

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

AMAZON.COM, INC.,
Petitioner,

v.

M2M SOLUTIONS LLC,
Patent Owner.

Case IPR2017-01895
Patent 8,577,358 B2

Before KARL D. EASTHOM, DAVID C. McKONE, and
STACY B. MARGOLIES, *Administrative Patent Judges*.

MARGOLIES, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. INTRODUCTION

In this *inter partes* review, instituted pursuant to 35 U.S.C. § 314, Amazon.com, Inc. (“Petitioner”) challenges the patentability of claims 1–30 of U.S. Patent No. 8,577,358 B2 (Ex. 1002, “the ’358 patent”), owned by M2M Solutions LLC (“Patent Owner”). We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision is entered pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. For the reasons discussed below, Petitioner has not shown by a preponderance of the evidence that claims 1–30 of the ’358 patent are unpatentable.

A. *Procedural History*

Petitioner filed a Petition for *inter partes* review of claims 1–30 of the ’358 patent. Paper 2 (“Pet.”). Patent Owner filed a Preliminary Response. Paper 6 (“Prelim. Resp.”). On February 8, 2018, we instituted an *inter partes* review of claims 1–30 of the ’358 patent on the following grounds:

References	Basis	Challenged Claim(s)
Saylor ¹ and Loughran ²	35 U.S.C. § 103(a) ³	1–3, 6–18, 20, and 23–30
Saylor, Loughran, and Chow ⁴	35 U.S.C. § 103(a)	4, 19, and 21
Saylor, Loughran, and GSM Security ⁵	35 U.S.C. § 103(a)	5
Saylor, Loughran, GSM Security, and Kuskin ⁶	35 U.S.C. § 103(a)	22

Paper 8 (“Inst. Dec.”), 32.

Subsequent to institution, Patent Owner filed a Request for Rehearing (Paper 10), which we denied (Paper 18). Patent Owner filed a Patent Owner Response (Paper 21, “PO Resp.”), Petitioner filed a Reply (Paper 24, “Reply”), and Patent Owner filed a Sur-Reply (Paper 28, “Sur-Reply”). Petitioner relies on the Declaration of Dr. George Kesidis (Ex. 1009). Patent Owner relies on the Declaration of Dr. Majid Sarrafzadeh (Ex. 2009).

¹ U.S. Patent No. 6,400,265 B1, filed Apr. 24, 2001, issued June 4, 2002 (Ex. 1010).

² U.S. Patent Application Publication No. 2002/0129107 A1, filed Mar. 12, 2001, published Sept. 12, 2002 (Ex. 1011).

³ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), revised 35 U.S.C. § 103, effective March 16, 2013. Because the challenged patent was filed before March 16, 2013, we refer to the pre-AIA version of § 103 in this Decision.

⁴ U.S. Patent Application Publication No. 2002/0191557 A1, filed June 14, 2001, published Dec. 19, 2002 (Ex. 1012)

⁵ *ETSI-GSM Technical Specification: European Digital Cellular Telecommunications System (Phase 1); Security-Related Network Functions*, European Telecommunications Standards Institute, Feb. 1992 (Ex. 1013).

⁶ U.S. Patent No. 7,185,196 B1, filed Sept. 15, 2000, issued Feb. 27, 2007 (Ex. 1014).

We held an oral argument on the morning of November 6, 2018, in related proceedings IPR2017-01891, IPR2017-01892, and IPR2017-01893. Paper 33 (“’1891 Tr.”). We held an oral argument later that afternoon in this proceeding and related proceeding IPR2017-01896. Paper 32 (“Tr.”). As previously agreed to by the parties, in light of the potential for subject matter overlap between the two oral arguments, we entered both transcripts into the records of all five related proceedings. Tr. 3:6–11; ’1891 Tr. 3:7–12.

B. Related Matters

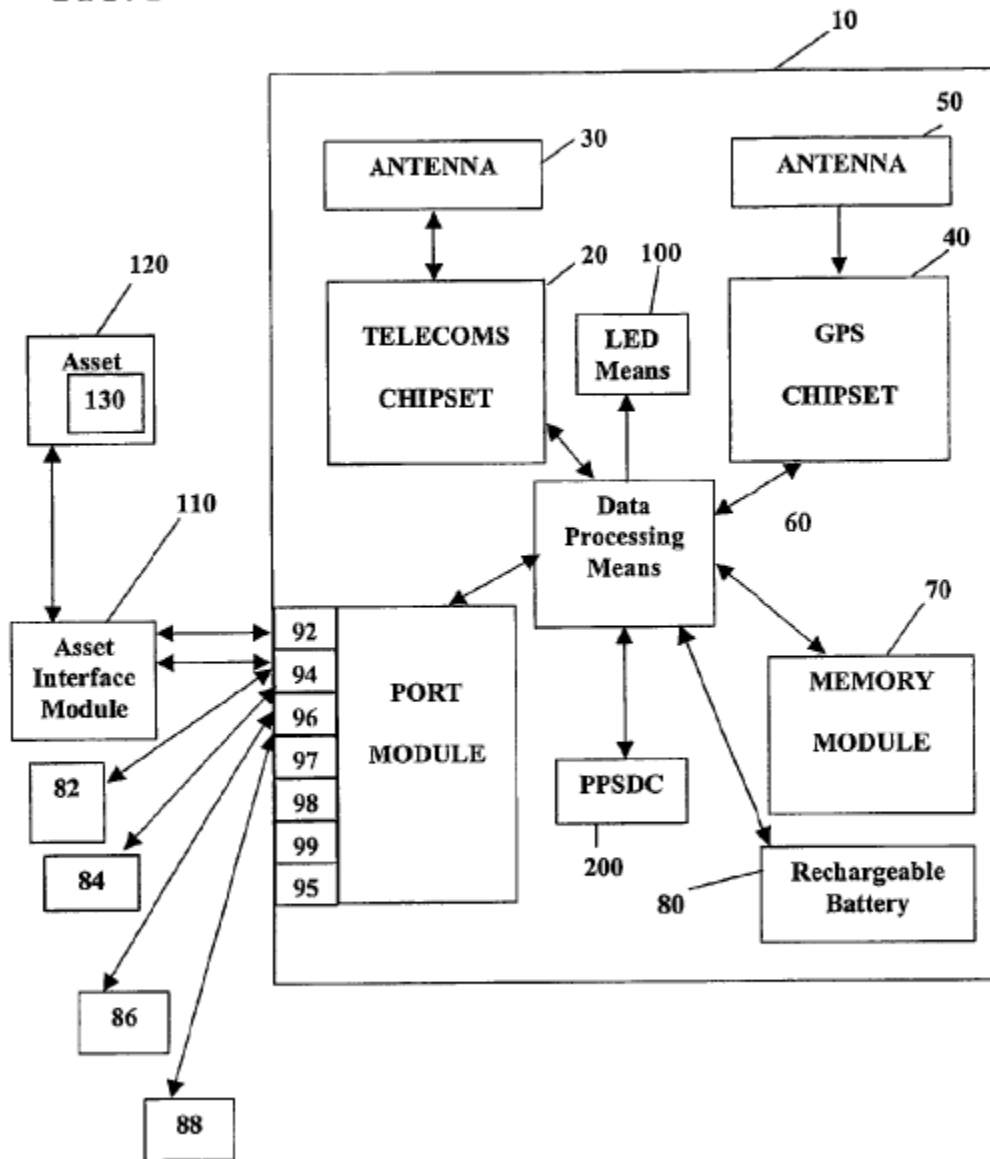
The parties indicate that the ’358 patent has been asserted in *M2M Solutions LLC v. Amazon.com, Inc.*, Case No. 1:17-cv-00202-LPS-CJB (D. Del.). Pet. 1; Paper 4, 1. The ’358 patent also is the subject of IPR2017-01892. Pet. 1–2. Patents related to the ’358 patent are the subjects of the following *inter partes* reviews: IPR2017-01891, IPR2017-01893, and IPR2017-01896. Pet. 1–2; Paper 4, 2–3.

