IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Reexamination of: Raleigh Patent No.: 10,321,320 Issue Date: June 11, 2019 For: WIRELESS NETWORK BUFFERED MESSAGE SYSTEM	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 1-18 of U.S. Patent No. 10,321,320 ("the '320 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 1-18 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)(l));
- 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 '320 Patent (37 C.F.R. § l.510(b)(3));
- A copy of the entire '320 Patent, including the front face, drawings, specification, and claims (37 C.F.R. § l.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)).

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 2 of 114

TABLE OF CONTENTS

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

A. Introduction 2

B. The '320 Patent and Prosecution History 2

1. Summary of the '320 Patent 2

a. Claims of the '320 Patent 6

2. Prosecution History of U.S. Application No. 15/582,350 10

3. Prior *Inter Partes* Review Proceedings 11

a. *Amazon.com Servs., LLC, et al. v. Headwater Rsch. LLC*, IPR2026-00106 11

b. *Target Corp. v. Headwater Rsch. LLC*, IPR2026-00153 12

4. Prior Relevant Federal District Court Litigation 12

5. Related *Ex Parte* Reexamination of '192 and '117 13

C. Overview of Cited Art and SNQs Raised 13

1. U.S. Patent Pub. No. 2002/0023010 ("*Rittmaster*") (Ex. C) 15

2. U.S. Patent Pub. No. 2006/0268696 ("*Konstantinov*") (Ex. D) 18

3. Andrew S. Tanenbaum and Maarten Van Steen, *Distributed Systems: Principles and Paradigms* (Pearson Education, 2d ed. 2007) ("*Distributed Systems*") (Ex. E) 19

4. Andrew S. Tanenbaum, *Computer Networks* (Pearson Education, 4th ed. 2003) ("*Computer Networks*") (Ex. F) 19

5. U.S. Patent No. 8,064,934 ("*Klassen*") (Ex. K) 20

6. U.S. Patent No. 7,082,615 ("*Ellison*") (Ex. L) 20

7. U.S. Patent No. 7,184,554 ("*Freese*") (Ex. M) 21

8. U.S. Patent No. 6,085,098 ("*Moon*") (Ex. N) 22

9. U.S. Patent Pub. No. 2008/0215883 ("*Fok*") (Ex. O) 22

10. U.S. Pat. Pub. 2006/0129691 ("*Coffee*") (Ex. S) 22

11. U.S. Pat. Pub. 2005/0108397 ("*Basso*") (Ex. T) 22

12. AU App. No. 2007200530 ("*Shenfield*") (Ex. U) 22

D. Discretionary Denial Under 35 U.S.C. § 325(d) Is Not Warranted 25

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 25

A. Level of Ordinary Skill in the Art 26

B. Claim Construction 26
1. "software components" 27
2. "device link agent" 27
3. "wherein the period of the timer is fractionally shorter than a maximum data message interval" 27
C. Ground 1: Claims 1-3, 5-7, 10, 12-13, and 15-18 are Anticipated by *Rittmaster* 28
1. Claim 1 29
a. 1[PRE] *"A networked system comprising:"* 29
b. 1[a] *"i) a network server system including a link interface to maintain a respective secure Internet data message link between the link interface and a respective device link agent on each of a plurality of wireless end-user devices,"* 30
c. 1[b] *"each of the wireless end-user devices comprising multiple software components authorized to receive messages via the device link agent on that device;"* 32
d. 1[c] *"a network interface to receive messages from a plurality of network elements, for delivery to respective ones of the software components identified in the messages, each network element authorized to send messages via the link interface to one or more of the software components on one or more of the wireless end-user devices; and"* 33
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 any of the wireless end-user devices,"* 35
f. 1[e] *"the logic to determine when one of a plurality of message delivery triggers for a 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"* 37
g. 1[f] *"upon determining that one of the message delivery triggers has occurred for the given one of the wireless end-user devices, the logic further to supply one or more messages comprising the buffered content for the given one of the wireless end-user devices to the transport services stack for delivery on the secure message link maintained*

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 4 of 114

between the transport services stack and a device link agent on the given one of the wireless end-user devices; and" 39

h. 1[g] *"ii) the device link agents on the respective wireless end-user devices, each of the device link agents configured to maintain the respective secure Internet data message link over a wireless network to the link interface,"* 39

i. 1[h] "[each of the device link agents configured to] *receive secure Internet data messages from the network server system over the respective secure Internet data message link, including messages collected from multiple ones of the network elements and messages corresponding to multiple ones of the software components authorized to receive messages via the device link agent on that respective device,"* 40

j. 1[i] *"wherein at least a first subset of the secure Internet data messages contain both a unique identifier for a corresponding one of the software agents and data to be consumed by that software component, the data supplied from a respective network element corresponding to that software component, and"* 40

k. 1[j] "[each of the device link agents configured to] *for software components that are authorized to access messages received via the device link agent, cause messages with a unique identifier corresponding to a given one of those software applications to be securely delivered to a software process corresponding to the given software component."* 42

2. Claim 2 – *"the message buffer system logic to determine, for each of the wireless end-user devices, when one of a plurality of message delivery triggers has occurred, at least one of the triggers for each given device specific to one or more states of that given device."* 42

3. Claim 3 – *"wherein one of the message delivery triggers is the expiration of a periodic timer."* 43

4. Claim 5 – *"wherein one of the message delivery triggers is the receipt of a transmission on the respective secure Internet data 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."* 44

5. Claim 6 – *"wherein one of the message delivery triggers is a heartbeat message generated by the given device link agent, or a request received from the given device link agent."* 44

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 5 of 114

6. Claim 7 – *"wherein one of the message delivery triggers is the receipt of a particular message from one of the network elements."* 44

7. Claim 10 – *"wherein a second subset of the secure Internet data messages contain a user message from a network element, the user message intended for display on a user interface of a given one of the wireless end-user devices."* 45

8. Claim 12 – *"the link interface to encrypt messages identified for delivery to each given one of the wireless end-user devices to create secure Internet data messages, the device link agent on each given device further configured to decrypt the received secure Internet data messages for that device prior to delivering those messages to a respective software process."* 46

