding policy files and permissions for policies. *Id.* ¶¶ 14, 51, 61, 103, 262, 208–284. As argued by Petitioner, Wright describes aspects of its policies that correspond to Limont's disclosures regarding policies. Ex. 1003 ¶¶ 395–398; Ex. 1005 ¶¶ 48, 180–184, Figs. 5B–5F.

Wright also shows a "protected partition" in its memory 220 and describes protecting stored policies by encryption. Ex. 1005 ¶¶ 47, 58–60, 176, 177, 280, Fig. 2B. We also agree with Petitioner that Wright's use of encryption to provide a "protected partition of the wireless end-user device" is consistent with the '042 patent's disclosure that "the memory protection function includes encrypting traffic to and from memory so that only authorized device program elements possess the counterpart encryption capability to access the memory." Ex. 1001, 9:27–30; Ex. 1003 ¶ 414.

The cited portions of Wright also describe that its protected partition is "configured to deter or prevent unauthorized modifications to the particular service policy setting," because the encryption, hiding, and permissions would prevent unauthorized modifications to Wright's stored policies. Ex. 1003 ¶ 416; Ex. 1005 ¶¶ 48, 78–104, 229–230, 259–264, 280–284. We agree with Petitioner that one of ordinary skill in the art would

have understood that Limont's policy settings should be protected with limited access. Ex. 1003 ¶ 417; Ex. 1004 ¶ 71.

A cited portion of Xu describes "a secure base for enforcing security and/or operating policies" for a "cellular telephone" or "personal digital assistant" with "secure storage" and "a cryptographic unit" so as to be "capable of being operated in compliance to a usage policy." Ex. 1016 ¶ 3. Other cited portions of Xu describe a "secure memory" for storing "policy data 332" "in a tamper resistant manner" and cryptography function 334 for encrypting and policy updates. *Id.* ¶¶ 23, 25, 29–32, claim 9.

We credit Petitioner's testimonial evidence regarding the above-quoted step, because the cited portions of the record support it. Ex. 1003 ¶¶ 378–410, 415–436; Ex. 1004 ¶¶ 13, 40, 44–53, 71, 86, Figs. 1, 3; Ex. 1005 ¶¶ 14, 46–48, 51, 58–62, 78–104, 131, 176, 177, 180–184, 229, 230, 259–264, 280–284, Figs. 2B, 3C, 5B–5F; Ex. 1006, code (57), ¶¶ 3, 22–25, 29–32, 34, Fig. 3. Patent Owner does not present an argument for the above-quoted limitations. *See* PO Resp.

Based on the full record, Petitioner persuades us, and we find, that (1) Limont teaches or suggests "the particular service policy setting being stored in . . . the wireless end-user device," and (2) Wright teaches or suggests the "service policy setting being stored in a protected partition of the wireless end-user device, the protected partition configured to deter or prevent unauthorized modifications to the particular service policy setting." Also, based on the full record, to the extent "stored in a protected partition" requires a secure execution environment, Petitioner persuades us, and we find, that Xu teaches or suggests such an environment. We analyze below Petitioner's proposed combination of these references.

e) "the particular service policy setting being associated with a service profile that provides for access by the wireless end-user device to a network data service over a wireless access network"

Petitioner argues that Limont's mobile device 101 wirelessly exchanges data and includes network interface 180 for receiving data from and transmitting data to external sources. Pet. 42 (citing Ex. 1003 ¶¶ 443–470; Ex. 1004 ¶ 41). Petitioner also argues that Limont teaches configuration versions and settings that include settings for network interface and wireless protocol. *Id.* at 42–43 (citing Ex. 1003 ¶¶ 444–446; Ex. 1004 ¶¶ 43, 45–53, 56, 75, 87).

Petitioner further argues that Limont's data exchange and network interface and wireless protocol settings would have been understood to be "service policy settings that provide[] for access . . . to a network data service over a wireless access network." Pet. 43 (citing Ex. 1003 ¶¶ 447–451). According to Petitioner, "Limont describes several forms of specific services with distinct accessed data also corresponding to the '*network data service*,'" such as email and web servers. *Id.* (citing Ex. 1004 ¶¶ 38, 45, 73).