C. The ’358 Patent

The ’358 patent is directed to a system for autonomously monitoring and managing consumer device assets registered with a remote computer server platform. Ex. 1002, Abstract. The ’358 patent explains as background that “a diverse range of electronic tags is available for determining the location of vehicles and such” and that “other systems are available for providing operational status data of remote devices.” *Id.* at 2:16–20. The ’358 patent states that “it would be beneficial if each [remote] asset would comprise the capability to enable a remote server to determine the operational status of the . . . asset and change its operational status according to preset conditions.” *Id.* at 2:25–31.

Figure 1 of the '358 patent, below, illustrates an embodiment of the remote asset management system, including wireless module 10. *Id.* at 13:4–7, 13:11–15.

FIG. 1



As illustrated in Figure 1 above, wireless module 10 includes telecommunications chipset 20 and antenna 30, GPS chipset 40 and antenna 50, data processing means 60, memory module 70, and port module 90.

Id. at 13:11–15. According to the '358 patent, data processing means 60 “is programmed with a data processing asset management application to manage the asset through the port module (90).” *Id.* at 13:28–31. Figure 1 also illustrates asset interface module 110, which is associated with an asset that the wireless module is managing (asset 120) and which makes possible direct communication between the wireless module and the operational control system of the asset or the data collection system of the asset (130). *Id.* at 13:44–49.

Figure 2 of the '358 patent is shown below.

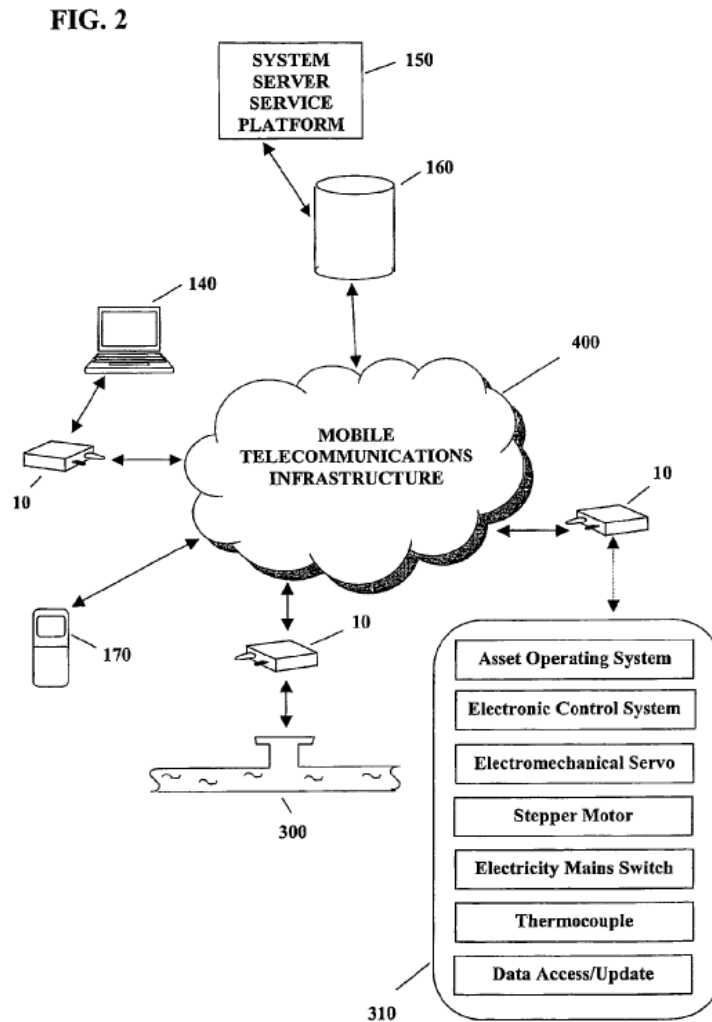


Figure 2 above “illustrates the different applications controlled by the wireless module in the particular example where the mobile telecommunications network operates according to the GSM standard.” *Id.* at 15:12–15. According to the ’358 patent, “[e]ach wireless module (10) comprises the capability to communicate via the mobile telecommunication infrastructure (400).” *Id.* at 15:22–24. The ’358 patent discloses that “[a] mobile phone or message-enabled wireless terminal (170) can communicate with a specific wireless module (10)” or with system server service platform 150 via point of interconnection 160 with mobile telecommunication infrastructure 400. *Id.* at 15:25–29. The ’358 patent also discloses that, “[f]or asset management applications, which comprise a small number of wireless modules (10), it is possible to manage these using a laptop PC (140).” *Id.* at 15:30–32.

