

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Reexamination of:
Raleigh

Patent No.: 9,615,192

Issue Date: April 4, 2017

For: MESSAGE LINK SERVER WITH
PLURAL MESSAGE DELIVERY
TRIGGERS

Examiner: Not Yet Assigned

Art Unit: Not Yet Assigned

REQUEST FOR *EX PARTE* REEXAMINATION

Mail Stop "Ex Parte Reexam"
Attn: Central Reexamination Unit
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir or Madam:

Walmart Inc. ("Walmart" or "Requestor") requests *ex parte* reexamination of claims 1-15 of U.S. Patent No. 9,615,192 ("the '192 Patent"), which is assigned to Headwater Research LLC ("Patent Owner"), in view of the substantial new questions of patentability raised by the prior art submitted with this request. The submitted prior art renders claims 1-15 unpatentable, thus warranting reexamination of those claims. In support of its request, Walmart provides the following:

- A statement pointing out each substantial new question of patentability for each claim for which Walmart is requesting reexamination (37 C.F.R. § 1.510(b)(1));
- A detailed explanation of the pertinence and manner of applying the cited prior art references to each identified claim, including how statements of the Patent Owner are being used (37 C.F.R. § 1.510(b)(2));
- Copies of the prior art relied on in establishing the substantial new question of patentability with respect to the above-listed claims of the '192 Patent (37 C.F.R. § 1.510(b)(3));

- A copy of the entire '192 Patent, including the front face, drawings, specification, and claims (37 C.F.R. § 1.510(b)(4));
- A certification that a copy of the request has been served in its entirety on the Patent Owner at the address as provided for in 37 C.F.R. § 1.33(c) (37 C.F.R. § 1.510(b)(5));
- A certification that the statutory estoppel provisions of 35 U.S.C. §§ 315(e)(1) & 325(e)(1) do not prohibit Walmart from filing this *ex parte* reexamination request (37 C.F.R. § 1.510(b)(6)); and
- Fees for requesting reexamination (37 C.F.R. § 1.20(c)(2))

TABLE OF CONTENTS

I.	STATEMENT UNDER 37 C.F.R. § 1.510(B)(1) POINTING OUT SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY	1
A.	Introduction.....	1
B.	The '192 Patent and Prosecution History	2
1.	Summary of the '192 Patent	2
a.	Claims of the '192 Patent.....	6
2.	Prosecution History of U.S. Application No. 15/211,430	10
3.	Prior Inter Partes Review Proceedings	13
a.	<i>Samsung Elecs. Co. v. Headwater Rsch. LLC</i> , IPR2024- 00010.....	13
b.	<i>Amazon.com Servs., LLC, et al. v. Headwater Rsch. LLC</i> , IPR2026-00088	13
c.	<i>Target Corp. v. Headwater Rsch. LLC</i> , IPR2026-00154.....	14
4.	Prior Relevant Federal District Court Litigation	15
C.	Overview of Cited Art and SNQs Raised	15
1.	U.S. Patent Pub. No. 2002/0023010 (" <i>Rittmaster</i> ") (Ex. C)	17
2.	U.S. Patent Pub. No. 2006/0268696 (" <i>Konstantinov</i> ") (Ex. D).....	20
3.	Andrew S. Tanenbaum and Maarten Van Steen, <i>Distributed Systems: Principles and Paradigms</i> (Pearson Education, 2d ed. 2007) (" <i>Distributed Systems</i> ") (Ex. E).....	21
4.	Andrew S. Tanenbaum, <i>Computer Networks</i> (Pearson Education, 4th ed. 2003) (" <i>Computer Networks</i> ") (Ex. F).....	21
5.	U.S. Patent No. 8,064,934 (" <i>Klassen</i> ") (Ex. K).....	22
6.	U.S. Patent No. 7,082,615 (" <i>Ellison</i> ") (Ex. L)	23
7.	U.S. Pat. Pub. 2009/0282256 (" <i>Rakic</i> ") (Ex. M).....	23
8.	U.S. Pat. Pub. 2002/0186845 (" <i>Dutta</i> ") (Ex. N).....	23
9.	U.S. Pat. Pub. 2005/0144294 (" <i>Gellens</i> ") (Ex. O).....	23
10.	U.S. Pat. Pub. 2006/0129691 (" <i>Coffee</i> ") (Ex. S).....	24
11.	U.S. Pat. Pub. 2005/0108397 (" <i>Basso</i> ") (Ex. T).....	24
12.	AU App. No. 2007200530 (" <i>Shenfield</i> ") (Ex. U).....	24
D.	Discretionary Denial Under 35 U.S.C. § 325(d) Is Not Warranted	27
II.	DETAILED EXPLANATION UNDER 37 C.F.R. § 1.510(B)(2) OF THE PERTINENCY AND MANNER OF APPLYING THE CITED PRIOR ART TO EVERY CLAIM FOR WHICH REEXAMINATION IS REQUESTED	27

A.	Level of Ordinary Skill in the Art.....	28
B.	Claim Construction	28
1.	“software components”	28
2.	“wherein one of the message delivery triggers is the receipt of a particular network element message from one of the network elements”	28
3.	“device messaging agent”	29
C.	Ground 1: Claims 1-3, 5-7, 9, and 11-15 are Anticipated by Rittmaster	29
1.	Claim 1	30
a.	1[PRE] “ <i>A message link server comprising:</i> ”	30
b.	1[a] “ <i>a transport services stack to maintain a respective secure message link through an Internet network between the message link server and a respective device link agent on each of a plurality of wireless end-user devices,</i> ”	31
c.	1[b] “ <i>each of the wireless end-user devices comprising multiple software components authorized to receive and process data from secure message link messages received via a device link agent on that device,</i> ”	34
d.	1[c] “ <i>an interface to a network to receive network element messages from a plurality of network elements, the received network element messages comprising respective message content and requests for delivery of the respective message content to respective wireless end-user devices, the respective message content including data for, and an identification of, a respective one of the authorized software components,</i> ”	35
e.	1[d] “ <i>a message buffer system including a memory and logic, the memory to buffer content from the received network element messages for which delivery is requested to a given one of the wireless end-user devices</i> ”	37
f.	1[e] “ <i>the logic to determine when one of a plurality of message delivery triggers for the given one of the wireless end-user devices has occurred, wherein for at least some of the received network element messages, the receipt of such a message by the message buffer system is not a message delivery trigger, and for at least one of the message delivery triggers, the trigger is an occurrence of an asynchronous event with time-critical messaging needs, and</i> ”	39
g.	1[f] “ <i>upon determining that one of the message delivery triggers has occurred, the logic further to supply one or more messages comprising the buffered content to the</i> ”	

	<i>transport services stack for delivery on the secure message link maintained between the transport services stack and a device link agent on the given one of the wireless end-user devices.”</i>	41
2.	Claim 2 – “ <i>an encrypt function to encrypt the one or more messages supplied to the transport services stack for delivery on the secure message link maintained between the message link server and the device link agent on the given one of the wireless end-user devices.</i> ”	41
3.	Claim 3 – “ <i>the encrypted one or more messages are transported to the device link agent on the given one of the wireless end-user devices using one or more of encryption on the transport services stack, IP (Internet Protocol) layer encryption, and tunneling.</i> ”	42
4.	Claim 5 – “ <i>wherein the transport services stack is further to receive, over each of the respective secure message links, upload messages forwarded by the respective device link agents from at least a subset of the device software components, each of the upload messages identifying a corresponding one of the network elements to which the device respective software component has requested delivery, the network server system using the interface to a network to deliver content from the upload messages to the respective identified network elements.</i> ”	43
5.	Claim 6 – “ <i>wherein at least one of the one or more messages for delivery by the transport services stack comprises multiple identifier/data pairs.</i> ”	43
6.	Claim 7 – “ <i>the device messaging agent on at least one of the wireless end-user devices further to initiate the respective secure Internet data message link to the transport services stack.</i> ”	44
7.	Claim 9 – “ <i>one of the message delivery triggers is the expiration of a periodic timer.</i> ”	44
8.	Claim 11 – “ <i>one of the message delivery triggers is the receipt of a transmission on the respective secure message link from the device link agent of the given one of the wireless end-user devices, or a response generated to a transmission received from that device link agent.</i> ”	45
9.	Claim 12 – “ <i>the transmission is a heartbeat message generated by the given device link agent, or a request received from the given device link agent.</i> ”	45
10.	Claim 13 – “ <i>one of the message delivery triggers is the receipt of a particular network element message from one of the network elements.</i> ”	45

11.	Claim 14 – “one of the message delivery triggers is based on an amount of wireless network data usage consumed by the given one of the wireless end-user devices.”	46
12.	Claim 15.....	47
a.	15[PRE] “A method of operating a message link server, comprising:”	47
b.	15[a] “maintaining a respective secure message link through an Internet network between the message link server and a respective device link agent on each of a plurality of wireless end-user devices, each of the wireless end-user devices comprising multiple software components authorized to receive and process data from secure message link messages received via a device link agent on that device;”	47
c.	15[b] “receiving network element messages from a plurality of network elements, the received network element messages comprising respective message content and requests for delivery of the respective message content to respective wireless end-user devices, the respective message content including data for, and an identification of, a respective one of the authorized software components;”	48
d.	15[c] “buffering content from the received network element messages for which delivery is requested to a given one of the wireless end-user devices;”	48
e.	15[d] “determining when one of a plurality of message delivery triggers for the given one of the wireless end-user devices has occurred, wherein for at least some of the received network element messages, the receipt of such a message is not a message delivery trigger, and for at least one of the message delivery triggers, the trigger is an occurrence of an asynchronous event with time-critical messaging needs; and”	49
f.	15[e] “upon determining that one of the message delivery triggers has occurred, supplying one or more messages comprising the buffered content for delivery on the secure message link maintained between the message link server and a device link agent on the given one of the wireless end-user devices.”	49
D.	Ground 2: The Combination of Rittmaster and Knowledge of a PHOSITA (as Evidenced by <i>Distributed Systems</i> and/or <i>Computer Networks</i> Textbooks) Render Obvious Claims 1-3, 5-7 and 9-15	50
1.	Claim 1.....	50
a.	1[PRE] “A message link server comprising:”	50

b.	1[a] “a transport services stack to maintain a respective secure message link through an Internet network between the message link server and a respective device link agent on each of a plurality of wireless end-user devices,”	50
c.	1[b] “each of the wireless end-user devices comprising multiple software components authorized to receive and process data from secure message link messages received via a device link agent on that device;”	52
d.	1[c] “an interface to a network to receive network element messages from a plurality of network elements, the received network element messages comprising respective message content and requests for delivery of the respective message content to respective wireless end-user devices, the respective message content including data for, and an identification of, a respective one of the authorized software components,”	54
e.	1[d] “a message buffer system including a memory and logic, the memory to buffer content from the received network element messages for which delivery is requested to a given one of the wireless end-user devices,”	56
f.	1[e] “the logic to determine when one of a plurality of message delivery triggers for the given one of the wireless end-user devices has occurred, wherein for at least some of the received network element messages, the receipt of such a message by the message buffer system is not a message delivery trigger, and for at least one of the message delivery triggers, the trigger is an occurrence of an asynchronous event with time-critical messaging needs, and”	58
g.	1[f] “upon determining that one of the message delivery triggers has occurred, the logic further to supply one or more messages comprising the buffered content to the transport services stack for delivery on the secure message link maintained between the transport services stack and a device link agent on the given one of the wireless end-user devices.”	59
2.	Claim 2 – “an encrypt function to encrypt the one or more messages supplied to the transport services stack for delivery on the secure message link maintained between the message link server and the device link agent on the given one of the wireless end-user devices.”	60
3.	Claim 3 – “the encrypted one or more messages are transported to the device link agent on the given one of the wireless end-user	

	<i>devices using one or more of encryption on the transport services stack, IP (Internet Protocol) layer encryption, and tunneling.”</i>	60
4.	Claim 5 – “ <i>wherein the transport services stack is further to receive, over each of the respective secure message links, upload messages forwarded by the respective device link agents from at least a subset of the device software components, each of the upload messages identifying a corresponding one of the network elements to which the device respective software component has requested delivery, the network server system using the interface to a network to deliver content from the upload messages to the respective identified network elements.</i> ”	61
5.	Claim 6 – “ <i>wherein at least one of the one or more messages for delivery by the transport services stack comprises multiple identifier/data pairs.</i> ”	62
6.	Claim 7 – “ <i>the device messaging agent on at least one of the wireless end-user devices further to initiate the respective secure Internet data message link to the transport services stack.</i> ”	62
7.	Claim 9 – “ <i>one of the message delivery triggers is the expiration of a periodic timer.</i> ”	63
8.	Claim 10 – “ <i>the period of the timer is fractionally shorter than a maximum data message interval beyond which the secure message link is taken down.</i> ”	63
9.	Claim 11 – “ <i>one of the message delivery triggers is the receipt of a transmission on the respective secure message link from the device link agent of the given one of the wireless end-user devices, or a response generated to a transmission received from that device link agent.</i> ”	64
10.	Claim 12 – “ <i>the transmission is a heartbeat message generated by the given device link agent, or a request received from the given device link agent.</i> ”	64
11.	Claim 13 – “ <i>one of the message delivery triggers is the receipt of a particular network element message from one of the network elements.</i> ”	64
12.	Claim 14 – “ <i>one of the message delivery triggers is based on an amount of wireless network data usage consumed by the given one of the wireless end-user devices.</i> ”	65
13.	Claim 15.....	65
a.	15[PRE], 15[a] “ <i>A method of operating a message link server, comprising: maintaining a respective secure message link through an Internet network between the message link server and a respective device link agent on each of a plurality of wireless end-user devices,</i> ”	65

b.	15[a] “each of the wireless end-user devices comprising multiple software components authorized to receive and process data from secure message link messages received via a device link agent on that device;”	66
c.	15[b] “receiving network element messages from a plurality of network elements, the received network element messages comprising respective message content and requests for delivery of the respective message content to respective wireless end-user devices, the respective message content including data for, and an identification of, a respective one of the authorized software components;”	66
d.	15[c] “buffering content from the received network element messages for which delivery is requested to a given one of the wireless end-user devices;”	66
e.	15[d] “determining when one of a plurality of message delivery triggers for the given one of the wireless end-user devices has occurred, wherein for at least some of the received network element messages, the receipt of such a message is not a message delivery trigger, and for at least one of the message delivery triggers, the trigger is an occurrence of an asynchronous event with time-critical messaging needs; and”	66
f.	15[e] “upon determining that one of the message delivery triggers has occurred, supplying one or more messages comprising the buffered content for delivery on the secure message link maintained between the message link server and a device link agent on the given one of the wireless end-user devices.”	67
E.	Ground 3: The Combination of <i>Rittmaster</i> and <i>Shenfield</i> and/or Knowledge of a PHOSITA (as Evidenced by <i>Distributed Systems</i> and/or <i>Computer Networks</i>) Render Obvious Claims 1-3, 5-7, and 9-15	67
1.	Claim 1	68
a.	1[PRE] “A message link server comprising;”	68
b.	1[a] “a transport services stack to maintain a respective secure message link through an Internet network between the message link server and a respective device link agent on each of a plurality of wireless end-user devices;”	68
c.	1[b] “each of the wireless end-user devices comprising multiple software components authorized to receive and process data from secure message link messages received via a device link agent on that device;”	71

d.	1[c] “an interface to a network to receive network element messages from a plurality of network elements, the received network element messages comprising respective message content and requests for delivery of the respective message content to respective wireless end-user devices, the respective message content including data for, and an identification of, a respective one of the authorized software components”	71
e.	1[d] “a message buffer system including a memory and logic, the memory to buffer content from the received network element messages for which delivery is requested to a given one of the wireless end-user devices”	72
f.	1[e] “the logic to determine when one of a plurality of message delivery triggers for the given one of the wireless end-user devices has occurred, wherein for at least some of the received network element messages, the receipt of such a message by the message buffer system is not a message delivery trigger, and for at least one of the message delivery triggers, the trigger is an occurrence of an asynchronous event with time-critical messaging needs, and”	73
g.	1[f] “upon determining that one of the message delivery triggers has occurred, the logic further to supply one or more messages comprising the buffered content to the transport services stack for delivery on the secure message link maintained between the transport services stack and a device link agent on the given one of the wireless end-user devices.”	74
2.	Claim 2 – “an encrypt function to encrypt the one or more messages supplied to the transport services stack for delivery on the secure message link maintained between the message link server and the device link agent on the given one of the wireless end-user devices”	75
3.	Claim 3 – “the encrypted one or more messages are transported to the device link agent on the given one of the wireless end-user devices using one or more of encryption on the transport services stack, IP (Internet Protocol) layer encryption, and tunneling.”	75
4.	Claim 5 – “wherein the transport services stack is further to receive, over each of the respective secure message links, upload messages forwarded by the respective device link agents from at least a subset of the device software components, each of the upload messages identifying a corresponding one of the network elements to which the device respective software component has requested delivery, the network server system using the interface to a network to deliver	

	<i>content from the upload messages to the respective identified network elements.”</i>	76
5.	Claim 6 – “wherein at least one of the one or more messages for delivery by the transport services stack comprises multiple identifier/data pairs.”	76
6.	Claim 7 – “the device messaging agent on at least one of the wireless end-user devices further to initiate the respective secure Internet data message link to the transport services stack.”	77
7.	Claim 9 – “one of the message delivery triggers is the expiration of a periodic timer.”	77
8.	Claim 10 – “the period of the timer is fractionally shorter than a maximum data message interval beyond which the secure message link is taken down.”	77
9.	Claim 11 – “one of the message delivery triggers is the receipt of a transmission on the respective secure message link from the device link agent of the given one of the wireless end-user devices, or a response generated to a transmission received from that device link agent.”	78
10.	Claim 12 – “the transmission is a heartbeat message generated by the given device link agent, or a request received from the given device link agent.”	78
11.	Claim 13 – “one of the message delivery triggers is the receipt of a particular network element message from one of the network elements.”	79
12.	Claim 14 – “one of the message delivery triggers is based on an amount of wireless network data usage consumed by the given one of the wireless end-user devices.”	79
13.	Claim 15.....	79
a.	15[PRE], 15[a] “A method of operating a message link server, comprising: maintaining a respective secure message link through an Internet network between the message link server and a respective device link agent on each of a plurality of wireless end-user devices,”	79
b.	15[a] “each of the wireless end-user devices comprising multiple software components authorized to receive and process data from secure message link messages received via a device link agent on that device;”	80
c.	15[b] “receiving network element messages from a plurality of network elements, the received network element messages comprising respective message content and requests for delivery of the respective message content to respective	

	<i>wireless end-user devices, the respective message content including data for, and an identification of, a respective one of the authorized software components;”</i>	80
d.	15[c] <i>“buffering content from the received network element messages for which delivery is requested to a given one of the wireless end-user devices;”</i>	81
e.	15[d] <i>“determining when one of a plurality of message delivery triggers for the given one of the wireless end-user devices has occurred, wherein for at least some of the received network element messages, the receipt of such a message is not a message delivery trigger, and for at least one of the message delivery triggers, the trigger is an occurrence of an asynchronous event with time-critical messaging needs; and”</i>	81
f.	15[e] <i>“upon determining that one of the message delivery triggers has occurred, supplying one or more messages comprising the buffered content for delivery on the secure message link maintained between the message link server and a device link agent on the given one of the wireless end-user devices.”</i>	81
F.	Ground 4: The Combination of <i>Rittmaster</i> and <i>Konstantinov</i> and/or <i>Klassen</i> Render Obvious Claims 1-3, 5-7, and 9-15	82
1.	Claim 1	84
a.	1[PRE] <i>“A message link server comprising:”</i>	84
b.	1[a] <i>“a transport services stack to maintain a respective secure message link through an Internet network between the message link server and a respective device link agent on each of a plurality of wireless end-user devices,”</i>	84
c.	1[b] <i>“each of the wireless end-user devices comprising multiple software components authorized to receive and process data from secure message link messages received via a device link agent on that device;”</i>	86
d.	1[c] <i>“an interface to a network to receive network element messages from a plurality of network elements, the received network element messages comprising respective message content and requests for delivery of the respective message content to respective wireless end-user devices, the respective message content including data for, and an identification of, a respective one of the authorized software components; and”</i>	86
e.	1[d] <i>“a message buffer system including a memory and logic, the memory to buffer content from the received network</i>	

	<i>element messages for which delivery is requested to a given one of the wireless end-user devices”</i>	87
f.	1[e] <i>“the logic to determine when one of a plurality of message delivery triggers for the given one of the wireless end-user devices has occurred, wherein for at least some of the received network element messages, the receipt of such a message by the message buffer system is not a message delivery trigger, and for at least one of the message delivery triggers, the trigger is an occurrence of an asynchronous event with time-critical messaging needs, and”</i>	88
g.	1[f] <i>“upon determining that one of the message delivery triggers has occurred, the logic further to supply one or more messages comprising the buffered content to the transport services stack for delivery on the secure message link maintained between the transport services stack and a device link agent on the given one of the wireless end-user devices.”</i>	89
2.	Claims 2-3 and 5-6	89
3.	Claim 7 – <i>“the device messaging agent on at least one of the wireless end-user devices further to initiate the respective secure Internet data message link to the transport services stack”</i>	89
4.	Claims 9-14	90
5.	Claim 15	90
a.	15[PRE], 15[a] <i>“A method of operating a message link server, comprising: maintaining a respective secure message link through an Internet network between the message link server and a respective device link agent on each of a plurality of wireless end-user devices,”</i>	90
b.	15[a] <i>“each of the wireless end-user devices comprising multiple software components authorized to receive and process data from secure message link messages received via a device link agent on that device,”</i>	90
c.	15[b] <i>“receiving network element messages from a plurality of network elements, the received network element messages comprising respective message content and requests for delivery of the respective message content to respective wireless end-user devices, the respective message content including data for, and an identification of, a respective one of the authorized software components,”</i>	90
d.	15[c] <i>“buffering content from the received network element messages for which delivery is requested to a given one of the wireless end-user devices;”</i>	91

e.	15[d] “determining when one of a plurality of message delivery triggers for the given one of the wireless end-user devices has occurred, wherein for at least some of the received network element messages, the receipt of such a message is not a message delivery trigger, and for at least one of the message delivery triggers, the trigger is an occurrence of an asynchronous event with time-critical messaging needs; and”	91
f.	15[e] “upon determining that one of the message delivery triggers has occurred, supplying one or more messages comprising the buffered content for delivery on the secure message link maintained between the message link server and a device link agent on the given one of the wireless end-user devices.”	91
G.	Ground 5: Any Combination of <i>Rittmaster</i> and/or <i>Shenfield</i> and/or <i>Konstantinov/Klassen</i> (as Discussed in Grounds 1-4) In Further Combination with <i>Ellison</i> Renders Obvious Claim 4.....	91
H.	Ground 6: Any Combination of <i>Rittmaster</i> and/or <i>Shenfield</i> and/or <i>Konstantinov/Klassen</i> (as Discussed in Grounds 1-4) In Further Combination with <i>Coffee</i> or <i>Basso</i> Renders Obvious Claim 6.....	93
I.	Ground 7: Any Combination of <i>Rittmaster</i> and/or <i>Shenfield</i> and/or <i>Konstantinov/Klassen</i> (as Discussed in Grounds 1-4) In Further Combination with <i>Computer Networks</i> , <i>Rakic</i> , or <i>Dutta</i> Renders Obvious Claim 8	94
J.	Ground 8: Any Combination of <i>Rittmaster</i> and/or <i>Shenfield</i> and/or <i>Konstantinov/Klassen</i> (as Discussed in Grounds 1-4) In Further Combination with <i>Gellens</i> Renders Obvious Claim 14.....	94
III.	CERTIFICATION UNDER 37 C.F.R. § 1.510(B)(5).....	95
IV.	CERTIFICATION UNDER 37 C.F.R. § 1.510(B)(6).....	95
V.	CONCLUSION.....	95

TABLE OF AUTHORITIES

Cases

<i>In re Am. Acad. of Sci. Tech. Ctr.</i> , 367 F.3d 1359 (Fed. Cir. 2004).....	28
<i>In re Bass</i> , 314 F.3d 575 (Fed. Cir. 2002).....	28
<i>In re Yamamoto</i> , 740 F.2d 1569 (Fed. Cir. 1984).....	28

Statutes

35 U.S.C. § 325(d).....	27
-------------------------	----

Other Authorities

MPEP § 2242.I.....	15
--------------------	----

EXHIBITS

Exhibit references in this request refer to the exhibits identified in, and attached to, the Declaration of Dr. Sam Malek, which accompanies this request for *ex parte* reexamination:

Ex. A	U.S. Patent No. 9,615,192
Ex. B	Curriculum Vitae of Dr. Sam Malek
Ex. C	U.S. Pat. Pub. 2002/0023010 to Rittmaster, et al. (" <i>Rittmaster</i> ")
Ex. D	U.S. Pat. Pub. 2006/0268696 to Konstantinov, et al. (" <i>Konstantinov</i> ")
Ex. E	Andrew S. Tanenbaum and Maarten Van Steen, <i>Distributed Systems: Principles and Paradigms</i> (Pearson Education, 2d ed. 2007) (" <i>Distributed Systems</i> ")
Ex. F	Andrew S. Tanenbaum, <i>Computer Networks</i> (Pearson Education, 4th ed. 2003) (" <i>Computer Networks</i> ")
Ex. G	<i>Headwater Research LLC v. Samsung Elecs. Co. Ltd.</i> , et al., No. 2:23-cv-00103, Claim Construction Order (Dkt. 118) (E.D. Tex. Aug. 22, 2024)
Ex. H	<i>Samsung Elecs. Co. Ltd., et al. v. Headwater Research LLC</i> , No. IPR2024-00010, Petitioner's Reply to Patent Owner's Response (Paper 16) (PTAB Dec. 18, 2024)
Ex. I	<i>Samsung Elecs. Co. Ltd., et al. v. Headwater Research LLC</i> , No. IPR2024-00010, Patent Owner's Response to the Petition (Paper 12) (PTAB Sept. 7, 2024)
Ex. J	<i>Samsung Elecs. Co. Ltd., et al. v. Headwater Research LLC</i> , No. IPR2024-00010, Patent Owner's Sur-Reply (Paper 19) (PTAB Jan. 23, 2025)
Ex. K	U.S. Patent No. 8,064,934 to Klassen (" <i>Klassen</i> ")
Ex. L	U.S. Patent No. 7,082,615 to Ellison, et al. (" <i>Ellison</i> ")
Ex. M	U.S. Pat. Pub. 2009/0282256 to Rakic, et al. (" <i>Rakic</i> ")
Ex. N	U.S. Pat. Pub. 2002/0186845 to Dutta, et al. (" <i>Dutta</i> ")
Ex. O	U.S. Pat. Pub. 2005/0144294 to Gellens, et al. (" <i>Gellens</i> ")
Ex. P	Excerpts of Original Prosecution History of U.S. Patent No. 9,615,192
Ex. Q	<i>Amazon.com Servs., LLC, et al. v. Headwater Research LLC</i> , No. IPR2026-00088, Petition (Paper 1) (PTAB Nov. 10, 2025)
Ex. R	<i>Target Corp. v. Headwater Research LLC</i> , No. IPR2026-00154, Petition (Paper 3) (PTAB Nov. 25, 2025)

Ex. S	U.S. Pat. Pub. 2006/0129691 to Coffee, et al. (“ <i>Coffee</i> ”)
Ex. T	U.S. Pat. Pub. 2005/0108397 to Basso, et al. (“ <i>Basso</i> ”)
Ex. U	Australian Pat. Pub. AU 2007200530 to Shenfield, et al. (“ <i>Shenfield</i> ”)

Other than the excerpts of the prosecution history (Ex. P), and except as otherwise noted herein, all citations to exhibits refer to original page numbers found in the underlying document, and all emphases are added. The claim analysis and interpretations herein are made under the broadest reasonable interpretation standard, and in light of Patent Owner’s litigation interpretation of the claims. Requester reserves the right to advance different arguments in the district court, based on, for example, the *Phillips* standard.

I. STATEMENT UNDER 37 C.F.R. § 1.510(B)(1) POINTING OUT SUBSTANTIAL NEW QUESTIONS OF PATENTABILITY

Walmart requests reexamination of Claims 1-15 of the '192 Patent (the "Challenged Claims"). All grounds raise substantial new questions of patentability as neither the primary references nor the specific combinations of references presented herein were considered by the Office during prosecution of the '192 Patent or during subsequent *inter partes* review proceedings. A summary of the grounds asserted in this reexamination request is provided below:

Ground No.	Claims	Grounds Presented Herein
1	1-3, 5-7, 9, 11-15	Anticipated by <i>Rittmaster</i>
2	1-3, 5-7, 9-15	Obvious in view of <i>Rittmaster</i> + <i>Distributed Systems</i> and <i>Computer Networks</i>
3	1-3, 5-7, 9-15	Obvious in view of <i>Rittmaster</i> + <i>Shenfield</i>
4	1-3, 5-7, 9-15	Obvious in view of <i>Rittmaster</i> and/or <i>Shenfield</i> (as in any of Grounds 1 - 2) + <i>Konstantinov</i> and <i>Klassen</i>
5	4	Obvious in view of any of Grounds 1 - 4 + <i>Ellison</i>
6	6	Obvious in view of any of Grounds 1 - 4 + <i>Coffee</i> or <i>Basso</i>
7	8	Obvious in view of any of Grounds 1 - 4 + <i>Computer Networks</i> + <i>Rakic</i> or <i>Dutta</i>
8	14	Obvious in view of any of Grounds 1 - 4 + <i>Gellens</i>

A. Introduction

The '192 Patent issued on April 4, 2017, from U.S. Patent Application No. 15/211,430 ("the '430 Application"), which was filed on July 15, 2016, and published on November 3, 2016. Ex. A, Cover. The '430 Application claims its earliest alleged priority to provisional application No. 61/207,739, filed on February 13, 2009. Ex. A, Cover at p. 2.

Although the specification of the '192 Patent is lengthy, its support under 35 U.S.C. § 112 for the specific subject matter that it claims is questionable. More importantly for this request for reexamination is the fact that most of the disclosure is nothing more than an assembly of known server architecture and common -- in many cases required -- communication protocols. In

particular, the claim language found in the '192 Patent amounts to no more than a handful of features that were already known and required to enable a network server to communicate with laptops and cellular phones over existing internet connections before the earliest possible priority date of the '192 Patent.

For the various reasons discussed below, each claim is anticipated or obvious in view of the prior art identified herein. This request raises substantial new questions of patentability because none of the primary references were cited during prosecution, nor have they been cited or considered in subsequent IPR challenges. This request also presents combinations of prior art references that have never been considered by the USPTO.

B. The '192 Patent and Prosecution History

I. Summary of the '192 Patent

Although the specification is long, and includes more than 100 pages of figures, the vast majority of the '192 Patent identifies and describes basic network elements and architecture that were well-known in the relevant time period. Declaration of Dr. Sam Malek ("Malek Decl.") at ¶ 34. The '192 Patent describes a "message link server [that] maintains secure message links with device link agents on each of a plurality of wireless end-user devices." Ex. A, Abstract. The "message link server" uses a "buffer" to store messages from network elements until one of several triggers occur, such that messages may be buffered until the occurrence of a trigger other than the receipt of that message by the server. *Id.* In other words, when the message link server receives certain messages from the network directed to a particular end-user device, it holds those messages in a buffer until receiving a specified trigger that is determined by the server to warrant sending the message to the intended end-user device. Malek Decl. at ¶ 34.