9. Claim 13 – *"wherein the encrypted messages are transported to the device link agent using one or more of encryption on a transport services stack, IP (Internet Protocol) layer encryption, and tunneling."* 47

10. Claim 15 – *"wherein the device link agent on a given one of the devices is further configured to receive, from one or more of the software components on that device, upload messages, each of the upload messages identifying a corresponding one of the network elements to which the device respective software component has requested delivery, the device link agent on that device transmitting the upload messages to the network message server over the respective secure Internet data message link, for delivery by the network message server to the respective identified network elements."* 47

11. Claim 16 – *"the device link agent on the given device further configured to buffer one or more of the upload messages for transmission to the network message server at a time selected by a heartbeat mechanism."* 48

12. Claim 17 – *"at least a given one of the devices further comprising a secure interprocess communication service separately secured from the secure Internet data message link, the device link agent for the given device causing messages to be securely delivered to a software process by initiating delivery of each such message on the secure interprocess communication service."* 49

13. Claim 18 – *"wherein at least one of the secure Internet data messages comprises multiple identifier/data pairs."* 49

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 1-7, 10, 12-13, and 15-18 49

1. Claim 1 50

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 6 of 114

a. 1[PRE] *"A network server system comprising:"* 50

b. 1[a] *"i) a network server system including a link interface to maintain a respective secure Internet data message link between the link interface 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 messages via the device link agent on that device;"* 52

d. 1[c] *"a network interface to receive messages from a plurality of network elements, for delivery to respective ones of the software components identified in the messages, each network element authorized to send messages via the link interface to one or more of the software components on one or more of the wireless end-user devices; and"* 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 any of the wireless end-user devices,"* 55

f. 1[e] *"the logic to determine when one of a plurality of message delivery triggers for a 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"* 56

g. 1[f] *"upon determining that one of the message delivery triggers has occurred for the given one of the wireless end-user devices, the logic further to supply one or more messages comprising the buffered content for the given one of the wireless end-user devices 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; and"* 58

h. 1[g] *"ii) the device link agents on the respective wireless end-user devices, each of the device link agents configured to maintain the respective secure Internet data message link over a wireless network to the link interface,"* 59

i. 1[h] "[*each of the device link agents configured to*] *receive secure Internet data messages from the network server system over the respective secure Internet data message*

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 7 of 114

link, including messages collected from multiple ones of the network elements and messages corresponding to multiple ones of the software components authorized to receive messages via the device link agent on that respective device," 59

j. 1[i] *"wherein at least a first subset of the secure Internet data messages contain both a unique identifier for a corresponding one of the software agents and data to be consumed by that software component, the data supplied from a respective network element corresponding to that software component, and"* 60

k. 1[j] "[each of the device agents configured to] *for software components that are authorized to access messages received via the device link agent, cause messages with a unique identifier corresponding to a given one of those software applications to be securely delivered to a software process corresponding to the given software component."* 61

2. Claim 2 – *"the message buffer system logic to determine, for each of the wireless end-user devices, when one of a plurality of message delivery triggers has occurred, at least one of the triggers for each given device specific to one or more states of that given device."* 62

3. Claim 3 – *"wherein one of the message delivery triggers is the expiration of a periodic timer."* 62

4. Claim 4 – *"wherein the period of the timer is fractionally shorter than a maximum data message interval beyond which the Internet data message link to the given device is taken down."* 62

5. Claim 5 – *"wherein one of the message delivery triggers is the receipt of a transmission on the respective secure Internet data 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."* 63

6. Claim 6 – *"wherein one of the message delivery triggers is a heartbeat message generated by the given device link agent, or a request received from the given device link agent."* 63

7. Claim 7 – *"wherein one of the message delivery triggers is the receipt of a particular message from one of the network elements."* 64

8. Claim 10 – *"wherein a second subset of the secure Internet data messages contain a user message from a network element, the user message intended for display on a user interface of a given one of the wireless end-user devices."* 64

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 8 of 114

9. Claim 12 – *"the link interface to encrypt messages identified for delivery to each given one of the wireless end-user devices to create secure Internet data messages, the device link agent on each given device further configured to decrypt the received secure Internet data messages for that device prior to delivering those messages to a respective software process."* 65

10. Claim 13 – *"wherein the encrypted messages are transported to the device link agent using one or more of encryption on a transport services stack, IP (Internet Protocol) layer encryption, and tunneling."* 65

11. Claim 15 – *"wherein the device link agent on a given one of the devices is further configured to receive, from one or more of the software components on that device, upload messages, each of the upload messages identifying a corresponding one of the network elements to which the device respective software component has requested delivery, the device link agent on that device transmitting the upload messages to the network message server over the respective secure Internet data message link, for delivery by the network message server to the respective identified network elements."* 66

12. Claim 16 – *"the device link agent on the given device further configured to buffer one or more of the upload messages for transmission to the network message server at a time selected by a heartbeat mechanism."* 67

13. Claim 17 – *"at least a given one of the devices further comprising a secure interprocess communication service separately secured from the secure Internet data message link, the device link agent for the given device causing messages to be securely delivered to a software process by initiating delivery of each such message on the secure interprocess communication service."* 68

14. Claim 18 – *"wherein at least one of the secure Internet data messages comprises multiple identifier/data pairs."* 68

E. Ground 3: The Combination of *Rittmaster* and *Shenfield* Renders Obvious Claims 1-7, 10, 12-13, and 15-18 69

1. Claim 1 71

a. 1[PRE] *"A network server system comprising:"* 71

b. 1[a] "*i) a network server system including a link interface to maintain a respective secure Internet data message link between the link interface and a respective device link agent on each of a plurality of wireless end-user devices*," 72

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 9 of 114

c. [1b] "*each of the wireless end-user devices comprising multiple software components authorized to receive messages via the device link agent on that device;*" 73

d. 1[c] "*a network interface to receive messages from a plurality of network elements, for delivery to respective ones of the software components identified in the messages, each network element authorized to send messages via the link interface to one or more of the software components on one or more of the wireless end-user devices; and*" 74