Petitioner also argues that Limont's policies allow for access to a network data service that provides data on or from a server. Pet. 44 (citing Ex. 1003 ¶¶ 452–466). Petitioner further argues that Limont's policy enforcement module 194 determines if the policy settings of the mobile device are appropriate for accessing the data on the server. *Id.* (citing Ex. 1003 ¶¶ 467–469; Ex. 1004 ¶ 77).

(1) Patent Owner's Response

Patent Owner responds that Petitioner relies only on Limont as allegedly disclosing the above-quoted limitation and only points to an email server and a web server providing a webpage for satisfying the recited

"network data service." PO Resp. 18–19 (citing Pet. 42–44; Ex. 2032 ¶¶ 55–60). Patent Owner argues that such servers do not provide "network data service" because "those servers do not offer the service of providing a 'network data,' and one of ordinary skill in the art would have understood "network data service" "refer[s] specifically to provision of a service that provides data network connectivity rather than a service that provides data which may be accessible over any number of unspecified networks." *Id.* at 19 (citing Ex. 2032 ¶ 56).

According to Patent Owner, the ordinarily skilled artisan's understanding of "'network data services' is consistent with the claim language itself" and the Specification. PO Resp. 19–20 (citing Ex. 2032 ¶¶ 39–43, 57). Patent Owner argues that the relied-upon servers "do not provide data connectivity via an access network." *Id.* at 19 (citing Ex. 2032 ¶ 56).

Patent Owner further argues that email and website services are content services and that the difference between a network data service and a content service is illustrated by the difference between subscriptions for data connectivity services (such as a 5G unlimited data plan), email, and content (such as the Wall Street Journal). *Id.* at 20 (citing Ex. 2032 ¶ 57). Patent Owner additionally argues that Petitioner is aware of the distinction between email, website data, and network data services. *Id.* at 20–21 (citing Ex. 2033; Ex. 2034). In Patent Owner's view, one of ordinary skill in the art would not have understood email and website content servers to be a "network data service" that provides network data connectivity. *Id.* at 21 (citing Ex. 2032 ¶¶ 58–59).

Patent Owner argues that Petitioner's interpretation of "network data service" that encompasses any service with data transmitted over a network

is inconsistent with the understanding of the ordinarily skilled artisan, leads to superfluous language in the claims, and rewrites the claim to eliminate "network data service." PO Resp. 21–22 (citing Ex. 2032 ¶ 59). Patent Owner also argues that one of ordinary skill in the art would have understood "'service policy setting' of claim 1 must relate specifically to the recited 'network data service,'" and Petitioner fails to identify a "service policy setting" because it fails to identify a "network data service" as understood by one of ordinary skill in the art. *Id.* at 22 (citing Ex. 2032 ¶¶ 52–53, 60).

(2) Petitioner's Reply

Petitioner replies that, as argued in the Petition, Limont teaches controlling service access to a connection to a particular computer that may host a website or email service and that the connection would connect to a destination using a URL or address on a network. Pet. Reply 7–8 (citing Ex. 1004 ¶¶ 4, 45, 73, 76–77, 82; Ex. 1028 ¶ 51). Petitioner also argues that Limont teaches an email application or web browser application connecting to a network and retrieving email or web pages, thereby teaching a "connection to the network by one or more applications." *Id.* at 8 (citing Ex. 1028 ¶ 53). Petitioner further argues that Limont's email messages and web pages would be transmissions of certain types of traffic and correspond to activities enumerated by the '042 patent. *Id.* at 8–9 (citing Ex. 1001, 4:5–10, 5:16–20; Ex. 1028 ¶¶ 46–47, 54). Limont's email messages and web pages, Petitioner argues, are also both a "file type" and "traffic associated with an application" that would be a type of service in parallel with the "connection to an access network" that Patent Owner asserts is a form of network data service. *Id.* at 9 (citing Ex. 1004 ¶¶ 72, 76–77, 85; Ex. 1028 ¶ 57).