Claim 1 of the '192 Patent is directed to a "message link server" that links "wireless end-user devices" to a network, as shown in Figure 1 below (Malek Decl. at ¶ 35):

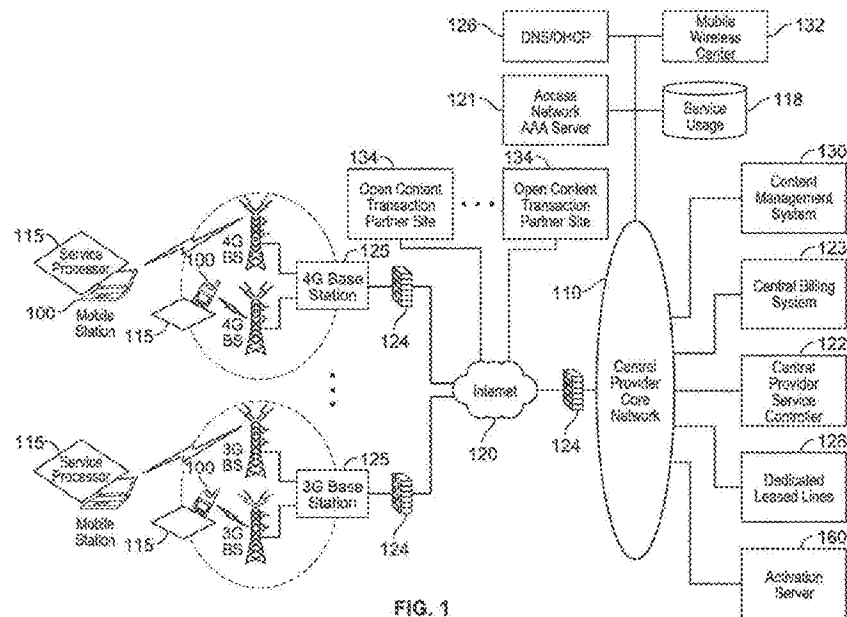


FIG. 1

As illustrated, end-user wireless devices such as laptop computers or mobile phones may connect to a central provider network 110 through the internet. Ex. A, Fig. 1. This network is capable of communicating with 3G and 4G devices, and the same service controller 122 manages services for both sets of devices. Ex. A, 12:13-59.

Another disclosed network architecture of the '192 Patent, shown in Fig. 6 below, includes a 4G LTE and Wi-Fi overlay configuration (Ex. A, 23:32-38; Malek Decl. at ¶ 36):

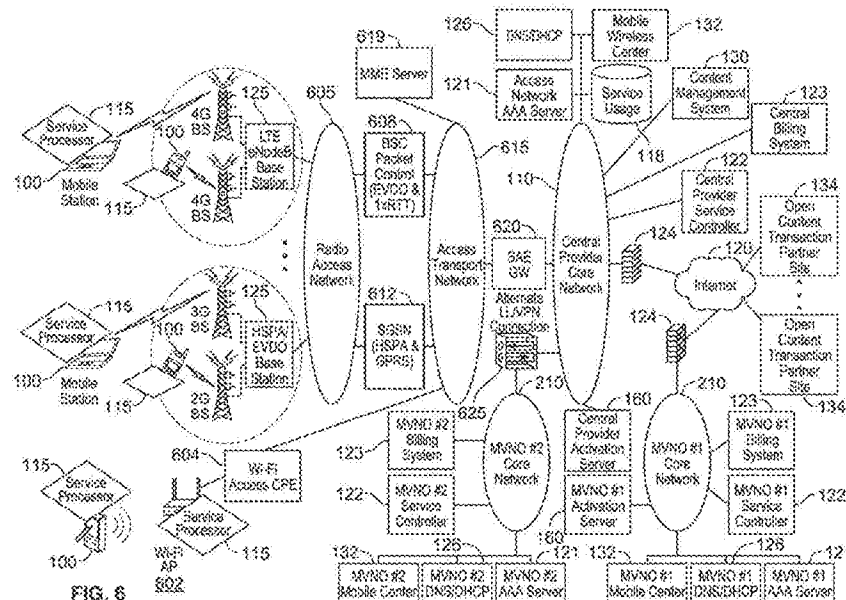
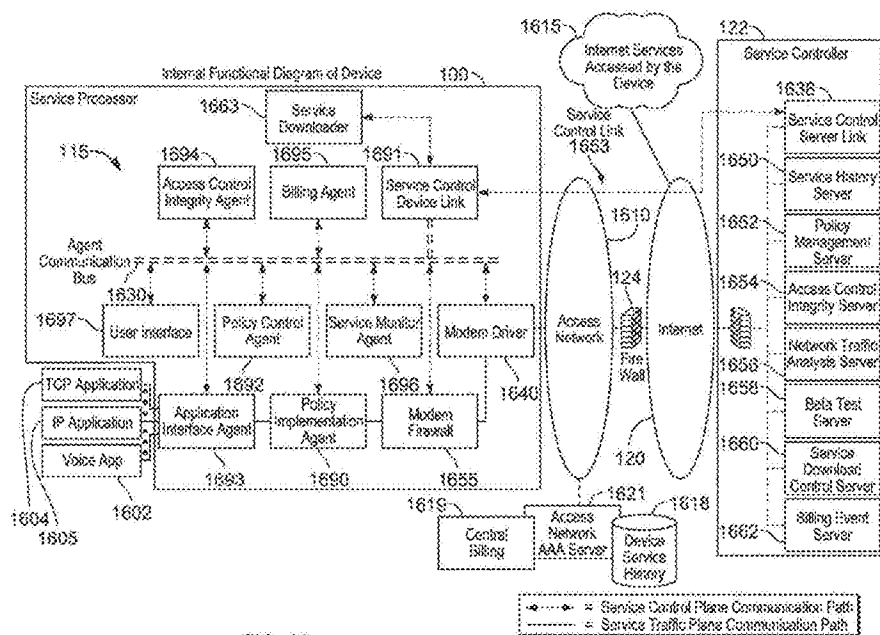


FIG. 6

In this illustration, the end-user wireless devices 100 connect through an access transport network 615 with the central provider service controller 122. Malek Decl. at ¶ 36. Similar networks are shown in Fig. 7 (in which Wi-Fi connections can be replaced with a femtocell and the Wi-Fi modem can be replaced with a femtocell modem) and Fig. 8 (which includes multiple wire line networks (*e.g.*, Data Over Cable Service Interface Specification (DOCSIS) and Digital Subscriber Line Access Multiplexer (DSLAM) wire line networks)). *Id.*; Ex. A, 24:12-25:57.

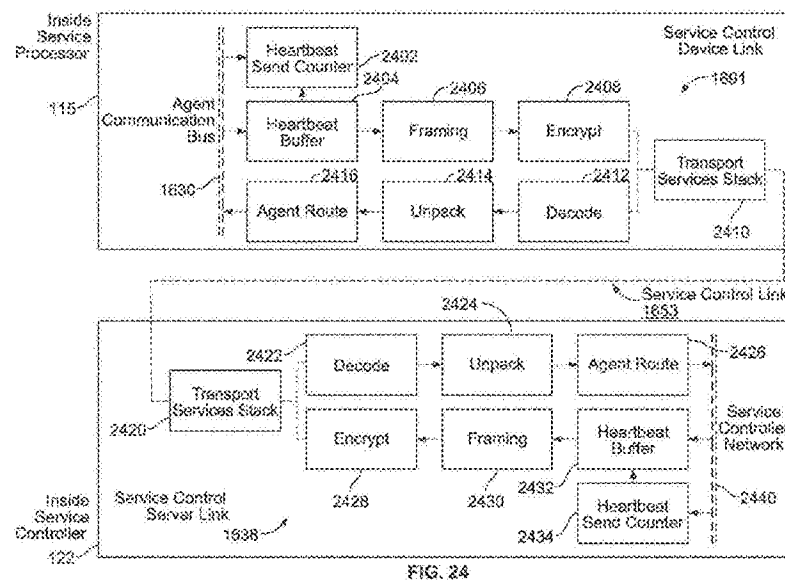
In each case, the service controller 122 can control each of these end-user devices with a consistent service experience, for example, using different service profiles, service capabilities, and service profile cost options depending on which network the device is connected to and/or other criteria. Malek Decl. at ¶ 36. For example, downloading a high definition movie may be allowed when the service controller 122 is managing service profile policies for a service processor 115 *residing on a DOCSIS device* 100 (*e.g.*, a computer or laptop connected to a cable modem), but not when the same service controller 122 is managing service profile policies for a service processor 115 *residing on a 3G device* 100 (*e.g.*, a smartphone connected to a mobile 3G network). Malek Decl. at ¶ 36; Ex. A, 23:32-26:20.

Figure 16 below illustrates a typical end-user device 100, such as a laptop or mobile phone, in communication with a network according to the '192 Patent:



Here, the service processor 115 includes a “Service Control Device Link” 1691 of the end-user device 100 that links to a “Service Control Server Link” 1638 of the service controller 122 through a “Service Control Link” 1653. Malek Decl. at ¶ 37; Ex. A, 37:26-42:58. The service controller 122 includes multiple servers (*e.g.*, 1650, 1652, 1654, 1656, 1662), all of which are coupled to the service control server link 1638. Malek Decl. at ¶ 38; Ex. A, 68:19-20. The service control device link 1691 of the end-user device 100 is coupled to multiple device “agents” (*e.g.*, 1697, 1695). Malek Decl. at ¶ 38; Ex. A, 37:34-46, 41:45-53, 45:26-30.

Shown below is another representation of the end-user device’s service processor 115, which is linked to the service controller 122 of the network server via one or more layers of encryption:



Malek Decl. at ¶ 39; Ex. A, 89:11-90:4. As illustrated, the service controller 122 includes a “Transport Services Stack” 2420 for sending and receiving messages to and from the “Transport Services Stack” 2410 of the end-user device 100. Malek Decl. at ¶ 39. These messages may be framed and encrypted by the service controller 122 for transport to the end-user device service processor 115 or received from the end-user device service processor 115 and subsequently decoded and unpacked by the server’s service controller 122. *Id.* A layer of encryption is implemented below the transport services stack, for example, with IPSEC or another IP layer encryption, VPN, or tunneling scheme. Malek Decl. at ¶ 39; Ex. A, 89:26-29. All of these were well known before the applications that led to the ’192 Patent, as evidenced by the explicit

statement that the “Transport Services Stack” 2420 provides “basic transport services” and can be “implemented with **standard secure or open Internet networking protocols**, such as TLS or TCP.” Malek Decl. at ¶ 39; Ex. A, 89:29-36 (emphasis added). A message received from server link element 1638 is associated with an identifier (*e.g.*, “an agent first function ID 2528”) and content (*e.g.*, “an agent first function message 2532”) included on the communication. Malek Decl. at ¶ 39; Ex. A, 91:51-92:19.

Messages from the server’s service controller 122 can be routed to an appropriate agent on the end-user device 100 by the “Service Control Device Link” 1691 based on the format of the message, which is shown in Fig. 25 below and includes an “Agent Function ID” 2528 along with the message length 2530 and the message content 2532, as shown in the lower half of the figure (Malek Decl. at ¶ 40):

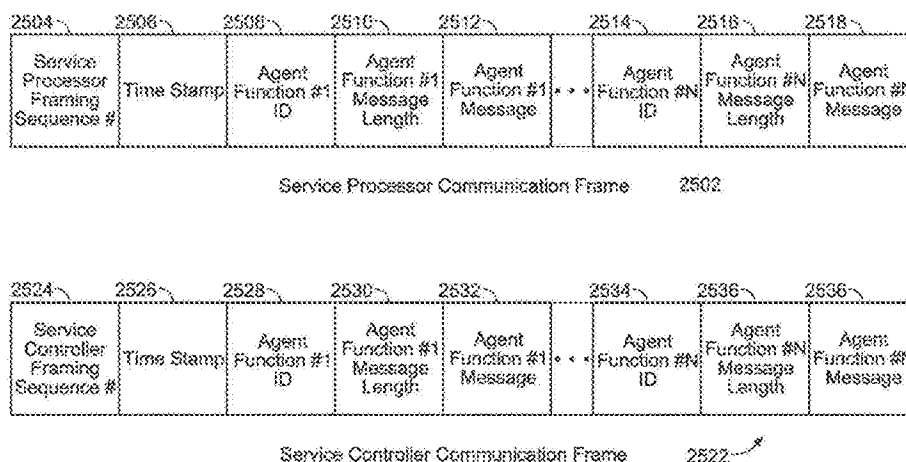


FIG. 25

This was a standard way of addressing messages long before the time that the applications that led to the '192 Patent were filed. *Id.* Communications from the end-user device’s service processor also included an “Agent ID” 2508 indicating from where the message originated. Ex. A, Fig. 25. Multiple messages may also be framed together in a single communication frame, each associated with a corresponding agent ID (as indicated by “Agent Function #1 ID” through “Agent Function #N ID”). *Id.*

a. Claims of the '192 Patent

Independent claim 1 of the '192 Patent is a system claim and independent claim 15 is a method claim. Claims 2-14 depend from claim 1. The following chart lists the Challenged Claims (*i.e.*, claims 1-15), with the element-by-element breakdown used throughout the Request.

Claim Element #	Limitation
1[PRE]	A message link server comprising:
1[a]	a transport services stack to maintain a respective secure message link through an Internet network between the message link server and a respective device link agent on each of a plurality of wireless end-user devices,
1[b]	each of the wireless end-user devices comprising multiple software components authorized to receive and process data from secure message link messages received via a device link agent on that device;
1[c]	an interface to a network to receive network element messages from a plurality of network elements, the received network element messages comprising respective message content and requests for delivery of the respective message content to respective wireless end-user devices, the respective message content including data for, and an identification of, a respective one of the authorized software components; and
1[d]	a message buffer system including a memory and logic, the memory to buffer content from the received network element messages for which delivery is requested to a given one of the wireless end-user devices,
1[e]	the logic to determine when one of a plurality of message delivery triggers for the given one of the wireless end-user devices has occurred, wherein for at least some of the received network element messages, the receipt of such a message by the message buffer system is not a message delivery trigger, and for at least one of the message delivery triggers, the trigger is an occurrence of an asynchronous event with time-critical messaging needs, and
1[f]	upon determining that one of the message delivery triggers has occurred, the logic further to supply one or more messages comprising the buffered content to the transport services stack for delivery on the secure message link maintained between the transport services stack and a device link agent on the given one of the wireless end-user devices.

Claim 2

- | | |
|---|---|
| 2 | The message link server of claim 1, further comprising an encrypt function to encrypt the one or more messages supplied to the transport services stack for delivery on the secure message link maintained between the message link server and the device link agent on the given one of the wireless end-user devices. |
|---|---|

Claim 3

- 3 The message link server of claim 2, wherein the encrypted one or more messages are transported to the device link agent on the given one of the wireless end-user devices using one or more of encryption on the transport services stack, IP (Internet Protocol) layer encryption, and tunneling.

Claim 4

- 4 The message link server of claim 1, wherein the device link agent executes in a secure execution environment on at least one of the devices, and at least one of the software components executes outside of the secure execution environment on that device.

Claim 5

- 5 The message link server of claim 1, wherein the transport services stack is further to receive, over each of the respective secure message links, upload messages forwarded by the respective device link agents from at least a subset of the device software components, each of the upload messages identifying a corresponding one of the network elements to which the device respective software component has requested delivery, the network server system using the interface to a network to deliver content from the upload messages to the respective identified network elements.

Claim 6

- 6 The message link server of claim 1, wherein at least one of the one or more messages for delivery by the transport services stack comprises multiple identifier/data pairs.

Claim 7

- 7 The message link server of claim 1, the device messaging agent on at least one of the wireless end-user devices further to initiate the respective secure Internet data message link to the transport services stack.

Claim 8

- 8 The message link server of claim 1, further comprising a secure server to provide secure authorization signatures to the given one of the wireless end-user devices, the secure authorization signatures indicating the authorized software components that are allowed to receive data from secure message link messages via the message link server.

Claim 9

- 9 The message link server of claim 1, wherein one of the message delivery triggers is the expiration of a periodic timer.

Claim 10

- 10 The message link server of claim 9, wherein the period of the timer is fractionally shorter than a maximum data message interval beyond which the secure message link is taken down.

Claim 11

- 11 The message link server of claim 1, wherein one of the message delivery triggers is the receipt of a transmission on the respective secure message link from the device link agent of the given one of the wireless end-user devices, or a response generated to a transmission received from that device link agent.

Claim 12

- 12 The message link server of claim 11, wherein the transmission is a heartbeat message generated by the given device link agent, or a request received from the given device link agent.

Claim 13

- 13 The message link server of claim 1, wherein one of the message delivery triggers is the receipt of a particular network element message from one of the network elements.

Claim 14

- 14 The message link server of claim 1, wherein one of the message delivery triggers is based on an amount of wireless network data usage consumed by the given one of the wireless end-user devices.

Claim 15

- 15[PRE] A method of operating a message link server, comprising:
- 15[a] maintaining a respective secure message link through an Internet network between the message link server and a respective device link agent on each of a plurality of wireless end-user devices, each of the wireless end-user devices comprising multiple software components authorized to receive and process data from secure message link messages received via a device link agent on that device;

- 15[b] receiving network element messages from a plurality of network elements, the received network element messages comprising respective message content and requests for delivery of the respective message content to respective wireless end-user devices, the respective message content including data for, and an identification of, a respective one of the authorized software components;
- 15[c] buffering content from the received network element messages for which delivery is requested to a given one of the wireless end-user devices;
- 15[d] determining when one of a plurality of message delivery triggers for the given one of the wireless end-user devices has occurred, wherein for at least some of the received network element messages, the receipt of such a message is not a message delivery trigger, and for at least one of the message delivery triggers, the trigger is an occurrence of an asynchronous event with time-critical messaging needs; and
- 15[e] upon determining that one of the message delivery triggers has occurred, supplying one or more messages comprising the buffered content for delivery on the secure message link maintained between the message link server and a device link agent on the given one of the wireless end-user devices.

2. Prosecution History of U.S. Application No. 15/211,430

As filed on July 15, 2016, the singular, original claim of the '430 Application was broadly directed to a simple system comprising only (a) a processor to store device credentials and request access to a network using those credentials, and (b) a memory for providing instructions. *See* Ex. P at p. 211. Three days later, Patent Owner filed a Preliminary Amendment, cancelling the sole claim filed, and adding new claims 2-16, the scope of which significantly deviated from the original claim filed. *Id.* at pp. 202-208.

Around the time of filing its Preliminary Amendment, Patent Owner filed five (5) IDS forms, citing more than 1,100 U.S. patents and publications, over 80 foreign references, and over 50 non-patent literature documents. Patent Owner later filed another IDS form, citing 50 more patent references, 20 publications, and nine (9) foreign patent documents. *See* Ex. P at pp. 66-201. The Examiner considered each reference cited by Patent Owner and cited an additional six (6) references. *Id.* at p. 65. No reference identified in this request for *ex parte* reexamination request was ever considered by the Examiner during prosecution of the '430 Application.

During prosecution, the Examiner issued only a single Non-Final Office Action rejecting, and objecting to, all claims on various grounds. *Id.* at pp. 53-65. In the Office Action, the Examiner objected to the independent claims (then claims 2 and 16) for reciting “received messages” without

proper antecedent basis, and rejected the independent system claim as indefinite for reciting a buffering system without disclosure of a corresponding structure in the specification. *Id.* at pp. 55-58. The Examiner further rejected all claims as obvious in light of U.S. Patent No. 7,151,764 (Heinonen, et al.) and U.S. Pub. No. 2006/0182137 (Zhou, et al.), and citing a third reference for some dependent claims from U.S. Patent No. 7,191,248 (Chattopadhyay, et al.), U.S. Pub. No. 2003/0184793 (Pineau), U.S. Pub. No. 2004/0054779 (Takeshima, et al.), and U.S. Pub. No. 2002/0138599 (Dilman, et al.). *Id.* at pp. 58-65.

Patent Owner amended the independent claims to address the antecedent basis objections and the indefiniteness rejections but traversed the obviousness rejections without amendment. *Id.* at pp. 38-51. Specifically, Patent Owner amended “message *buffering* system” to recite “message *buffer* system” in independent claim 2 and removed reference to “the message buffering system” in independent claim 16 to purportedly clarify that a definite structure (*e.g.*, a buffer) is recited in the claim element itself. *Id.* at pp. 44-45. Patent Owner specifically pointed to “‘service control server link 1638,’ which is an embodiment of a ‘message link server.’” *Id.* at p. 45. Relying on Fig. 24 (provided below), Patent Owner argued that the combination of the encryption element 2428, framing element 2430, heartbeat buffer 2432, and heartbeat send counter 2434 “combine to perform as the ‘message buffering system’” to supply buffered messages to the transport services stack 2420. *Id.*

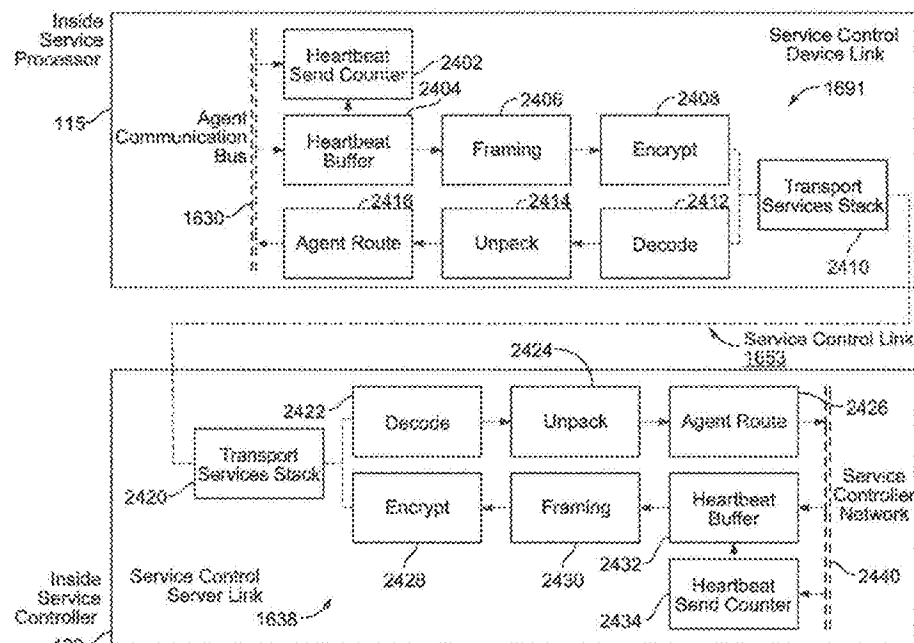


FIG. 24

As to its obviousness arguments, Patent Owner distinguished Heinonen by asserting its system indiscriminately distributes Bluetooth inquiry packets to mobile devices “without establishing a session,” and thereby bypassing any protocol stack of the mobile device. *Id.* at pp. 46-47 (emphasis in original). Patent Owner distinguished Zhou by arguing the reference executes program threads “in the same operating system” by creating channels that allow asynchronous messaging from a “producer” program to a “consumer” program. *Id.* at p. 48 (emphasis in original).

Patent Owner ultimately concluded that the combination lacked (1) a message link server, (2) a stack that maintains a respective secure message link, (3) multiple software components authorized to receive messages via a device link agent, (4) an interface for network elements using the access point as a message link server, and (5) a message buffering system. *Id.* at pp. 47-48 As to the *message link server* limitation, Patent Owner argued that Heinonen has no mechanism to deliver a message from a network element to an identified software component on an identified device, and that Zhou does not use a single channel to communicate between multiple “producers” and multiple “consumers.” *Id.* As to the *transport services stack* limitation, Patent Owner distinguished Heinonen by arguing it failed to maintain a *secure* link when transmitting an ASPI message, and distinguished Zhou by asserting it is not used “on the Internet.” *Id.* As to the *multiple software components* and *device link agent* limitations, Patent Owner argued Heinonen can only identify one message for delivery to one place, while Zhou again does not use a single channel to communicate between multiple “producers” and multiple “consumers.” *Id.* As to the *interface to a network* limitation, Patent Owner argued that Heinonen fails to queue specific messages and Zhou has no interface shared by multiple elements. *Id.* Finally, as to the *message buffering system* limitation, Patent Owner argues that Heinonen fails to teach buffering at all, and Zhou requires individual buffers for individual pairs of communicating programs (*i.e.*, no buffer shared for multiple sources directing messages to a same remote device). *Id.*

The Examiner initiated an interview just over a week later, during which Patent Owner authorized the Examiner to amend the independent claims “to clarify the claimed invention,” and to “overcome the rejection...under 35 U.S.C. 112 second paragraph.” *See id.* at p. 37. The Examiner’s Amendment, attached to the Notice of Allowance, changed the independent claims to require that messages require data for and identification of authorized software components and added specificity to independent and dependent claims. *Id.* at pp. 31-35.

3. Prior Inter Partes Review Proceedings

a. Samsung Elecs. Co. v. Headwater Rsch. LLC, IPR2024-00010

Samsung Electronics Co., Ltd. (“Samsung”), filed a petition for *inter partes* review of claims 1-9, 11-13, and 15 of the ’192 Patent on November 17, 2023. *See* Ex. P at p. 2. Samsung relied on a number of references in its petition, none of which are primary references in this Request. The cited prior art included:

- 3GPP TS 23.140 v6.9.0 (2005-03), 3rd Generation Partnership Project, Technical Specification Group Terminals, Multimedia Messaging Service (MMS), Functional Description, Stage 2;
- U.S. Pub. No. 2005/0207379 (Shen);
- U.S. Pat. No. 7,082,615 (Ellison);
- U.S. Pub. No. 2009/0282256 (Rakic);
- WO 2006/077283 (Houghton), and
- U.S. Pub. No. 2009/0240807 (Munson).

Id. at p. 6. Patent Owner did not file a Preliminary Response. *Id.* at p. 2. The Board issued a Decision Granting Institution on May 23, 2024, and Patent Owner filed its response on September 7, 2024. *Id.* An oral hearing was held on March 5, 2025. Patent Owner argued only (i) that a first combination of references showed only a single trigger (rather than a plurality of message delivery triggers); (ii) that a second combination of references did not disclose that messages received by the message link server comprise data for, and an identification of, a responsive one of the authorized software components; and (iii) that neither of the combinations disclosed one of the message delivery triggers is the expiration of a periodic timer as in claim 9. Patent Owner and Samsung subsequently settled and moved to terminate the IPR. The Board terminated the IPR without issuing a final written decision.

b. Amazon.com Servs., LLC, et al. v. Headwater Rsch. LLC, IPR2026-00088

Amazon.com Services, LLC and Amazon Web Services, Inc. (collectively, “Amazon”) filed a petition for *inter partes* review of claims 1-15 of the ’192 Patent on November 10, 2025. Ex. R. Amazon relied on a number of references in its petition, none of which are primary references in this Request. The cited prior art includes:

- 3GPP TS 23.140 v6.9.0 (2005-03), 3rd Generation Partnership Project, Technical Specification Group Terminals, Multimedia Messaging Service (MMS), Functional Description, Stage 2;
- WO 2006/077283 (Houghton);
- U.S. Pub. No. 2009/0240807 (Munson).
- U.S. Pub. No. 2005/0207379 (Shen);
- U.S. Pat. No. 7,082,615 (Ellison);
- U.S. Pub. No. 2009/0282256 (Rakic);
- U.S. Pub. No. 2009/0158397 (Herzog);
- U.S. Pub. No. 2005/0144294 (Gellens); and
- U.S. Pub. No. 2008/0162637 (Adameczyk).

Id. at p. 2. Patent Owner's Preliminary Response is due February 20, 2026. This IPR is still pending, and as such, the Board has not issued a final written decision.

***c. Target Corp. v. Headwater Rsch. LLC,
IPR2026-00154***

Target Corporation filed a petition for *inter partes* review of claims 1-15 of the '192 Patent on November 25, 2025. Ex. S. Target relied on a number of references in its petition, none of which are primary references in this Request. The cited prior art includes:

- 3GPP TS 23.140 v6.9.0 (2005-03), 3rd Generation Partnership Project, Technical Specification Group Terminals, Multimedia Messaging Service (MMS), Functional Description, Stage 2;
- WO 2006/077283 (Houghton);
- U.S. Pub. No. 2009/0240807 (Munson).
- U.S. Pub. No. 2005/0207379 (Shen);
- U.S. Pat. No. 7,082,615 (Ellison);
- U.S. Pub. No. 2009/0282256 (Rakic);
- U.S. Pub. No. 2009/0158397 (Herzog);
- U.S. Pub. No. 2005/0144294 (Gellens); and
- U.S. Pub. No. 2008/0162637 (Adameczyk).

See *id.* at p. 2. This IPR is still pending, and as such, the Board has not issued a final written decision.

4. Prior Relevant Federal District Court Litigation

Patent Owner has asserted the '192 Patent against numerous entities in the Eastern and Western Districts of Texas, but no court (as of the filing of this request for *ex parte* reexamination) has issued a final holding of invalidity that would preclude presence of a substantial new question of patentability in this request. See MPEP § 2242.I. Except where indicated, the following lawsuits asserting the '192 Patent remain open and pending as of the date of filing of this request:

Federal District Court Litigation

Headwater Rsch. LLC v. Samsung Elecs. Am., Inc., et al., No. 2:23-cv-103 (E.D. Tex. Mar. 10, 2023) (Case CLOSED Sep. 29, 2025 following pre-trial settlement)

Headwater Rsch. LLC v. Google LLC, No. 7:25-cv-231 (W.D. Tex. May 16, 2025)

Headwater Rsch. LLC v. Amazon.com, Inc., et al., No. 7:25-cv-286 (W.D. Tex. June 20, 2025)

Headwater Rsch. LLC v. Apple Inc., No. 7:25-cv-371 (W.D. Tex. Aug. 27, 2025)

Headwater Rsch. LLC v. Amazon.com Services LLC, et al., No. 2:25-cv-897 (E.D. Tex. Aug. 27, 2025)*

Headwater Rsch. LLC v. Walmart Inc., No. 2:25-cv-961 (E.D. Tex. Sep. 18, 2025)*

Headwater Rsch. LLC v. Uber Techs., Inc., et al., No. 2:25-cv-962 (E.D. Tex. Sep. 18, 2025)*

Headwater Rsch. LLC v. Target Corp., No. 2:25-cv-963 (E.D. Tex. Sep. 18, 2025)*

Headwater Rsch. LLC v. Supercell Oy, No. 2:25-cv-964 (E.D. Tex. Sep. 18, 2025)

Headwater Rsch. LLC v. Tencent Holdings Ltd., No. 2:25-cv-965 (E.D. Tex. Sep. 18, 2025)

*The court consolidated these cases under Case No. 2:25-cv-961 on October 23, 2025.