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 any of the wireless end-user devices,"* 76

f. 1[e] *"the logic to determine when one of a plurality of message delivery triggers for a 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"* 77

g. 1[f] *"upon determining that one of the message delivery triggers has occurred for the given one of the wireless end-user devices, the logic further to supply one or more messages comprising the buffered content for the given one of the wireless end-user devices 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; and"* 78

h. 1[g] *"ii) the device link agents on the respective wireless end-user devices, each of the device link agents configured to maintain the respective secure Internet data message link over a wireless network to the link interface,"* 79

i. 1[h] "[each of the device link agents configured to] *receive secure Internet data messages from the network server system over the respective secure Internet data message link, including messages collected from multiple ones of the network elements and messages corresponding to multiple ones of the software components authorized to receive messages via the device link agent on that respective device,"* 79

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 10 of 114

j. 1[i] *"wherein at least a first subset of the secure Internet data messages contain both a unique identifier for a corresponding one of the software agents and data to be consumed by that software component, the data supplied from a respective network element corresponding to that software component, and"* 80

k. 1[j] "[each of the device link agents configured to] *for software components that are authorized to access messages received via the device link agent, cause messages with a unique identifier corresponding to a given one of those software applications to be securely delivered to a software process corresponding to the given software component."* 81

2. Claim 2 – *"the message buffer system logic to determine, for each of the wireless end-user devices, when one of a plurality of message delivery triggers has occurred, at least one of the triggers for each given device specific to one or more states of that given device."* 82

3. Claim 3 – *"wherein one of the message delivery triggers is the expiration of a periodic timer."* 82

4. Claim 4 – *"wherein the period of the timer is fractionally shorter than a maximum data message interval beyond which the Internet data message link to the given device is taken down."* 82

5. Claim 5 – *"wherein one of the message delivery triggers is the receipt of a transmission on the respective secure Internet data 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."* 82

6. Claim 6 – *"wherein one of the message delivery triggers is a heartbeat message generated by the given device link agent, or a request received from the given device link agent."* 83

7. Claim 7 – *"wherein one of the message delivery triggers is the receipt of a particular message from one of the network elements."* 83

8. Claim 10 – *"wherein a second subset of the secure Internet data messages contain a suer message from a network element, the user message intended for display on a user interface of a given one of the wireless end-user devices."* 84

9. Claim 12 – *"the link interface to encrypt messages identified for delivery to each given one of the wireless end-user devices to create secure Internet data messages, the device link agent on each given device further configured to decrypt the received secure Internet data messages for that device prior to delivering those messages to a respective software process."* 84

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 11 of 114

10. Claim 13 – *"wherein the encrypted messages are transported to the device link agent using one or more of encryption on a transport services stack, IP (Internet Protocol) layer encryption, and tunneling."* 84

11. Claim 15 – *"wherein the device link agent on a given one of the devices is further configured to receive, from one or more of the software components on that device, upload messages, each of the upload messages identifying a corresponding one of the network elements to which the device respective software component has requested delivery, the device link agent on that device transmitting the upload messages to the network message server over the respective secure Internet data message link, for delivery by the network message server to the respective identified network elements."* 85

12. Claim 16 – *"the device link agent on the given device further configured to buffer one or more of the upload messages for transmission to the network message server at a time selected by a heartbeat mechanism."* 85

13. Claim 17 – *"at least a given one of the devices further comprising a secure interprocess communication service separately secured from the secure Internet data message link, the device link agent for the given device causing messages to be securely delivered to a software process by initiating delivery of each such messages on the secure interprocess communication service."* 85

14. Claim 18 – *"wherein at least one of the secure Internet data messages comprises multiple identifier/data pairs."* 86

F. Ground 4: The Combination of *Rittmaster*, *Klassen*, and *Konstantinov* Renders Claims 1-7, 10, 12-13, and 15-18 Obvious. 86

G. Ground 5: The Combination of *Rittmaster* (as in any of Grounds 1-4) and *Freese* Renders Obvious Claims 8-9 89

1. Claim 8 – *"further comprising a secure server to store a secure authorization list, the secure authorization list indicating the authorized software components and the authorized network elements that are allowed to communicate using the network server system."* 89

2. Claim 9 – *"further comprising the respective device link agent on each wireless end-user device receiving access authorization information from the secure server, the access authorization indicating, respectively for each wireless end-user device, the software components authorized to receive messages via the device link agent on that device."* 91

H. Ground 6: The Combination of *Rittmaster* (as in any of Grounds 1-4) and *Freese* and/or *Moon* Renders Obvious Claim 11 92

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 12 of 114

1. Claim 11 – *"wherein one of the software components on a given one of the wireless end-user devices is a policy control agent, and the data to be consumed by the policy control agent comprises service settings and/or configuration information for the given device."* 92

I. Ground 7: The Combination of *Rittmaster* (as in any of Grounds 1-4) and *Ellison* Render Obvious Claim 14 94

1. Claim 14 – *"wherein the device link agent on a given device executes in a secure execution environment, and at least one of the software components on that device executes outside of the secure execution environment."* 94

J. Ground 8: The Combination of *Rittmaster* (as in any of Grounds 1-4) and *Fok* and/or *Ellison* Render Obvious Claim 17 95

1. Claim 17 – *"at least a given one of the devices further comprising a secure interprocess communication service separately secured from the secure Internet data message link, the device link agent for the given device causing messages to be securely delivered to a software process by initiating delivery of each such message on the secure interprocess communication service."* 95

K. Ground 9: The Combination of *Rittmaster* (as in any of Grounds 1-4) and *Coffee* and/or *Basso* Render Obvious Claim 18 97