The ’358 patent discloses that the remotely located system server service platform “receives data relating to any specific remotely located asset either directly from the wireless module in response to a status request interrogation message . . . or periodically and automatically according to a predetermined and pre-programmed data generation period.” *Id.* at 15:58–64. The ’358 patent describes a number of uses for the invention. For example, the ’358 patent describes an embodiment in which the wireless module can “update an associated in-vehicle GPS car navigation system with map data and localised real-time data relating to traffic congestion events.” *Id.* at 20:45–49. The patent also gives an example of remotely monitoring “the operational characteristics of the asset, such as a car engine performance.” *Id.* at 22:42–45.

D. Illustrative Claim

Among the challenged claims (claims 1–30), claims 1 and 20 are independent. Claim 1 is illustrative of the subject matter of the challenged claims and reads as follows:

1. A method of operating a remote computer server platform to provide a range of consumer services by autonomously monitoring and managing a plurality of consumer device assets wirelessly connected to one or more communications networks, each asset having operating system and application software, nonvolatile memory for storing files of data content for display to a consumer user of the device, and a display apparatus for displaying the stored data content, said method comprising:

providing a remote computer server platform connected to the one or more communications networks, the remote computer server platform configured to execute software applications for monitoring and managing the plurality of consumer device assets, each of said assets being registered with the remote computer server platform;

receiving at the remote computer server platform communications sent from the plurality of consumer device assets containing operational status information and consumer usage information, said communications having automatically resulted from at least one selected from the group consisting of preprogrammed conditions and programming instructions generated by the remote computer server platform;

monitoring the plurality of consumer device assets by the remote computer server platform by automatically processing, according to preprogrammed conditions, the received operational status information and the received consumer usage information;

managing the plurality of consumer device assets by the remote computer server platform, based upon the results of having processed at least some of the received consumer usage information, by sending communications containing

management instructions that cause the stored data content files of one or more assets to be automatically modified; and

wherein the communications received by and sent from the remote computer server platform are transmitted over the one or more communication networks and comprise at least one selected from the group consisting of General Packet Radio Service (GPRS) data messages, Enhanced Data rates for GSM Evolution (EDGE) data messages, and other packet switched data messages.

Id. at 25:15–57 (emphasis added to disputed limitations).

II. DISCUSSION

A. Principles of Law

To prevail in its challenge to Patent Owner’s patent claims, Petitioner must demonstrate by a preponderance of the evidence that the claims are unpatentable. 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d). “In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring *inter partes* review petitions to identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim”)). The burden of persuasion never shifts to Patent Owner. *See Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (citing *Tech. Licensing Corp. v. Videotek, Inc.*, 545 F.3d 1316, 1326–27 (Fed. Cir. 2008)) (discussing the burden of proof in *inter partes* review).

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time of the invention to a

person having ordinary skill in the art. *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 the following: (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 ordinary skill in the art; and (4) objective evidence of nonobviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). “A determination of whether a patent claim is invalid as obvious under § 103 requires consideration of all four *Graham* factors, and it is error to reach a conclusion of obviousness until all those factors are considered.” *Apple Inc. v. Samsung Elecs. Co.*, 839 F.3d 1034, 1048 (Fed. Cir. 2016) (en banc) (citations omitted). “This requirement is in recognition of the fact that each of the *Graham* factors helps inform the ultimate obviousness determination.” *Id.*

B. Level of Ordinary Skill in the Art

In determining whether an invention would have been obvious at the time it was made, 35 U.S.C. § 103 requires us to resolve the level of ordinary skill in the pertinent art at the time of the invention. *Graham*, 383 U.S. at 17. “The importance of resolving the level of ordinary skill in the art lies in the necessity of maintaining objectivity in the obviousness inquiry.” *Ryko Mfg. Co. v. Nu-Star, Inc.*, 950 F.2d 714, 718 (Fed. Cir. 1991). The person of ordinary skill in the art is a hypothetical person who is presumed to have known the relevant art at the time of the invention. *In re GPAC, Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995). Factors that may be considered in determining the level of ordinary skill in the art include, but are not limited to, the types of problems encountered in the art, the sophistication of the technology, and educational level of active workers in the field. *Id.* In a

given case, one or more factors may predominate. *Id.* Generally, it is easier to establish obviousness under a higher level of ordinary skill in the art. *Innovation Toys, LLC v. MGA Entm't, Inc.*, 637 F.3d 1314, 1323 (Fed. Cir. 2011) (“A less sophisticated level of skill generally favors a determination of nonobviousness . . . while a higher level of skill favors the reverse.”).

Petitioner, relying on the testimony of its declarant, Dr. Kesidis, asserts that a person having ordinary skill in the art at the time of the alleged invention would have had “(a) a master’s degree in electrical engineering, computer engineering, computer science or the equivalent, with coursework covering networked devices and servers, or (b) a bachelor’s degree in one of those fields and at least two years of industry experience working with networked devices and servers[,] or (c) four years of industry experience working with networked devices and servers.” Pet. 17 (citing Ex. 1009 ¶ 54)

Patent Owner does not address Dr. Kesidis’s opinion regarding the level of ordinary skill. *See generally* PO Resp. Patent Owner’s declarant, Dr. Sarrafzadeh, likewise does not challenge Dr. Kesidis’s opinion and instead proposes that a person of ordinary skill in the art in May 2002 would have had “(1) a bachelor’s degree in computer engineering, electrical engineering, mathematics, computer science or a closely related field; and (2) a minimum of 2–3 years of industry experience with consumer electronics and related software and firmware, and networked electronic devices.” Ex. 2009 ¶ 14. Dr. Sarrafzadeh also opines that an individual with an advanced degree in a relevant field, such as computer or electrical engineering, would require less industry experience (e.g., 1–2 years). *Id.*

We do not ascertain a meaningful difference between the declarants’ proposals as applied to this case and the parties do not argue that any issue in

the case turns on such a difference. We determine that the level of ordinary skill proposed by Petitioner and Dr. Kesidis is consistent with the challenged patent and the asserted prior art and we therefore adopt that level for the purposes of the analysis below.