C. Overview of Cited Art and SNQs Raised

The following references are cited herein as prior art. Only Exhibits L, M, and O have been cited in other proceedings relating to the '192 Patent, and those references are presented herein only in combination with other references that have never been considered by the USPTO.

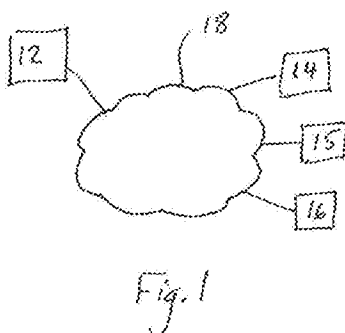
Exhibit	Overview of the Cited Art
Ex. C	<i>Rittmaster</i> published on February 21, 2002 from U.S. Patent Application No. 09/812,296, filed on March 20, 2001. <i>Rittmaster</i> qualifies as prior art under § 102(e) ¹ .
Ex. D	<i>Konstantinov</i> published on November 30, 2006 from U.S. Patent Application No. 11/231,858, filed on September 22, 2005. <i>Konstantinov</i> qualifies as prior art under § 102(e).
Ex. E	<i>Distributed Systems</i> is a second edition textbook, with a copyright date of 2007. <i>Distributed Systems</i> qualifies as prior art under § 102(b).
Ex. F	<i>Computer Networks</i> is a fourth edition textbook, with a copyright date of 2003. <i>Computer Networks</i> qualifies as prior art under § 102(b).
Ex. K	<i>Klassen</i> issued November 22, 2011, from U.S. Patent Application No. 11/584,418, filed on October 19, 2006. <i>Klassen</i> qualifies as prior art under § 102(e).
Ex. L	<i>Ellison</i> issued July 25, 2006, from U.S. Patent Application No. 09/668,610, filed on September 22, 2000. <i>Ellison</i> qualifies as prior art under § 102(e).
Ex. M	<i>Rakic</i> published on November 12, 2009, from U.S. Patent Application No. 12/118,871, filed on May 12, 2008. <i>Rakic</i> qualifies as prior art under § 102(e).
Ex. N	<i>Dutta</i> published on December 12, 2002, from U.S. Patent Application No. 09/878,468, filed on June 11, 2001. <i>Dutta</i> qualifies as prior art under § 102(e).
Ex. O	<i>Gellens</i> published on June 30, 2005, from U.S. Patent Application No. 10/727,688, filed on December 3, 2003. <i>Gellens</i> qualifies as prior art under § 102(e).
Ex. S	<i>Coffee</i> published on June 15, 2006, from U.S. Patent Application No. 11/190,236, filed on July 26, 2005. <i>Coffee</i> qualifies as prior art under § 102(e).
Ex. T	<i>Basso</i> published on May 19, 2005, from U.S. Patent Application No. 10/713,343, filed on November 14, 2003. <i>Basso</i> qualifies as prior art under § 102(e).

¹ Citations are to the pre-AIA statute; analysis would be identical if the post-AIA statute applied.

Ex. U *Shenfield* published on September 6, 2007, from Australian Patent Application No. AU 2007200530, filed on February 7, 2007. *Shenfield* qualifies as prior art under § 102(b).

1. U.S. Patent Pub. No. 2002/0023010 (“Rittmaster”) (Ex. C)

Just like the '192 Patent, *Rittmaster* discloses a network for providing information to user devices upon determining that the users are eligible to receive such information. Malek Decl. at ¶ 44. For instance, messages may be sent from the server when end-user devices are determined to be in a designated geographic location. *Id.* Figure 1 shows a very basic system in which a server 12 is connected to a plurality of user devices 14-16 through a network (e.g., the internet):



Rittmaster explains that “FIG. 1 may be considered a generalized representation of an Internet or WWW embodiment, wherein the provider server 12 comprises an Internet product or service provider computer or server (hereinafter referred to as the provider server) coupled for communication” to “a plurality of network enabled user devices (such as those described above as recipient processors).” Malek Decl. at ¶ 44; Ex. C, ¶ 42.

A more detailed diagram of this system is shown in Fig. 2, where the server 12 has associated server software 29 and a storage means 13, and each user device (recipients 14, 15, and 16) has a different method for tracking a geographic position (*id.*):

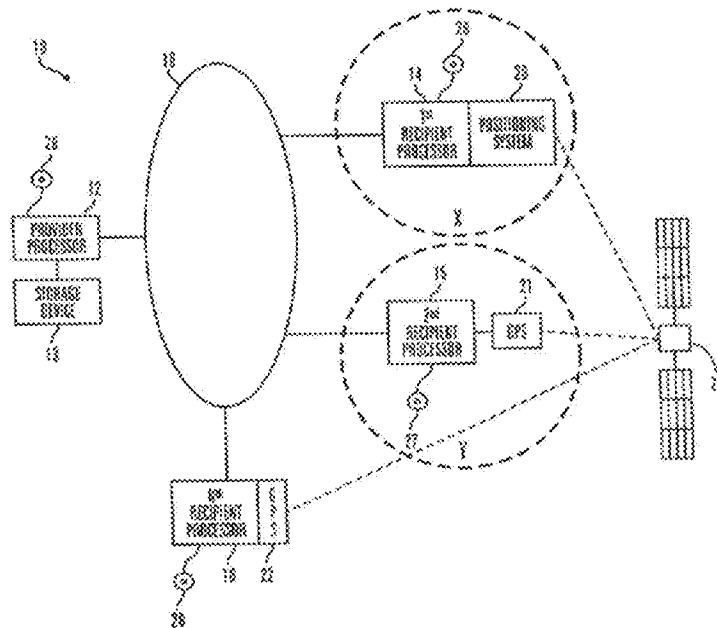
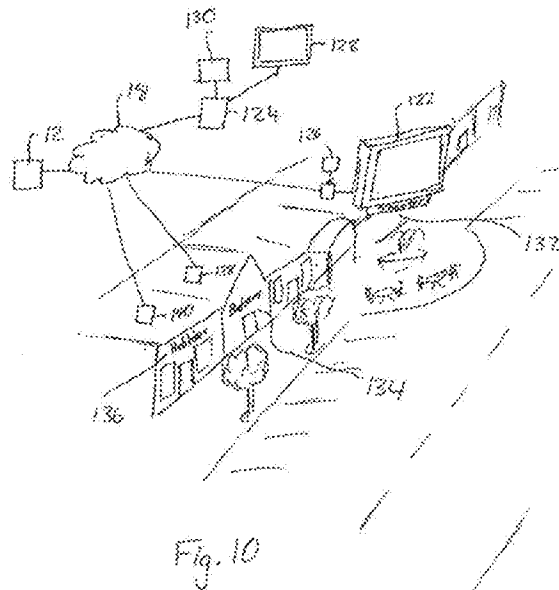


FIG. 2

Any number of user devices may be connected through the internet 18 to the network server 12. *Id.* The user devices and provider device (or server) 12 may each comprise any suitable computer or processor device having means for interfacing with and communicating on a communications network, preferably under the control of software programs. *Id.* *Rittmaster* specifies that “[s]uch computers and communication interfacing are well known in the art and are not described in further detail herein for purposes of simplifying the present disclosure.” *Id.* Furthermore, any number and type of network elements may provide information through the server, with *Rittmaster* stating that “[t]he provider processor 12 is capable of providing information from any suitable source (including, but not limited to an on-line source or a computer readable storage medium such as a hard or floppy disk, random access memory RAM, read only memory ROM, compact disk (CD), other optical storage disk, such as a DVD, or the like). . . .” Malek Decl. at ¶ 44; Ex. C, ¶ 33.

Rittmaster further discloses that content is not provided by the server *until* a determination is made that specific restrictions have been satisfied. Malek Decl. at ¶ 45. For instance, “a set of rules may be implemented, which depend upon the geographic information (and, thus, the geographic location or region of the recipient processor), such that . . . if a recipient processor provides geographic information corresponding to a first geographic location or region, then the provider processor may be controlled to not provide selective information to the recipient processor, unless further requirements are met.” Malek Decl. at ¶ 45; Ex. C, ¶ 40.

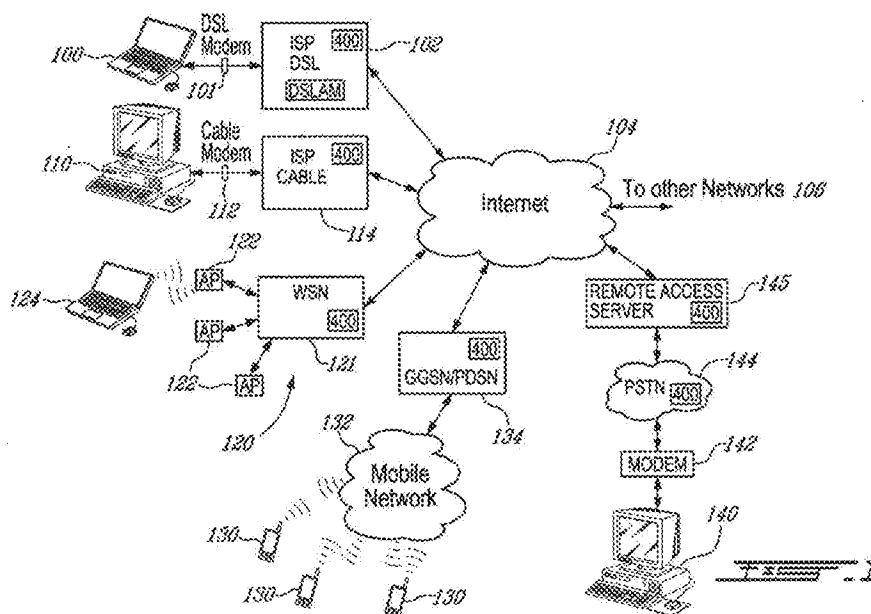
Rittmaster also discusses a plurality of network elements in the form of provider computers connected to a server to provide information to the plurality of end-user devices, such as the below embodiment that determines whether to provide specific content from networked content providers to one or more users in a shopping area based on the relative positions of the provider computers (138, 140) and display devices (122, 128, 138, 140) (as well as other potential criteria). *Id.*



In this example, advertising from computers associated with stores, restaurants, theaters, or other “bricks and mortar” establishments is provided to users in a particular nearby region. Malek Decl. at ¶ 46; Ex. C, ¶¶ 115-17. Each recipient (user) processor 120 is coupled to a wide area network (preferably, the internet) 18 and is provided access to certain content based on the location of the processor, as determined by GPS. *Id.* *Rittmaster* discloses that the user’s devices may be a “computer, ... PDA, mobile telephone, or the like” and that “[i]t is to be understood that not only the user, but the content provider or both could be mobile.” Ex. C, ¶¶ 90 and 143; Malek Decl. at ¶ 46. In fact, “[i]n accordance with one preferred embodiment, users carrying such portable communication devices within (or suitably near) the first shopping are[a] may access information provided by content provider 12 over the network 18 . . .” so that “similar to the FIG. 10 embodiment, people within the first shopping area (in this case, the users of portable communication devices within the first shopping area) may be provided access to advertisement or promotional information from establishments such as the bakery 134 or hobby store 136 located in the first shopping area.” Ex. C, ¶¶ 127-28; Malek Decl. at ¶ 46.

2. U.S. Patent Pub. No. 2006/0268696 (“*Konstantinov*”) (Ex. D)

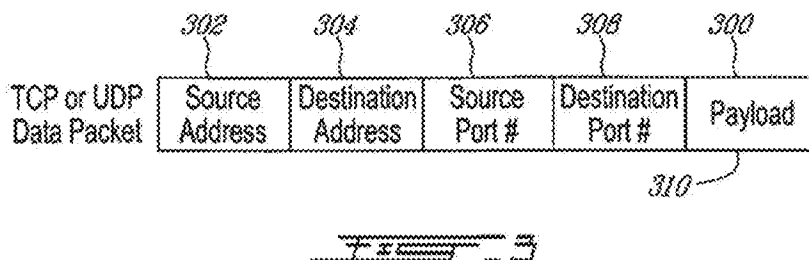
Konstantinov discloses a system in which a plurality of user devices (such as computers and mobile phones) access a server (or other network) over the internet to obtain content. Malek Decl. at ¶ 47; Ex. D. One such network is shown below:



In this high-level network diagram, laptop terminal 100, personal computer 110, multiple mobile clients 130, and PC-based terminal 140 can link to the internet via respective access points. Malek Decl. at ¶ 47; Ex. D, ¶ 32. As illustrated, each device that connects the user devices to the internet, such as remote access server 145, includes a scrambling module 400. The scrambling module 400 detects data traffic that matches certain criteria or rules, so that illegitimate Voice over Internet Protocol (VoIP) data traffic is detected, and the individual data packets are intercepted, delayed and scrambled. Malek Decl. at ¶ 47; Ex. D, ¶ 33. The scrambling module 400 also creates an “access list” 404 of various rules 406 that may specify indications and/or conditions in which data packets should be intercepted and scrambled. Malek Decl. at ¶ 47; Ex. D, ¶ 34. These rules include, for example, indications of source IP addresses, destination IP addresses of parties whose communications are to be intercepted and scrambled, protocols used for carrying on VoIP communication, and the like. *Id.*

Konstantinov further discloses that messages sent to and from devices through the network include unique identifiers for both applications on the source device and destination device. Malek Decl. at ¶ 48. For instance, Fig. 3 shows that each data packet includes, in addition to a “payload”

(content provided from a source device), addressing information relating to the “destination address” (*i.e.*, recipient device IP address), and a “destination port #” (*i.e.*, a port number identifying the virtual location on the recipient device at which a specific software application is located):



Id.; Ex. D, Fig. 3, ¶ 39. The packet also includes the same type of identifying information for the source device and its associated software. *Id.*

3. Andrew S. Tanenbaum and Maarten Van Steen, *Distributed Systems: Principles and Paradigms* (Pearson Education, 2d ed. 2007) (“*Distributed Systems*”) (Ex. E)

Distributed Systems was a widely used textbook in the computer science curricula of many universities at the relevant time and outlined basic requirements for network systems that would have been known to a PHOSITA. Malek Decl. at ¶ 52. Although *Distributed Systems* bears a 2007 copyright, the publication date is listed as October 12, 2006, on Amazon.com.² *Distributed Systems* discloses, among other things, that communication between devices over the internet utilized protocol stacks to establish secure message links between devices. Malek Decl. at ¶ 53. *Distributed Systems* also discloses that as of 2007 the standard message format included source and destination IP addresses and port numbers, identifying not only the device but also the software component on that device for which the message was intended. *Id.*

4. Andrew S. Tanenbaum, *Computer Networks* (Pearson Education, 4th ed. 2003) (“*Computer Networks*”) (Ex. F)

Computer Networks was a widely used textbook in many computer science programs available at the relevant time and teaches foundational concepts in computer networks and the internet. Malek Decl. at ¶ 53. Although *Computer Networks* bears a 2003 copyright, the publication date is listed as January 1, 2002, on Amazon.com.³ *Computer Networks* discloses, among other

² See <https://www.amazon.com/Distributed-Systems-Principles-Paradigms-2nd/dp/0132392275>.

³ See <https://www.amazon.com/Computer-Networks-4th-Andrew-Tanenbaum/dp/0130661023>.

things, various encryption methods that were widely known as of at least 2003, including use of digital signatures. Malek Decl. at ¶ 59.

5. U.S. Patent No. 8,064,934 (“*Klassen*”) (Ex. K)

Klassen discloses a network for sending messages to a variety of mobile end-user devices through a network server:

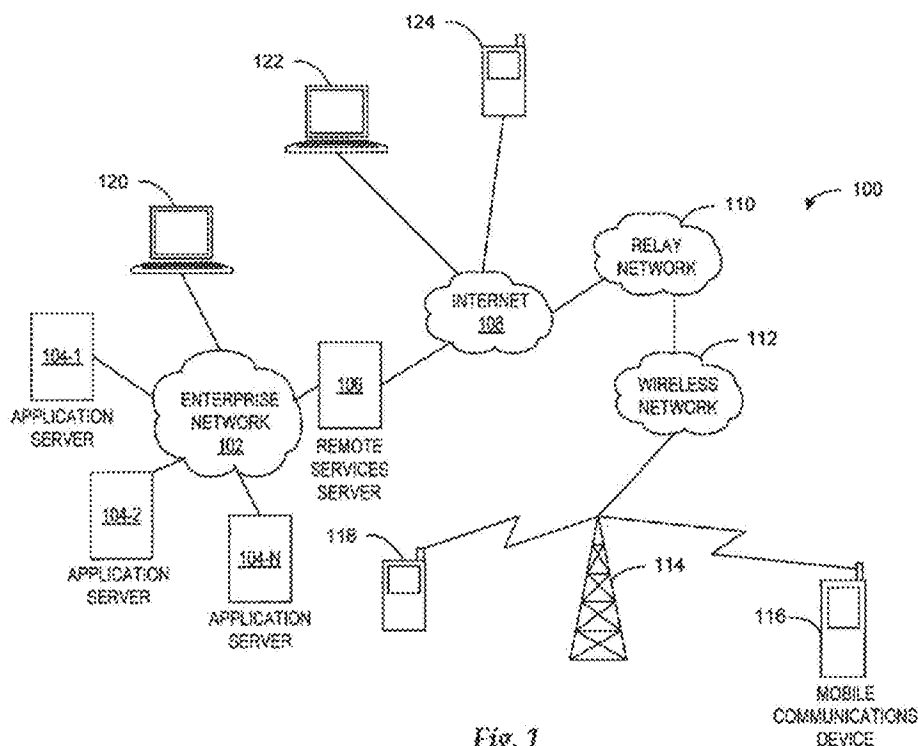


Fig. 1

Malek Decl. at ¶ 76; Ex. K, Fig. 1. As illustrated above, *Klassen* discloses a remote services server 106 linking a plurality of network elements (application servers 104-1 through 104-N) through the internet to a plurality of mobile communications devices (e.g., 116, 124). Malek Decl. at ¶¶ 49, 76. In some embodiments, the mobile device may include a chat application 216 with a status update module 218 to monitor the status of the chat application and communicate recent or upcoming status changes to devices in communication with the chat application. Ex. K, 4:1-6. The status update module 218 can ascertain a status change due to an instruction from a user or some other source and can also detect the status change due to the existence of certain conditions. Ex. K, 6:31-44. *Klassen* further discloses that the status update module 218 may automatically send a notification of the status change to other devices. *Id*

6. U.S. Patent No. 7,082,615 (“Ellison”) (Ex. L)

Ellison illuminates how processors are vulnerable to malicious software attacks, and discloses a method to protect processors and, more generally, subsets of a software environment. Malek Decl. at ¶ 86; Ex. L, Abstract, 1:16-51. To inhibit such attacks, *Ellison* isolates different software elements using a hierarchy, or “rings,” to divide hardware and software components designed to perform dedicated tasks within an operating system. Malek Decl. at ¶ 86; Ex. L, 1:41-51. The division of a component into rings is typically based on the degree or level of privilege. Malek Decl. at ¶ 86; Ex. L, 1:51-53.

7. U.S. Pat. Pub. 2009/0282256 (“Rakic”) (Ex. M)

Rakic recognizes the risks associated with unverified transmissions and proposes use of electronic signatures to verify the parties to the transmission. Ex. M, ¶¶ 47-49, 66-67. Specifically, *Rakic* discloses that a push-message server 504 generates an electronic signature, which is appended to the message and/or other information to verify message authenticity and source. Malek Decl. at ¶ 90; Ex. M, ¶¶ 41-49, 66-67, 109-112. A client device 102 then uses a secure-push-message client 404 to validate the message and sender using the electronic signature. Ex. M, ¶¶ 41, 109-112. Message validity is confirmed if the received and generated signature portions match. *Id.*

8. U.S. Pat. Pub. 2002/0186845 (“Dutta”) (Ex. N)

Dutta discloses use of digital signatures in mobile networks. Malek Decl. at ¶ 90; Ex. N, Abstract. Specifically, *Dutta* discloses systems for mobile e-commerce and relies on mobile devices employing secure messaging that employs private and public key-pairs and digital signatures for authentication for carrying out secure transactions. Ex. N, ¶ 1. In *Dutta*, push messages are authenticated by a digital signature of the Remote Security Element Access Control Service (RSE-ACS) of the mobile device, and an address of the mobile device is included in each message to make it device-specific. Ex. N, ¶ 28.

9. U.S. Pat. Pub. 2005/0144294 (“Gellens”) (Ex. O)

Gellens recognized that allowing applications to open connections for “low priority” messages could lead to “excessive and wasteful traffic channel usage.” Malek Decl. at ¶ 96; Ex. O, Abstract, ¶¶ 2-6, 27, 29. To remedy this problem, *Gellens* proposes using triggers (like *Rittmaster*) to control when messages are delivered to clients based on network usage. Malek Decl.

at ¶ 96; Ex. O, ¶¶ 35-36. For example, delivery of low priority application messages may be triggered only after a higher-priority application initiates a link. *Id.*

10. U.S. Pat. Pub. 2006/0129691 (“Coffee”) (Ex. S)

Coffee discloses that multiple messages can be bundled together and each can still retain their “own unique identifier.” Malek Decl. at ¶ 88; Ex. S, ¶¶ 117-119. This allows for larger bundled messages to be sent less frequently and helps alleviate problems with throughput. Ex. S, ¶¶ 117-119. *Coffee*’s solution allows messages to keep their own unique identifiers even while bundled with others. *Id.*

11. U.S. Pat. Pub. 2005/0108397 (“Basso”) (Ex. T)

Basso recognizes that multiple messages sent from a network processor may be bundled into one single message. Malek Decl. at ¶ 88; Ex. T, Abstract. Specifically, *Basso* reduces the number of messages that a control processor has to process in a load balancer. Ex. T, Abstract. This solution allows for less messages to be sent and improved performance of the system. *Id.*

12. AU App. No. 2007200530 (“Shenfield”) (Ex. U)

Just like the ‘192 Patent and *Rittmaster*, *Shenfield* discloses networks in which a plurality of network elements communicate and interface with a plurality of mobile user devices over the internet. Malek Decl. at ¶ 103.; see Ex. U, Fig. 1. *Shenfield* discloses the delivery and processing of push content communicated to a mobile station. Ex. U, Abstract. One such network is shown below in Figure 1:

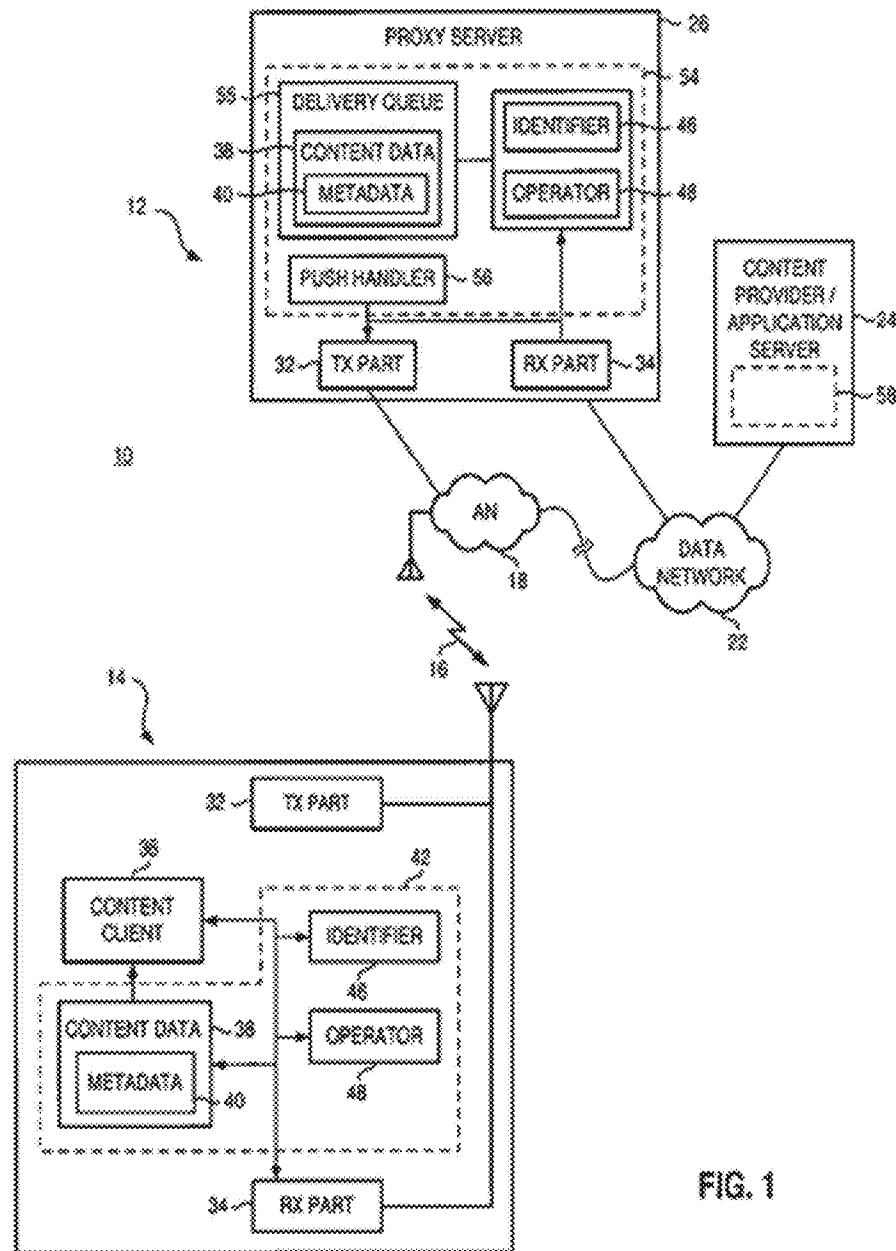


FIG. 1

Ex. U, Fig. 1. The proxy server (message link server) communicates content with a mobile station (wireless end-user device) via a push handler. Ex. U, ¶ 31. *Shenfield* maintains links between the server and end user devices, and notes that severance of the link results in a suspension of content being delivered. Malek Decl. at ¶ 117. Notably, the proxy server can communicate content to multiple mobile stations and multiple applications (software components) within each mobile station. Each application is a “content client” which is “representative of an application, an application environment, or, generically, a push agent that consumes content pushed to the mobile

station.” Malek Decl. at ¶ 107; Ex. U, ¶ 34. Figure 2, below, shows the communication layer that receives content pushed from the push handler of the proxy server.

14

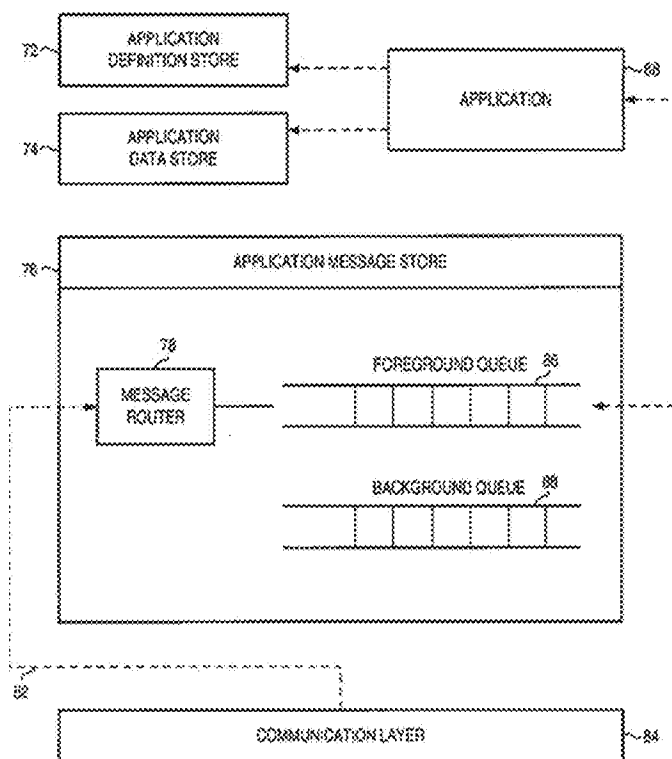


FIG. 2

Ex. U, Fig. 2. Every incoming message contains an application identification and a message identification. *Id.* ¶ 69. The communication layer of each mobile station receives the incoming messages sent by the push handler and places them in the appropriate message store of the content client according to their respective application identification. Malek Decl. at ¶ 106; Ex. U, ¶ 69.

Further, content or messages from content providers may be stored in a queue at the proxy server for distribution at a later time to user devices. Malek Decl. at ¶ 103; Ex. U, ¶¶ 36 and 40. This storage can occur until a trigger is effectuated. *Shenfield* discloses that messages from the proxy server can be triggered as “push” messages, which are initiated by a party other than the user, or “request-response” messages, which are initiated by the user. Malek Decl. at ¶ 111; Ex. U, ¶ 4. *Shenfield* also discloses other types of triggers for push message systems, including geographic location, time, and receipt of an updated message. Ex. U, ¶ 36. This indicates that the

proxy server also contains logic for determining when messages should be sent to mobile stations. *Id.* Content can be tracked via unique message identifiers as well, and older messages in the queue can be replaced with updated versions. *Id.* at ¶ 46.

D. Discretionary Denial Under 35 U.S.C. § 325(d) Is Not Warranted

Discretionary denial is only warranted under § 325(d) when “the same or substantially the same prior art or arguments” were previously considered by the Office. 35 U.S.C. § 325(d). And “[t]he existence of a substantial new question of patentability is **not precluded** by the fact that a patent or printed publication was previously cited by or to the Office or considered by the office.” 35 U.S.C. § 303(a) (emphasis added). No primary reference relied on in this request (*i.e.*, *Rittmaster*, *Shenfield*, *Konstantinov*, *Klassen*, *Distributed Systems*, *Computer Networks*) was presented to the Office during prosecution of the '430 Application or during any *inter partes* review proceeding. While secondary references *Ellison*, *Gellens*, and *Rakic* were relied on by Target, Amazon, and Samsung in support of their petitions for *inter partes* review of the '192 Patent, the grounds presented herein that rely in part on those references relate only to dependent claims and assert combinations that were not presented or considered in any *inter partes* review, *ex parte* reexamination, or other USPTO proceeding. As such, this request presents a substantial new question of patentability in view of the references and arguments presented, and therefore discretionary denial under § 325(d) is not warranted.

II. DETAILED EXPLANATION UNDER 37 C.F.R. § 1.510(B)(2) OF THE PERTINENCY AND MANNER OF APPLYING THE CITED PRIOR ART TO EVERY CLAIM FOR WHICH REEXAMINATION IS REQUESTED

In the subsections below, this Request demonstrates: (1) how claims 1-3, 5-7, 9, and 11-15 of the '192 Patent are anticipated over *Rittmaster*; (2) how claims 1-3, 5-7, and 9-15 of the '192 Patent are obvious over *Rittmaster* in combination with any of *Distributed Systems* and *Computer Networks*; (3) how claims 1-3, 5-7, and 9-15 of the '192 Patent are obvious over the combination of *Rittmaster* and *Shenfield*; (4) how claims 1-3, 5-7, and 9-15 are obvious over *Rittmaster* and/or *Shenfield* in combination with any of *Konstantinov* and *Klassen*; (5) how claim 4 of the '192 Patent is obvious in view of a combination of references including *Ellison*; (6) how claim 6 of the '192 Patent is obvious in view of a combination of references including *Coffee* or *Basso*; (7) how claim 8 of the '192 Patent is obvious in view of a combination of references including *Computer Networks* and either *Rakic* or *Dutta*; and (8) how claim 14 of the '192 Patent is obvious in view of a combination of references including *Gellens*.