1. Claim 18 – *"wherein at least one of the secure Internet data messages comprises multiple identifier/data pairs."* 97

III. CERTIFICATION UNDER 37 C.F.R. § 1.510(B)(5) 98

IV. CERTIFICATION UNDER 37 C.F.R. § 1.510(B)(6) 98

V. CONCLUSION 98

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 13 of 114

TABLE OF AUTHORITIES

Cases

In re Am. Acad. of Sci. Tech. Ctr.,
367 F.3d 1359 (Fed. Cir. 2004) 26

In re Bass,
314 F.3d 575 (Fed. Cir. 2002) 26

In re Yamamoto,
740 F.2d 1569 (Fed. Cir. 1984) 26

Nautilus, Inc. v. Biosig Instruments, Inc.,
572 U.S. 898 (2014) 27

Statutes

35 U.S.C. § 303(a) 25

35 U.S.C. § 325(d) 25

Other Authorities

MPEP § 2111 28

MPEP § 2242.I 12

Regulations

37 CFR § 1.75(d)(1) 28

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 14 of 114

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. 10,321,320
Ex. B	Curriculum Vitae of Dr. Sam Malek
Ex. C	U.S. Pat. Pub. 2002/0023010 to Rittmaster, et al. ("*Rittmaster*")
Ex. D	U.S. Pat. Pub. 2006/0268696 to Konstantinov, et al. ("*Konstantinov*")
Ex. E	Andrew S. Tanenbaum and Maarten Van Steen, *Distributed Systems: Principles and Paradigms* (Pearson Education, 2d ed. 2007) ("*Distributed Systems*")
Ex. F	Andrew S. Tanenbaum, *Computer Networks* (Pearson Education, 4th ed. 2003) ("*Computer Networks*")
Ex. G	*Headwater Research LLC v. Samsung Elecs. Co. Ltd., et al.*, No. 2:23-cv-00103, Claim Construction Order (Dkt. 118) (E.D. Tex. Aug. 22, 2024)
Ex. H	*Samsung Elecs. Co. Ltd., et al. v. Headwater Research LLC*, No. IPR2024-00010, Petitioner's Reply to Patent Owner's Response (Paper 16) (PTAB Dec. 18, 2024)
Ex. I	*Samsung Elecs. Co. Ltd., et al. v. Headwater Research LLC*, No. IPR2024-00010, Patent Owner's Response to the Petition (Paper 12) (PTAB Sept. 7, 2024)
Ex. J	*Samsung Elecs. Co. Ltd., et al. v. Headwater Research LLC*, 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 ("*Klassen*")
Ex. L	U.S. Patent No. 7,082,615 to Ellison, *et al.* ("*Ellison*")
Ex. M	U.S. Patent No. 7,184,554 to Freese, *et al.* ("*Freese*")
Ex. N	U.S. Patent No. 6,085,098 to Moon, *et al.* ("*Moon*")
Ex. O	U.S. Pat. Pub. No. 2008/0215883 to Fok, *et al.* ("*Fok*")
Ex. P	Excerpts from the Prosecution History of U.S. Patent No. 10,321,320
Ex. Q	*Amazon.com Servs., LLC, et al. v. Headwater Research LLC*, No. IPR2026-00106, Petition for *Inter Partes* Review of U.S. Patent No. 10,321,320 (Paper 1) (PTAB Nov. 10, 2025)

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 15 of 114

Ex. R	*Target Corp. v. Headwater Research LLC*, No. IPR2026-00153, Petition for *Inter Partes* Review (Paper 3) (PTAB Nov. 25, 2025)
Ex. S	U.S. Pat. Pub. 2006/0129691 to Coffee, et al. ("*Coffee*")
Ex. T	U.S. Pat. Pub. 2005/0108397 to Basso, et al. ("*Basso*")
Ex. U	Australian Pat. Pub. AU 2007200530 to Shenfield, et al. ("*Shenfield*")
Ex. V	*Headwater Research LLC v. Amazon.com Services LLC, et al.*, No. 7:25-cv-00286, Defendants' Opening Claim Construction Brief (Dkt. 40) (W.D. Tex. Feb. 11, 2026)
Ex. W	*Headwater Research LLC v. Amazon.com Services LLC, et al.*, No. 7:25-cv-00286, Plaintiff Headwater Research LLC's Responsive Claim Construction Brief (Dkt. 42) (W.D. Tex. Feb. 25, 2026)

Other than 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.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 16 of 114

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

Walmart requests reexamination of Claims 1-18 of the '320 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 '320 Patent or during subsequent *inter partes* review proceedings. A summary of the grounds asserted in this reexamination request is provided below:

No.	Claims	Grounds Presented Herein
1	1-3, 5-7, 10, 12-13, and 15-18	Anticipated by *Rittmaster*
2	1-7, 10, 12-13, and 15-18	Obvious in view of *Rittmaster* + knowledge of PHOSITA (as evidenced by *Distributed Systems* and/or *Computer Networks* textbooks)
3	1-7, 10, 12-13, and 15-18	Obvious in view of *Rittmaster* + *Shenfield*
4	1-7, 10, 12-13, and 15-18	Obvious in view of *Rittmaster* and/or *Shenfield* (as in any of Grounds 1 - 2) + *Klassen* and *Konstantinov*
5	8-9	Obvious in view of *Rittmaster* (as in any of Grounds 1-4) + *Freese*
6	11	Obvious in view of *Rittmaster* (as in any of Grounds 1-4) + *Freese* and/or *Moon*
7	14	Obvious in view of *Rittmaster* (as in any of Grounds 1-4) + *Ellison*
8	17	Obvious in view of *Rittmaster* (as in any of Grounds 1-4) + *Fok* and/or *Ellison*
9	18	Obvious in view of *Rittmaster* (as in any of Grounds 1-4) + *Coffee* and/or *Basso*

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 17 of 114

A. Introduction

The '320 Patent issued on June 11, 2019, from U.S. Patent Application No. 15/582,350 ("the '350 Application"), which was filed on April 28, 2017, and published on November 16, 2017. Ex. A, Cover.