C. Claim Construction

In an *inter partes* review based on a petition filed before November 13, 2018, we construe claim terms in an unexpired patent according to their broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b) (2017)⁷; *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016) (upholding the use of the broadest reasonable interpretation standard). Consistent with the broadest reasonable construction, claim terms are presumed to have their ordinary and customary meaning as understood by a person of ordinary skill in the art in the context of the entire patent disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). An inventor may provide a meaning for a term that is different from its ordinary meaning by defining the term in the specification with reasonable clarity, deliberateness, and precision. *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994).

Petitioner proposes constructions for “consumer device asset,” “operational status information,” “consumer usage information,” and “management instructions.” Pet. 7–11. Patent Owner disagrees with Petitioner’s proposed constructions of “consumer device asset,” “operational

⁷ See Changes to the Claim Construction Standard for Interpreting Claims in Trial Proceedings Before the Patent Trial and Appeal Board, 83 Fed. Reg. 51,340 (Oct. 11, 2018) (to be codified at 37 C.F.R. pt. 42).

status information,” and “consumer usage information,” and proposes alternative constructions for each. PO Resp. 14–20. Patent Owner also states that it disagrees with Petitioner’s proposed construction of “management instructions” but that construction of the term is not necessary. *Id.* at 1 n.1.

Patent Owner further argues that the preambles of claims 1 and 20 are limiting because the preambles provide antecedent basis and recite essential structure for the bodies of the claims. *Id.* at 1–14. Petitioner contends that the preambles are not limiting. Pet. 24, 53; Reply 1–4.

We determine that no claim terms require express construction in order to determine the patentability issues raised in this proceeding.

D. Asserted Obviousness over Saylor and Loughran

Petitioner contends that claims 1–3, 6–18, 20, and 23–30 are unpatentable under 35 U.S.C. § 103(a) as obvious over Saylor and Loughran. Pet. 3, 19–56. Relying in part on the testimony of Dr. Kesidis, Petitioner explains how the references allegedly teach or suggest the claim limitations and provides reasoning for combining the teachings of the references as claimed. *Id.* at 19–56.

We have reviewed Petitioner’s and Patent Owner’s arguments and evidence of record. For the reasons that follow, we determine that Petitioner has not shown by a preponderance of the evidence that any one of claims 1–3, 6–18, 20, and 23–30 is unpatentable under 35 U.S.C. § 103(a) as obvious over Saylor and Loughran.

1. Summary of Saylor

Saylor is a U.S. patent titled “System and Method for Monitoring Security Systems by Using Video Images.” Ex. 1010, [54]. Saylor discloses

“a security system where a user may personalize alert notifications for various security devices.” *Id.* at 3:41–43. Figure 1 of Saylor is shown below:

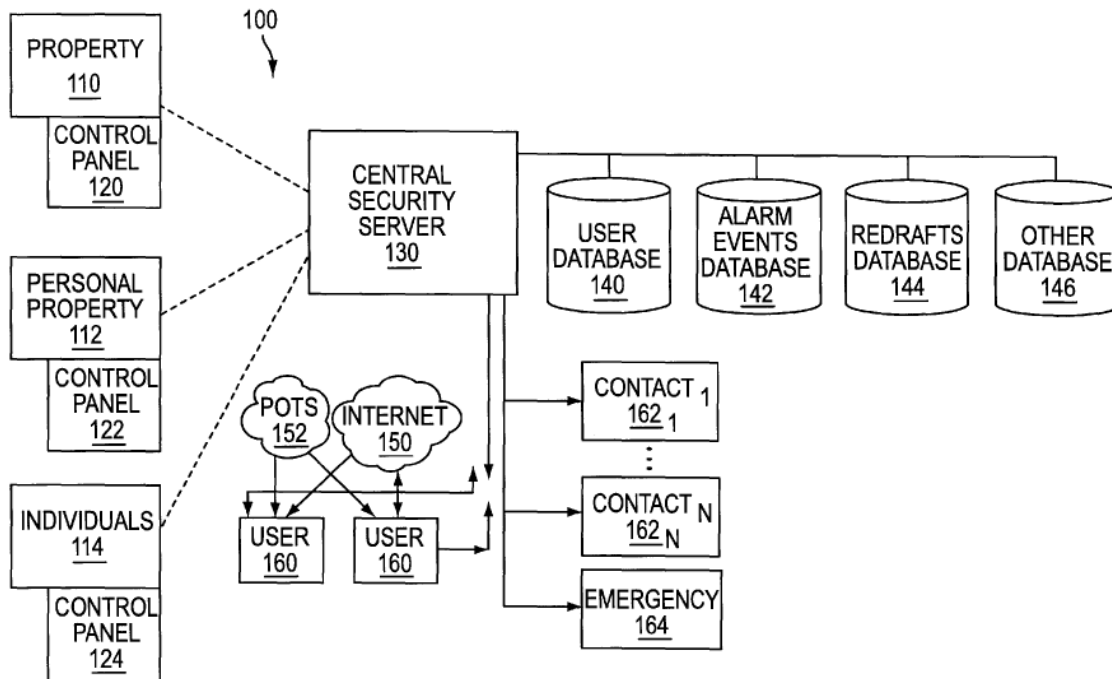


FIG. 1

Figure 1 above illustrates an embodiment of central network security system 100. *Id.* at 4:18–20. Saylor discloses that “[a] user may register various types of security devices, including those associated with property 110, personal property 112 and/or individuals 114[,] with the central security network 130.” *Id.* at 4:20–23. According to Saylor, property 110 may include a user’s home or office and personal property 112 may include a car, boat, or other mobile property. *Id.* at 4:59–64. Saylor explains that “[f]or property 110, security devices may include sensors, detectors and/or other devices for detecting alarm situations,” “[f]or personal property 112, security devices may include global positioning devices,” and “[f]or individuals 114,

security devices may include a panic button or other similar device.” *Id.* at 5:1–8.