A. Level of Ordinary Skill in the Art

A person having ordinary skill in the art (“PHOSITA”) of digital communication and content distribution networks at the relevant time would have had a bachelor’s or master’s degree in computer science and one or two years of industry experience. Malek Decl. at ¶ 26. More advanced education could make up for lack of industry experience and vice versa. *Id.*

B. Claim Construction

In determining whether a “substantial new question of patentability” exists as to make reexamination appropriate, “the PTO must apply the broadest reasonable meaning to the claim language, taking into account any definitions presented in the specification.” *In re Bass*, 314 F.3d 575, 577 (Fed. Cir. 2002) (citing *In re Yamamoto*, 740 F.2d 1569, 1571 (Fed. Cir. 1984)); *accord In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1369 (Fed. Cir. 2004) (the “PTO is obligated to give claims their broadest reasonable interpretation during examination.”). Walmart submits that under the broadest reasonable interpretation, substantial new questions of patentability are presented herein. Furthermore, for the purposes of this request for *ex parte* reexamination, and without conceding that the claims satisfy 35 U.S.C. § 112, Walmart submits that all terms should be interpreted according to their broadest reasonable interpretation.

With that in mind, on August 22, 2024, the United States District Court for the Eastern District of Texas issued a Claim Construction Order in *Headwater Rsch. LLC v. Samsung Elecs. Am., Inc., et al.*, No. 2:23-cv-103 (Dkt. 118). Ex. G. The court construed the following terms as reflected in Ex. G. Although these constructions do not necessarily govern in a reexamination proceeding, Walmart asserts that the broadest reasonable interpretation of each term is at least as broad as the court’s construction.

1. “software components”

The term “software components” appears in claims 1, 4, and 15. Both Samsung and Patent Owner agreed that “software components” has a plain meaning to a skilled artisan. Ex. G at p. 17. The court agreed and construed the term “software components” to be “components of software.” *Id.* at pp. 17-18, 19.

2. “wherein one of the message delivery triggers is the receipt of a particular network element message from one of the network elements”

The term “wherein one of the message delivery triggers is the receipt of a particular network element message from one of the network elements” appears in claim 13. The court held the term should have a “plain and ordinary meaning.” Ex. G at pp. 18, 19.

3. “device messaging agent”

The term “device messaging agent” appears only in dependent claim 7 and was argued and construed in relation to U.S. Patent No. 9,198,117 (the “’117 Patent”)⁴ to Raleigh, where it appears in claim 1 and various dependent claims. The term “device messaging agent” of claim 7 of the ’192 Patent has no antecedent basis in claim 1, from which it depends, and the closest analogue is “device link agent.” Neither “device link agent” nor “device messaging agent” appear in the ’117 Patent or ’192 Patent disclosures. In construing the term “device messaging agent,” the court explained that the words “device” and “messaging” are “simply modifiers of ‘agent.’” Ex. G at p. 16. The court ultimately construed “device messaging agent” to be “a piece of software on a mobile end-user device that performs certain messaging functions for other software.” Ex. G at p. 19. For purposes of this reexamination request, we will assume that “device messaging agent” and “device link agent” are synonyms.

C. Ground 1: Claims 1-3, 5-7, 9, and 11-15 are Anticipated by Rittmaster

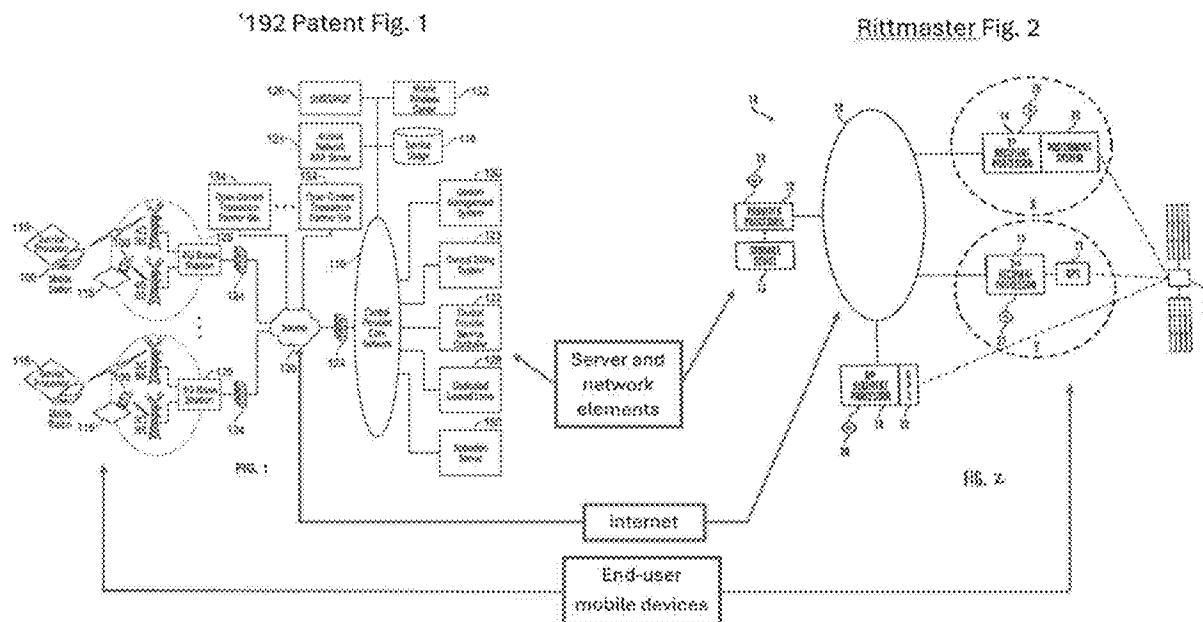
Rittmaster discloses all of the elements of claims 1-3, 5-7, 9, and 11-15 either expressly or inherently. While *Rittmaster* omits certain protocol-level elements recited in the claims, those elements are so basic to the types of networks employed at the time of the alleged invention and discussed in *Rittmaster* that a PHOSITA would have understood them to be necessarily present. In fact, these details were so basic that their inherency is evidenced in college-level textbooks widely in use before the alleged invention of the ’192 Patent.

More specifically, all of the claims of the of the ’192 Patent relate to a message link server (or operation of a message link server) that includes (i) a transport services stack to maintain secure message links with multiple end-user devices, (ii) an interface with a network to receive messages from a plurality of network elements, and (iii) a message buffer system that delays delivery of at least some messages from the network elements to user devices until one of a plurality of triggers is satisfied. Malek Decl. at ¶ 50. Such a server was not new in January 2009. *Id.* Various devices in at least the early 2000s, such as those disclosed in *Rittmaster*, were designed for conditional

⁴ The ’117 Patent and the ’192 Patent share priority to the same four provisional applications and share the same disclosure. Ex. G at p. 1.

delivery of message content based on occurrences of specific triggers. *Id.* A PHOSITA would have recognized that *Rittmaster* discloses each of the elements claimed in the '192 Patent either explicitly or inherently. *Id.* To the extent *Rittmaster* is interpreted to be missing any details, such details should be readily understood to be obvious design choices based on typical network architecture common and available at the time that the applications that led to the '192 Patent were filed, as discussed in Ground 2. *Id.*

To better demonstrate the similarities between the system architectures of the '192 Patent and *Rittmaster*, an annotated comparison of Fig. 1 of the '192 Patent and Fig. 2 of *Rittmaster* is provided below. The diagram illustrates that the two systems plainly share a plurality of end-user mobile devices (left, solid line) communicating to a content provider server (right, dashed line) through the internet (center, dotted line):



I. Claim 1

a. 1[PRE] "A message link server comprising:"

The preamble of claim 1 recites a "message link server." Like the '192 Patent, *Rittmaster* discloses a server for providing message content to linked user devices. Malek Decl. at ¶ 51. Fig. 2 illustrates that the *Rittmaster* provider server 12 maintains links with any number of recipients (user devices 14, 15, 16):

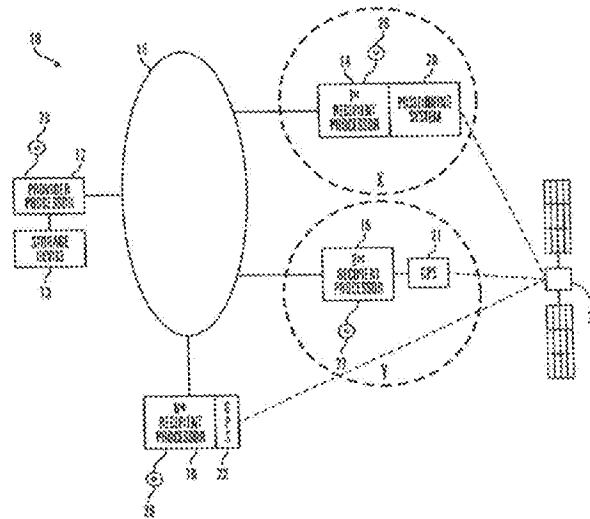


FIG. 2.

Malek Decl. at ¶ 51; Ex. C, ¶ 42 (“provider server 12 comprises an Internet product or service provider computer or server...coupled for communication...to a plurality of network enabled user devices.”)

- b.** 1[a] “a transport services stack to maintain a respective secure message link through an Internet network between the message link server and a respective device link agent on each of a plurality of wireless end-user devices,”

Rittmaster discloses element 1[a] of the '192 Patent. As shown above, *Rittmaster* discloses “wireless end-user devices” in that its server 12 “comprises an Internet product or service provider computer or server . . .” coupled through the internet 18 for communication to “a plurality of network enabled user devices.” Malek Decl. at ¶ 52; Ex. C, ¶¶ 32, 42. The user devices 14-16 (which may be “portable communication devices”) and the provider server 12 have “means for interfacing with and communicating on a communications network.” Malek Decl. at ¶ 52; Ex. C, ¶¶ 42, 126-27. *Rittmaster* explains that “[s]uch computers and communication interfacing are well known in the art and are not described in further detail herein for purposes of simplifying the present disclosure.” Malek Decl. at ¶ 52; Ex. C, ¶ 42.

Rittmaster also explicitly describes a “secure message link” through disclosure of a *secure* network connection, with the provider server 12 sending content to user devices 14-16 “in an encrypted format.” Malek Decl. at ¶ 52; Ex. C, ¶ 82. *Rittmaster* notes that “[m]any forms of encryption are commonly used” in the art; for example, messages may employ an encryption key

algorithm utilizing location information of the user device using “a secure message link,” as recited in claim 1 of the ’192 Patent. *Id.*; *see also*, Ex. C, Fig. 9.

Rittmaster omits specific transport layer protocols for sending or receiving messages, instead acknowledging that “[s]uch computers and communication interfacing are well known in the art and are not described in further detail herein for purposes of simplifying the present disclosure.” Malek Decl. at ¶ 52; Ex. C, ¶ 42. *Rittmaster* does, however, explicitly disclose a message link agent as in the ’192 Patent and that software is responsible for maintaining a link, *e.g.* through the internet, between the server and recipient (end-user) processors, stating that “[t]he processors may comprise any suitable data processing and communicating device controlled, preferably, by a software program” and that the processors have “means for interfacing with and communicating on a communications network and for operating, preferably under the control of software programs.” Ex. C, ¶¶ 32 and 42. *Rittmaster* also discloses that encrypted communications are received over an “internet connection” at a decryption module of the recipient (end-user) device (shown in Fig. 7) described as comprising “a hardware, firmware, software or hybrid decryption system for performing decryption operations in accordance with any suitable decryption technique.” Ex. C ¶¶ 84-87. This is similar to the “Device Link” 1691)⁵ shown in Fig. 24 of the ’192 patent, which serves to receive and decrypt messages before they are transported to the appropriate software program, as shown below:

⁵ The terms “device link agent” or “link agent” do not appear in the specification of the ’192 patent.

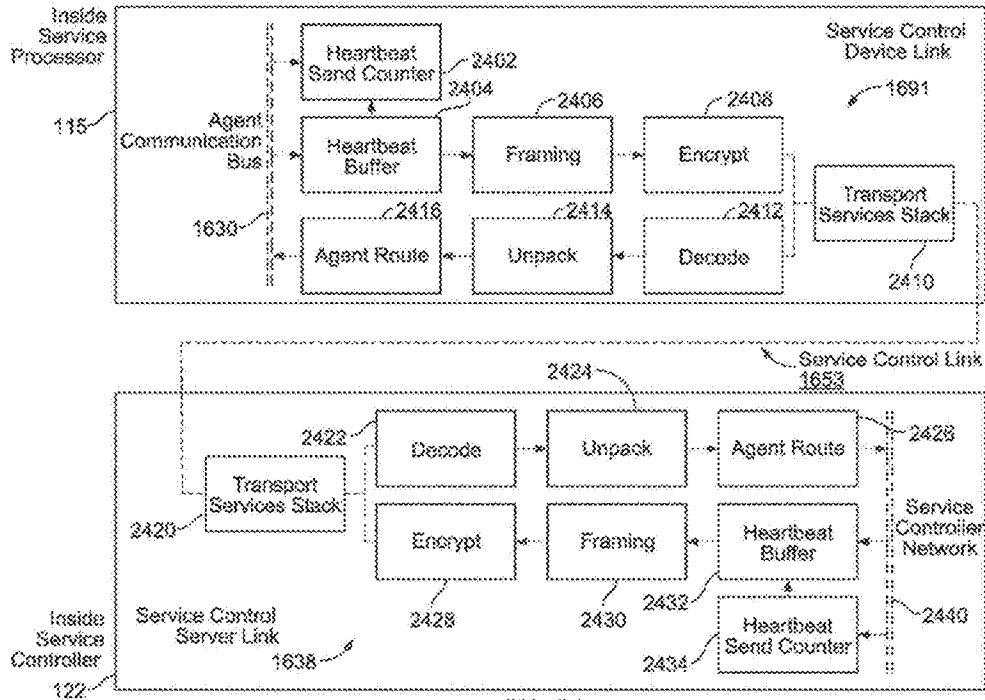


FIG. 24

Ex. A, Fig. 24; *see also* Ex. A, 9:52-64 (including a “...a decode element 2412 for decoding any received service controller 122 communications (e.g., decrypting encrypted communications)...”) Messages received via *Rittmaster’s* link would be received by the decryption module before being routed to software at the appropriate port number for displaying the message, then “software . . . residing on the recipient device” may “selectively deny, limit or allow access to predefined information on the network, display warning or other messages, or enable or disable processing or receiving circuitry or routines necessary to receive or effectively use the predefined information on the network.” *Id.* ¶ 81.

Further, the '192 Patent itself admits that a transport services stack on a mobile device communicating with a transport services stack on a network server was standard, showing a transport stack on each device in Fig. 24 and stating that the “Transport Services Stack” 2420 provides “basic transport services” and can be “implemented with **standard** secure or open Internet networking protocols, such as TLS or TCP.” Malek Decl. at ¶ 39; Ex. A, 89:29-36 (emphasis added). A PHOSITA at the time of the alleged invention would have recognized that *Rittmaster’s* statement regarding “communication interfacing [that is] well known in the art” incorporates well-known and common Transport Layer Security (TLS) level protocols for maintaining a secure link that is discussed as “standard” in the '192 Patent, and would further have recognized that a “transport services stack” at the server and “message link agent” on the end-user

device would have been inherent (necessarily present) because that was standard for communication over the internet. Malek Decl. at ¶ 52. For instance, even textbooks at the time recognized that networks were organized as stacks of layers, with a given layer on one machine (e.g. a server) communicating with a corresponding layer on another machine (e.g. a mobile device). *See* Ex. F at p. 28 (“Layer n on one machine carries on a conversation with layer n on another machine”).

Rittmaster’s disclosure of a device link agent on a user device is further described below in Section II.C.1.c. *Rittmaster*’s disclosure of a respective secure message link maintained by the transport services stack is further described below in Sections II.C.5 and 6. In short, however, communication over the internet “would have inherently (necessarily) been between a stack on the server and a software program on the mobile devices,” as shown by basic textbooks such as *Distributed Systems*. Malek Decl. at ¶ 52. Device link agents comprising a corresponding transport stack on the end-user device for communication with the server were also described in, for instance, Klassen. Malek Decl. at ¶ 78; Ex. E Fig. 2.

- c. 1[b] “each of the wireless end-user devices comprising multiple software components authorized to receive and process data from secure message link messages received via a device link agent on that device;”

Rittmaster further discloses element 1[b] of the ’192 Patent. Malek Decl. at ¶ 53. *Rittmaster* specifies that in some instances “the recipient processors comprise online user terminals, including, but not limited to conventional personal computers (PCs), portable communication devices (such as portable telephones, personal digital assistants, or other portable information units), or vehicle-mounted computers connected to a wide area network, such as, but not limited to, the Internet.” Malek Decl. at ¶ 53; Ex. C, ¶ 35. Furthermore, *Rittmaster* explains, “the user devices 14-16 ... may each comprise any suitable computer or processor device having means for interfacing with and communicating on a communications network and for operating, *preferably under the control of software programs*, in the manner described.... Such computers and communication interfacing are well known in the art and are not described in further detail herein....” Malek Decl. at ¶ 53; Ex. C, ¶ 42 (emphasis added). Specifically, *Rittmaster* discloses that encrypted communications are received over an “internet connection” at a decryption module of the recipient (end-user) device, shown in Fig. 7 and described as comprising “a hardware, firmware, software or hybrid decryption system for performing decryption operations in

accordance with any suitable decryption technique.” Ex. C ¶¶ 84-87. As discussed in the previous section, this performs the same functions as the “Device Link” shown in the ’192 patent at Fig. 24 and comprises software for decrypting messages for use by other software components.

Rittmaster also discloses software components for using the information received as messages, discussing that “software . . . residing on the recipient device” may “selectively deny, limit or allow access to predefined information on the network, display warning or other messages, or enable or disable processing or receiving circuitry or routines necessary to receive or effectively use the predefined information on the network.” *Id.* ¶ 81; Malek Decl. at ¶ 53. *Rittmaster* also discloses downloading or accessing various different media, such as music files, graphics files, electronic books, movies or television shows, video games, or radio transmissions, which would each operate on different software of the end-user device. *See, e.g.*, Ex. C ¶¶ 70 and 132. A PHOSITA at the time of the alleged invention also would have readily recognized that the portable communication devices identified by *Rittmaster* (e.g. portable telephones, personal digital assistants, or other portable information units) inherently have a plurality of software applications on them that are each associated with their own port number, as confirmed by the *Computer Networks* textbook (Ex. F). Malek Decl. at ¶ 53.

- d.** **1[c]** “an interface to a network to receive network element messages from a plurality of network elements, the received network element messages comprising respective message content and requests for delivery of the respective message content to respective wireless end-user devices, the respective message content including data for, and an identification of, a respective one of the authorized software components,”

Element 1[c] requires that the network-facing side of the server include an “interface” to receive messages from two or more “network elements,” and that the messages include “message content” and “requests for delivery” of that content to specific end-user devices by including data for, and an identification of, authorized software. Malek Decl. at ¶ 54. This does little more than describe the basic manner in which messages were delivered from a network at the relevant time (January 2008), and how messages are still delivered today. *Id.* Even so, *Rittmaster* explicitly discloses element 1[c], explaining that “[t]he provider processor 12 is capable of providing information from any suitable source (including, but not limited to an on-line source...).” Malek Decl. at ¶ 54, Ex. C, ¶ 33. This necessarily includes an “interface” connecting the server to each suitable source. *Rittmaster* also discloses specific embodiments in which multiple computers

associated with retail establishments provide advertising information to a provider processor (server) to be stored on a memory device for communication to recipient processors (end-user devices) at appropriate times, or alternatively linking the recipient processors to the establishment computers at appropriate times to obtain information directly from those establishment computers. Ex. C, ¶ 121. In other words, *Rittmaster* discloses that message content is sent and delivered from the computers for retail establishments (network elements) through the provider processor (server) in the form of a message to the end-user devices, or alternatively that the messages may be sent directly from the retail establishments to the recipients, so that messages from the retail establishment computers would be addressed to specific software on specific end-user devices.

The “network elements” in *Rittmaster* can include, for instance, a plurality of computers from different establishments such as restaurants, stores, or other shopping establishments. Malek Decl. at ¶¶ 46 and 54. The message “data” can include, for instance, advertising information. *Id.* “For example, the owner of each of these establishments may have communicated advertisement information to the provider processor 12, from suitable computers 138 and 140 coupled to the network 18.” Ex. C, ¶ 121; Malek Decl. at ¶ 54. Further, “the establishment’s processor 138 or 140 may be programmed to automatically communicate a signal to the provider processor 12 to cause a specified piece of content to be displayed on one or more selected display devices 122 and 128. Ex. C, ¶ 125; Malek Decl. at ¶ 54.

Messages from network elements may include, for instance, “promotional or advertisement information for a plurality of different establishments within the same shopping area.” Ex. C, ¶ 120. “For example, the owner of each of these establishments may have communicated advertisement information to the provider processor 12, from suitable computers 138 and 140 coupled to the network 18.” Ex. C, ¶ 121. Further, “the establishment’s processor 138 or 140 may be programmed to automatically communicate a signal to the provider processor 12 to cause a specified piece of content to be displayed on one or more selected display devices 122 and 128. Ex. C, ¶ 125

Every such message in *Rittmaster* would inherently have had an address identifying where to deliver the message (*i.e.*, a combination of (i) an IP address identifying a specific user device and (ii) a port number specifying a virtual location on that device where the relevant software designed to receive the message is located), because that is already how all messages were directed from provider servers to user devices connected to servers (*e.g.*, in 3G or 4G networks) at the

relevant time. Malek Decl. at ¶ 54. This is confirmed by basic textbooks showing that by the time of the alleged invention standard structure for IP packets for transmitting information over the internet included a destination address specifying the IP address of the recipient device, and the standard TCP message format also included a destination port number identifying the virtual location of recipient software on that device. *See, e.g., Computer Networks*, Ex. F at p. 340; Malek Decl. at ¶ 54. Including the address in the message ensures the message content is delivered to the appropriate software application. *Id.*

The messages sent from network elements to the server would comprise message content (e.g. advertising in the examples discussed above) and requests for delivery to respective wireless end-user devices. As discussed above at II.C.1.b., standard message formats at the time would have included an IP address to direct messages to a particular IP address. *See also* Malek Decl. at ¶ 52-53. This is verified by textbooks such as *Distributed Systems*, which discloses that as of 2007 the standard message format included source and destination IP addresses and port numbers, identifying not only the device but also the software component on that device for which the message was intended. *Id.*; Ex. F, pp. 329-30 and 410. In fact, *Rittmaster* discloses that the users may be pre-authorized subscribers, meaning that the content provider would know the user in advance and send messages directed to authorized users, although access to the requested content would be controlled by the server based on the user's geographic position. Ex. C, ¶ 112. Likewise, the messages would have included respective message content including data for, and an identification of, a respective one of the authorized software components because standard communication protocols also included a port number to direct the message to a particular software application.

- e. 1[d] “a message buffer system including a memory and logic, the memory to buffer content from the received network element messages for which delivery is requested to a given one of the wireless end-user devices”

Rittmaster discloses a buffer system that prevents transmission of messages to end-user devices until a determination is made, using a set of rules or logic, that one or more specific end-user devices are authorized to receive the message, such as by virtue of being located in a specific geographic region. Malek Decl. at ¶ 55. For instance, Fig. 2 below illustrates a storage device 13 (i.e., a memory) associated with the server 12, which may store messages prior to sending them to end-user devices:

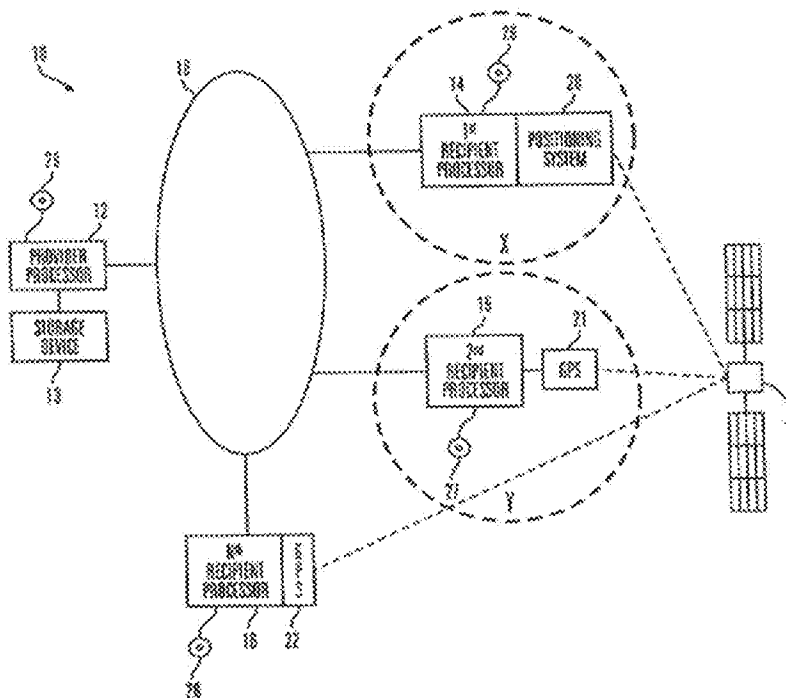


FIG. 2.

Id.

Rittmaster further explains that the server 12 does not provide content to a user device until a determination is made that specific restrictions have been satisfied. *Id.* at ¶ 56. For instance, *Rittmaster* explains, “a set of rules may be implemented, which depend upon the geographic information (and, thus, the geographic location or region of the recipient processor), such that...if a recipient processor provides geographic information corresponding to a first geographic location or region, then the provider processor may be controlled to not provide selective information to the recipient processor, unless further requirements are met.” Malek Decl. at ¶ 56; Ex. C, ¶ 40. *Rittmaster* specifies that “the determination of the region in which the user device is located is performed at the provider server, under control of a routine of software 29 (as represented by step 32 in FIG. 3).” Malek Decl. at ¶ 56; Ex. C, ¶ 53. As such, the logic of the server determines in what region a particular user device is located. Malek Decl. at ¶ 56. *Rittmaster* further specifies that a software routine controls the provider server to determine whether or not the determined region is a restricted region (step 34). Malek Decl. at ¶ 56; Ex. C, ¶ 53.

All of the foregoing are forms of server-based logic to determine whether a particular end-user device is located in a particular geographic region. Malek Decl. at ¶ 56. And executing this

logic results in buffering of messages to the end user. *Id.* For instance, when the user device is in a non-restricted region, then it is provided access to the content. *Id.*; Ex. C, ¶ 56. In such a scenario, the server 12 downloads to the user device 14, “software files, programs, data, decode keys, or other information that defines the requested product or service or that are necessary for the user to obtain the requested product or service” from “any suitable source,” (including an online source, a computer readable storage medium, etc.) by communicating such information over the communications network 18. Malek Decl. at ¶ 56; Ex. C, ¶ 33. Thus, *Rittmaster* at least inherently discloses buffering content.

In one further example of buffering, *Rittmaster* indicates that advertisements from different establishments may be communicated to the provider server 12 “and stored in advance.” Malek Decl. at ¶ 56; Ex. C, ¶¶ 120-21. More specifically, *Rittmaster* expressly discloses that “the provider processor maintains a listing or inventory of advertisements” that can be provided to a recipient processor. Malek Decl. at ¶ 56; Ex. C, ¶ 134. The provider server “operates with an associated memory device on which advertisement or other display content is stored, for communication to the recipient processors for displaying at appropriate times.” Malek Decl. at ¶ 56; Ex. C, ¶¶ 120-21.

f. 1[e] “the logic to determine when one of a plurality of message delivery triggers for the given one of the wireless end-user devices has occurred, wherein for at least some of the received network element messages, the receipt of such a message by the message buffer system is not a message delivery trigger, and for at least one of the message delivery triggers, the trigger is an occurrence of an asynchronous event with time-critical messaging needs, and”

Rittmaster further discloses element 1[e] of claim 1 of the '192 Patent because providing content to an end-user device is dependent on one or more triggers. Malek Decl. at ¶ 57. Notably, in addition to geographic location, *Rittmaster* contemplates that “the provider processor [server] may... not provide selective information to the recipient processor [end-user device], unless further criteria is met,” such as a “minimum user age, a particular period of the day, week, month or year, or other suitable criteria” demonstrating that certain received messages are not triggers *Id.*; Ex. C, ¶ 14. In addition, specific content alternatively can be provided in response to a request for such content by a user. Ex. C, ¶¶ 112-14. Thus, there are plural triggers for sending messages from the server to end-user devices, and these triggers may be used as alternatives or in combination. The

criteria may also differ from region to region, resulting in a plurality of different triggers that determine whether a message will be sent depending on where the recipient is located. Ex. C, ¶ 14. Thus there are a variety of different triggers that may be put in place to cause the server to buffer and then transmit messages from network elements.

As to the portion of claim element 1[e] specifically requiring an “asynchronous event with time-critical messaging needs,” *any* reaction to a request for content from an end user would be considered to be an asynchronous event with time-critical messaging needs because (1) the requesting and the responsive providing of content are asynchronous (*i.e.*, they do not occur at the same time), and (2) the response is time-critical (*i.e.*, provided in response to a trigger, rather than residing on the network server indefinitely).⁶ Malek Decl. at ¶ 57.

This is consistent with how the patent owner interpreted the phrase, since the '192 Patent confirms that “asynchronous events with time-critical messaging needs” are, for example, a “transaction or service billing event or a user request.” Malek Decl. at ¶ 57; Ex. A, 38:59-63. Furthermore, in litigation with Samsung, the patent owner did not attribute any particular meaning to the phrase during claim construction. *See, generally*, Ex. G (*Headwater Rsch. LLC v. Samsung Elecs. Co. Ltd.*, et al., No. 2:23-cv-00103, Claim Construction Order (Dkt. 118)). Even more striking, during *Inter Partes* Review of the '192 Patent, Samsung noted that the patent owner both directly admitted that a message retrieval request from the user constitutes a message delivery trigger, and did not deny, given the opportunity, that such a basic request constitutes “an asynchronous event with time-critical messaging needs.” *See*, Ex. H (IPR2024-00010, Petitioner’s Reply to Patent Owner’s Response (Paper 16), at p. 4 (PTAB Dec. 18, 2024)), Ex. J (IPR2024-00010, Patent Owner’s Sur-Reply (Paper 19) (PTAB Jan. 23, 2025)).