Although the specification of the '320 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 '320 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 '320 Patent. For all the reasons discussed below, each claim is anticipated or rendered 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 '320 Patent and Prosecution History

1. Summary of the '320 Patent

Although the specification is long, and includes more than 100 pages of figures, the vast majority of the '320 Patent identifies and describes basic network elements and architecture that were well-known before its priority date. Declaration of Dr. Sam Malek ("Malek Decl.") at ¶ 34. The '320 Patent describes a "network server system [that] maintains secure Internet data message links with respective device link agents on each of many wireless end-user devices." Ex. A, Abstract. The "network server system" 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 network server system receives certain messages from the network directed to a particular end-user device, it holds those messages in a buffer until a specified trigger occurs 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 '320 Patent is directed to a "networked system" that links "wireless end-user devices" to a network, as shown in Figure 1 below (Malek Decl. at ¶ 35):

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 18 of 114

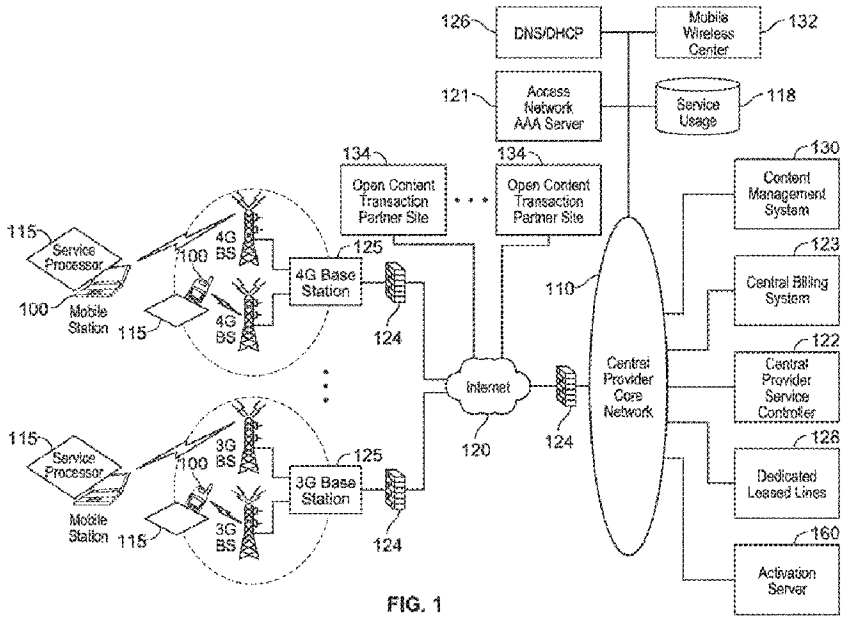


FIG. 1

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; Malek Decl. at ¶ 35.

Another disclosed network architecture of the '320 Patent, shown in Fig. 6 below, includes a 4G LTE and Wi-Fi overlay configuration:

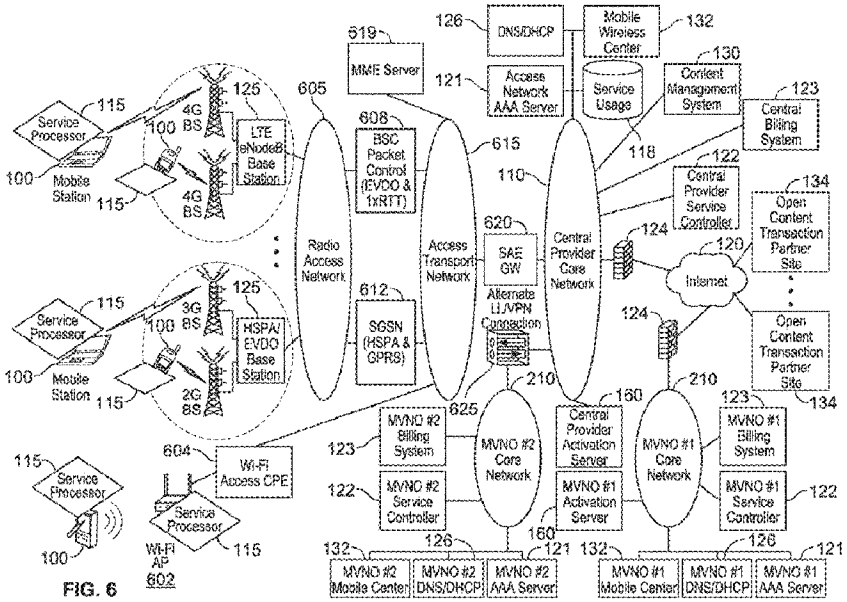


FIG. 6

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 19 of 114

Ex. A, 23:32-38; Malek Decl. at ¶ 36. 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 types of 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 '320 Patent:

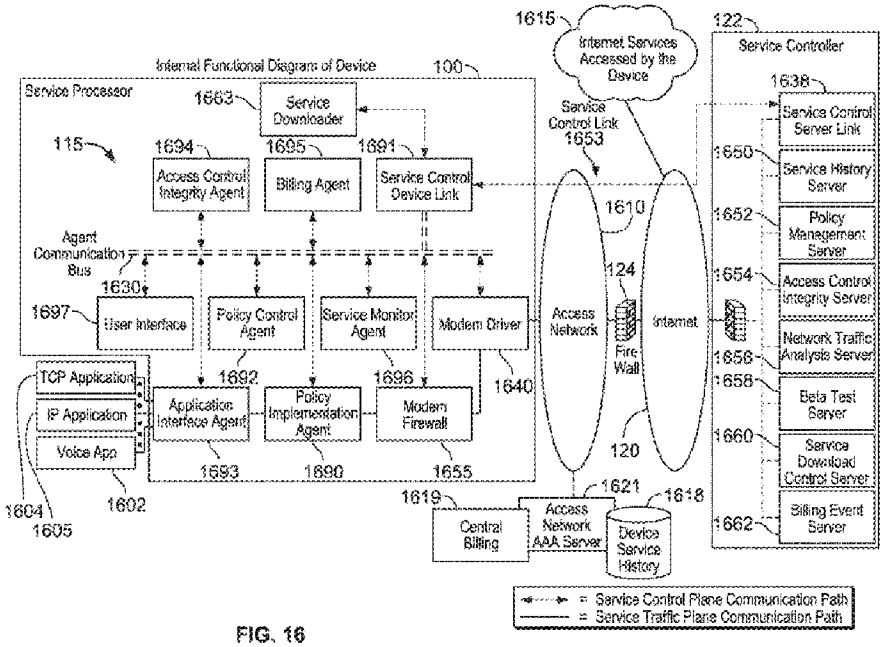


FIG. 16

Malek Decl. at ¶ 37; Ex. A, 37:26-42:58. Here, the service processor 115 includes a "Service Control Device Link" 1691 that links to a "Service Control Server Link" 1638 of the service controller 122 through a "Service Control Link" 1653. *Id.* 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. Finally, the end-user device 100 includes service control device link 1691, which 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:

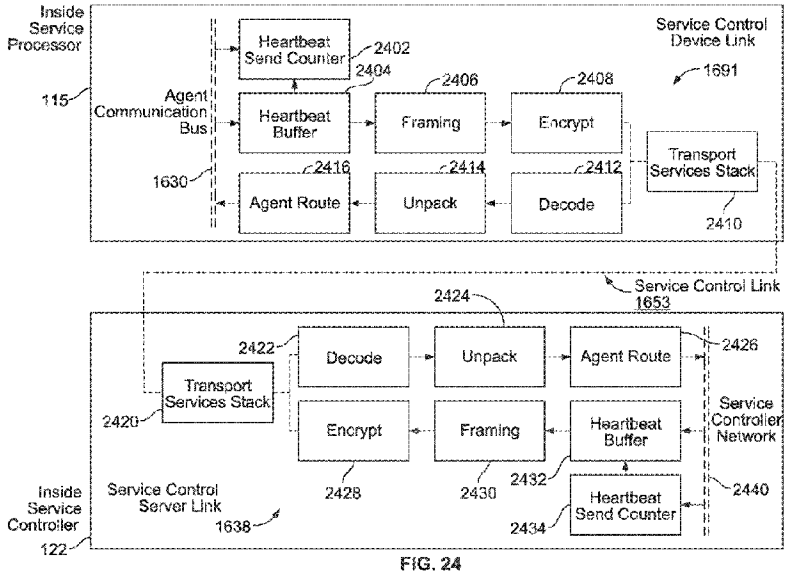


FIG. 24

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. 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 '320 Patent, as evidenced by the explicit statement that the "Transport

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 21 of 114

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 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):

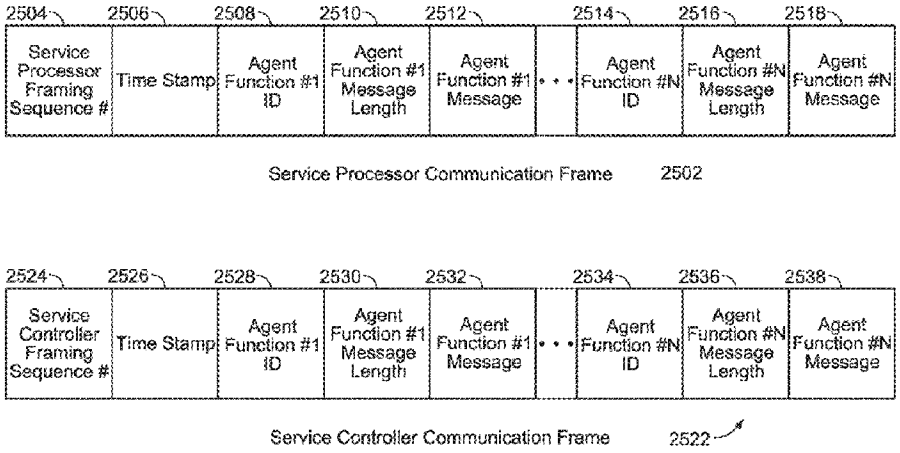


FIG. 25

This was a standard way of addressing messages long before the time that the applications that led to the '320 Patent were filed. *Id.* Communications from the end-user device 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 '320 Patent

Independent claim 1 of the '320 Patent is a system claim. Claims 2-18 depend from claim 1. The following chart lists the Challenged Claims (*i.e.*, claims 1-18), with the element-by-element breakdown used throughout the Request.

Claim Element #	Limitation
1[PRE]	A networked system comprising:
1[a]	i) a network server system including a link interface to maintain a respective secure Internet data message link between the link interface 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 messages via the device link agent on that device;
1[c]	a network interface to receive messages from a plurality of network elements, for delivery to respective ones of the software components identified in the messages, each network element authorized to send messages via the link interface to one or more of the software components on one or more of the wireless end-user devices; 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 any of the wireless end-user devices,
1[e]	the logic to determine when one of a plurality of message delivery triggers for a 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 for the given one of the wireless end-user devices, the logic further to supply one or more messages comprising the buffered content for the given one of the wireless end-user devices 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; and
1[g]	ii) the device link agents on the respective wireless end-user devices, each of the device link agents configured to maintain the respective secure Internet data message link over a wireless network to the link interface,
1[h]	receive secure Internet data messages from the network server system over the respective secure Internet data message link, including messages collected from multiple ones of the network elements and messages corresponding to multiple ones of the software components authorized to receive messages via the device link agent on that respective device,