According to Saylor, and as illustrated in Figure 1 above, “[a]larm situations may be detected by a control panel 120, 122, 124 associated with and preferably local to each security device and/or system (e.g., property, personal property, individual, or combination).” *Id.* at 4:23–27. Saylor states that “[c]ontrol panels 120, 122, 124 may transmit alarm information to central security network 130.” *Id.* at 4:27–28.

Saylor discloses that the security devices “may be predominantly wireless and communicate locally over short-range radio.” *Id.* at 5:17–20. According to Saylor, each of the sensors “may be equipped with a transmitter and the control panel may be equipped with a receiver.” *Id.* at 5:20–22. Saylor discloses that the control panel “may receive regular status information from the sensors and may be alerted when a sensor detects an alarm situation.” *Id.* at 5:22–25.

Saylor further discloses that “[w]hen an alarm situation is detected, a local control panel 120 or other similar device may communicate to a central security network 130.” *Id.* at 5:32–34. Saylor explains that “[c]ontrol panels 120 may serve as a link between an alarm system (for each property, personal property, individual, or combination) and a central security network.” *Id.* at 5:34–38. Saylor discloses that “[c]ommunication may be established through various mediums,” including “POTS (plain old telephone service), cable modem, DSL (digital subscriber links), wireless (two-way pager, packet switched, telephone cellular networks) and others.” *Id.* at 5:38–49.

Figure 2 of Saylor appears below:

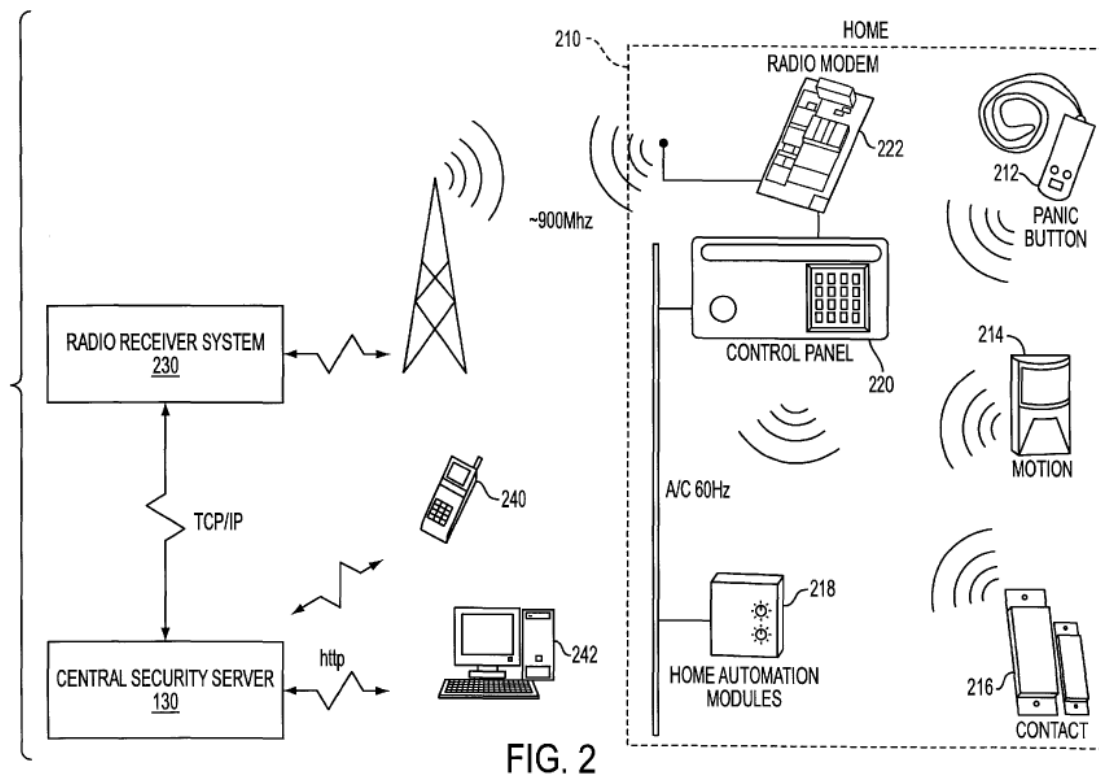


Figure 2 above illustrates an example of an alarm transmission. *Id.* at 5:50–51. According to Saylor, a location such as home 210 may include various security and other devices, including “panic button 212, motion sensor 214, motion contact 216, home automation modules 218, which communicate with control panel 220.” *Id.* at 5:50–55. Saylor discloses that “[c]ontrol panel 220 may send a signal via radio modem 222 to radio receiver system 230” and that “[r]adio receiver system 230 may then communicate with central security server 130 via a TCP/IP connection.” *Id.* at 5:55–57, 5:59–61. “Central security server 130 may then alert users and other identified entities via wireless and/or other devices, such as mobile device 240, via a voice alarm, text message or other notifications.” *Id.* at 5:62–65.

2. *Summary of Loughran*

Loughran is a U.S. patent application publication titled “Method and Apparatus for Automatic Content Handling.” Ex. 1011, [54]. Loughran discloses a mail server that notifies a mobile computing device that the server has received new email. *Id.* at Abstract. Loughran states that its invention, with modification, “may also be used in the area of remote network and/or hardware management . . . , including situations of monitoring, locating and remotely controlling computer hardware.” *Id.* ¶ 2.

Loughran describes as background that when a user maintains a constant, live connection to the network, a notifying signal such as an icon or an audible tone is sent to the user interface when a new email arrives. *Id.* ¶ 3. Loughran states that “mobile users must actively initiate a connection to read their new email” and that without doing so, “there is no way the user can know whether there is new incoming email waiting to be downloaded or read.” *Id.* Loughran discloses a method in which “a mail server notifies a mobile computing device that the server has received new email.” *Id.* at Abstract; *see also id.* ¶¶ 11, 15, 19 (describing method). According to Loughran, the mobile computing device, acting in accordance with an instruction contained within the notification, connects to the server and downloads the email. *Id.* at Abstract. Loughran discloses that “[t]he data connection is preferably a wireless connection and the notification is preferably in the form of a SMS message.” *Id.*

Loughran discloses that its method can also apply to a software upgrade or database update. *Id.* at Abstract, ¶¶ 25, 49. For example, according to Loughran, the notification message “may contain instructions

which cause the computing platform to connect to the data source, download the upgrade software, and install the upgrade.” *Id.* ¶ 25.