According to Petitioner, the '042 patent describes without distinction multiple different types of service activities and usages that reflect different types of network data services that can be controlled with policy-based settings. Pet. Reply 9 (citing Ex. 1028 ¶ 58). Petitioner argues that one of ordinary skill in the art would not have excluded one of the described activities and usages from "network data service." *Id.* at 9–10 (citing Ex. 1028 ¶ 59).

Petitioner also argues that, even if Patent Owner's proposed interpretation of "network data service" were adopted, Limont teaches a service that provide network data connectivity. Pet. Reply 10 (citing PO Resp. 1). Petitioner refers to its arguments regarding how Limont teaches updating policy settings to assist in controlling one or more communications. *Id.* (citing Pet. 44–45). According to Petitioner, controlling one or more communications provides network data connectivity by allowing or not allowing connection across the network between Limont's mobile device and network-based server. *Id.* at 10–11 (citing Ex. 1028 ¶ 61).

Petitioner also replies that, even if only certain types of companies can be an "entity that provides access network connectivity," Limont teaches and would have rendered obvious the claims, because one of ordinary skill in the art would have understood Limont discloses such entities that provide network connectivity. Pet. Reply 15 (citing PO Resp. 13; Ex. 1028 ¶¶ 66–69), 16 (citing Ex. 1028 ¶¶ 65–69). Petitioner argues that Limont is not restricted to any particular type of company and, instead, covers systems for enforcing device settings so that mobile devices can access data across wireless networks. *Id.* at 15–16 (citing Ex. 1004, code (57), ¶¶ 16, 18, 32–94, Figs. 1–4; Ex. 1028 ¶¶ 66–69). Petitioner also argues that email and web pages can be provided by an "entity that provides access network

connectivity" and that Patent Owner does not provide any basis to assert differences between text and mail provided by Limont's systems. *Id.* at 16 (citing PO Resp. 13; Ex. 1028 ¶¶ 68–69).

Petitioner further replies that Patent Owner mischaracterizes Petitioner's argument by alleging incorrectly and without citation that the Petition asserted an overly broad interpretation of "network data service" to encompass any service involving any data transmitted over a network. Pet. Reply 19 (citing PO Resp. 21). Petitioner clarifies that its position is that "network data service" corresponds to the embodiments described in the '042 patent that include more than connecting to an access network. *Id.* at 19–20 (citing Ex. 1001, 5:4–20). Petitioner argues that there is no basis to select Patent Owner's preferred service over another. *Id.* at 20.

Petitioner additionally replies that Patent Owner's arguments regarding "service policy setting" rely on Patent Owner's overly narrow view of "network data service" and fail for the same reasons as Patent Owner's arguments regarding "network data service" fail. Pet. Reply 20.

(3) Petitioner Shows that Limont Teaches or Suggests the Limitation

Petitioner cites a portion of Limont that discloses "[m]obile device 101 is connectable to networks, such as, for example, an office-wide or enterprise-wide computer network, an intranet, and/or the Internet" and "includes network interface 180 that can . . . receive data from external sources and/or transmit data to external sources." Ex. 1004 ¶ 41. Petitioner also cites a portion that discloses configuration versions and settings include settings for the network interface and wireless protocol. *Id.* ¶ 87 ("Implemented configuration settings can alter the current configuration of one or more of . . . a network interface, and wireless protocol settings, at the

mobile device."). Other cited portions of Limont describe that "mobile device 101, computer system 141, and other network connected computer systems (not shown) can exchange data via network 131," and that "in response to a mobile device data request, policy enforcement module 194 can determine if a requesting mobile device's policy settings are appropriate for accessing data." *Id.* ¶¶ 38, 77.

As discussed above, we find that Limont teaches or suggests mobile device 101 sending request 176 over communication links 132, 133 that use wireless protocols. Ex. 1004 ¶¶ 38, 43, 56, 80, 81, Figs. 1, 3, 4. We credit Petitioner's testimonial evidence that the data exchange and network interface and wireless protocol settings would have been understood to be a "particular service policy setting being associated with a service profile that provides for access by the wireless end-user device . . . over a wireless access network," because the cited portions of the record support it. Ex. 1003 ¶¶ 447–451; Ex. 1004 ¶¶ 43, 45–53, 56, 75, 87.