⁶ A PHOSITA not only would have understood at the relevant time that such criteria represent a plurality of triggers because delivery of message content depends on logic determining that required criteria are met, but would also understand that these triggers are “asynchronous events with time-critical messaging needs,” because the logic of *Rittmaster* is configured to determine if these triggers are satisfied and to provide content to the user device automatically upon determining that one or more of the triggers is satisfied. Malek Decl. at ¶ 57. Like the “transaction or service billing event” and “user requests” mentioned in the '192 Patent, the triggers of *Rittmaster* result in a system that does not require an immediate real-time response from the recipient while still ensuring that the message is delivered and processed within a short timeframe. *Id.*

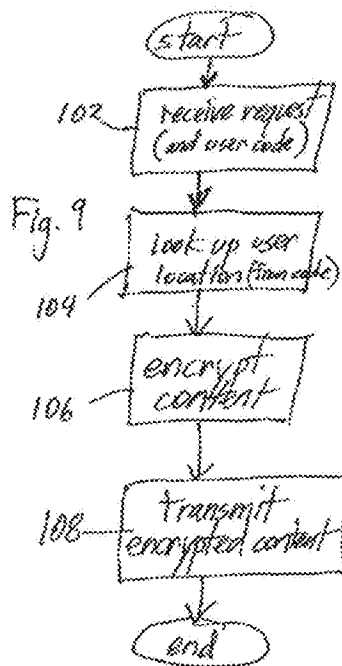
Further reinforcing the time-criticality of its triggers, *Rittmaster* also discloses logic that determines whether a trigger (e.g., receipt of recipient request) occurred **within a required time period**, which a PHOSITA would understand to be a trigger with “time-critical messaging needs.” Malek Decl. at ¶ 57; Ex. C, ¶¶ 62-67; *see also* Ex. C, ¶ 130. Indeed, *Rittmaster* considers the time information so critical in this embodiment that *Rittmaster* suggests encrypting the time information. Malek Decl. at ¶ 57; Ex. C, ¶ 66.

- g.* 1[f] “upon determining that one of the message delivery triggers has occurred, the logic further to supply one or more messages comprising the buffered content to the transport services stack for delivery on the secure message link maintained between the transport services stack and a device link agent on the given one of the wireless end-user devices.”

Rittmaster also discloses 1[f], the final element of claim 1. As explained above, *Rittmaster*’s message content is transmitted through a link between a stack on a server and a software agent on one of a plurality of end-user devices, simply by communicating through a secured internet connection. Malek Decl. at ¶ 58. The specific system in *Rittmaster* is designed to deliver messages from the server to the end-user device(s) in response to determining that a trigger has occurred, such as the end-user device entering a specific geographic region. *Id.* Such disclosure anticipates this claim element of the ’192 Patent. Another possible trigger is receipt of a request within a given time period, verifying a minimum user age, or other suitable criteria. Malek Decl. at ¶ 58.

- 2. **Claim 2** – “an encrypt function to encrypt the one or more messages supplied to the transport services stack for delivery on the secure message link maintained between the message link server and the device link agent on the given one of the wireless end-user devices.”

Claim 2 depends from claim 1. As described briefly above, *Rittmaster* contemplates encrypting content from network elements prior to transmission of the encrypted content from the network server to one or more of the plurality of end-user devices. Malek Decl. at ¶ 59. For instance, Fig. 9 illustrates the process of receiving a request from an end-user device (step 102), determining user location (step 104), encrypting content (step 106), and transmitting the encrypted content (step 108).



Id.; Ex. C, Fig. 9. *Rittmaster* explains that after receiving location information and, optionally, a user code (or other information used to determine whether a particular user should be given access to specific content from the network), “[t]he provider processor may then encrypt the content with an encryption algorithm or technique for which the expected user location is part of the decryption key or decryption processes used to decrypt the content” and “may also employ the user code (and user identification or recipient processor identification information) as part of the decryption key or decryption process” before “encrypted content is communicated to the recipient processor over the network (108 in FIG. 9).” Malek Decl. at ¶ 59; Ex. C, ¶¶ 97-98.

3. **Claim 3** – “the encrypted one or more messages are transported to the device link agent on the given one of the wireless end-user devices using one or more of encryption on the transport services stack, IP (Internet Protocol) layer encryption, and tunneling.”

Claim 3 is also disclosed by *Rittmaster*, as communications in *Rittmaster* would have inherently utilized Transport Layer Security (TLS) protocols (as standardized by the Internet Engineering Task Force (IETF)) at least by the relevant time period. Malek Decl. at ¶¶ 52, 60. Such utilization creates an encrypted channel at the transport layer (*i.e.*, Transmission Control Protocol (TCP)) and, by definition, has encryption on the transport services stack. *Id.*

Rittmaster expressly describes using one or more keys to encrypt content, which would, at a minimum, inherently include encryption of the payload of the message to be sent by the server.

Malek Decl. at ¶ 60; Ex. C, ¶¶ 97-98. These keys, for instance, could be derived from location information and/or a user code. *Id.*

4. **Claim 5** – “*wherein the transport services stack is further to receive, over each of the respective secure message links, upload messages forwarded by the respective device link agents from at least a subset of the device software components, each of the upload messages identifying a corresponding one of the network elements to which the device respective software component has requested delivery, the network server system using the interface to a network to deliver content from the upload messages to the respective identified network elements.*”

Claim 5 depends from claim 1 and specifies that the stack receives “upload messages” from at least some applications on user devices, and that the messages are then sent from the server to identified network elements. Malek Decl. at ¶ 61. Likewise, *Rittmaster* discloses that, upon request or command from the provider server, a user device may communicate a user code to the provider server. Malek Decl. at ¶ 61; Ex. C, ¶¶ 96-97. Additionally, information from the user may be transmitted to a content provider (network element) in order to assist in selection of content to be sent to that user. Malek Decl. at ¶ 61; Ex. C, ¶ 132. In other cases, the user may communicate its preferences directly to the network element. Malek Decl. at ¶ 61; Ex. C, ¶ 142. Therefore, not only does the *Rittmaster* server provide content to end-user devices, the server may also deliver “upload messages” from specific software on a user device to a specified network element, such as by sending a user code or user preference to a computer associated with a specific establishment (restaurant, bakery, store, etc.) in embodiments where messages are delivered based on proximity to a shopping area, or by sending a user code or preference to a content provider when requesting content from that network element.

5. **Claim 6** – “*wherein at least one of the one or more messages for delivery by the transport services stack comprises multiple identifier/data pairs.*”

Claim 6 depends from claim 1. The additional element of this claim is disclosed by *Rittmaster* alone, which indicates that two or more payloads may be included in a single message, with each payload associated with identifiers for the same device. Malek Decl. at ¶ 62. *Rittmaster* describes this element by discussing an embodiment in which a user located in a shopping area, such as a mall, may receive content with information from multiple network elements (*e.g.*, multiple store computers within the shopping area): “the first content provided to the recipient processor 120 for display on the display device 122 comprises information, such as promotional or advertisement information for a plurality of different establishments within the same shopping

area.” *Id.*; Ex. C, ¶ 120. *Rittmaster* further explains that such information would have been sent to the user in a single message: “for example, the **first content** may include advertisement information for a bakery 134 **and further** advertisement information for a hobby shop 136 located within the same shopping area as the recipient processor 120 and display device 122.” *Id.*

6. **Claim 7** – “*the device messaging agent on at least one of the wireless end-user devices further to initiate the respective secure Internet data message link to the transport services stack.*”

Claim 7 depends from claim 1. As discussed above, a laptop, smartphone, or other wireless device communicating with a server would inherently have a link between its device messaging agent and a transport services stack on the server. Malek Decl. at ¶ 63. *Rittmaster* indicates that such a link could be made secure using various layers of encryption (discussed above in relation to claim elements 1[a] and 1[b] and claims 2-3), and that such a secure link may be initiated by the user device (and thus the device messaging agent on the user device). *Id.* Specifically, *Rittmaster* explains, “the user may send a request for content, products or services, over the network, for example, the Internet, (100 in FIG. 8) and the provider processor may then receive the request over the network (102 in FIG. 9).” *Id.*; Ex. C, ¶ 94. The request may be initiated by a user, for example in attempting to access a web page or otherwise request information, and that the user’s request may “include (or be accompanied by) the assigned user code. *Id.* The request would inherently be transmitted from a software application (“agent”) on the user device to initiate and/or maintain a link to a server, as would be recognized by a PHOSITA. Malek Decl. at ¶ 63.

7. **Claim 9** – “*one of the message delivery triggers is the expiration of a periodic timer.*”

Claim 9 depends from claim 1. This additional element is disclosed in *Rittmaster*, which explains that prohibition or allowance of a transmission of a message may be based on recurring events, such as a time, day, week, etc. Malek Decl. at ¶ 64. For example, *Rittmaster* discloses that “the user device 14-16 is controlled by software 26-28 to periodically (or otherwise successively) communicate location and/or time information generated by the associated positioning system 20-22 during a communication interchange between the provider server 12 and the user device.” *Id.*; Ex. C, ¶ 69; *see also*, ¶ 70. These periodic transmissions of location and/or time information are trigger events, as described above in connection with the discussion of “triggers” in relation to claim elements 1[e] and 1[f]. Malek Decl. at ¶ 64.

8. **Claim 11** – “*one of the message delivery triggers is the receipt of a transmission on the respective secure message link from the device link agent of the given one of the wireless end-user devices, or a response generated to a transmission received from that device link agent.*”

Claim 11 depends from claim 1, and requires that a request from a user device, or a response to such a request, at least in part causes the release of a buffered message from the server. Malek Decl. at ¶ 66. Such a trigger is disclosed in *Rittmaster*, because at least one condition for transferring data from the network to users through the server is the user requesting a product or service. *Id.*; see, e.g., Ex. C, ¶¶ 8-9. *Rittmaster* expressly discloses that the process of providing content in response to a trigger is first initiated by a request from an end-user device. Malek Decl. at ¶ 66; Ex. C, ¶¶ 74-76, Fig. 6.

9. **Claim 12** – “*the transmission is a heartbeat message generated by the given device link agent, or a request received from the given device link agent.*”

Claim 12 depends from claim 11. The term “heartbeat” is (and was, at the relevant time) known by a PHOSITA to mean that the user device periodically sends a message to the server, such as “pinging” the server with specific information with respect to a request. Malek Decl. at ¶ 67. For instance, the ’192 Patent indicates that the heartbeat messages can be agent information messages, agent check-in messages, or agent cross-check messages. Ex. A, 39:44-47, 40:1-3. *Rittmaster* discloses such a periodic communication. In one preferred embodiment, “the user device 14-16 is controlled by software 26-28 to periodically (or otherwise successively) communicate location and/or time information generated by the associated positioning system 20-22 during a communication interchange between the provider server 12 and the user device.” *Id.*; Ex. C, ¶ 69. This is done to provide the provider server with “multiple location and/or time information packets over the course of a communication interchange... to monitor the user device’s location (or region).” *Id.* These multiple, periodic requests issued from the user device constitute a heartbeat message that triggers delivery of content from the server to the user device. Malek Decl. at ¶ 67.

10. **Claim 13** – “*one of the message delivery triggers is the receipt of a particular network element message from one of the network elements.*”

Claim 13 depends from claim 1. Receipt of information from a network element acts as a trigger in embodiments of *Rittmaster* in which the server obtains information from network elements and then sends such information to user devices. Malek Decl. at ¶ 68. For example,

turning back to the advertising embodiment introduced above in relation to claim element 1[e], advertisers may communicate advertisement information to the provider server 12 from “suitable computers 138 and 140 coupled to the network 18.” *Id.*; Ex. C, ¶ 121. Here, “the provider processor operates with an associated memory device on which advertisement or other display content is stored, for communication to the recipient processors for displaying at appropriate times.” *Id.*

After the messages are stored (buffered), further instructions from network elements to the server constitute triggers for releasing messages to users. For instance, *Rittmaster* discloses that each advertiser “may modify, add or delete advertisement information” by communicating such instructions from the advertiser’s computer (*i.e.*, network element) to the provider server. Malek Decl. at ¶ 68; Ex. C, ¶ 124. Furthermore, “[i]n preferred embodiments, each advertiser may control the general time at which the advertiser’s message will be displayed, for example, by communicating instructions to the provider processor 12 (or directly to the recipient processor 120) from the advertiser’s computer 138 or 140.” *Id.* When such instructions are communicated through a website, the advertiser may request content to be displayed immediately on selected devices. *Id.* This indicates that the provider server receives a message from a network element (a device or website associated with the advertiser), which triggers the message (content) to be sent to user devices. *Id.*

II. Claim 14 — “one of the message delivery triggers is based on an amount of wireless network data usage consumed by the given one of the wireless end-user devices.”

Claim 14 depends from claim 1 and requires that one of the message delivery triggers is based on an amount of wireless network data usage consumed by the given one of the wireless end-user devices. *Rittmaster* discloses this element, explaining that users may be charged for access to requested content and that user access to such content may be limited based on usage:

The content provider may charge subscribing users a fee for allowing access to requested content. Such a fee may allow unlimited access for a period of time (for example a day, month, year, etc.) or may be calculated on a per-use basis (wherein the subscriber is charged for each viewing or playing of the content). The content provider may maintain a record of subscriber charges, for example, associating each subscriber’s usage charge with the subscribers identification information and/or user code. In one embodiment, the content provider maintains an account record for pre-paid amounts received by subscribers, for example, in a table in which pre-paid amounts are associated with subscriber information, such as user code. In this manner, as part of the request processing carried out by the content provider, the content provider may determine whether the user making the request has enough

funds in the corresponding user account to cover the fees for the requested content.

Malek Decl. at ¶ 69; Ex. C, ¶ 114. This access limitation adds an additional trigger to those already discussed above, such that a user requesting information from network elements will only receive this content if the network elements confirm that the user's data usage is within allowed limits. *Id.*

12. Claim 15

a. 15[PRE] *“A method of operating a message link server, comprising:”*

The preamble of independent claim 15 recites a **“method of operating a message link server”** comprising a series of steps. Claim 15 is substantively similar to claim 1, except that it is framed as a series of steps rather than elements of a server configured to carry out those steps. Malek Decl. at ¶ 70. As discussed above, *Rittmaster* discloses a server for providing message content to linked user devices, and as such it also discloses the steps performed by such a server. *Id.* As further discussed above in connection with claim 1, *Rittmaster* discloses a provider server 12 that “comprises an Internet product or service provider computer or server ... coupled for communication” to “a plurality of network enabled user devices” *Id.*; Ex. C, ¶ 42. Various methods of operating this server in order to deliver message content obtained from providers to one or more of a plurality of end-user devices are explained in detail throughout the *Rittmaster* reference.

b. 15[a] *“maintaining a respective secure message link through an Internet network between the message link server and a respective device link agent on each of a plurality of wireless end-user devices, each of the wireless end-user devices comprising multiple software components authorized to receive and process data from secure message link messages received via a device link agent on that device;”*

Rittmaster discloses element 15[a] of the '192 Patent. As discussed above relative to claim element 1[a], *Rittmaster* discloses that its server 12 “comprises an Internet product or service provider computer or server ...” coupled through the internet 18 for communication to “a plurality of network enabled user devices” (Ex. C, ¶ 42), and further that such communications network “may comprise any suitable means which allows the recipient processors and the provider processor to communicate with each other, including, but not limited to, the Internet or WWW, intranet, cable or other hard-wired networks, optical, electromagnetic or other wireless networks, as well as hybrids thereof, or the like.” Malek Decl. at ¶ 71; Ex. C, ¶ 32. Use of a “secure message link,” maintained by a “transport services stack” on the server and “device link agents” on the

various end-user devices (such as cellular phones or laptops), is inherent for at least the reasons discussed above relative to claim element 1[a]. Malek Decl. at ¶ 71; *see also, id.* at ¶ 52.

- c. 15[b] *“receiving network element messages from a plurality of network elements, the received network element messages comprising respective message content and requests for delivery of the respective message content to respective wireless end-user devices, the respective message content including data for, and an identification of, a respective one of the authorized software components;”*

Rittmaster further discloses element 15[b] of the '192 Patent. Malek Decl. at ¶ 72. *Rittmaster* specifies that in some instances “the recipient processors comprise online user terminals, including, but not limited to conventional personal computers (PCs), portable communication devices (such as portable telephones, personal digital assistants, or other portable information units), or vehicle-mounted computers connected to a wide area network, such as, but not limited to, the Internet.” Malek Decl. at ¶ 72; Ex. C, ¶ 35. A PHOSITA in the relevant time period would readily recognize that these types of devices each have one or more software applications, with each application having a port number to associate the specific application with a virtual location on the device. Malek Decl. at ¶ 72. Since *Rittmaster* discloses that the server receives information from various provider computers to be directed to end-user devices, it is inherent that messages received from network elements would have “an identification of” the recipient authorized software component along with the message content (e.g., an image or video content requested by the end-user device). *Id.*; *see also, id.* at ¶ 53.

- d. 15[c] *“buffering content from the received network element messages for which delivery is requested to a given one of the wireless end-user devices;”*

Rittmaster clearly identifies buffering that prevents transmission of messages to user devices until a determination is made by logic or “rule sets” that the user device is authorized to receive the message, such as by virtue of being located in a specific geographic region. Malek Decl. at ¶ 73. As discussed above, in connection with claim element 1[d], *Rittmaster* discloses that content is not provided by the server until a determination is made, using a set of rules or logic, that one or more specific end-user devices are authorized to receive the message, such as by virtue of being located in a specific geographic region. *Id.*; *see also, id.* at ¶ 55. And in some embodiments, *Rittmaster* explains that a plurality of other triggers can be present, stating that “if a recipient processor provides geographic information corresponding to a first geographic location

or region, then the provider processor may be controlled to not provide selective information to the recipient processor, unless further requirements are met.” *Id.*; Ex. C, ¶ 40.

- e.** 15[d] “*determining when one of a plurality of message delivery triggers for the given one of the wireless end-user devices has occurred, wherein for at least some of the received network element messages, the receipt of such a message is not a message delivery trigger, and for at least one of the message delivery triggers, the trigger is an occurrence of an asynchronous event with time-critical messaging needs; and*”

Rittmaster further discloses element 15[d], because providing content to an end-user device is dependent on one or more triggers. Malek Decl. at ¶ 74; *see also id.* at ¶ 57. Providing content to an end-user device is dependent on one or more triggers in *Rittmaster* that qualify as *asynchronous events with time-critical messaging needs*, as discussed in great detail above in connection with claim element 1[e]. *Id.* For instance, content might be provided upon user request or when the user is determined to be within a certain proximity to a content provider’s establishment. A plurality of other triggers also may be implemented, and “the provider processor [server] may be controlled to not provide selective information to the recipient processor [end-user device], unless further criteria is met” such as “minimum user age, a particular period of the day, week, month or year, or other suitable criteria.” *Id.*; Ex. C, ¶ 14.

- f.** 15[e] “*upon determining that one of the message delivery triggers has occurred, supplying one or more messages comprising the buffered content for delivery on the secure message link maintained between the message link server and a device link agent on the given one of the wireless end-user devices.*”

Finally, *Rittmaster* discloses element 15[e] of claim 15. Simply by communicating through an internet connection, as in *Rittmaster*, message content would be transmitted through a link between a stack on a server and a software agent on one of a plurality of end-user devices, as discussed in greater detail with respect to claim element 1[f] above. Malek Decl. at ¶ 75; *see also, id.* at ¶ 58. The *Rittmaster* system is specifically designed to deliver messages from the server to an end-user device in response to determining that a trigger has occurred, such as by the end-user device entering a specific geographic region. *Id.* at ¶ 75. By sending the message upon occurrence of a trigger after storing it at the server level, as discussed above, the message is by definition buffered. *Id.*

D. Ground 2: The Combination of Rittmaster and Knowledge of a PHOSITA (as Evidenced by *Distributed Systems* and/or *Computer Networks* Textbooks) Render Obvious Claims 1-3, 5-7 and 9-15

To the extent one might argue that protocol-level details such as a “transport services stack” or “device link agent” are not strictly inherent, they would have been extremely obvious because they were basic features of network servers communicating over the internet as of the time of the alleged invention. *Rittmaster* explicitly acknowledges that protocol-level or software-level details are unnecessary because they would be readily understood by those skilled in the art, stating that “[s]uch computers and communication interfacing are well known in the art and are not described in further detail herein for purposes of simplifying the present disclosure.” Ex. C, ¶ 42. This is both a direct acknowledgement that missing protocol-level details would have been obvious and an invitation to combine *Rittmaster*’s disclosure with background knowledge of a PHOSITA and well-known network structure and protocols. As discussed further below, *Rittmaster*’s above explicit teaching, suggestion, and motivation to use well-known knowledge and skill in the art would have led a PHOSITA to combine *Rittmaster* with basic network communication details such as those discussed in widely-available prior art textbooks.

I. Claim 1

a. 1[PRE] “A message link server comprising:”

As discussed above, the preamble of claim 1 is anticipated by *Rittmaster* because the provider server 12 “comprises an Internet product or service provider computer or server ... coupled for communication” to “a plurality of network enabled user devices.” *See supra* Section II.C.1.a.; Malek Decl. at ¶ 51; Ex. C, ¶ 42.

b. 1[a] “a transport services stack to maintain a respective secure message link through an Internet network between the message link server and a respective device link agent on each of a plurality of wireless end-user devices,”

Rittmaster discloses claim element 1[a] for the reasons described above. *See supra* Section II.C.1.b.; Malek Decl. at ¶ 52. To the extent, however, that specific protocols for sending or receiving messages are determined to be missing from *Rittmaster*, it would have been obvious to employ Transport Layer Security level (TLS) protocols that were not only well-known, but also common at the relevant time, to maintain a secure link between the server and a plurality of user

devices. Malek Decl. at ¶ 52. This is especially true in view of *Rittmaster*'s invitation to use "communication interfacing" that was "well known in the art." Malek Decl. at ¶ 52; Ex. C, ¶ 42.

In addition, to the extent *Rittmaster* fails to explicitly state that the secure link exists between a "transport services stack" on the server and a "message link agent" on the mobile devices, a PHOSITA would have easily recognized that communication over the internet as in *Rittmaster* inherently (necessarily) involved a link between a stack on the server and a software program on the mobile devices. *See supra* Section II.C.1.b.; Malek Decl. at ¶ 52. And, even if a "secure" message link through an internet network between the message link server and a respective device link agent were considered to be not inherent in *Rittmaster*, incorporating such a link in *Rittmaster* would have involved nothing more than combining known elements using known elements to yield predictable results. In fact, such a secure link was so well-known at the time of the alleged invention that it was literally textbook knowledge, as shown by the *Distributed Systems* textbook (Ex. E).⁷ *Distributed Systems* was a widely used textbook in the computer science curricula of many universities at the relevant time, and outlined basic requirements for network systems. Malek Decl. at ¶ 52. The *Distributed Systems* textbook explains the importance of maintaining a secure communication link between server and client devices on the internet. *See Distributed Systems* at p. 584; Malek Decl. at ¶ 52. *Distributed Systems* notes that "[t]he predominant approach for setting up a secure channel in the Web is to use the Secure Socket Layer (SSL)" and that "[a]lthough SSL has never been formally standardized, **most Web clients and servers nevertheless support it.**" *Id.* (emphasis added). *Distributed Systems* also noted at the time that an update to SSL had formally laid down standards published by the Internet Engineering Task Force (IETF), and this update is now referred to as the Transport Layer Security (TLS) protocol that includes the security layers shown below in the server's "internet protocol stack" as shown in the textbook:

⁷ Andrew S. Tanenbaum and Maarten Van Steen, *Distributed Systems: Principles and Paradigms*. Second Edition (2007). Pearson Education, 2007, available at https://vowi.fsinf.at/images/b/bc/TU_Wien-Verteilte_Systeme_VO_%28Göschka%29_-_Tannenbaum-distributed_systems_principles_and_paradigms_2nd_edition.pdf.

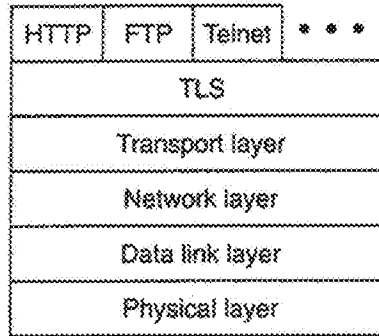


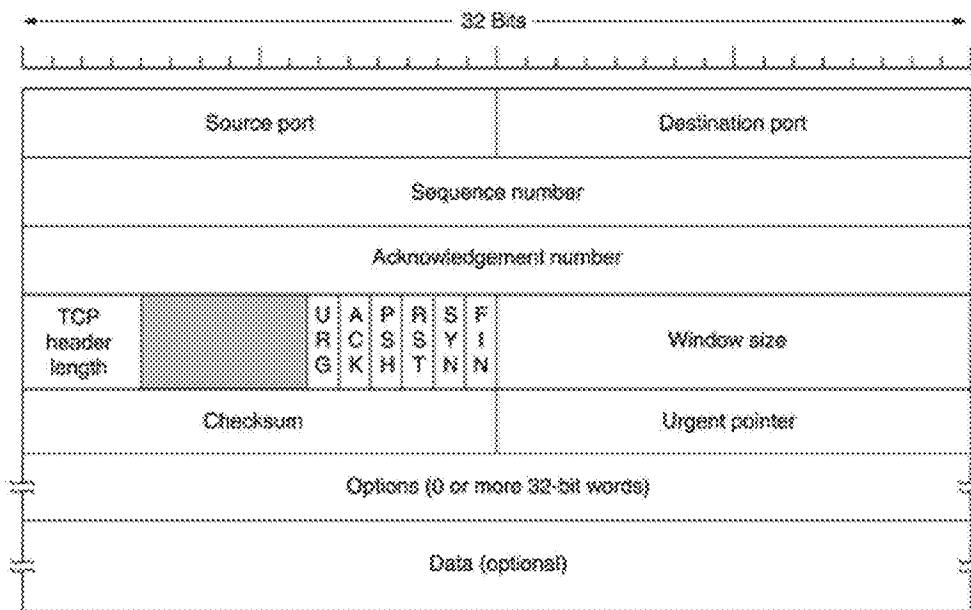
Figure 12-22. The position of TLS in the Internet protocol stack.

Ex. E at p. 584; Malek Decl. at ¶ 52. A PHOSITA would have known that either the widely used SSL protocol or the standardized TLS protocol would have been used to maintain a secure communication link between the above server stack and a software program on client devices. Malek Decl. at ¶ 52. The *Distributed Systems* textbook also explains that “TLS (and SSL) implementations are usually based on TCP,” which a PHOSITA would have understood to refer to “Transmission Control Protocol” that was, and still is, the standard transport-layer protocol used for exchanging data and messages on the internet. *Id.* A PHOSITA would have found it extremely obvious to employ the foregoing protocols to maintain a secure connection between a network stack and a mobile device link agent because having such a secure connection was standard and broadly recognized as superior to an unsecured connection. *Id.* In fact, it would have been unusual not to have a secure connection to a network at the time of the invention. *Id.*

- c. 1[b] “each of the wireless end-user devices comprising multiple software components authorized to receive and process data from secure message link messages received via a device link agent on that device;”

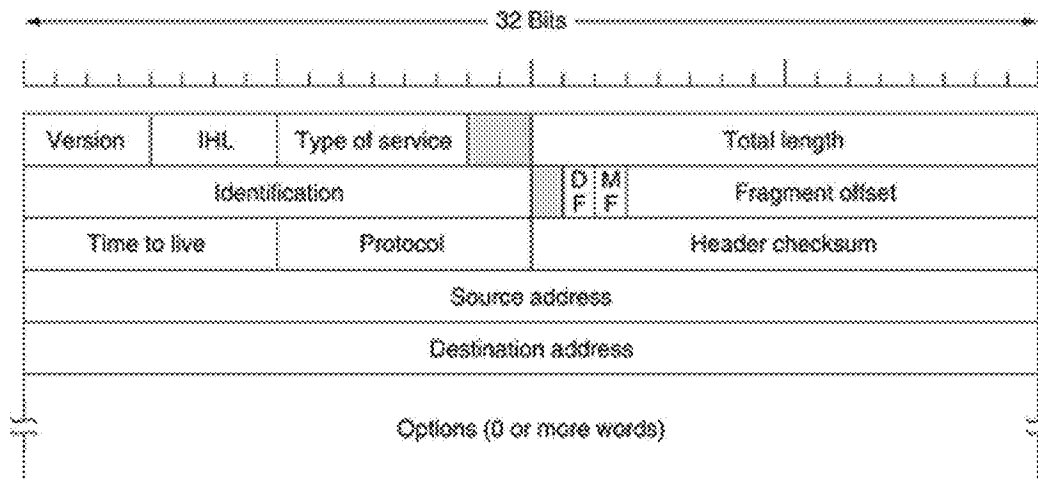
Rittmaster also discloses element 1[b]. See *supra* Section II.C.1.c. For instance, *Rittmaster* discloses that a plurality of personal computers (PCs), portable communication devices (telephones, PDAs, etc.), or vehicle-mounted computers may be connected to a wide area network such as the internet. *Id.*; Ex. C, ¶ 35; Malek Decl. at ¶ 53. A PHOSITA would have readily recognized that these types of devices each inherently included a plurality of software applications each associated with a port number to identify a virtual location on the device associated with that specific application. Malek Decl. at ¶ 53. However, to the extent that *Rittmaster* alone is not considered to anticipate element 1[b], employing end-user devices with multiple software

applications that process data from secure messages received via a device link agent on that device would have been obvious in view of common background knowledge known to a PHOSITA, as shown by *Computer Networks* (Ex. F)⁸, a widely used textbook at the time of the alleged invention. *Id.* *Computer Networks* explains that when a process on a device establishes a TCP connection with a remote process it attaches itself to an unused TCP port on its own machine, which identifies where to send incoming packets belonging to this connection. *See* Ex. F at p. 340; Malek Decl. at ¶ 53. The process also supplies a destination port to tell who to give the packets to on the remote side. *Id.* Each outgoing TCP message contains both a source port and a destination port, serving to identify the processes using the connection on both ends. *Id.* The standard TCP message format shown below for transmitting data on the internet includes both a source port number and a destination port number.



Ex. F at p. 410; Malek Decl. at ¶ 53. A PHOSITA would have also been familiar with the structure of standard IP packets used for transmitting data on the internet, as shown below. *See* Ex. F at pp. 329-330, Malek Decl. at ¶ 53.