3. Analysis

a. Independent claim 1

Claim 1 includes the following limitations regarding communications from the consumer device assets to the remote computer server:

receiving at the remote computer server platform communications sent from the plurality of consumer device assets containing operational status information and consumer usage information, said communications having automatically resulted from at least one selected from the group consisting of preprogrammed conditions and programming instructions generated by the remote computer server platform

* * *

wherein the communications received by and sent from the remote computer server platform are transmitted over the one or more communication networks and comprise at least one selected from the group consisting of General Packet Radio Service (GPRS) data messages, Enhanced Data rates for GSM Evolution (EDGE) data messages, and other packet switched data messages.

Ex. 1002, 25:15–57 (emphases added).

According to Petitioner, Saylor teaches that central security server 130 (illustrated in Figures 1 and 2) communicates with two consumer device assets—control panel 220 and mobile phone 240 (both illustrated in Figure 2). Pet. 26–27. Petitioner asserts that, for the receiving step of claim 1, both operational status information and consumer usage information “must come from some, though not all, of the assets” and that, for example, the mobile phone need only send one of the types of information. Reply 10 (arguing that the ’358 patent specification “discusses numerous

embodiments . . . in which assets do not send both types of information”). With respect to mobile phone 240, Petitioner asserts that, “upon the user pressing the panic button,” the mobile phone sends consumer usage information—“information about the *act* of the button-press and GPS location data indicating *where the user took* the phone.” Reply 18–19; *see also* Pet. 31 (“[A] mobile phone with built-in wireless panic button and GPS transponder automatically sends information regarding the user’s panic button press and GPS position where the user is using the device.”). Petitioner also asserts that the mobile phone sends operational status information in the form of “data about the *existence* of the alert/alarm situation” to the server. Reply 12, 14–16.

Petitioner asserts that the mobile phone sends the communications containing the operational status information and consumer usage information to the central security server *through a control panel*. According to Petitioner, a mobile phone with a built-in panic button is one of the individual security devices 114 with associated control panel 124 illustrated in Saylor’s Figure 1. Pet. 31–32; Reply 16, 17; Tr. 34:13–20 (Petitioner’s counsel confirming that Petitioner is relying on the server receiving communications from the mobile phone *through the control panel*), 91:13–92:16 (same), 21:10–22:11 (Petitioner relying on mobile phone with panic button *and control panel*).

Petitioner relies on communications through the control panel to show that the mobile phone sends communications containing the operational status information and consumer usage information to the central security server *automatically based on preprogrammed conditions*. Reply 16, 17; Pet. 32 (citing Ex. 1010, 3:59–61, 5:32–34, 15:16–20) (relying on Saylor’s

teaching that a control panel is preprogrammed to send information to the central server as soon as an alarm situation is triggered); Ex. 1009 ¶¶ 434, 437, 720. Specifically, Petitioner argues that “Saylor’s mobile phones with built-in panic buttons are individual security devices, which in turn include control panels. Saylor’s teaching that control panels automatically send status information, therefore, encompasses mobile phone 240.” Reply 17; *see also id.* at 16 (“In regard to mobile phone 240 with integrated control panel 124, Saylor teaches that ‘when an alert situation is detected, a security device may inform a local control panel, which may then inform a central security network.’ Thus, mobile phone 240 automatically sends information about an alert/alarm situation to the server upon detecting that situation.”) (citations omitted).

Petitioner further asserts that Saylor teaches that the communications sent from the mobile phone via the control panel to the central security server comprise packet switched messages. Pet. 37 (relying on the control panel for sending packet switched communications to the central security server).

Patent Owner argues that Saylor does not teach that a mobile phone with a built-in panic button sends operational status information and consumer usage information automatically to the remote computer server platform as a result of preprogrammed conditions. PO Resp. 36–39. According to Patent Owner, the disclosures on which Petitioner relies regarding automatic communications describe communications from the control panel to the server, and Saylor does not teach that a mobile phone with built-in panic button is integrated with a control panel or communicates with the central security server through a control panel. *Id.* at 37. Patent

Owner also argues that any communication directly between the mobile phone and the central security server containing alert information and GPS information is not sent automatically to the server; rather, it is sent manually—upon the user pressing a button. *Id.* at 37–38.

Having considered the evidence and arguments presented by Petitioner and Patent Owner, we are not persuaded that Petitioner has shown by a preponderance of the evidence that Saylor teaches that a mobile phone sends information regarding the existence of an alert situation, information regarding the act of a panic button press, or GPS location data to the central security server *automatically* based on preprogrammed conditions—either through a control panel or directly to the server.

First, we agree with Patent Owner that Petitioner has not shown persuasively that Saylor teaches that a mobile phone with a built-in panic button also has a control panel. Figures 1 and 2 of Saylor illustrate standalone panic devices with an associated control panel, but do not illustrate a mobile phone with a control panel. The only mobile phone illustrated in the figures is shown in Figure 2 as communicating directly with the central security server and not via a control panel.

Turning to Figure 2, Saylor discloses that home 210 may include various security devices, such as panic button 212, motion sensor 214, and motion contact 216, “which communicate with control panel 220.” Ex. 1010, 5:51–55. Saylor states that a control panel “may receive regular status information from the sensors and may be alerted when a sensor detects an alarm situation.” *Id.* at 5:22–25. For example, according to Saylor, “the sensors may send digital data packets providing status and other data at 10 second intervals.” *Id.* at 5:27–29. Saylor also discloses that

“when an alert situation is detected, a security device may inform a local control panel, which may then inform a central security network.” *Id.* at 3:59–61; *see also id.* at 5:32–34 (referring to control panel 120 in Figure 1) (“When an alarm situation is detected, a local control panel 120 or other similar device may communicate to a central security network 130 . . .”).