Turning to the recited "network data service," Petitioner cites a portion of Limont that describes "[c]omputer system 141 includes server module 142B (e.g., an electronic mail server) and storage 147," "[s]erver module 142B further includes policy enforcement module 143 and data access module 144," and "storage 147 can store data . . . electronic mail messages, Web pages, . . . [and] policy settings," such as, "policy settings 117 representing a group of policy settings that mobile devices can implement." Ex. 1004 ¶ 45.

Petitioner also cites a portion that describes "[c]omputer system 141 includes server module 193B (e.g., a Web server)," "[s]erver module 193B fu[]rther includes policy enforcement module 194 and data access module 195," "configuration settings 191 include policy setting 191A, policy setting

191B, and policy setting 191Z," and "[c]onfiguration settings can include: . . . network interface settings, wireless protocol settings, etc." Ex. 1004 ¶ 73.

Petitioner, thus, persuades us that "Limont describes several forms of specific services with distinct accessed data also corresponding to the '*network data service*,'" such as email and web servers. Pet. 43 (citing Ex. 1004 ¶¶ 38, 45, 73). Based on our findings from Limont discussed above, Petitioner also persuades us that Limont teaches controlling service access to a connection to a particular computer that may host a website or email service and that the connection would be a connection to a destination that uses a URL or address on a network. Pet. Reply 7–8 (citing Ex. 1004 ¶¶ 4, 45, 73, 76–77, 82; Ex. 1028 ¶ 51); Ex. 1004 ¶¶ 4, 45, 73, 76–77, 82.

We also credit Petitioner's testimonial evidence regarding the limitation because the cited portions of the record support it. Ex. 1003 ¶¶ 443–470; Ex. 1004, code (57), ¶¶ 4, 16, 18, 38, 41, 43, 45–56, 60–73, 75–78, 82, 83, 85–91, Figs. 2, 4; Ex. 1028 ¶¶ 46, 47, 51, 53, 54, 57–59, 61, 65–69.

Under Patent Owner's first proposed interpretation of "network data service" to mean "a service that provides network data" that we adopted, we find that the cited portions of Limont teach or suggest "a service that provides network data," because the cited portions teach computer system 141 that includes, at least, server module 193B with policy enforcement module 194, and, as discussed above, "in response to a mobile device data request, policy enforcement module 194 can determine if a requesting mobile device's policy settings are appropriate for accessing data" stored on server module 142B or 193B. Inst. Dec. 16–17; Ex. 1004 ¶¶ 73, 77. Thus, as argued by Petitioner, Limont teaches or suggests

network interface settings and wireless protocol settings associated with mobile device 101 so that mobile device 101 can access "a service that provides network data" over a network. Pet. 43. In particular, Limont discloses settings for accessing services that provide email and web pages to mobile device 101 over network 131. Ex. 1004 ¶¶ 38, 45, 73.

Patent Owner does not argue explicitly that the adopted interpretation of "network data service" is incorrect. *See* PO Resp. Patent Owner, instead, provides another narrower interpretation. *Id.* at 7–18. Even if we applied that interpretation, Petitioner still persuades us that Limont teaches or suggests the recited "network data service."

Under Patent Owner's second proposed interpretation of "network data service" to refer to "connectivity to an access network such that data service can be used (i.e., network data provided by a network data service provider), rather than specific services that might make use of such network data services (such as a content service provider like a webpage provider)," Limont discloses that mobile device 101 can exchange data via network 131 with computer system 141 that includes, at least, server module 193B and that "in response to a mobile device data request, policy enforcement module 194 can determine if a requesting mobile device's policy settings are appropriate for accessing data" or its configuration settings are "inappropriate for accessing data maintained by server module 193B." Ex. 1004 ¶¶ 38, 45, 77, 82.