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 23 of 114

1[i]	wherein at least a first subset of the secure Internet data messages contain both a unique identifier for a corresponding one of the software agents and data to be consumed by that software component, the data supplied from a respective network element corresponding to that software component, and
1[j]	for software components that are authorized to access messages received via the device link agent, cause messages with a unique identifier corresponding to a given one of those software applications to be securely delivered to a software process corresponding to the given software component.
Claim 2	
2	The networked system of claim 1, the message buffer system logic to determine, for each of the wireless end-user devices, when one of a plurality of message delivery triggers has occurred, at least one of the triggers for each given device specific to one or more states of that given device.
Claim 3	
3	The networked system of claim 1, wherein one of the message delivery triggers is the expiration of a periodic timer.
Claim 4	
4	The networked system of claim 3, wherein the period of the timer is fractionally shorter than a maximum data message interval beyond which the Internet data message link to the given device is taken down.
Claim 5	
5	The networked system of claim 1, wherein one of the message delivery triggers is the receipt of a transmission on the respective secure Internet data 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 6	
6	The networked system of claim 1, wherein one of the message delivery triggers is a heartbeat message generated by the given device link agent, or a request received from the given device link agent.
Claim 7	
7	The networked system of claim 1, wherein one of the message delivery triggers is the receipt of a particular message from one of the network elements.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 24 of 114

Claim 8	
8	The networked system of claim 1, further comprising a secure server to store a secure authorization list, the secure authorization list indicating the authorized software components and the authorized network elements that are allowed to communicate using the network server system.
Claim 9	
9	The networked system of claim 8, further comprising the respective device link agent on each wireless end-user device receiving access authorization information from the secure server, the access authorization indicating, respectively for each wireless end-user device, the software components authorized to receive messages via the device link agent on that device.
Claim 10	
10	The networked system of claim 1, wherein a second subset of the secure Internet data messages contain a user message from a network element, the user message intended for display on a user interface of a given one of the wireless end-user devices.
Claim 11	
11	The networked system of claim 1, wherein one of the software components on a given one of the wireless end-user devices is a policy control agent, and the data to be consumed by the policy control agent comprises service settings and/or configuration information for the given device.
Claim 12	
12	The networked system of claim 1, the link interface to encrypt messages identified for delivery to each given one of the wireless end-user devices to create secure Internet data messages, the device link agent on each given device further configured to decrypt the received secure Internet data messages for that device prior to delivering those messages to a respective software process.
Claim 13	
13	The networked system of claim 12, wherein the encrypted messages are transported to the device link agent using one or more of encryption on a transport services stack, IP (Internet Protocol) layer encryption, and tunneling.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 25 of 114

Claim 14	
14	The networked system of claim 1, wherein the device link agent on a given device executes in a secure execution environment, and at least one of the software components on that device executes outside of the secure execution environment.
Claim 15	
15	The networked system of claim 1, wherein the device link agent on a given one of the devices is further configured to receive, from one or more of the software components on that device, upload messages, each of the upload messages identifying a corresponding one of the network elements to which the device respective software component has requested delivery, the device link agent on that device transmitting the upload messages to the network message server over the respective secure Internet data message link, for delivery by the network message server to the respective identified network elements.
Claim 16	
16	The networked system of claim 15, the device link agent on the given device further configured to buffer one or more of the upload messages for transmission to the network message server at a time selected by a heartbeat mechanism.
Claim 17	
17	The networked system of claim 1, at least a given one of the devices further comprising a secure interprocess communication service separately secured from the secure Internet data message link, the device link agent for the given device causing messages to be securely delivered to a software process by initiating delivery of each such message on the secure interprocess communication service.
Claim 18	
18	The networked system of claim 1, wherein at least one of the secure Internet data messages comprises multiple identifier/data pairs.

2. Prosecution History of U.S. Application No. 15/582,350

As filed on April 28, 2017, the singular, original claim of the '350 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, p. 3. More than three months later, Patent Owner filed a Preliminary Amendment, cancelling the sole claim filed, and adding new claims 2-19, the scope of which significantly deviated from the original claim filed. *Id.* at pp. 9-16.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 26 of 114

At the time of filing its Preliminary Amendment, Patent Owner filed five (5) IDS forms, citing more than 1,200 U.S. patents and publications, over 90 foreign references, and over 50 non-patent literature documents. Patent Owner later filed four more IDS forms, citing more than 100 more patent references and six (6) foreign patent documents. The Examiner indicated that he considered each reference cited by Patent Owner and cited an additional 13 references. No reference identified in this request for *ex parte* reexamination request was ever considered by the Examiner during prosecution of the '350 Application.

During prosecution, the Examiner did not issue any office actions and issued a notice of allowance on April 4, 2019. *Id.*, p. 20. The notice of allowance simply stated that claims 2-19 were allowed over all the cited prior art, whether considered individually or in combination. *Id.*, p. 25.

3. Prior *Inter Partes* Review Proceedings

a. *Amazon.com Servs., LLC, et al. v. Headwater Rsch. LLC*, IPR2026-00106

Amazon.com Services, LLC and Amazon Web Services, Inc. (collectively, "Amazon") filed a petition for *inter partes* review of claims 1-18 of the '320 Patent on November 10, 2025. Ex. Q. Amazon relied on a number of prior art 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. 2008/0243999 (Pazhyannur);
- U.S. Pub. No. 2009/0158397 (Herzog);
- U.S. Pub. No. 2008/0215883 (Fok); and
- U.S. Pub. No. 2008/0162637 (Adamczyk).

Id., p. 2. Patent Owner filed its Request for Discretionary Denial on January 20, 2026. Amazon filed its Opposition to Patent Owner's Request on February 20, 2026. On March 10, 2026, the Director indicated pursuant to 35 U.S.C. § 314(a), after review of discretionary considerations, IPR2026-00106 will be reviewed for merits and non-discretionary considerations. Patent Owner

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 27 of 114

did not file a Patent Owner Preliminary Response. The Director or the Board is expected to issue an institution decision by May 20, 2026. This IPR is still pending, and as such, the Board has not issued a final written decision.

b. *Target Corp. v. Headwater Rsch. LLC*, IPR2026-00153

Target Corporation filed a petition for *inter partes* review of claims 1-18 of the '320 Patent on November 25, 2025. Ex. R. Target relied on a number of prior art 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. 2008/0243999 (Pazhyannur);
- U.S. Pub. No. 2009/0158397 (Herzog);
- U.S. Pub. No. 2008/0215883 (Fok); and
- U.S. Pub. No. 2008/0162637 (Adamczyk).