Figure 1 of Saylor also illustrates control panels as part of the security system. *Id.* at Fig. 1, 4:18–27. Saylor discloses that control panel 120 is associated with property 110, which may include a “user’s home, office, vacation house or other locations,” control panel 122 is associated with personal property 112, “such as a car, boat or other mobile property,” and control panel 124 is associated with “personal security devices for individuals 114, such as a panic device.” *Id.* at Fig. 1, 4:20–23, 4:59–65. Saylor discloses that “[c]ontrol panels 120, 122, 124 may transmit alarm information to central security network 130,” which “may process the alarm situation, status data, and/or other relevant information.” *Id.* at 4:27–30.

Saylor provides some additional examples of security devices for property 110, personal property 112, and individuals 114 (*id.* at 4:66–5:8), again giving the example of a panic device for 114, and then states the following:

Other security devices may be implemented with the system of the present invention. *For example, wireless panic buttons with GPS transponders may be available as stand alone devices and may be built into mobile phones, cars, walkmen, bicycles, wristwatches and/or other portable or mobile devices. Thus, a user may alert the authorities any time the user is in danger, from anywhere, and transmit location information detailing the user’s position and other information.*

Id. at 5:8–16 (emphasis added). Saylor thus separately describes a “panic device” that has an associated control panel 124 from “[o]ther” security devices such as a wireless panic button with GPS transponder, which may be built into a mobile phone, and which may be used to alert the authorities and transmit location information “from anywhere.” *Id.* at 4:66–5:16. Saylor does not provide any additional details regarding the mobile phone with built-in panic button and GPS transponder, such as whether the phone has an integrated control panel. Saylor also does not explain how the mobile phone transmits the alert and location information, such as whether it uses packet switched messages, which claim 1 requires because the server must receive communications that comprise packet switched data messages. Saylor also does not describe whether the mobile phone sends GPS data at regular increments or sends such data only upon the pressing of a panic button.

Petitioner’s expert does not further expand upon Saylor’s disclosures regarding the mobile phone with panic button. *See* Ex. 1009 ¶¶ 434 (opining regarding automatic sending of operational status information), 436–437 (opining regarding automatic sending of consumer usage information), 719–720. Like the Petition, Dr. Kesidis merely quotes the passage above from Saylor regarding a built-in panic button and GPS transponder and does not explain whether the mobile phone has an integrated or associated control panel or how it would communicate with the central security server. *See id.* at ¶¶ 436–437, 719–720.

Petitioner thus has not shown that Saylor teaches that the mobile phone sends information to the central security server through a control panel. Nevertheless, even if Petitioner had made such a showing, Petitioner has not shown that Saylor teaches that the mobile phone sends either the

alleged operational status information or the alleged consumer usage information automatically based on preprogrammed conditions.

Petitioner relies on the control panel to show an automatic communication to the server because, according to Petitioner, software in the control panel “decides what to do” when there is a panic button press. Tr. 90:15–17; *see also* Pet. 32 (citing Ex. 1010, 3:59–61, 5:32–34, 15:16–20) (relying on Saylor’s teaching that a control panel is preprogrammed to send information to the central server as soon as an alarm situation is triggered). At the hearing, Petitioner’s counsel gave the example of deciding to “directly call 911 instead of notifying the server” upon a panic button press. Tr. 90:18–20. Petitioner, however, fails to cite any teaching in Saylor in support of its attorney argument that the control panel executes software or otherwise determines whether or not to send information to the central security server that a panic button has been pressed. Saylor describes an example of *the central security network* dialing 911 in response to a panic button press (Ex. 1010, 9:55–57), but Saylor does not disclose that the control panel determines whether or not to send the panic information to the central security server. Nor does Dr. Kesidis provide any testimony explaining how Saylor teaches that the control panel determines whether to automatically send panic button press information *to the server*.

Saylor discloses customizing notifications *from the server* after receiving alarm or alert information, but does not disclose customizing whether to send the panic information to the server in the first instance. *See* Ex. 1010, 9:26–57, 10:35–65. Thus, even if Saylor teaches that the mobile phone with built-in panic button and GPS transponder also has or is associated with a control panel (which Petitioner has not shown

persuasively), Petitioner does not show persuasively that Saylor teaches that information regarding a panic button press is *automatically* sent to the central security server. As briefly described in Saylor, a mobile phone with built-in panic button and GPS transponder sends information regarding a panic alert and the location of the phone upon the pressing of the panic button by the user. *Id.* at 5:13–16. Moreover, Dr. Kesidis does not further expand upon Saylor’s disclosure and explain how the mobile phone with such a panic button sends status and usage information “automatically” even though the information is sent upon the user pressing a button. *See* Ex. 1009 ¶¶ 434 (opining regarding automatic sending of operational status information), 436–437 (opining regarding automatic sending of consumer usage information), 719–720.

Moreover, Petitioner does not point us to any disclosure in the challenged patent that supports reading the “automatically” limitation to encompass a consumer device asset sending operational status or consumer usage information upon a user’s manual press of a button. The ’358 patent describes automatically prioritizing pull down menus based on consumer usage information, but does not describe sending the consumer usage information automatically to the server, let alone sending it automatically in response to a trigger by the user. Ex. 1002, 3:60–4:3. Petitioner’s position in this proceeding also is inconsistent with its position in IPR2017-01891, in which Petitioner conceded that a system requiring a user to manually press a synchronization button on a personal data assistant would not send the synchronization information automatically because the process is not fully automatic, even though some of the processing handling the communication is automatic. ’1891 Tr. 30:7–19. Petitioner’s concession is equally

applicable here, where Petitioner contends that a manually triggered signal satisfies “said communications having automatically resulted from the group consisting of preprogrammed conditions and programming instructions generated by the remote computer server platform,” as recited in claim 1.