Thus, Limont teaches or suggests determining if mobile device 101's policy and configuration settings are appropriate for exchanging data via network 131 with computer system 141, specifically "appropriate for accessing data" or "inappropriate for accessing data maintained by server module 193B." Ex. 1004 ¶¶ 38, 45, 77, 82. Those settings include settings

for network interface 180 so that mobile device 101 can receive from and transmit data to external sources, such as "an office-wide or enterprise-wide computer network, an intranet, and/or the Internet." *Id.* ¶¶ 41, 87. Limont, therefore, teaches or suggests providing "connectivity to an access network such that data service can be used (i.e., network data provided by a network data service provider)."

Based on the full record and for the reasons above, Petitioner persuades us, and we find, that Limont teaches or suggests "the particular service policy setting being associated with a service profile that provides for access by the wireless end-user device to a network data service over a wireless access network."

f) "the particular service policy setting configured to assist in controlling one or more communications associated with the wireless end-user device over the wireless access network"

Petitioner contends with reference to previous arguments that Limont's servers 142, 193 evaluate and modify configuration or policy settings for accessing requested server data and different types of communications, such as email and web service. Pet. 44–45 (citing Ex. 1003 ¶¶ 452–466, 473–475). Petitioner also contends that Limont's configuration settings can alter network interface and wireless protocol settings and, thus, teach "control[ling] one or more communications associated with the wireless end-user device over the wireless access network." *Id.* at 45 (citing Ex. 1003 ¶ 476; Ex. 1004 ¶¶ 73, 87).

As discussed above, we find that Limont discloses servers 142, 193 evaluating configuration and policy settings to determine if those settings allow access to specific data requested and modifying policy settings to be appropriate to access requested server data. Ex. 1003 ¶¶ 343–375; Ex. 1004

¶¶ 60–64, 73, 79, 82–89, Figs. 2, 4. Petitioner cites portions of Limont that disclose "[c]onfiguration settings can include: . . . network interface settings, wireless protocol settings" (Ex. 1004 ¶ 73) and "[i]mplemented configuration settings can alter the current configuration of one or more of . . . a network interface, and wireless protocol settings, at the mobile device" (*id.* ¶ 87).

We credit Petitioner's testimonial evidence regarding the above-quoted step, because the cited portions of the record support it. Ex. 1003 ¶¶ 452–466, 473–476; Ex. 1004 ¶¶ 45, 54, 55, 60–70, 73, 76–78, 82, 83, 85–91, Figs. 1–4. Patent Owner does not present an argument for the above-quoted limitations. *See* PO Resp.

Based on the full record, Petitioner persuades us, and we find, that Limont teaches or suggests that "the particular service policy setting [is] configured to assist in controlling one or more communications associated with the wireless end-user device over the wireless access network."

> g) *"is in response to determining that the particular service policy setting needs to be modified, sending configuration information to the wireless end-user device over the service control link, the configuration information configured to assist in modifying or allowing modifications to the particular service policy setting"*

Petitioner argues with reference to previous arguments that Limont discloses determining that a service policy setting needs to be modified and sending modified settings to a mobile device for implementation. Pet. 45–46 (citing Ex. 1003 ¶¶ 479–486; Ex. 1004 ¶¶ 65, 66, 84–89, Figs. 1, 3, 4, claim 6).

Petitioner cites portions of Limont that describe methods 200, 400 include sending updated policy settings or configuration settings to the

mobile device, and that the sent configuration settings can alter current configuration settings for the network interface and wireless protocol settings to comply with configuration settings appropriate for accessing server data. Ex. 1004 ¶¶ 65, 66, 84–87, Figs. 1, 3, 4, claim 6. The method can include receiving an indication that the mobile device has been configured and then permitting the mobile device to access the data. *Id.* ¶¶ 88, 89. We credit Petitioner's testimonial evidence regarding the above-quoted step, because the cited portions of the record support it. Ex. 1003 ¶¶ 479–486; Ex. 1004 ¶¶ 65, 66, 84–89, Figs. 1, 3, 4, claim 6. Patent Owner does not present an argument for the above-quoted limitations. *See* PO Resp.