⁸ Andrew S. Tanenbaum, *Computer Networks*, Fourth Edition, Pearson Education, 2003, <https://theswisschocolate.ch/pdf/Gentoomen%20Library/Networking/Prentice%20Hall%20-%20Computer%20Networks%20Tanenbaum%204ed.pdf>



A PHOSITA thus would have known that messages could be sent from a network to multiple applications (software components) on an end-user device by identifying the appropriate port number in messages so that the messages are routed appropriately by a software program (device link agent) on the end-user device. *Id.*

- d. 1[c] “an interface to a network to receive network element messages from a plurality of network elements, the received network element messages comprising respective message content and requests for delivery of the respective message content to respective wireless end-user devices, the respective message content including data for, and an identification of, a respective one of the authorized software components,”

Rittmaster discloses element 1[c]. See *supra* Section II.C.1.d. This element requires that the network-facing side of the server include an “interface” to receive messages from two or more “network elements,” and that the messages include “message content” and “requests for delivery” of that content to specific end-user devices by including data for, and an identification of, authorized software. Malek Decl. at ¶ 54. This does little more than describe the basic manner in which all messages were delivered from a network including multiple computers at the relevant time (January 2008), and how messages are still delivered today. *Id.* Nevertheless, *Rittmaster* explicitly discloses that “[t]he provider processor 12 is capable of providing information from any suitable source (including, but not limited to an on-line source. . .),” thus disclosing a plurality of potential “network elements” from which the server may obtain messages through an interface. Malek Decl. at ¶ 54; Ex. C, ¶ 33. *Rittmaster* further discloses that the messages from network elements may include, for instance, “promotional or advertisement information for a plurality of

different establishments within the same shopping area” and that “the owner of each of these establishments may have communicated advertisement information to the provider processor 12, from suitable computers 138 and 140 coupled to the network 18.” Ex. C, ¶¶ 120-21 (emphasis added); Malek Decl. at ¶ 54. Further, “the establishment’s processor 138 or 140 may be programmed to automatically communicate a signal to the provider processor 12 to cause a specified piece of content to be displayed on one or more selected display devices 122 and 128. Ex. C, ¶ 125; Malek Decl. at ¶ 54. *Rittmaster*’s advertising information (data) from computers associated with the shopping establishments (network elements) would necessarily include a port number to identify the authorized recipient software for which the advertisements are intended. “In this manner, the content provider 12 may control the distribution of advertisement information for a plurality of establishments to a particular recipient processor (or a plurality of particular recipient processors and associated display devices), based on the geographic location of the establishments and the recipient processor.” Ex. C, ¶ 123.

Furthermore, *Rittmaster*’s advertising information (data) from computers associated with the shopping establishments (network elements) would necessarily include a port number to identify the authorized recipient software for which the advertisements are intended. Malek Decl. at ¶ 54. In fact, *Rittmaster* explicitly states that “the content provider 12 may control the distribution of advertisement information for a plurality of establishments to a particular recipient processor (or a plurality of particular recipient processors and associated display devices), based on the geographic location of the establishments and the recipient processor.” *Id.*; Ex. C, ¶ 123. In other words, *Rittmaster*’s system requires the messages to be targeted to specific users, which would require addressing information regarding end-user devices and applications on those devices able to process the messages. *See* Malek Decl. at ¶ 54. Even if *Rittmaster* were considered not to expressly or inherently disclose the elements of 1[d], a PHOSITA would have recognized that it would have been extremely obvious to implement standard message formats for communication with servers over the internet at the relevant time, which would have included those features. For instance, a PHOSITA would have known based on baseline textbook knowledge that “[e]ach outgoing TCP message contains both a source port and a destination port” and that “together, these ports serve to identify the processes using the connection on both ends.” (emphasis added) *See* Malek Decl. at ¶ 54; Ex. F at p. 340. It would have been obvious to implement such features in the messages of *Rittmaster* because that is simply how communications

over networks worked at the time of the invention (and still work now), and also because *Rittmaster* invited those skilled in the art to look to known devices and techniques to carry out aspects of the invention not fully described by stating that its “computers and communication interfacing are well known in the art and are not described in further detail herein for purposes of simplifying the present disclosure.” Ex. C, ¶ 42; Malek Decl. at ¶ 52.

- e. 1[d] “a message buffer system including a memory and logic, the memory to buffer content from the received network element messages for which delivery is requested to a given one of the wireless end-user devices,”

Rittmaster discloses element 1[d] for the reasons discussed above. See *supra* Section II.C.1.e. *Rittmaster* clearly discloses a buffer system that prevents transmission of messages to end-user devices until a determination is made, using a set of rules or logic, that one or more specific end-user devices are authorized to receive the message, such as by virtue of being located in a specific geographic region. Malek Decl. at ¶ 56. For instance, Fig. 2 shows that there is a Storage Device 13 (*i.e.*, memory) associated with the Server 12 in which messages may be stored prior to sending them to end-user devices. Ex. C, ¶¶ 33 and 163; Malek Decl. at ¶ 56. *Rittmaster* discloses logic by stating that “a set of rules may be implemented, which depend upon the geographic information (and, thus, the geographic location or region of the recipient processor), such that ... if a recipient processor provides geographic information corresponding to a first geographic location or region, then the provider processor may be controlled to not provide selective information to the recipient processor, unless further requirements are met.” Malek Decl. at ¶ 56; Ex. C, ¶ 40. *Rittmaster* specifically mentions that in preferred embodiments the logic of the server determines in what region a particular one of a plurality of end-user devices is located, stating that “geographic information is communicated from the first user device to the server 12 and the determination of the region in which the user device is located is performed at the provider server. . . .” Malek Decl. at ¶ 56; Ex. C, ¶ 53. For instance, “if the region X is determined in step 34 to be within a non-restricted region, then the user device 14 may be provided access to the product or service (step 38).” Malek Decl. at ¶ 56; Ex. C, ¶ 56. In such a scenario, “the server 12 downloads to the user device 14, software files, programs, data, decode keys, or other information that defines the requested product or service or that are necessary for the user to obtain the requested product or service.” *Id.*

In other words, *Rittmaster* discloses buffering content from the other on-line sources (*i.e.*, network elements) because the server (processor 12) receives and stores that information until logic determines user location. Malek Decl. at ¶ 56. In one example of buffering, *Rittmaster* discloses that advertisements from different establishments may be “communicated to the content provider 12 and stored in advance” and that “the provider processor operates with an associated memory device on which advertisement or other display content is stored, for communication to the recipient processors for displaying at appropriate times.” Malek Decl. at ¶ 56; Ex. C, ¶¶ 120-21. In another example, *Rittmaster* expressly discloses that “the provider processor maintains a listing or inventory of advertisements” that can be provided to a recipient processor. Malek Decl. at ¶ 56; Ex. C, ¶ 134. To the extent that one could possibly consider *Rittmaster* not to expressly disclose a “buffer,” a PHOSITA would have found this to be an extremely obvious design choice given the presence of a server memory. Malek Decl. at ¶ 56. Buffers and buffering content were a well-known concept in the context of data exchange, and it was textbook knowledge at the time that when an application sends data to TCP, there were two choices: “TCP may send it immediately or **buffer it** (in order to collect a larger amount to send at once), at its discretion.” (emphasis added) Malek Decl. at ¶ 56; Ex. F at p. 408.

Furthermore, as demonstrated in the immediately foregoing Section II.D.1.d., the purpose of a buffer is to buffer content. *Rittmaster* specifically discloses that content such as advertisements from network elements (*e.g.*, different computers from various establishments in a shopping area) may be “communicated to the content provider 12 and stored in advance” on the server, and that the server stores this content “for communication to the recipient processors for displaying at appropriate times.” Malek Decl. at ¶ 56; Ex. C, ¶¶ 120-21. To the extent that one could possibly consider *Rittmaster* not to expressly disclose “buffering” the provided content during the time that logic determines whether or not it should be sent through to an end user, a PHOSITA would have found the step of buffering the content to be an extremely obvious design choice given the presence of a server memory and the fact that buffering content was not only well-known, but was a more convenient choice for the end user (recipient) than waiting to retrieve the message content from network elements until after logic has made a determination regarding whether to send a message to a user. Malek Decl. at ¶ 56.

A PHOSITA also would have found it obvious to buffer content because buffering was a well-known concept in the context of data exchange using the standard TCP protocol on the

internet. For example, it was well-known at the time that when a sender “application passes data to TCP, TCP may send it immediately or **buffer it** (in order to collect a larger amount to send at once), at its discretion.” (emphasis added) *See* Ex. F at p. 408. In addition to the sender buffering data, it was well-known at the time that TCP required the receiver to buffer incoming data *Id.* at p. 416.

f. 1[e] “the logic to determine when one of a plurality of message delivery triggers for the given one of the wireless end-user devices has occurred, wherein for at least some of the received network element messages, the receipt of such a message by the message buffer system is not a message delivery trigger, and for at least one of the message delivery triggers, the trigger is an occurrence of an asynchronous event with time-critical messaging needs, and”

Rittmaster discloses element 1[g] for the reasons discussed above. *See supra* Section II.C.1.h.; *see also* Malek Decl. at ¶¶ 56-57. For instance, *Rittmaster* discloses logic for determining when triggers have occurred by stating that “a set of rules may be implemented, which depend upon the geographic information (and, thus, the geographic location or region of the recipient processor), such that ... if a recipient processor provides geographic information corresponding to a first geographic location or region, then the provider processor may be controlled to not provide selective information to the recipient processor, unless further requirements are met.” Malek Decl. at ¶ 56; Ex. C, ¶ 40. Those additional conditions being met would trigger sending of messages from the server that were previously received from network elements and stored in the server’s buffer system. In other instances, determination of location alone is a trigger such that “if the region X is determined in step 34 to be within a non-restricted region, then the user device 14 may be provided access to the product or service (step 38).” Malek Decl. at ¶ 56; Ex. C, ¶ 56. In such a scenario, “the server 12 downloads to the user device 14, software files, programs, data, decode keys, or other information that defines the requested product or service or that are necessary for the user to obtain the requested product or service.” Malek Decl. at ¶ 56; Ex. C, ¶ 56.

While *Rittmaster* primarily discusses geographic location, additional triggers are contemplated. For instance, “the provider processor [server] may be controlled to not provide selective information to the recipient processor [end-user device], unless further criteria is met” such as “minimum user age, a particular period of the day, week, month or year, or other suitable

criteria.” Malek Decl. at ¶ 57; Ex. C, ¶ 14. Alternatively, inputting of geographic coordinates may act as a trigger or a user request may trigger the release of content. Ex. C, ¶¶ 51 - 54.

Thus, a plurality of triggers exist that could each result in sending content to user-devices, for instance (1) determination that the user device is in an unrestricted zone and (2) determining that the user is in a restricted zone but also detecting a trigger such as meeting minimum age requirements.

These triggers are clearly not receipt of the message by the buffer system. These types of triggers also are an “asynchronous event with time-critical messaging needs” because the request and responsive providing of content are asynchronous (*i.e.*, do not occur at the same time) and the response is time-critical (*i.e.*, is provided in response to a trigger rather than residing on the network server indefinitely).⁹ Malek Decl. at ¶ 57. Further reinforcing the time-criticality of its triggers, *Rittmaster* discloses logic that determines whether a recipient request (*i.e.*, trigger) was received **within a required time period**, which a PHOSITA would understand to be a trigger with “time-critical messaging needs.” Malek Decl. at ¶ 57; Ex. C, ¶¶ 62-67; *see also* ¶ 130. Indeed, *Rittmaster* considers the time information so critical in this embodiment that *Rittmaster* suggests encrypting the time information. Malek Decl. at ¶ 57; Ex. C, ¶ 66.

- g.* 1[f] *“upon determining that one of the message delivery triggers has occurred, the logic further to supply one or more messages comprising the buffered content to the transport services stack for delivery on the secure message link maintained between the transport services stack and a device link agent on the given one of the wireless end-user devices.”*

⁹ This is consistent with how the patent owner appears to have interpreted the term, because the ’192 Patent confirms that “asynchronous events with time-critical messaging needs” are, for example, a “transaction or service billing event or a user request.” Malek Decl. at ¶ 57; Ex. A, 38:59-63. In litigation with Samsung, the patent owner did not attribute any particular meaning to the term during claim construction. Ex. G (Claim Construction Order, 2:23-cv-00103 Dkt. 118 (E.D. Tex.)). Even more striking, Samsung pointed out during prior *Inter Partes* Review of the ’192 Patent that the patent owner directly admitted that a message retrieval request is a message delivery trigger and did not deny, given the opportunity, that such a basic request is “an asynchronous event with time-critical messaging needs.” Malek Decl. at ¶ 57; Ex. H (Samsung Reply Brief in IPR2024-00010, Paper 16 at p. 4); *see also* Malek Decl. at ¶ 57; Ex. I (PO Response Brief in IPR2024-00010, Paper 12) and Malek Decl. at ¶ 57; Ex. J (PO Sur-Reply Brief in IPR2024-00010, Paper 19) where patent owner failed to challenge the meaning of “asynchronous event with time-critical messaging needs” in the ’192 Patent.

Rittmaster discloses element 1[f] for the reasons discussed above. *See supra* Section II.C.1.g.; *see also* Malek Decl. at ¶ 58. As discussed above relative to element 1[f], messages are sent when the logic determines that one of multiple triggers has been satisfied. Simply by communicating through a secured internet connection as in *Rittmaster*, message content would be transmitted through a link between a stack on a server and a software agent on one of a plurality of end-user devices. *See supra* Section II.C.1.b.

2. **Claim 2** – “*an encrypt function to encrypt the one or more messages supplied to the transport services stack for delivery on the secure message link maintained between the message link server and the device link agent on the given one of the wireless end-user devices.*”

Claim 2 depends from claim 1. *Rittmaster* discloses this additional element for the reasons discussed above. *See supra* Section II.C.2. *Rittmaster* contemplates encryption of content from network elements prior to transmission of the encrypted content from the network server to one or more of the plurality of end-user devices. Malek Decl. at ¶ 59; Ex. C Fig. 9. *Rittmaster* further discloses that the provider processor (server) may “encrypt the content with an encryption algorithm or technique for which the expected user location is part of the decryption key or decryption processes used to decrypt the content” and “may also employ the user code (and user identification or recipient processor identification information) as part of the decryption key or decryption process” before “encrypted content is communicated to the recipient processor over the network (108 in FIG. 9).” Malek Decl. at ¶ 59; Ex. C, ¶¶ 97-98.

3. **Claim 3** – “*the encrypted one or more messages are transported to the device link agent on the given one of the wireless end-user devices using one or more of encryption on the transport services stack, IP (Internet Protocol) layer encryption, and tunneling.*”

Claim 3 is also disclosed by *Rittmaster*. *See supra* Section II.C.3.; Malek Decl. at ¶ 60. Communications in *Rittmaster* would have utilized TLS, which creates an encrypted channel at the transport layer (*i.e.*, TCP) and by definition has encryption on the transport services stack. *Rittmaster* expressly describes using one or more keys to encrypt content, which would at a minimum necessarily include the payload of the message to be sent by the server. Malek Decl. at ¶ 60; Ex. C, ¶¶ 97-98. These keys, for instance, could be derived from location information and/or a user code. *Id.* Further, the '192 Patent explains that encryption may be performed at or below the transport services stack “with IPSEC or another IP layer encryption, VPN or tunneling scheme.” Malek Decl. at ¶ 60; Ex. A, 89:26-29. As discussed above relative to element 1[a], the *Distributed*

Systems textbook explains that “[t]he predominant approach for setting up a secure channel in the Web is to use the Secure Socket Layer (SSL),” which was updated as Transport Layer Security (TLS) protocol that includes the security layers in the server’s “internet protocol stack.” Ex. E p. 584; Malek Decl. at ¶ 52.

At a minimum this was extremely well-known to any PHOSITA, and an obvious option that would be easily implemented in response to a clear motivation to further increase security. *Computer Networks* evidences that these layers of encryption were baseline knowledge to a PHOSITA at the relevant time, and the textbook describes IPsec (IP security), a popular secure communication protocol operating at the IP layer, just like the ’192 Patent does. Malek Decl. at ¶ 60; Ex. F at pp. 596-599. A PHOSITA would also have known that in tunnel mode, IPsec encrypts and protects the entire original IP packet and then encapsulates it within a new IP packet for transmission. *Id.* Most Virtual Private Networks (VPNs) at the relevant time (and today) relied on IPsec tunneling for creating the secure communication channels, and thus it would have been obvious to implement in *Rittmaster* even if not necessarily present. *See* Malek Decl. at ¶ 60; Ex. F at pp. 602-603.

4. **Claim 5** – “*wherein the transport services stack is further to receive, over each of the respective secure message links, upload messages forwarded by the respective device link agents from at least a subset of the device software components, each of the upload messages identifying a corresponding one of the network elements to which the device respective software component has requested delivery, the network server system using the interface to a network to deliver content from the upload messages to the respective identified network elements.*”

Claim 5 depends from claim 1. *Rittmaster* discloses this additional element as discussed above. *See supra* Section II.C.5.; Malek Decl. at ¶ 61. For instance, *Rittmaster* discloses providing a user code from a user device and then the provider processor (server) also providing the user code as part of a request for content from network elements. Malek Decl. at ¶ 61; Ex. C, ¶¶ 96-97. Additionally, some embodiments in *Rittmaster* allow “the selection of commercial, promotional, or informational content” to “be determined ... by the physical location of the user.” Ex. C, ¶ 132; Malek Decl. at ¶ 61. Thus, identifying information about the user device is provided in order to request content from a network source. The user can also communicate their advertising preferences to the network. Ex. C, ¶ 142; Malek Decl. at ¶ 61. In embodiments where geographic location information is transmitted by end-user devices and the network server provides that

information to the content provider, the claimed “upload message” also would be present. Malek Decl. at ¶ 61.

5. **Claim 6 – “wherein at least one of the one or more messages for delivery by the transport services stack comprises multiple identifier/data pairs.”**

Claim 6 depends from claim 1. To the extent that the added element of this claim indicates that a single message contains two or more payloads, each with its own separate identifier, it is either disclosed in *Rittmaster* (see *supra* Section II.C.5.), or obvious in view of *Rittmaster*. In discussing an embodiment where a user located in a shopping area may receive content that includes information from multiple network elements (e.g., multiple store computers within the shopping area), *Rittmaster* states that “the first content provided to the recipient processor 120 for display on the display device 122 comprises information, such as promotional or advertisement information for a plurality of different establishments within the same shopping area.” Malek Decl. at ¶ 62; Ex. C, ¶ 120. If this information was collected at the server for distribution to users, it would have been sent in a single message, or at a minimum it would have been obvious to “piggy-back” two or more pieces of provider content for delivery to a single user in view of *Rittmaster*’s statement that “for example, the **first content** may include advertisement information for a bakery 134 **and further** advertisement information for a hobby shop 136 located within the same shopping area as the recipient processor 120 and display device 122.” Malek Decl. at ¶ 62, Ex. C, ¶ 120. Piggybacking was a well-known and routine option for reducing the number of messages sent, as shown by the *Distributed Systems* textbook. Malek Decl. at ¶ 62; Ex. E at p. 344. A PHOSITA would understand that two independent data elements (e.g., advertisements), each having a data payload and identifier, could be assembled into a single message in order to allow for better handling of a high number of messages. Malek Decl. at ¶ 62.

6. **Claim 7 – “the device messaging agent on at least one of the wireless end-user devices further to initiate the respective secure Internet data message link to the transport services stack.”**

Claim 7 depends from claim 1. A laptop or smartphone communicating with a server would inherently have a link between a device messaging agent of the laptop/smartphone and a transport services stack on the server. Malek Decl. at ¶ 63; see also *supra* Section II.C.1.b. *Rittmaster* indicates that such a link could be initiated by the user device (and thus the device messaging agent on the user device) by stating that “[o]nce a user has registered with the content provider and has received or has been assigned a user code, the user may send a request for content, products or

services, over the network, for example, the Internet, (100 in FIG. 8) and the provider processor may then receive the request over the network (102 in FIG. 9).” Malek Decl. at ¶ 63; Ex. C, ¶ 94. *Rittmaster* specifies that “[i]n an Internet embodiment, the request may be initiated over the Internet by a user, for example, attempting to access a web page, attempting to access a link on a web page, submitting request or order information, or the like” and that “[t]he user request may include (or be accompanied by) a user code assigned to the user making the request, as described above.” *Id.* Such a request would inherently come from a software application (“agent”) on the device that serves the purpose of initiating/maintaining a link to a server, as would be recognized by a PHOSITA. Malek Decl. at ¶ 63. At a minimum, it would have been obvious for a device messaging agent on an end-user devices to initiate a secure link to the transport services stack of a server because the link would be initiated either by the messaging software on the user device or by the protocol stack of the server, and either of those two options would have been obvious.

7. **Claim 9 – “one of the message delivery triggers is the expiration of a periodic timer.”**

Claim 9 depends from claim 1. This additional element is disclosed in *Rittmaster*, as explained in Section II.C.7., *supra*. *Rittmaster* discloses prohibition or allowance of transmission of messages based on recurring events such as time, day, week, etc. Malek Decl. at ¶¶ 64, 74, 82. As one example, *Rittmaster* discloses that “the user device 14-16 is controlled by software 26-28 to periodically (or otherwise successively) communicate location and/or time information generated by the associated positioning system 20-22 during a communication interchange between the provider server 12 and the user device.” Malek Decl. at ¶ 64; Ex. C, ¶ 69; *see also* ¶ 70. These periodic transmissions of location and/or time are trigger events. Malek Decl. at ¶ 64.

8. **Claim 10 – “the period of the timer is fractionally shorter than a maximum data message interval beyond which the secure message link is taken down.”**

Claim 10 depends from claim 9 and adds that messages are designed to be sent shortly before a link to the server is terminated. Malek Decl. at ¶ 65. This would have been obvious in view of *Rittmaster* because a PHOSITA at the relevant time would have known that causing a connection to a server to “time out” was common to maintain security of the network, and ensuring that messages that are delayed to be sent at a specific hour, day, or week, etc., would need to be sent prior to the timeout of the connection. *Id.* Thus, when *Rittmaster* discloses that “the user device 14-16 is controlled by software 26-28 to periodically (or otherwise successively)

communicate location and/or time information generated by the associated positioning system 20-22 during a communication interchange between the provider server 12 and the user device”, a PHOSITA would find it obvious as common sense to send such periodic messages prior to the closing of the link. *Id.*; Ex. C, ¶ 69; *see also*, ¶ 70. Otherwise, the location and/or time information would not be transmitted.

9. **Claim 11** – “*one of the message delivery triggers is the receipt of a transmission on the respective secure message link from the device link agent of the given one of the wireless end-user devices, or a response generated to a transmission received from that device link agent.*”

Claim 11 depends from claim 1. Malek Decl. at ¶ 66. As discussed in Section II.C.9, *supra*, this is disclosed in *Rittmaster* because at least one condition for transferring data from the network to users through the server is the user requesting a product or service. *See, e.g.*, Malek Decl. at ¶ 66; Ex. C, ¶¶ 8-9. *Rittmaster* expressly discloses that the process of providing content in response to a trigger is first initiated by a request from an end-user device. Malek Decl. at ¶ 66; Ex. C, ¶¶ 74-76 and Fig. 6.

10. **Claim 12** – “*the transmission is a heartbeat message generated by the given device link agent, or a request received from the given device link agent.*”

Claim 12 depends from claim 11. Malek Decl. at ¶ 67. As discussed in Section II.C.9., *supra*, *Rittmaster* discloses this added element by stating that “the user device 14-16 is controlled by software 26-28 to periodically (or otherwise successively) communicate location and/or time information generated by the associated positioning system 20-22 during a communication interchange between the provider server 12 and the user device” so that “the provider server is provided with multiple location and/or time information packets over the course of a communication interchange, to continue to monitor the user device’s location (or region) and reported time, thus, to allow the provider server a greater confidence that the user device is located at the location or region that corresponds to the location information during the time of the communication interchange.” Malek Decl. at ¶ 67; Ex. C, ¶ 69.

11. **Claim 13** – “*one of the message delivery triggers is the receipt of a particular network element message from one of the network elements.*”

Claim 13 depends from claim 1, and its added element is disclosed by *Rittmaster* for the reasons discussed in Section II.C.10., *supra*. *See also* Malek Decl. at ¶ 68. For instance, in *Rittmaster* “the provider processor operates with an associated memory device on which

advertisement or other display content is stored, for communication to the recipient processors for displaying at appropriate times.” Malek Decl. at ¶ 68; Ex. C, ¶ 121. Then, “each advertiser may control the general time at which the advertiser’s message will be displayed, for example, by communicating instructions to the provider processor 12 (or directly to the recipient processor 120) from the advertiser’s computer 138 or 140.” Malek Decl. at ¶ 68; Ex. C, ¶ 124. These instructions from the advertiser computer (network element) trigger sending of a message stored at the server. See Malek Decl. at ¶ 68. In some embodiments of *Rittmaster* “the establishment’s processor 138 or 140 [network element] may be programmed to automatically communicate a signal to the provider processor 12 [server] to cause a specified piece of content to be displayed on one or more selected display devices 122 and 128 [end-user devices].” Ex. C, ¶ 125.

12. Claim 14 – “one of the message delivery triggers is based on an amount of wireless network data usage consumed by the given one of the wireless end-user devices.”

Claim 14 depends from claim 1 and adds that at least one trigger is based on network usage of a given wireless end-user device. As discussed in Section II.C.11., *supra*, *Rittmaster* discloses this element by stating that users may be charged for access to requested content and that user access to such content may be limited based on usage. Malek Decl. at ¶ 69; Ex. C, ¶ 114. This limitation on access provides an additional trigger to those discussed above, so that a user requesting information from network elements will only receive this content if the network elements confirm that the user’s data usage is within allowed limits. To the extent that the added subject matter of claim 14 could be considered not disclosed expressly or inherently by *Rittmaster*, the above would have at least suggested to a PHOSITA to make delivery of content to a specific user device dependent on how much (or how little) data is being used by that specific device.

13. Claim 15

a. 15[PRE], 15[a] “A method of operating a message link server, comprising: maintaining a respective secure message link through an Internet network between the message link server and a respective device link agent on each of a plurality of wireless end-user devices,”

Claim 15 is substantively very similar to claim 1 discussed at II.D.1. above except that it is framed as a series of steps rather than elements of a server configured to carry out those steps. This element in particular is the same as the function recited in element 1[a] of claim 1 without requiring the “transport services stack” that performs that function, and therefore would have been

obvious for the same reasons discussed above at Section II.D.1.b. *See also* Malek Decl. at ¶¶ 52 and 70-71.

- b.** 15[a] *“each of the wireless end-user devices comprising multiple software components authorized to receive and process data from secure message link messages received via a device link agent on that device;”*

This element of claim 15 is identical to element 1[b] of claim 1 and is therefore rendered obvious for the same reasons discussed above at Section II.D.1.c. *See also* Malek Decl. at ¶¶ 53, 71.

- c.** 15[b] *“receiving network element messages from a plurality of network elements, the received network element messages comprising respective message content and requests for delivery of the respective message content to respective wireless end-user devices, the respective message content including data for, and an identification of, a respective one of the authorized software components;”*

This element is the same as the function recited in element 1[c] of claim 1 without explicitly requiring the “interface” to a network that performs that function and is therefore rendered obvious for the same reasons discussed above at Section II.D.1.d. *See also* Malek Decl. at ¶¶ 54, 72.

- d.** 15[c] *“buffering content from the received network element messages for which delivery is requested to a given one of the wireless end-user devices;”*

This element is the same as the function of element 1[d] of claim 1 except that it does not require the “memory” that performs that function and is therefore rendered obvious for the same reasons discussed above at Section II.D.1.e. *See also* Malek Decl. at ¶¶ 55-56, 73.

- e.** 15[d] *“determining when one of a plurality of message delivery triggers for the given one of the wireless end-user devices has occurred, wherein for at least some of the received network element messages, the receipt of such a message is not a message delivery trigger, and for at least one of the message delivery triggers, the trigger is an occurrence of an asynchronous event with time-critical messaging needs; and”*

This element is the same as the function of element 1[e] of claim 1 except that it does not require the “logic” that performs that function and is therefore rendered obvious for the same reasons discussed above at Section II.D.1.f. *See also* Malek Decl. at ¶¶ 57, 74.

- f. 15[e] “upon determining that one of the message delivery triggers has occurred, supplying one or more messages comprising the buffered content for delivery on the secure message link maintained between the message link server and a device link agent on the given one of the wireless end-user devices.”*

This element is the same as the functions of element 1[f] of claim 1 except that it does not require the “logic” or “transport services stack” that perform those functions and is therefore rendered obvious for the same reasons discussed above at Section II.D.1.g. *See also* Malek Decl. at ¶¶ 58, 75.

E. Ground 3: The Combination of *Rittmaster* and *Shenfield* and/or Knowledge of a PHOSITA (as Evidenced by *Distributed Systems* and/or *Computer Networks*) Render Obvious Claims 1-3, 5-7, and 9-15

To the extent *Rittmaster* is considered not to disclose all of the elements of claim 1 explicitly or inherently, any missing elements would have been obvious in view of AU 2007200530 to Shenfield, et al. (hereinafter, “*Shenfield*” (Ex. U)). Malek Decl. at ¶ 103. *Shenfield* was filed on February 7, 2007, and published September 6, 2007, more than one year prior to earliest claimed priority for the ’192 Patent. *Id.*; Ex. U, Cover. As discussed above, *Rittmaster* describes networks having all of the functional aspects of claim 1 but does not explicitly describe certain software-level details. *Shenfield* discloses networks similar to those of *Rittmaster* in which a plurality of network elements communicate with a plurality of mobile user devices over the internet. Malek Decl. at ¶ 103; Ex. U, Fig. 1.