Finally, Petitioner’s reliance on Patent Owner’s expert’s deposition testimony regarding information that is automatically sent to a server is misplaced. *See* Reply 18 (citing Ex. 1022, 202:25–204:22). Dr. Sarrafzadeh testified about using Google Maps in 2018 and did not testify about any teaching in Saylor or what one of ordinary skill in the art would have understood about Saylor’s disclosure at the time of the claimed invention. *See* Ex. 1022, 202:25–204:22.

In sum, Petitioner has not shown that Saylor teaches receiving at the central security server either operational status information or consumer usage information sent from a mobile phone with a built-in panic button automatically as a result of preprogrammed conditions or programming instructions generated by the central security server. Petitioner thus has not shown by a preponderance of the evidence that Saylor teaches the receiving step of claim 1. Petitioner does not rely on Loughran for teaching any aspect of this claim limitation. Pet. 30–32.

Accordingly, Petitioner has not shown that the subject matter of claim 1 of the ’358 patent would have been obvious over Saylor and Loughran.

b. Independent claim 20

Independent claim 20 is similar to claim 1 in material respects but recites in the preamble two pluralities of consumer device assets—a first plurality “wirelessly connected to a cellular mobile telecommunications

network” and a second plurality “wirelessly connected to the Internet.” The receiving step and the wherein clause are also different in that they account for communications from the two pluralities of consumer device assets as follows:

receiving at the remote computer server platform communications sent *over the one or more communications networks* from *the first and second pluralities* of consumer device assets containing operational status information and consumer usage information, said communications having automatically resulted from at least one selected from the group consisting of preprogrammed conditions and programming instructions generated by the remote computer server platform, and

wherein *said* communications comprise at least one selected from the group consisting of General Packet Radio Service (GPRS) data messages, Enhanced Data rates for GSM Evolution (EDGE) data messages, and other packet switched data messages.

Ex. 1002, 27:26–28:14 (emphases added).

Petitioner contends that the “first plurality of consumer device assets” are “the cellular phones of multiple users being monitored concurrently by the central security server” and the “second plurality of consumer device assets” are “the control panels 220 of multiple homes being concurrently monitored by the central security server.” Pet. 53–54. Petitioner relies on its analysis of the receiving step of claim 1 for the analysis of the receiving step of claim 20. *Id.* at 54.

For the reasons explained above in connection with claim 1, Petitioner has not shown that the subject matter of claim 20 would have been obvious over Saylor and Loughran.

c. Dependent claims 2, 3, 6–18, and 23–30

Claims 2, 3, and 6–18 depend directly or indirectly from claim 1 and claims 23–30 depend directly or indirectly from claim 20. Petitioner does not provide any additional analysis of the receiving step of the corresponding independent claim in its analysis of these dependent claims. *See* Pet. 38–52, 55–56. Accordingly, for the reasons explained above, Petitioner has not shown that the subject matter of any of claims 2, 3, 6–18, and 23–30 would have been obvious over Saylor and Loughran.

E. Asserted Obviousness over Saylor, Loughran, and Chow

Petitioner contends that claims 4, 19, and 21 of the '358 patent are unpatentable under 35 U.S.C. § 103(a) as obvious over Saylor, Loughran, and Chow. Pet. 3, 57–63. Claims 4 and 19 depend from claim 1 and claim 21 depends from claim 20. In its analysis of the dependent claims, Petitioner does not add to its analysis of the limitations of claims 1 and 20. *Id.* at 57–63. Accordingly, for the reasons explained above in connection with claims 1 and 20, Petitioner has not shown that the subject matter of claim 4, 19, or 21 would have been obvious over Saylor, Loughran, and Chow.

F. Asserted Obviousness over Saylor, Loughran, and GSM Security

Petitioner contends that claim 5 of the '358 patent is unpatentable under 35 U.S.C. § 103(a) as obvious over Saylor, Loughran, and GSM Security. Pet. 3, 63–64. Claim 5 depends from claim 1. In its analysis of claim 5, Petitioner does not add to its analysis of the limitations of claim 1. *Id.* at 63–64. Accordingly, for the reasons explained above in connection with claim 1, Petitioner has not shown that the subject matter of claim 5 would have been obvious over Saylor, Loughran, and GSM Security.

G. Asserted Obviousness over Saylor, Loughran, GSM Security, and Kuskin

Petitioner contends that claim 22 is unpatentable under 35 U.S.C. § 103(a) as obvious over Saylor, Loughran, GSM Security, and Kuskin. Pet. 3, 64–66. Claim 22 depends from claim 20. In its analysis of claim 22, Petitioner does not add to its analysis of the limitations of claim 20. *Id.* at 63–64. Accordingly, for the reasons explained above in connection with claim 20, Petitioner has not shown that the subject matter of claim 22 would have been obvious over Saylor, Loughran, GSM Security, and Kuskin.

III.CONCLUSION

Petitioner has *not* proved by a preponderance of the evidence that (i) any of claims 1–3, 6–18, 20, and 23–30 are unpatentable under 35 U.S.C. § 103(a) as obvious over Saylor and Loughran; (ii) any of claims 4, 19, and 21 of the '358 patent are unpatentable under 35 U.S.C. § 103(a) as obvious over Saylor, Loughran, and Chow; (iii) claim 5 of the '358 patent is unpatentable under 35 U.S.C. § 103(a) as obvious over Saylor, Loughran, and GSM Security; or (iv) claim 22 is unpatentable under 35 U.S.C. § 103(a) as obvious over Saylor, Loughran, GSM Security, and Kuskin.

IV. ORDER

Accordingly, it is

ORDERED that claims 1–30 of U.S. Patent No. 8,577,358 B2 have not been shown to be unpatentable based on the grounds presented in this proceeding; and

FURTHER ORDERED that, because this is a final written decision, 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.

IPR2017-01895
Patent 8,577,358 B2

FOR PETITIONER:

Christina J. McCullough
Daniel T. Shvodian
Wing H. Liang
PERKINS COIE LLP
cmccullough@perkinscoie.com
dshvodian@perkinscoie.com
wliang@perkinscoie.com

FOR PATENT OWNER:

Denis J. Sullivan
Thomas Hoehner
BARCLAY DAMON LLP
dsullivan@barclaydamon.com
thoehner@barclaydamon.com