Based on the full record, Petitioner persuades us, and we find, that Limont teaches or suggests that "is in response to determining that the particular service policy setting needs to be modified, sending configuration information to the wireless end-user device over the service control link, the configuration information configured to assist in modifying or allowing modifications to the particular service policy setting."

h) Petitioner's Asserted Rationale for Modifying

For the reasons below, based on the full record, Petitioner persuades us that one of ordinary skill in the art would have been motivated to modify Limont with Wright and Xu for the reasons asserted with a reasonable expectation of success.

(1) Analogous Art

Petitioner argues that Limont, Wright, and Xu each "teach[es] the same subject of managing and updating secure data, including policies, wirelessly on mobile devices," and because of their similar identification of problems and proposed solutions, one of ordinary skill in the art would have

been motivated to consider and combine their teachings. Pet. 19 (citing Ex. 1003 ¶¶ 264–267), 20 (citing Ex. 1003 ¶¶ 278–287; Ex. 1004 ¶ 13; Ex. 1005 ¶ 9). Petitioner also argues that the citing of Wright during prosecution of Limont supports that the ordinarily skilled artisan would have considered Limont and Wright to be closely related. *Id.* at 19–20 (citing Ex. 1003 ¶¶ 268–277; Ex. 1013, 140–141, 145–148, 229–230). Patent Owner does not present any arguments regarding analogous art. *See* PO Resp.

Based on the full record, we determine that Limont, Wright, and Xu are analogous art. Pet. 19; Ex. 1003 ¶¶ 264–287; Ex. 1004 ¶ 13; Ex. 1005 ¶ 9; Ex. 1013, 140–141, 145–148, 229–230.

(2) Motivation to Combine

According to Petitioner, one of ordinary skill in the art would have recognized from the references that policy information needs to be protected during transmission and that malicious users should be prevented from accessing critical data on mobile devices. Pet. 20–21 (citing Ex. 1003 ¶¶ 283–287). Petitioner argues that "Limont does not expressly provide protection for data on the device" but "Wright provides the complementary solutions of encrypting data." *Id.* at 21–22 (citing Ex. 1003 ¶¶ 283, 289–294; Ex. 1004 ¶¶ 47–49); *see also id.* at 35 (arguing "Wright addresses the same issues identified by Limont" and "provides a solution for the problems identified in Limont") (citing Ex. 1003 ¶¶ 410–413; Ex. 1005 ¶¶ 14, 131–132, Figs. 2B, 3C).

Petitioner argues that one of ordinary skill in the art would have been "motivated to modify Limont's teachings of storing policy settings on the mobile device by encrypting the policy settings as taught by Wright" because a "malicious user" could access policies to allow access to data and

prevent even an "authorized" user from changing policies. Pet. 22–23 (citing Ex. 1003 ¶¶ 293, 295). Petitioner also argues that using Wright in Limont would have been merely an application of a well-known operation on a known component for known and intended purposes. *Id.* at 23 (citing Ex. 1003 ¶¶ 296–297). Petitioner further argues that the ordinarily skilled artisan "would have been motivated to consider Xu's supplementary solution for the same reasons as discussed above for Wright." *Id.* (citing Ex. 1003 ¶¶ 165–222, 427–440). Petitioner additionally argues that it was known in the art to protect confidential data. *Id.* at 23–24 (citing Ex. 1003 ¶¶ 165–222); *see also id.* at 9–10 (contending protected partitions were known in the art at the time of invention).

In its mapping of the claim limitations to the references, Petitioner argues that one of ordinary skill in the art would have been "motivated to implement a secure environment as taught by Xu on Limont's mobile device incorporating Wright's encryption functionality" so as "to provide for the protection of data in mobile devices using techniques such as hardware protections and encryptions" and to address "'malicious users' accessing confidential information." Pet. 40–41 (citing Ex. 1003 ¶¶ 263–267, 379–286, 431–440; Ex. 1004 ¶ 13; Ex. 1016 ¶ 30). Petitioner also argues that one of ordinary skill in the art would have been "motivated to modify Wright's encryption functionality using a secure environment as taught by Xu" because "the teachings of Xu beneficially increase Limont's and Wright's protections." *Id.* at 41 (citing Ex. 1003 ¶ 437; Ex. 1005 ¶¶ 78, 267; Ex. 1016 ¶¶ 25–26). Patent Owner does not present an argument regarding Petitioner's asserted motivation to combine. *See* PO Resp.