Furthermore, like *Rittmaster*, *Shenfield* discloses storing messages from content providers at the server for distribution to user devices at a later time (*e.g.*, at a specific time), or when the user devices are in range (*i.e.*, within a specified area). *Id.* It would have been obvious to implement the device-level and software-level details of *Shenfield* in a network according to *Rittmaster* using routine skill in order to build a functional network. Malek Decl. at ¶ 103. This would require nothing more than a predictable use of known elements, or, at most, use of known techniques to improve similar devices. *Id.* In fact, *Rittmaster*’s statement that “[t]he communications network may comprise any suitable means which allows the recipient processors and the provider processor to communicate with each other, including, but not limited to, the Internet or WWW, intranet, cable or other hard-wired networks, optical, electromagnetic or other wireless networks, as well as hybrids thereof, or the like” (Ex. C, ¶ 32) is an explicit teaching, suggestion, and motivation to

combine *Rittmaster* with other prior art server networks like *Shenfield* in order to fill in any details not explicitly disclosed. *Id.*

1. Claim 1

a. 1[PRE] “A message link server comprising:”

The preamble of claim 1 is disclosed by *Rittmaster* because the provider server 12 “comprises an Internet product or service provider computer or server ... coupled for communication” to “a plurality of network enabled user devices.” *See supra* Section II.C.1.a.; Malek Decl. at ¶ 51; Ex. C, ¶ 42. *Shenfield*, like *Rittmaster* and the ’192 patent, discloses a server (Proxy Server 26) linking a plurality of network elements (Data Network 22 including content provider servers 24) to a plurality of wireless end-user devices (including mobile device 14) through an the internet (Access Network 18 that is connected to the Data Network 22). Ex. U, Abstract and Fig. 1; Malek Decl. at ¶¶ 104-105.

b. 1[a] “a transport services stack to maintain a respective secure message link through an Internet network between the message link server and a respective device link agent on each of a plurality of wireless end-user devices,”

Rittmaster discloses claim element 1[a] for the reasons described above. *See supra* Section II.C.1.b.; Malek Decl. at ¶ 52. Briefly, *Rittmaster* discloses that server 12 “comprises an Internet product or service provider computer or server” coupled for “communication” to “a plurality of network enabled user devices.” Ex. C, ¶ 42; Malek Decl. at ¶ 106. To the extent *Rittmaster* is considered not to disclose details of how its server maintains links to end-user devices, based on its disclosure that “[s]uch computers and communication interfacing are well known in the art and are not described in further detail herein for purposes of simplifying the present disclosure” (Ex. C, ¶ 42) a PHOSITA would have known that common messaging protocols of the time, such as those disclosed in *Shenfield*, could be implemented in *Rittmaster* to make a functional network. *Id.*

Shenfield discloses a “delivery queue 55” and “push handler” 56 for communicating messages from a server to a communication layer 84 of one or more mobile stations, as shown below:

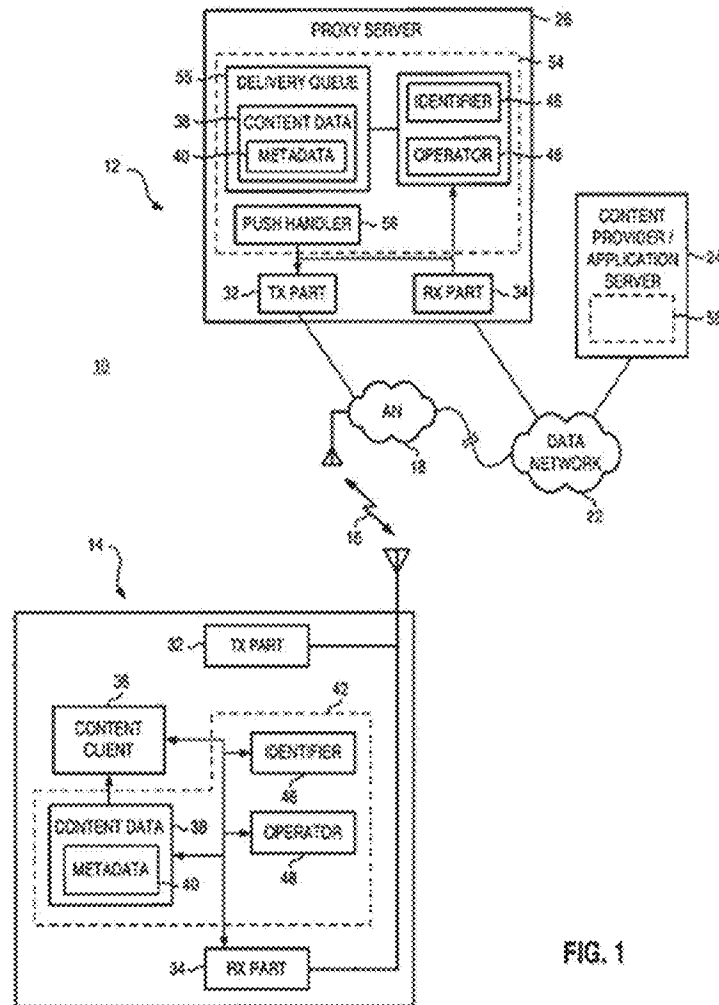


FIG. 1

Ex. U, Fig. 1. The server is capable of determining when similar messages are maintained in the delivery queue and which one of those similar messages has the most up-to-date content, which are typically the most recent notifications. *Id.* ¶44. The appropriate message is then communicated to the mobile station, and more particularly to the communication layer 84 of the mobile station, as illustrated below in Fig. 2:

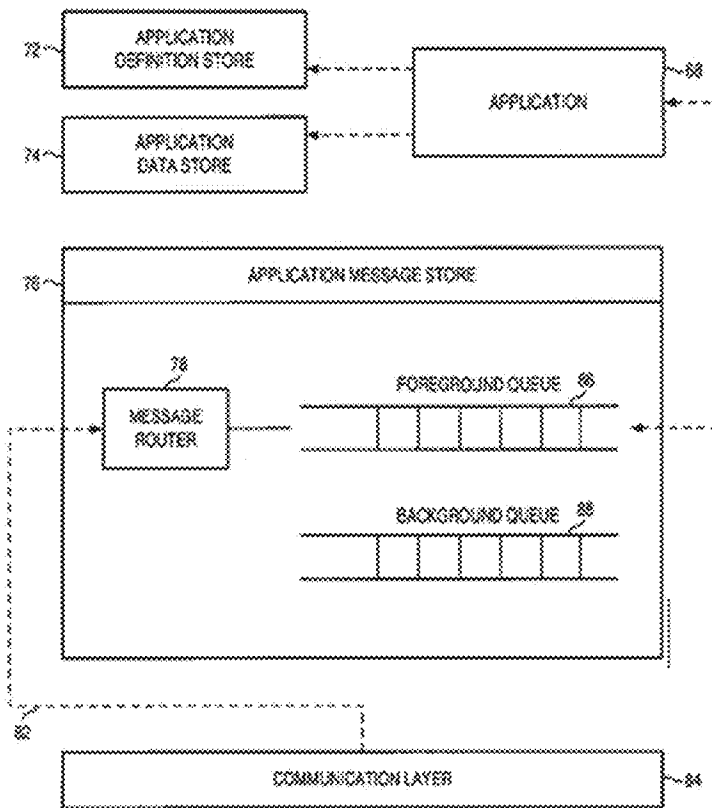


FIG. 2

Ex. U, Fig. 2; Malek Decl. at ¶ 106-107. The communication layer 84 of each mobile device receives messages sent from the queue/push handler of the server, for distribution to the message store 76 of the appropriate application on the mobile device based on the incoming message's application identification. Ex. U, ¶ 69; Malek Decl. at ¶ 106. This is therefore a device link agent as described by the '192 patent. *Shenfield* notes that a link is maintained between the server and end-user devices, stating that "the link defined upon a radio air interface between the mobile station and the wireless network is susceptible to severance" and that "[w]hen the link is severed, the delivery of content is suspended until the link is restored." *Id.* ¶ 47; Malek Decl. at ¶ 106. If *Rittmaster* and *Shenfield* are not considered to have rendered this element obvious, a PHOSITA would have found it quite obvious to incorporate a stack in view of the *Distributed Systems* textbook for the reasons discussed above. *See supra* Section II.D.1.b.; Malek Decl. at ¶ 52.

- c. 1[b] *“each of the wireless end-user devices comprising multiple software components authorized to receive and process data from secure message link messages received via a device link agent on that device;”*

To the extent that *Rittmaster* is considered not to disclose details such as multiple software components on each end-user device authorized to receive and process data from a secure message link or a device link agent on end-user devices for receiving messages from a secure link, it would have been obvious to implement those features based on *Shenfield*, which discloses that “[t]he proxy server 26 interacts with ... mobile stations, such as the mobile station 14, and the applications resident thereat.” Ex. U, ¶ 36 (emphasis added); Malek Decl. at ¶ 107. These multiple applications may all be associated with the same processor or have their own processor. Ex. U, ¶ 71; Malek Decl. at ¶ 107. *Shenfield* refers to each application as a content client 36, representative of an application, an application environment, or, generically, a push agent that consumes content pushed to the mobile station.” Ex. U, ¶ 34; Malek Decl. at ¶ 107. A simple illustration of a mobile station is shown in Fig. 1 of *Shenfield*, as discussed above, including a single example of a content client application. Further, as discussed above in relation to Fig. 2, the communication layer 84 of the communication device 14 “uses the application identification to place the message in the appropriate message store 76 [of the content client],” making it clear that each content client (application) is authorized to receive and process information delivered from the communication layer (device link agent). Id. ¶ 69; Malek Decl. at ¶ 107. A PHOSITA would have had a clear motivation to implement protocol-level details of *Shenfield* in *Rittmaster* to create a functional system, also advantageously combining *Shenfield*’s system of queuing messages and updating/modifying them so that users of *Rittmaster*’s system do not receive outdated advertisements or other content. Malek Decl. at ¶ 107.

- d. 1[c] *“an interface to a network to receive network element messages from a plurality of network elements, the received network element messages comprising respective message content and requests for delivery of the respective message content to respective wireless end-user devices, the respective message content including data for, and an identification of, a respective one of the authorized software components”*

This element requires that the network-facing side of the server include an “interface” to receive messages from two or more “network elements.” The messages include both “message content” and “requests for delivery” of that content to specific end-user devices by including data

for, and an identification of, authorized software. As previously discussed, *Rittmaster* discloses network element messages from a plurality of network elements, such as advertisements from multiple providers connected to the server through the internet. *See supra* Section II.C.1.d. *Shenfield* likewise discloses a proxy server 26 that interfaces with and receives messages from an application server 24 for delivery to mobile devices. Malek Decl. at ¶ 108. *Shenfield* contemplates multiple content provider computers/servers (network elements) interfacing with the proxy server, noting that “[t]he data network here forms a packet data network, such as the internet, and **communication devices**, such as the application server 24 that contains, or generates, content, and shall, at times, herein be referred to as a ‘content provider.’” Ex. U, ¶ 32 (emphasis added) (see also ¶ 36, stating that “proxy server 26 interacts with external content **providers**” (emphasis added)); Malek Decl. at ¶ 108. *Shenfield* specifically discloses that the messages from the content provider/application server can be targeted to a specific mobile station, such as where the content provider targets users based on a subscription and sends messages to subscribers through the proxy server, stating that “[t]he content provider embodied at, or forming, the application server 24 offers dynamic content, e.g., a push-enabled XML web service, and supports content subscription by, or on behalf of, an end-user of the mobile station 14. When content is to be communicated to a mobile station, the content provider sends the content to the proxy server 26 that, in turn, delivers the content using a notification mechanism.” Ex. U, ¶ 35; Malek Decl. at ¶ 108.

At a minimum, both *Rittmaster* and *Shenfield* disclose transmitting message data from network elements to a server and ultimately to user devices, and it would have been obvious to include destination information targeting a specific application on a specific mobile device in the message transmitted from the content provider to the server. Malek Decl. at ¶ 108. *Shenfield* specifically notes that messages received by the user device include information regarding the destination application so that the user device may route the message appropriately. Ex. U, ¶ 69; Malek Decl. at ¶ 108. This information could be provided either at the content provider server 24 or appended to the message at the proxy server level. Malek Decl. at ¶ 108. Given that the content provider would have information regarding subscribers and their registered devices, it would have been obvious to include target device and application information in the message sent from the content provider. *Id.*

- e. 1[d] “a message buffer system including a memory and logic, the memory to buffer content from the received network element

messages for which delivery is requested to a given one of the wireless end-user devices”

Rittmaster discloses element 1[d] including a message buffer system including memory and logic for reasons discussed above. *See supra* Section II.C.1.e. For instance, *Rittmaster* states that “a set of rules may be implemented, which depend upon the geographic information (and, thus, the geographic location or region of the recipient processor), such that ... if a recipient processor provides geographic information corresponding to a first geographic location or region, then the provider processor may be controlled to not provide selective information to the recipient processor, unless further requirements are met.” Ex. C, ¶ 40; Malek Decl. at ¶ 109. This results in messages being buffered and stored in memory at the server until a trigger is satisfied. Likewise, *Shenfield* specifically mentions a delivery queue in its proxy server and temporary storage of content. Ex. U, ¶¶ 36, 40; Malek Decl. at ¶ 109. *Shenfield*’s proxy server includes a delivery queue 55, indicating that it has a memory to hold messages. *Id.* “In operation, the proxy server further mediates subscription and notification work flows between the content provider and the mobile station” and can provide “scheduled delivery, temporary storage of content when a mobile station is out of communication range, broadcast services, group subscriptions, and other services,” indicating that the server also contains logic for determining when messages should be sent to mobile devices. Ex. U, ¶ 36; Malek Decl. at ¶ 109. It would have been obvious to implement the features of *Shenfield* into the buffer of *Rittmaster* in order to avoid delivering outdated content.

f. 1[e] *“the logic to determine when one of a plurality of message delivery triggers for the given one of the wireless end-user devices has occurred, wherein for at least some of the received network element messages, the receipt of such a message by the message buffer system is not a message delivery trigger, and for at least one of the message delivery triggers, the trigger is an occurrence of an asynchronous event with time-critical messaging needs, and”*

As discussed above, *Rittmaster* discloses element 1[e] at least because it discloses that providing content to an end-user device is dependent on one or more triggers. *See supra* Section II.C.1.f. *Rittmaster* primarily discusses geographic location as a trigger but also contemplates that “the provider processor [server] may be controlled to not provide selective information to the recipient processor [end-user device], unless further criteria is met” such as “minimum user age, a particular period of the day, week, month or year, or other suitable criteria.” *See supra* Section II.C.1.f.; Ex. C, ¶ 14; Malek Decl. at ¶ 110. Alternatively, inputting of geographic coordinates may

act as a trigger or a user request may trigger the release of content. Ex. C, ¶¶ 51 - 54. Thus, *Rittmaster* discloses a plurality of triggers that could each result in sending content to user-devices, for instance either a determination that the user device is in an unrestricted zone or a determination that the user is in a restricted zone but also detecting a trigger such as meeting minimum age requirements. *Shenfield*'s similar system of delaying messages as determined by certain rules (triggers) such as geographic location (communication range) and updating of message content would have been obvious to combine with *Rittmaster*. Ex. U, ¶¶ 26 and 36; Malek Decl. at ¶ 110. *Shenfield* further discloses that message delivery from the proxy server may be in the form of "push" messages (initiated by the content provider or another party other than the user) or "request-response" messages initiated by user request. Ex. U, ¶ 4; Malek Decl. at ¶ 110. These messages are two different triggers that cause messages to be released from a buffer (queue). Malek Decl. at ¶ 110. "Triggering of the content push is triggered asynchronously, e.g., by a content provider, by a device client, or by a third party," indicating multiple possible triggers for push content. Ex. U, ¶ 6; Malek Decl. at ¶ 110. "Additionally, the push event is sometimes also performed as the result of a data broadcast to a selected group of client devices." *Id.* *Shenfield* also identifies other triggers that can lead to release of messages from a queue as determined by the server, such as timing ("scheduled delivery") and location ("temporary storage of content when a mobile station is out of communication range"). *Id.* Because both *Rittmaster* and *Shenfield* disclose providing content to subscribers in response to a user request, on a scheduled basis, and/or dependent on geographic location, it would have been obvious to combine *Shenfield* with *Rittmaster* to implement *Shenfield*'s queuing system in *Rittmaster* to avoid delivery of duplicated or updated content accumulated while messages are buffered and awaiting a trigger to be satisfied.

- g.** 1[f] *"upon determining that one of the message delivery triggers has occurred, the logic further to supply one or more messages comprising the buffered content to the transport services stack for delivery on the secure message link maintained between the transport services stack and a device link agent on the given one of the wireless end-user devices."*

Finally, as discussed above, *Rittmaster* and *Shenfield* each discuss transmission of messages through a link between a stack on a server and a software agent on one of a plurality of end-user devices by the mere fact that the messages are sent through the internet. *See supra* Sections II.C.1 g., II.C.1 b., II.E.1.b.; Malek Decl. at ¶ 111. *Rittmaster* is designed to deliver messages from the server to the end-user device in response to determining that a trigger has

occurred, like when the end-user device enters a specific geographic region, as discussed in detail above. Malek Decl. at ¶ 111. *Shenfield*'s triggers satisfy this element for essentially the same reasons, timing the release of messages according to specific rules and sending the messages from the push manager of the server to the message layer of mobile devices, as discussed above. *Id.*

2. **Claim 2** — “*an encrypt function to encrypt the one or more messages supplied to the transport services stack for delivery on the secure message link maintained between the message link server and the device link agent on the given one of the wireless end-user devices*”

The added elements of claim 2 are explicitly disclosed in *Rittmaster* for reasons discussed above and therefore would be present in a combination of *Rittmaster* and *Shenfield*. See *supra* Section II.C.2. For instance, *Rittmaster* contemplates encryption of content from network elements prior to transmission of encrypted content from the network server to one or more of the plurality of user devices, for instance as shown in Fig. 9. Ex. C, Fig. 9; Malek Decl. at ¶ 112. *Rittmaster* explains that after receiving appropriate location information and, optionally, a user code or other information used to determine whether a particular user should be given access to specific content from the network, “[t]he provider processor may then encrypt the content with an encryption algorithm or technique for which the expected user location is part of the decryption key or decryption processes used to decrypt the content.” Ex. C, ¶¶ 97-98; Malek Decl. at ¶ 112. The provider processor “may also employ the user code (and user identification or recipient processor identification information) as part of the decryption key or decryption process” before “encrypted content is communicated to the recipient processor over the network (108 in FIG. 9).” *Id.* It would have been obvious to utilize such encryption in any combination of *Rittmaster* and *Shenfield* in order to provide security to communications. Malek Decl. at ¶ 112.

3. **Claim 3** — “*the encrypted one or more messages are transported to the device link agent on the given one of the wireless end-user devices using one or more of encryption on the transport services stack, IP (Internet Protocol) layer encryption, and tunneling.*”

The added elements of claim 2 are disclosed in *Rittmaster* and/or obvious in view of *Rittmaster* and basic knowledge of a PHOSITA for reasons discussed above and therefore would be present in a combination of *Rittmaster* and *Shenfield*. See *supra* Section II.C.3 and II.D.3. The '192 Patent explains that encryption may be performed at or below the transport services stack “with IPSEC or another IP layer encryption, VPN or tunneling scheme.” Ex. A, 89:26-29. These were well-known and common encryption techniques prior to the critical date of the '192 Patent,

so much so that they were discussed in detail in college-level textbooks at the relevant time. *See supra* Section II.D.3. To the extent that there is any doubt that *Rittmaster* discloses these types of encryption, it would have been extremely obvious to implement the claimed forms of encryption in order to provide security to messages sent to and from the server of *Rittmaster* and a plurality of end-user mobile devices. Malek Decl. at ¶ 113.

4. **Claim 5** – “*wherein the transport services stack is further to receive, over each of the respective secure message links, upload messages forwarded by the respective device link agents from at least a subset of the device software components, each of the upload messages identifying a corresponding one of the network elements to which the device respective software component has requested delivery, the network server system using the interface to a network to deliver content from the upload messages to the respective identified network elements.*”

The added elements of claim 2 are explicitly disclosed in *Rittmaster* for reasons discussed above and therefore would be present in a combination of *Rittmaster* and *Shenfield*. *See supra* Section II.C.4 *Rittmaster* discloses that “[d]epending upon the process and system embodiment employed, the user may or may not be prompted (or the user computer may or may not be controlled) to communicate user location information to the content provider, over the network” and that “the user may be prompted (or the user computer may be controlled) to communicate user code information to the content provider, over the network.” *See supra* Section II.C.4; Ex. C, ¶ 113; Malek Decl. at ¶ 115. Thus, not only does *Rittmaster*’s network server provide content to user devices, but the server may also deliver “upload messages” from specific software on a user device to a specified network element, such as by sending a user code to a specific network element when content is requested from that element. Malek Decl. at ¶ 115. Likewise, *Shenfield* provides content based on a user request. Ex. U, ¶ 4; Malek Decl. at ¶ 115. *Shenfield* also discloses that its described methods of communication to a mobile device can be reversed to allow communication from a mobile device to servers through the proxy server. Ex. U, ¶ 31; Malek Decl. at ¶ 115. Both scenarios involve identifying the relevant content provider from which content is requested. Malek Decl. at ¶ 115. Thus, it would have been obvious based on these disclosures to allow messages to be uploaded to the server from user devices in order to identify network elements from which messages are to be sent to one or more end-user devices. *Id.*

5. **Claim 6** – “*wherein at least one of the one or more messages for delivery by the transport services stack comprises multiple identifier/data pairs.*”

Claim 6 recites that, in addition to the elements of claim 1, two or more payloads, each having an identifier, may be sent in a single message. *Rittmaster* describes this added element for the reasons discussed above in Section II.C.5. *See also* Malek Decl. at ¶ 116. Alternatively, this claim is obvious in view of the combination of *Rittmaster* and *Shenfield*, for the reasons discussed below in Ground 6.

6. **Claim 7** – “*the device messaging agent on at least one of the wireless end-user devices further to initiate the respective secure Internet data message link to the transport services stack.*”

As noted above in Section II.D.6., a laptop or smartphone communicating with a server would inherently have a link between a device messaging agent of the laptop/smartphone and a transport services stack on the server. *Rittmaster*’s end-user devices could initiate such a link, and the link could be made secure by using various layers of encryption, as discussed above. Malek Decl. at ¶ 117. *Shenfield* likewise notes that a link is maintained between the server and end-user devices, stating that “the link defined upon a radio air interface between the mobile station and the wireless network is susceptible to severance” and that “[w]hen the link is severed, the delivery of content is suspended until the link is restored.” Ex. U, ¶ 47; Malek Decl. at ¶ 117. Given that the link is between mobile devices on the one hand and a server on the other, there are two options as to which device initiates a connection: mobile devices or the server. Therefore, having the mobile devices initiate links to the server would have been obvious as one of only two options. Malek Decl. at ¶ 117.

7. **Claim 9** – “*one of the message delivery triggers is the expiration of a periodic timer.*”

This added element is disclosed in *Rittmaster*, as discussed above in Section II.C.7., and therefore would have been obvious. *Rittmaster* explains that prohibition or allowance of transmission of messages may be based on recurring events such as time, day, week, and the like. Malek Decl. at ¶ 119. As one example, *Rittmaster* discloses that a “provider processor [server] may be controlled to not provide selective information to the recipient processor, unless further criteria is met” and that “further criteria may include, but is not limited to, ... a particular period of the day, week, month or year, or other suitable criteria.” Ex. C, ¶ 14; Malek Decl. at ¶ 119.

8. **Claim 10** – “*the period of the timer is fractionally shorter than a maximum data message interval beyond which the secure message link is taken down.*”

Claim 10 depends from claim 9 and further requires that messages are designed to be sent shortly before the link to the server is terminated. This would have been obvious in view of *Rittmaster* for the reasons discussed above in Section II.D.8. *See also* Malek Decl. at ¶¶ 65 and 120.

9. **Claim 11** – “*one of the message delivery triggers is the receipt of a transmission on the respective secure message link from the device link agent of the given one of the wireless end-user devices, or a response generated to a transmission received from that device link agent.*”

Claim 11 recites that, in addition to the elements of claim 1, that either a request from a user device, or a response to such a request, causes the release of a buffered message from the server, at least in part. Malek Decl. at ¶ 121. This is disclosed in *Rittmaster* for the reasons discussed above in Section II.C.8., including that at least one potential condition for transferring data from the network to users through the server is the user requesting a product or service. *See, e.g.,* Ex. C, ¶¶ 8-9; *see also supra* Section II.D.8.; Malek Decl. at ¶ 121.

10. **Claim 12** – “*the transmission is a heartbeat message generated by the given device link agent, or a request received from the given device link agent.*”

Claim 12 depends from claim 11 and further recites that the transmission received from the device link agent of the end-user device is a “heartbeat message” generated by the given device link agent. As discussed above, the device link agent is the software program responsible for receiving and transmitting messages from other applications on the end-user device. As noted above in Section II.D.10., a PHOSITA would have recognized that *Rittmaster* discloses this claim limitation at least because, in one preferred embodiment “the user device 14-16 is controlled by software 26-28 to periodically (or otherwise successively) communicate location and/or time information generated by the associated positioning system 20-22 during a communication interchange between the provider server 12 and the user device” so that “the provider server is provided with multiple location and/or time information packets over the course of a communication interchange, to continue to monitor the user device’s location (or region) and reported time, thus, to allow the provider server a greater confidence that the user device is located at the location or region that corresponds to the location information during the time of the communication interchange.” Ex. C, ¶ 69; Malek Decl. at ¶ 122. Receipt of these multiple periodic requests issued from the server constitutes a heartbeat message that acts a trigger to cause delivery of content from the server to the user device issuing the heartbeat messages, thus rendering claim 12 obvious in view of *Rittmaster*. Malek Decl. at ¶ 122.

11. Claim 13 – “one of the message delivery triggers is the receipt of a particular network element message from one of the network elements.”

Claim 13 recites that, in addition to the elements of claim 1, one of the message delivery triggers is receipt of a particular network element message from one of the network elements, which is shown in *Rittmaster*. See *supra* Sections II.C.10, II.D.11. Receipt of information from a network element (e.g., provider computer) is necessary for embodiments of *Rittmaster* in which the server obtains information from network elements and then sends such information to user devices. *Id.* Additionally, further instructions from network elements to the server may constitute triggers for releasing messages to users. Malek Decl. at ¶ 123. For instance, *Rittmaster* discloses that “each advertiser [network element] may modify, add or delete advertisement information, for example, from the advertiser’s computer 134 and 136, by communicating suitable instructions to the provider processor 12,” and that “[i]n preferred embodiments, each advertiser may control the general time at which the advertiser’s message will be displayed, for example, by communicating instructions to the provider processor 12 (or directly to the recipient processor 120) from the advertiser’s computer 138 or 140.” Ex. C, ¶ 124; Malek Decl. at ¶ 123. Likewise, *Shenfield* discloses that push messages to users can be triggered by the content provider. Ex. U, ¶ 6; Malek Decl. at ¶ 122. In view of these disclosures, it would have been obvious to include one of the triggers to be the receipt of a specific message from one of the network elements so that the network elements (e.g., advertiser computers) can control when new messages (e.g., new offers or advertisements) are sent to users. Malek Decl. at ¶ 122.

12. Claim 14 – “one of the message delivery triggers is based on an amount of wireless network data usage consumed by the given one of the wireless end-user devices.”

Claim 14 recites that, in addition to the elements of claim 1 at least one trigger is based on network usage of a given wireless end-user device. *Rittmaster* describes this added element for the reasons discussed above in Sections II.C.11., II.D.12. See also Malek Decl. at ¶ 124. Alternatively, this claim is obvious in further view of *Gellens*, for the reasons discussed below in Ground 8.

13. Claim 15

- a. 15[PRE], 15[a] “A method of operating a message link server, comprising: maintaining a respective secure message link through an Internet network between the message link server and a respective device link agent on each of a plurality of wireless end-user devices,”**

As previously noted, claim 15 is substantively very similar to claim 1 except that it is framed as a series of steps rather than elements of a server configured to carry out those steps. As to the preamble, *Rittmaster* discloses a server for providing message content to linked user devices, and as such it also discloses the steps performed by such a server. *See supra* Sections II.C.12 a., II.D.13.a. As discussed above in connection with claim 1, *Rittmaster* discloses a provider server 12 that “comprises an Internet product or service provider computer or server” coupled for communication” to “a plurality of network enabled user devices.” Ex. C, ¶ 42; *see also supra* Section II.E.1.a.; Malek Decl. at ¶ 125. *Shenfield* likewise discloses a proxy server that maintains links to mobile stations operated by users. Various methods of operating these servers in order to deliver message content obtained from providers to one or more of a plurality of end-user devices are explained in detail below.

- b.** **15[a]** *“each of the wireless end-user devices comprising multiple software components authorized to receive and process data from secure message link messages received via a device link agent on that device;”*

This element of claim 15 is identical to element 1[b] of claim 1 and is therefore rendered obvious for the same reasons discussed above at Section II.E.1.c. *See also* Malek Decl. at ¶¶ 125, 126. To the extent that there is any doubt that *Rittmaster* discloses this element, it would have been obvious in view of *Shenfield* for the reasons discussed above in connection with claim 1. *Id.*

- c.** **15[b]** *“receiving network element messages from a plurality of network elements, the received network element messages comprising respective message content and requests for delivery of the respective message content to respective wireless end-user devices, the respective message content including data for, and an identification of, a respective one of the authorized software components;”*

This element is the same as the function recited in element 1[c] of claim 1 without explicitly requiring the “interface” to a network that performs that function and is therefore rendered obvious for the same reasons discussed above at Section II.E.1.d. *See also* Malek Decl. at ¶ 127. Furthermore, the *Rittmaster* publication specifies that in some instances “the recipient processors comprise online user terminals, including, but not limited to conventional personal computers (PCs), portable communication devices (such as portable telephones, personal digital assistants, or other portable information units), or vehicle-mounted computers connected to a wide area network, such as, but not limited to, the Internet.” Ex. C, ¶ 35; Malek Decl. at ¶ 127; *see also supra* Section

II.D.13.c. To the extent that there is any doubt that *Rittmaster* discloses this element, it would have been obvious in view of *Shenfield* for the reasons discussed above in connection with claim 1. See *supra* Section II.E.1.d.; Malek Decl. at ¶ 127.

- d.** 15[c] “*buffering content from the received network element messages for which delivery is requested to a given one of the wireless end-user devices;*”

This element is the same as the function of element 1[d] of claim 1 except that it does not require the “memory” that performs that function and is therefore rendered obvious for the same reasons discussed above at Section II.E.1.e. See also Malek Decl. at ¶ 128. To the extent that there is any doubt that *Rittmaster* discloses this element, it would have been obvious in view of *Shenfield* for the reasons discussed above in connection with claim 1. Malek Decl. at ¶ 128.

- e.** 15[d] “*determining when one of a plurality of message delivery triggers for the given one of the wireless end-user devices has occurred, wherein for at least some of the received network element messages, the receipt of such a message is not a message delivery trigger, and for at least one of the message delivery triggers, the trigger is an occurrence of an asynchronous event with time-critical messaging needs; and*”

This element is the same as the function of element 1[e] of claim 1 except that it does not require the “logic” that performs that function and is therefore rendered obvious for the same reasons discussed above at Section II.E.1.f. See also Malek Decl. at ¶ 129. Additionally, providing content to an end-user device is dependent on one or more triggers in *Rittmaster*, and a PHOSITA would have understood the above claim element to be disclosed in *Rittmaster* for all of the reasons discussed above in connection with claim 1. To the extent that there is any doubt that *Rittmaster* discloses this element, it would have been obvious in view of *Shenfield*, which explicitly refers to asynchronous message triggers. *Id.*

- f.** 15[e] “*upon determining that one of the message delivery triggers has occurred, supplying one or more messages comprising the buffered content for delivery on the secure message link maintained between the message link server and a device link agent on the given one of the wireless end-user devices.*”

This element is the same as the functions of element 1[f] of claim 1 except that it does not require the “logic” or “transport services stack” that perform those functions and is therefore rendered obvious for the same reasons discussed above at Section II.E.1.g. See also Malek Decl.

at ¶ 130. To the extent that there is any doubt that *Rittmaster* discloses one or more aspects of this claim element, it would have been obvious in view of *Shenfield* for the reasons discussed above in connection with claim 1. *Id.*

F. Ground 4: The Combination of *Rittmaster* and *Konstantinov* and/or *Klassen* Render Obvious Claims 1-3, 5-7, and 9-15

Rittmaster discloses all of the elements of the claims for the various reasons explained above in Grounds 1 and 2. To the extent *Rittmaster* is considered to not disclose certain software-level details, a PHOSITA would have looked to other prior art references that do explicitly describe the basic protocol-level elements of such networks, as discussed in Grounds 2 and 3. Malek Decl. at ¶ 76.