Based on the full record, Petitioner persuades us, and we determine, that one of ordinary skill in the art would have recognized from the

references that policy information needs to be protected. Pet. 20–22, 35; Ex. 1003 ¶¶ 283–287, 289–294, 410–413; Ex. 1004 ¶¶ 47–49; Ex. 1005 ¶¶ 14, 131–132, Figs. 2B, 3C. We also determine that one of ordinary skill in the art, thus, would have been motivated to modify Limont with Wright for the reasons asserted by Petitioner. Pet. 22–23.

We credit Petitioner's testimonial evidence regarding that motivation. Ex. 1003 ¶¶ 293, 295. We also credit Petitioner's testimonial evidence that using Wright in Limont would have been merely an application of a well-known operation on a known component for known and intended purposes. Ex. 1003 ¶ 297.

We further credit Petitioner's testimonial evidence that one of ordinary skill in the art would have been motivated to further combine with Xu because the cited portions of the record support it. Ex. 1003 ¶¶ 427–438; Ex. 1004 ¶ 13; Ex. 1005 ¶¶ 78, 267; Ex. 1016 ¶¶ 25, 26, 29–32, 34. We find that the cited portions of the record also support that it was known in the art to protect confidential data, including policies, using protected partitions of memory using encryption and hardware techniques because the cited portions of the record support it. Ex. 1003 ¶¶ 165–222; Ex. 1010, 1, 5, 6, 7; Ex. 1011, codes (54), (57), ¶¶ 4–6, 46; Ex. 1012, codes (54), (57), 1:13–42, 1:49–52, 20:43–62, 37:23–50:17; Ex. 1013, 140–141, 145–148, 229–230; Ex. 1014 ¶¶ 12–13, 124–141, 144–147; Ex. 1015 ¶¶ 31, 34–49, 53, 54, 75–77.

(3) Reasonable Expectation of Success

Petitioner argues that one of ordinary skill in the art would have had a reasonable expectation of success in making the proposed combination. Pet. 19 (citing Ex. 1003 ¶¶ 165–222, 263–298, 427–440), 23 (citing Ex. 1003 ¶¶ 296–297; Ex. 1004 ¶¶ 9, 40, Fig. 1), 42 (citing Ex. 1003 ¶¶ 438–

440). Patent Owner does not present an argument regarding reasonable expectation of success. *See* PO Resp.

Based on the full record, we credit Petitioner's testimonial evidence that one of ordinary skill in the art would have had a reasonable expectation of success in making the proposed combination. Ex. 1003 ¶¶ 296, 417, 438; Ex. 1004 ¶ 71.

i) Objective Indicia of Non-obviousness

Patent Owner does not present any arguments or evidence regarding any objective indicia of nonobviousness for any of the challenged claims. *See* PO Resp.

j) Petitioner Shows by a Preponderance of the Evidence that Claim 1 is Unpatentable

"Once all relevant facts are found, the ultimate legal determination [of obviousness] involves weighing of the fact findings to conclude whether the claimed combination would have been obvious to an ordinary artisan." *Arctic Cat Inc. v. Bombardier Recreational Prods. Inc.*, 876 F.3d 1350, 1361 (Fed. Cir. 2017) (quoting *In re Cyclobenzaprine Hydrochloride Extended-Release Capsule Patent Litig.*, 676 F.3d 1063, 1068–69 (Fed. Cir. 2012)). Above, based on full record before us, we provide our factual findings regarding (1) the level of ordinary skill in the art, (2) the scope and content of the prior art, (3) any differences between the claimed subject matter and the prior art, and (4) objective evidence of nonobviousness.

In particular, we find that (1) Petitioner's proposed level of ordinary skill in the art is consistent with the prior art of record, (2) Limont, Wright, and Xu teach or suggest all the limitations of claim 1, (3) one of ordinary skill in the art would have combined Limont, Wright, and Xu in the manner asserted with a reasonable expectation of success, and (4) no objective

evidence of nonobviousness has been presented in relation to any of the challenged claims. Weighing these underlying factual determinations, a preponderance of the evidence persuades us that claim 1 of the '042 patent is unpatentable over Limont, Wright, and Xu. *Arctic Cat*, 876 F.3d at 1361.

5. Claims 2 and 6–18

Claims 2 and 6–18 depend directly or indirectly from claim 1. Ex. 1001, 19:46–49, 20:13–49. Petitioner argues with citations to the record that Limont or Limont and Wright teach, suggest, or would have been understood to disclose the additional limitations of claims 2 and 6–18. Pet. 46–62. Patent Owner does not contest Petitioner's challenges to these claims apart from its contentions regarding claim 1. *See* PO Resp.

We find that the record fully supports Petitioner's arguments regarding these dependent claims. Accordingly, weighing our factual determinations, a preponderance of the evidence persuades us that claims 2 and 6–18 would have been obvious in view of Limont, Wright, and Xu.

E. Asserted Obviousness Based on Limont, Wright, Xu, and Polson

1. Polson (Ex. 1008)

Polson is specifically "related to bridging local area networks (LAN) and wireless wide area networks (WWAN)." Ex. 1008 ¶ 2. A system of Polson includes gateway 108 with wireless LAN interface 106, a socket to receive WWAN interface 110, and subscriber determination logic. *Id.* ¶¶ 20, 29–40, Fig. 1. A routing engine of gateway 108 facilitates two-way transmission between a LAN and WWAN. *Id.* ¶¶ 39, 43, 56, 63–67, 70–73, Figs. 4, 6. The WWAN may be cellular. *Id.* ¶¶ 5, 51, 54–56.

2. Claims 3–5

Claims 3–5 each directly depend from claim 1 and include "wherein the end-user device is an intermediate network device." Ex. 1001, 19:50–

20:12. Petitioner argues with citations to the record that adding Polson to its proposed combination teaches or suggests the additional limitations of claims 3–5. Pet. 69–77. Petitioner also argues with record support that one of ordinary skill in the art would have had reason to further combine with Polson and would have had a reasonable expectation of success in making that combination. *Id.* at 64–69.

We find that the record fully supports Petitioner's contentions regarding these dependent claims. Patent Owner does not provide arguments specifically for claims 3–5, other than its arguments for claim 1. *See* PO Resp. 18–23.

Accordingly, weighing our factual determinations, a preponderance of the evidence persuades us that claims 3–5 would have been obvious in view of Limont, Wright, Xu, and Polson.

III. CONCLUSION[2]

In summary:

Claims	35 U.S.C. §	References/Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1, 2, 6–18	103(a)	Limont, Wright, Xu	1, 2, 6–18	
3–5	103(a)	Limont, Wright, Xu, Polson	3–5	
Overall Outcome			1–18	

[2] Should Patent Owner wish to pursue amendment of the challenged claim in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding. See* 84 Fed. Reg.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–18 of U.S. Patent No. 9,198,042 B2 have been shown, by a preponderance of the evidence, to be unpatentable; and

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

16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. § 42.8(a)(3), (b)(2).

FOR PETITIONER:

Patrick D. McPherson
Kevin P. Anderson
DUANE MORRIS LLP
PDMcPherson@duanemorris.com
kpanderson@duanemorris.com

FOR PATENT OWNER:

Reza Mirzaie
Dale Chang
James A. Milkey
Neil Rubin
Philip X. Wang
RUSS, AUGUST & KABAT
rmirzaie@raklaw.com
dchang@raklaw.com
jmilkey@raklaw.com
nrubin@raklaw.com
pwang@raklaw.com
rak_headwater@raklaw.com