It would have been obvious to a PHOSITA at the relevant time to implement those details in *Rittmaster* using routine skill in order to build a functional network. *Id.* This would have been nothing more than a predictable use of known elements, or at most use of known techniques to improve similar devices. *Id.* In fact, *Rittmaster*'s statement that "[t]he communications network may comprise any suitable means which allows the recipient processors and the provider processor to communicate with each other, including, but not limited to, the Internet or WWW, intranet, cable or other hard-wired networks, optical, electromagnetic or other wireless networks, as well as hybrids thereof, or the like" (Ex. C, ¶ 32) is an explicit teaching, suggestion, and motivation to combine *Rittmaster* with other prior art server networks to supplement its disclosure. *Id.*

For instance, network elements are described in more detail in U.S. Patent No. 8,064,934 to *Klassen* (which was filed October 19, 2006, more than two years prior to the applications that led to the '192 Patent). *See* Ex. K. *Klassen* discloses a network similar to those of the '192 Patent and *Rittmaster* for sending messages to a variety of mobile end-user devices through a network server:

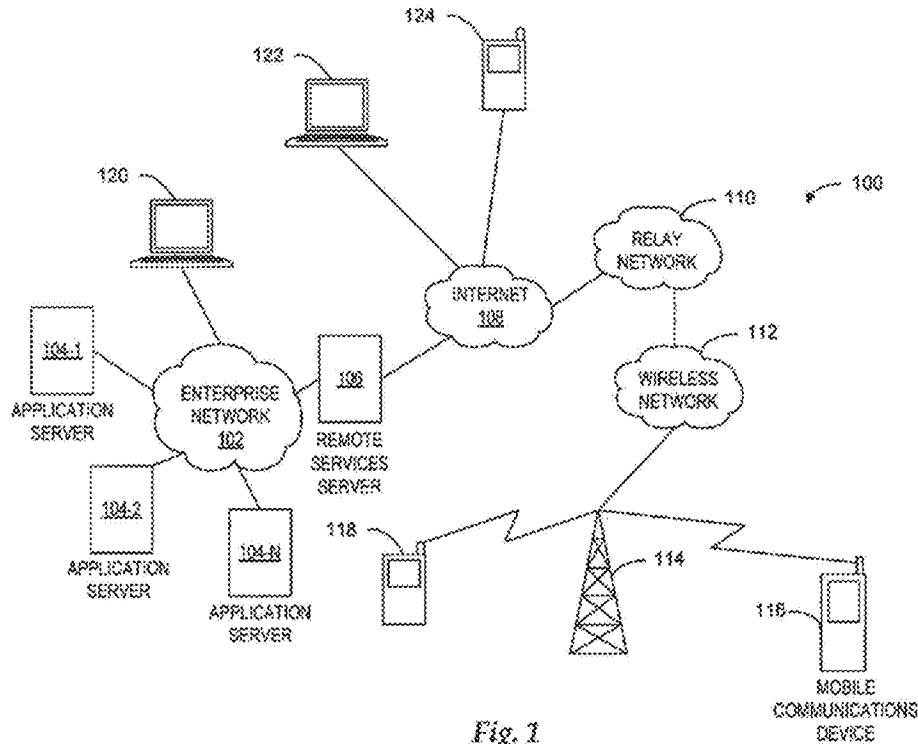
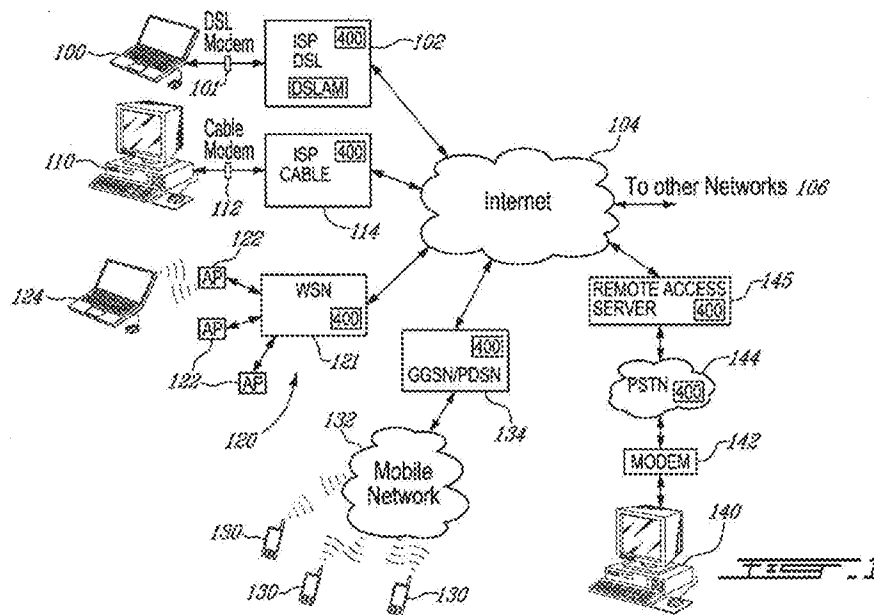


Fig. 1

Malek Decl. at ¶ 76; Ex. K, Fig. 1. As illustrated above, *Klassen* discloses a remote services server 106 that links a plurality of network elements (application servers 104-1 through 104-N) to a plurality of mobile communications devices through the internet, just like the '192 Patent and *Rittmaster*. Malek Decl. at ¶ 76.

Like *Rittmaster*, *Klassen*, and the '192 Patent, *Konstantinov* (Ex. D) also discloses a network where a plurality of mobile computers and cellular phones access a server over the internet to obtain content from a plurality of network elements:



Malek Decl. at ¶ 47; Ex. D, Fig. 1. A PHOSITA would have looked to *Konstantinov* (which was filed in September 2005, more than three years prior to the applications that led to the '192 Patent) at least because of its greater detail as to messaging protocol and message format, and especially because of its use of message delivery triggers. Malek Decl. at ¶ 80.

These and further motivations to combine these references are detailed below with respect to each claim or claim element.

I. Claim 1

a. 1[PRE] “A message link server comprising:”

As discussed above in relation to Ground 1, the preamble of claim 1 is disclosed by *Rittmaster* because it shows a server for providing message content to linked user devices. See *supra* Section II.C.1.a.; Malek Decl. at ¶ 51; Ex. C, ¶ 42. *Klassen* likewise discloses such a server that links a plurality of network elements to a plurality of mobile devices through the internet. Malek Decl. at ¶¶ 76-77; Ex. K, Fig. 1.

b. 1[a] “a transport services stack to maintain a respective secure message link through an Internet network between the message link server and a respective device link agent on each of a plurality of wireless end-user devices,”

Element 1[a] is both disclosed by and obvious over *Rittmaster*, which discloses that server 12 “comprises an Internet product or service provider computer or server ... coupled for communication” to “a plurality of network enabled user devices.” See *supra* Section II.C.1.b.;

Malek Decl. at ¶ 78; Ex. C, ¶ 42. To the extent there is any doubt that *Rittmaster* discloses technical details such as “a transport services stack” or “device link agents,” its own disclosure admits that “[s]uch computers and communication interfacing are well known in the art and are not described in further detail herein for purposes of simplifying the present disclosure.” Ex. C, ¶ 42; *see supra* Section II.D.1.b. A PHOSITA would know that common messaging protocols of the time, such as encrypted transport layer security (TLS) protocol, would be employed in such a system, and thus a “secure message link” would be maintained by a TLS protocol stack (“transport services stack”) and software programs (“device link agents”) on various end-user devices. *Id.*; Malek Decl. at ¶ 78.

Further, to the extent that there is any doubt that *Rittmaster* discloses communication between a server-side transport services stack and end-user mobile device message link agents, a PHOSITA would have simply implemented details from the similar network of *Klassen*, which includes a mobile device with a device link agent with a “multi-layer transport stack” 206 for communicating messages from a server to multiple “user applications” 207 on the mobile device, as shown in Fig. 2 below:

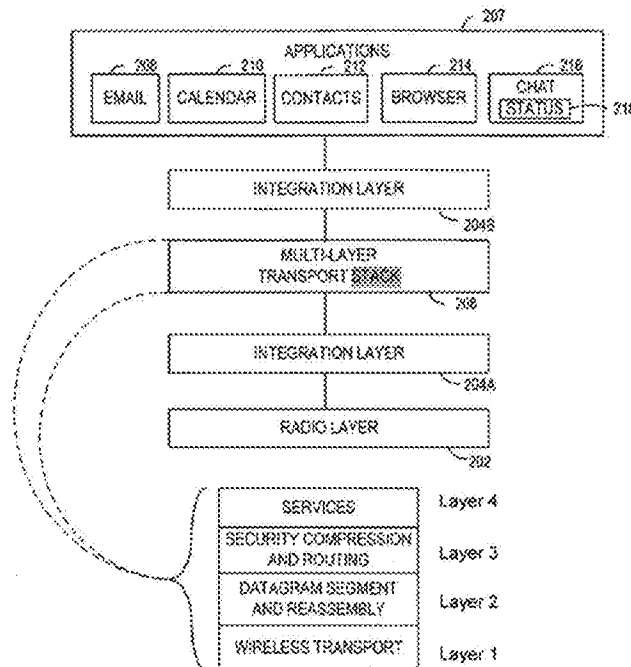


Fig. 2

Malek Decl. at ¶ 78; Ex. K, Fig. 2 (annotated). A PHOSITA would have further understood that *Klassen*'s remote services server has a corresponding transport services stack for communication with the above mobile device. Malek Decl. at ¶¶ 52 and 78.

- c. 1[b] “each of the wireless end-user devices comprising multiple software components authorized to receive and process data from secure message link messages received via a device link agent on that device;”

Rittmaster discloses element 1[b] of claim 1. *See supra* Section II.C.1.c., II.D.1.c.; Malek Decl. at ¶ 79. To the extent any doubt exists that *Rittmaster* discloses multiple software components on the user device authorized to receive and process data received via a device link agent on that device, Fig. 2 of *Klassen* makes this feature clear, and a PHOSITA would have had a clear motivation to fill in any perceived gaps of *Rittmaster* with details from the same type of network like that of *Klassen*. Malek Decl. at ¶ 79.

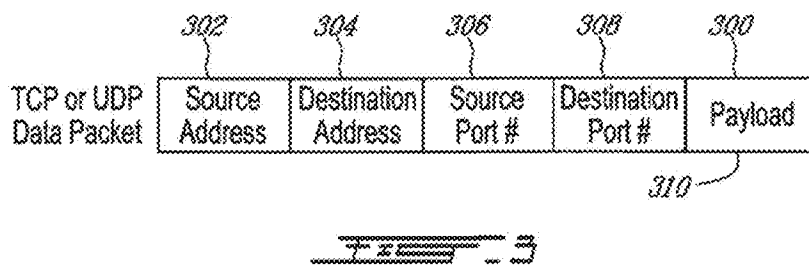
- d. 1[c] “an interface to a network to receive network element messages from a plurality of network elements, the received network element messages comprising respective message content and requests for delivery of the respective message content to respective wireless end-user devices, the respective message content including data for, and an identification of, a respective one of the authorized software components; and”

Rittmaster further discloses element 1[c]. *See supra* Sections II.C.1.d., II.D.1.d.; Malek Decl. at ¶ 80. This element requires the network-facing side of the server to include an “interface” to receive messages from two or more “network elements,” and requires the messages to include “message content” and “requests for delivery” of that content to specific end-user devices by including data for and an identification of authorized software. Malek Decl. at ¶ 80. This does little more than describe the basic manner in which all messages were delivered from a network at the relevant time, and how messages are still delivered today. *Id.* *Rittmaster* discloses transmission of messages (such as advertisements) from network elements (multiple providers) that are connected to the server through the internet. *Id.*; *see supra* Section II.D.1.d, *see also Klassen*, Ex. K, Fig. 1. *Rittmaster* also clearly relies on the ability to direct messages to correct applications on correct end-user devices. Malek Decl. at ¶ 80.

To the extent there is any doubt that *Rittmaster* or *Klassen* disclose sending messages that include data for, and identification of, authorized software components, or to determine specific ways in which to accomplish delivery of messages to the appropriate software component on a

recipient device, a PHOSITA would look to other prior art such as *Konstantinov* (Ex. D) for appropriate message formats. *Id.*

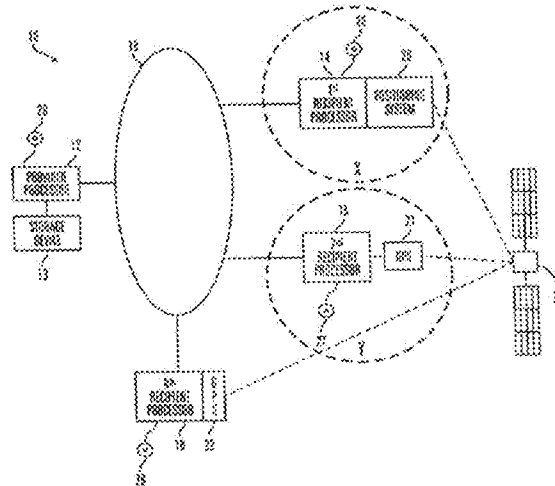
Konstantinov expressly describes addressing messages to one of a plurality of user devices from a server by utilizing not only an IP address, but also a port number. *See, e.g.,* Malek Decl. at ¶ 80; Ex. D, ¶ 39. Such disclosure acknowledges that both the content provider and the plurality of potential recipients (end-user devices such as laptop computers and mobile phone devices) have a plurality of software agents identified by port number. *Id.* A PHOSITA would have been motivated to look to *Konstantinov* because of its greater detail as to messaging protocol, and also because *Konstantinov* describes security measures to delay data packets according to certain rules to diminish the quality of illegitimate data traffic. Malek Decl. at ¶ 80; Ex. D, ¶ 33. Figure 3 of *Konstantinov* illustrates that each data packet includes a “payload” (content provided from a source device) and addressing information that identifies both a “destination address” (*i.e.*, recipient device IP address) and a “destination port #” (*i.e.*, the port number identifying the virtual location on the recipient device at which a specific software application is located):



Malek Decl. at ¶ 80; Ex. D, Fig. 3, ¶ 39.

- e. 1[d] “a message buffer system including a memory and logic, the memory to buffer content from the received network element messages for which delivery is requested to a given one of the wireless end-user devices”

Rittmaster further discloses element 1[d]. *See supra* Sections II.C.1.e., II.D.1.e.; Malek Decl. at ¶ 82. *Rittmaster* clearly identifies a buffer system that prevents transmission of messages to user devices until a determination is made that the user device is authorized to receive the message. *Id.* Briefly, Fig. 2 of *Rittmaster* shows a storage device 13 (*i.e.*, memory) associated with a server 12:



Malek Decl. at ¶ 82. Again, content is not provided by the server until a determination is made that specific rules have been satisfied. *Id.* For instance, *Rittmaster* states that “a set of rules may be implemented, which depend upon the geographic information ... such that ... if a recipient processor provides geographic information corresponding to a first geographic location or region, then the provider processor may be controlled to not provide selective information to the recipient processor, unless further requirements are met.” *Id.*; Ex. C, ¶ 40. Likewise, *Konstantinov* discloses buffering of messages upon certain conditions, specifically mentioning delaying transmission of data packets by transferring them into a buffer. *Id.*; Ex. D, ¶ 42. It would have been obvious to combine *Konstantinov* with *Rittmaster* in order to scramble certain messages if the requester is not deemed to be authorized by the server logic. Malek Decl. at ¶ 82.

f. 1[e] “the logic to determine when one of a plurality of message delivery triggers for the given one of the wireless end-user devices has occurred, wherein for at least some of the received network element messages, the receipt of such a message by the message buffer system is not a message delivery trigger, and for at least one of the message delivery triggers, the trigger is an occurrence of an asynchronous event with time-critical messaging needs, and”

Rittmaster further discloses element 1[e], as discussed above. *See supra* Sections II.C.1.f., II.D.1.f.; Malek Decl. at ¶ 82. Providing content to an end-user device is dependent on one or more triggers in *Rittmaster*, which primarily discusses geographic location but also contemplates that “the provider processor [server] may be controlled to not provide selective information to the recipient processor [end-user device], unless further criteria is met” such as “minimum user age, a

particular period of the day, week, month or year, or other suitable criteria.” *Id.*; Ex. C, ¶ 14. For similar reasons, *Konstantinov*’s system of delaying messages as determined by certain rules or triggers would have been obvious to combine with *Rittmaster* to delay delivery of messages to unauthenticated users. Malek Decl. at ¶ 82.

- g.** 1[f] “upon determining that one of the message delivery triggers has occurred, the logic further to supply one or more messages comprising the buffered content to the transport services stack for delivery on the secure message link maintained between the transport services stack and a device link agent on the given one of the wireless end-user devices.”

Rittmaster also discloses the final element of claim 1. *See supra* Sections II.C.1.g., II.D.1.g.; Malek Decl. at ¶ 83. *Rittmaster* and *Konstantinov* disclose transmission of messages through a link between a server-side stack and an end-user device-side software agent simply by disclosing that the messages are sent through the internet. *Id.* The *Rittmaster* system is specifically designed to deliver messages from the server to an end-user device in response to determining that a trigger has occurred, such as the end-user device entering a specific geographic region. *Id.* *Konstantinov*’s triggers satisfy this element for essentially the same reasons — timing the release of messages according to specific rules, and messages that may be used to determine whether those rules are satisfied. Malek Decl. at ¶ 83; Ex. D, ¶¶ 34, 41.

2. Claims 2-3 and 5-6

Claims 2-3 and 5-6 depend from independent claim 1. *Rittmaster* discloses the features added by these dependent claims, and therefore claims 2-3 and 5-6 would have been obvious in view of *Rittmaster* combined with *Konstantinov* and *Klassen* for at least the reasons explained above in Grounds 1-2. *See supra* Sections II.C.2-5, II.D.2-5.

- 3. Claim 7 — “the device messaging agent on at least one of the wireless end-user devices further to initiate the respective secure Internet data message link to the transport services stack”**

As discussed above, a laptop or smartphone communicating with a server would inherently have a link between a device messaging agent of the laptop/smartphone and a transport services stack on the server. *Id.*; *see supra* Sections II.C.6. In addition, *Rittmaster* indicates that end-user devices could initiate such a link, and that the link could be made secure by using various layers of encryption. *Id.* *Konstantinov* likewise indicates that a user device may issue a connection request. Malek Decl. at ¶ 89; Ex. D, ¶ 41. It would have been at least obvious to permit users to

initiate links to a network to allow users to have control over whether they receive messages from a given network and to allow users to request information from specific content providers. Malek Decl. at ¶ 89.

4. Claims 9-14

Claims 9-14 ultimately depend from independent claim 1. *Rittmaster* discloses the features added by these dependent claims, and therefore claims 9-14 would have been obvious in view of *Rittmaster* combined with *Konstantinov* and *Klassen* for at least the reasons explained above in Grounds 1-2. See *supra* Sections II.C.7-11, II.D.7-12.

5. Claim 15

- a. 15[PRE], 15[a] “*A method of operating a message link server, comprising: maintaining a respective secure message link through an Internet network between the message link server and a respective device link agent on each of a plurality of wireless end-user devices,*”

Claim 15 comprises a series of steps, and is substantively very similar to claim 1 (discussed at Sections II.C.1., II.D.1., II.F.1 above), except that it is framed as a method rather than elements of a server configured to carry out that method. Malek Decl. at ¶ 97. To the extent that there is any doubt that *Rittmaster* anticipates and/or alone renders obvious claim 15 (when combined with knowledge of a PHOSITA), it at least would have been obvious in view of *Konstantinov* and *Klassen* for the reasons discussed above in connection with claim 1.

Furthermore, the above quoted portion of claim 15’s preamble and element 15[a] is the same as the function recited in element 1[a] of claim 1 without requiring the “transport services stack” that performs that function, and therefore would have been obvious for the same reasons discussed above at Section II.F.1.a.-b.

- b. 15[a] “*each of the wireless end-user devices comprising multiple software components authorized to receive and process data from secure message link messages received via a device link agent on that device;*”

This element of claim 15 is identical to element 1[b] of claim 1, and is therefore rendered obvious for the same reasons discussed above at Section II.F.1.c. See also Malek Decl. at ¶ 98.

- c. 15[b] “*receiving network element messages from a plurality of network elements, the received network element messages comprising respective message content and requests for delivery of the respective message content to respective wireless end-user*

devices, the respective message content including data for, and an identification of, a respective one of the authorized software components;”

This portion of element 15[b] is the same as the function recited in element 1[c] of claim 1 without explicitly requiring the “interface” to a network that performs that function, and is therefore rendered obvious for the same reasons discussed above at Section II.F.1.d. *See also* Malek Decl. at ¶ 99.

- d.** 15[c] *“buffering content from the received network element messages for which delivery is requested to a given one of the wireless end-user devices;”*

This element is the same as the function of element 1[d] of claim 1 except that it does not require the “memory” that performs that function, and is therefore rendered obvious for the same reasons discussed above at Section II.F.1.e. *See also* Malek Decl. at ¶ 100.

- e.** 15[d] *“determining when one of a plurality of message delivery triggers for the given one of the wireless end-user devices has occurred, wherein for at least some of the received network element messages, the receipt of such a message is not a message delivery trigger, and for at least one of the message delivery triggers, the trigger is an occurrence of an asynchronous event with time-critical messaging needs; and”*

This element is the same as the function of element 1[e] of claim 1 except that it does not require the “logic” that performs that function, and is therefore rendered obvious for the same reasons discussed above at Section II.F.1.f. *See also* Malek Decl. at ¶ 101.

- f.** 15[e] *“upon determining that one of the message delivery triggers has occurred, supplying one or more messages comprising the buffered content for delivery on the secure message link maintained between the message link server and a device link agent on the given one of the wireless end-user devices.”*

This element is the same as the functions of element 1[f] of claim 1 except that it does not require the “logic” or “transport services stack” that perform those functions, and is therefore rendered obvious for the same reasons discussed above at Section II.F.1.g. *See also* Malek Decl. at ¶ 102.

- G.** Ground 5: Any Combination of *Rittmaster* and/or *Shenfield* and/or *Konstantinov/Klassen* (as Discussed in Grounds 1-4) in Further Combination with *Ellison* Renders Obvious Claim 4

Claim 4 adds to claim 1 a feature where the end-user device's link agent executes in a secure environment while at least some software is outside of that secure environment. Malek Decl. at ¶¶ 76, 86 (“Claim 4 recites that ‘**the device link agent executes in a secure execution environment on at least one of the devices, and at least one of the software components executes outside of the secure execution environment on that device.**’”) It would have been obvious to divide the memory of an end-user device into such rings based on the sensitivity of particular applications, and a PHOSITA would have followed the teachings of *Ellison* or similar prior art references in order to divide applications between secure and unsecure operating environments. All of the elements of claim 1 would have been obvious for the reasons discussed above in Grounds 1-4, and a PHOSITA would have been motivated to include the elements of claim 4 in further view of *Ellison*. This would have been an obvious optimization and prioritization of security resources, and a PHOSITA would have known that certain software on an end-user device that is not sensitive could operate outside of a secure execution environment in order to reduce costs and preserve resources. Malek Decl. at ¶ 76.

Additionally, claim 4 depends from claim 1, which is anticipated and rendered obvious by *Rittmaster* alone or in combination with other references as discussed in detail in Grounds 1-4 above. *See supra* Sections II.C.1., II.D.1., II.E.1., II.F.1.; Malek Decl. at ¶¶ 86, 114. The '192 Patent does not appear to suggest that there is any advantage to having some software components outside of a secure execution environment, but protecting some but not all software of a device in a secure environment was known at the relevant time, and would have been used by a PHOSITA to protect sensitive applications while allowing unimportant software components to remain in a secured environment in order to conserve resources. Malek Decl. at ¶¶ 86, 114. Regardless, protecting some but not all software on a device in a secure environment was known at the relevant time and would have been used by a PHOSITA to protect sensitive applications while allowing unimportant software components to remain in a less secured environment to conserve resources.

For instance, the *Ellison* reference discloses a method to protect a subset of a software environment. Malek Decl. at ¶¶ 86, 114; Ex. L, Abstract. *Ellison* describes providing a hierarchy, or “rings,” dividing hardware and software components designed to perform dedicated tasks within an operating system. Malek Decl. at ¶¶ 86, 114; Ex. L, 1:41-51. The division of a component into rings is typically based on the degree or level of privilege. *Id.*; *see also* Ex. L, 1:51-53. It would have been obvious to divide the memory of an end-user device of *Rittmaster* (including as modified

by *Shenfield* or *Konstantinov/Klassen*) into such rings based on the sensitivity of particular applications, and a PHOSITA would have followed the teachings of *Ellison* or similar prior art references to divide applications between secure and unsecure operating environments. Malek Decl. at ¶¶ 86, 114.

H. Ground 6: Any Combination of *Rittmaster* and/or *Shenfield* and/or *Konstantinov/Klassen* (as Discussed in Grounds 1-4) in Further Combination with *Coffee* or *Basso* Renders Obvious Claim 6

Claim 6 specifies that two or more data portions, each having an identifier, may be sent in a single message. Malek Decl. at ¶¶ 88, 116 (“Claim 6 recites ‘wherein at least one of the one or more messages for delivery by the transport services stack comprises multiple identifier/data pairs.’”) *Rittmaster* describes this element for the reasons discussed above in Sections II.C.5., II.D.5, II.E.4, and II.F.2. If one were to consider the elements of claim 6 not to be adequately disclosed in *Rittmaster* (or *Rittmaster* as modified by *Shenfield* or *Konstantinov/Klassen* as discussed above), however, a PHOSITA would have been motivated to look to *Coffee* or *Basso* to remedy such deficiencies. More specifically, a PHOSITA would understand that two independent data elements (e.g., advertisements), each having a data payload and identifier, could be assembled into a single message in order to allow for better handling of a high number of messages. For instance, *Coffee* discloses bundling of multiple messages, each having their own unique identifier¹⁰, to reduce throughput problems by bundling small messages into larger, less frequent messages. Malek Decl. at ¶¶ 88, 116; Ex. S, ¶¶ 117-119. Similarly, the *Basso* reference discloses that multiple messages to be sent from a network processor may be bundled into a single message to reduce the number of messages and improve performance. Malek Decl. at ¶ 88; Ex T, Abstract. A PHOSITA would have combined message bundling as in *Coffee* or *Basso* with the system of *Rittmaster* (or *Rittmaster* as modified by *Shenfield* or *Konstantinov/Klassen*) to enhance throughput by reducing the number of messages sent to a single end-user device. Malek Decl. at ¶¶ 88, 116.

¹⁰ *Coffee* discusses use of MSMQ messages, which is a messaging technology from Microsoft. See [https://learn.microsoft.com/en-us/previous-versions/windows/desktop/msmq/ms711472\(v=vs.85\)](https://learn.microsoft.com/en-us/previous-versions/windows/desktop/msmq/ms711472(v=vs.85)). MSQM messages have a “Destination” property that identifies the recipient of the message. See <https://learn.microsoft.com/en-us/previous-versions/windows/desktop/msmq/ms706292%28v%3Dvs.85%29>.

I. Ground 7: Any Combination of *Rittmaster* and/or *Shenfield* and/or *Konstantinov/Klassen* (as Discussed in Grounds 1-4) in Further Combination with *Computer Networks*, *Rakic*, or *Dutta* Renders Obvious Claim 8

Claim 8 adds to claim 1 “a secure server to provide secure authorization signatures to the given one of the wireless end-user devices, the secure authorization signatures indicating the authorized software components that are allowed to receive data from secure message link messages via the message link server.” Malek Decl. at ¶¶ 90, 118. While *Rittmaster* and *Shenfield*, *Konstantinov*, and *Klassen* do not explicitly mention use of signatures to indicate that software components are authorized to receive data from a server through a secure link, use of signatures was well-known at the relevant time and was not invented by the inventor of the ’192 Patent. Malek Decl. at ¶¶ 90, 118. For instance, the *Computer Networks* textbook discusses the advantages of digital signatures in increasing security. Ex. F at pp. 584-89. There would be a clear motivation to implement digital signatures to ensure that various components of a network have authorization to receive various messages, and implementation of digital signatures would have been well within ordinary skill in the art. Additionally, U.S. Pat. Pub. 2009/0282256 to Rakic, et al. (“*Rakic*,” Ex. M) discloses that a server may generate an electronic signature which is appended to the message or other information to verify message authenticity and source. Ex. M, ¶¶ 41-49, 66-67, and 109-112. Likewise, U.S. Pat. Pub. 2002/0186845 to Dutta, et al. (“*Dutta*,” Ex. N) discloses use of digital signatures in mobile networks. Malek Decl. at ¶¶ 90, 118; Ex. N, Abstract. It would have been obvious and routine to implement digital signatures such as described in *Rakic* and/or *Dutta* in the system of *Rittmaster* to increase security, giving those skilled in the art a clear motivation to combine the digital signature aspects of *Rakic* or *Dutta* with the references and combinations of references discussed above in Grounds 1-4.

J. Ground 8: Any Combination of *Rittmaster* and/or *Shenfield* and/or *Konstantinov/Klassen* (as Discussed in Grounds 1-4) in Further Combination with *Gellens* Renders Obvious Claim 14

Claim 14 depends from claim 1, specifying that “one of the message delivery triggers is based on an amount of wireless network data usage consumed by the given one of the wireless end-user devices.” *Rittmaster* discloses this element for the reasons discussed above in Sections II.C.11 and II.D.12. Malek Decl. at ¶¶ 96, 124. To the extent that there is any doubt that *Rittmaster* discloses the elements of claim 14, however, limiting communication of messages to specific end-user devices based on usage would have been obvious in view of *Gellens* (Ex. O). *Gellens* discloses

control data delivery over cellular networks due to, *e.g.*, costs and bandwidth, and permitting applications to open connections for “low priority” messages can drive up costs leading to “excessive and wasteful traffic channel usage.” Malek Decl. at ¶¶ 96, 124; Ex. O, Abstract, ¶¶ 2-6, 27, 29. *Gellens* uses triggers to control when messages are delivered to clients, one of which triggers delivery of low priority application messages only after a higher-priority application initiates a link. Malek Decl. at ¶¶ 96, 124; Ex. O, ¶¶ 35-36. A PHOSITA would have been motivated to combine *Gellens* with *Rittmaster* and/or *Shenfield* to save costs and conserve bandwidth. Malek Decl. at ¶¶ 96, 124.

III. CERTIFICATION UNDER 37 C.F.R. § 1.510(B)(5)

Walmart has served a copy of the request in its entirety on the Patent Owner at the address as provided for in 37 C.F.R. § 1.33(c):

Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

IV. CERTIFICATION UNDER 37 C.F.R. § 1.510(B)(6)

Walmart has not previously filed or joined a post-grant review or petition for reexamination for any claim of the '192 Patent. Therefore, the statutory estoppel provisions of 35 U.S.C. § 315(e)(1) and 35 U.S.C. § 325(e)(1) do not prohibit Walmart from filing this *ex parte* reexamination request.

V. CONCLUSION

For the reasons provided herein, Walmart respectfully submits that the cited references render Claims 1-15 of the '192 Patent unpatentable, thereby raising substantial new questions of patentability regarding these claims. *Ex parte* reexamination should be commenced, and claims 1-15 should be found invalid.

Respectfully submitted,

FITCH EVEN TABIN & FLANNERY LLP

Dated: December 24, 2025

By: /Nicholas T. Peters/
Nicholas T. Peters
Registration No. 53,456
ntpete@fitcheven.com

Headwater Research LLC
Ex. 2008, IPR2026-00088
Page 112 of 113

120 South LaSalle Street
Suite 2100
Chicago, Illinois 60603
(312) 577-7000
(312) 577-7007 (fax)

*Attorney for Requester
Walmart Inc.*