See id., p. 2. Patent Owner filed its Request for Discretionary Denial on February 2, 2026. Target filed its Opposition to Patent Owner's Request on March 2, 2026. On March 10, 2026, the Director discretionarily denied institution of IPR2026-00153 under 35 U.S.C. § 314(a). As of the date of this request for *ex parte* reexamination, IPR2026-00153 is not moving forward, and as such, the Board has not issued, and will not issue, a final written decision.

4. Prior Relevant Federal District Court Litigation

Patent Owner has asserted the '320 Patent against numerous entities in the Eastern and Western Districts of Texas and the Northern District of California, 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 '320 Patent remain open and pending as of the date of filing of this request:

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 28 of 114

Federal District Court Litigation
Headwater Rsch. LLC v. Google LLC, No. 3:26-cv-01460 (N.D. Cal. May 16, 2025) (transferred from W.D. Tex. Feb. 26, 2026)
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) (Case CLOSED Nov. 4, 2025 following pre-trial settlement)
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.*

5. Related *Ex Parte* Reexamination of '192 and '117

There are co-pending *ex parte* reexaminations of related patents U.S. Pat No. 9,198,117 and U.S. Pat No. 9,615,192. Both of those patents have nearly identical specifications to the '320 patent and contain numerous identical or overlapping claim elements. In both of those reexamination proceedings, a Substantial New Question of patentability was determined:

Ex Parte Reexamination of Related Patents
Serial No. 90/015,831 (Reexamination of U.S. Pat No. 9,615,192)
Serial No. 90/019,753 (Reexamination of U.S. Pat No. 9,198,117)

C. Overview of Cited Art and SNQs Raised

The following references are cited herein as prior art. Only Exhibits L and O have been cited in other proceedings relating to the '320 Patent, and those references are presented herein only in combination with other references that have never been considered by the USPTO.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 29 of 114

Exhibit	Overview of the Cited Art
Ex. C	*Rittmaster* published on February 21, 2002 from U.S. Patent Application No. 09/812,296, filed on March 20, 2001. *Rittmaster* qualifies as prior art under § 102(b)[1].
Ex. D	*Konstantinov* published on November 30, 2006 from U.S. Patent Application No. 11/231,858, filed on September 22, 2005. *Konstantinov* qualifies as prior art under § 102(b).
Ex. E	*Distributed Systems* is a second edition textbook, with a copyright date of 2007. *Distributed Systems* qualifies as prior art under § 102(b).
Ex. F	*Computer Networks* is a fourth edition textbook, with a copyright date of 2003. *Computer Networks* qualifies as prior art under § 102(b).
Ex. K	*Klassen* issued November 22, 2011, from U.S. Patent Application No. 11/584,418, filed on October 19, 2006. *Klassen* qualifies as prior art under § 102(e).
Ex. L	*Ellison* issued July 25, 2006, from U.S. Patent Application No. 09/668,610, filed on September 22, 2000. *Ellison* qualifies as prior art under § 102(b).
Ex. M	*Freese* issued February 27, 2007, from U.S. Patent Application No. 10/363,040, filed on February 28, 2003. *Freese* qualifies as prior art under § 102(b).
Ex. N	*Moon* issued July 4, 2000, from U.S. Patent Application No. 08/955,974, filed on October 22, 1997. *Moon* qualifies as prior art under § 102(b).
Ex. O	*Fok* published on September 4, 2008 from U.S. Patent Application No. 11/947,738, filed on November 29, 2007 and claiming priority to provisional applications dated December 5, 2006 and March 14, 2007. *Fok* qualifies as prior art under § 102(e).
Ex. S	*Coffee* published on June 15, 2006 from U.S. Patent Application No. 11/190,236, filed on July 26, 2005. *Coffee* qualifies as prior art under § 102(b).

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

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 30 of 114

Ex. T	*Basso* published on May 19, 2005 from U.S. Patent Application No. 10/713,343, filed on November 14, 2003. *Basso* qualifies as prior art under § 102(b).
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 '320 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 example, 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 basic communication system in which a server 12 is connected to a plurality of user devices 14-16 through a network 18 (*e.g.*, the Internet):

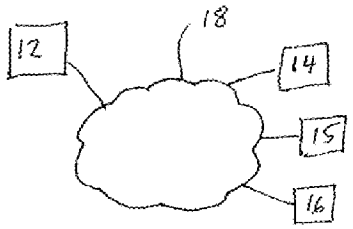


Fig. 1

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)." Ex. C, ¶ 42; Malek Decl. at ¶ 44.

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.*):

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 31 of 114

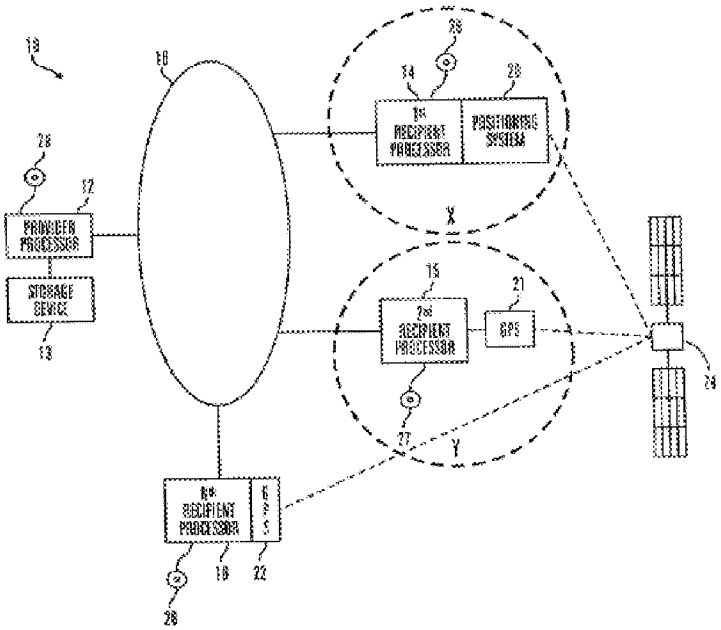


FIG. 2.

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.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 32 of 114

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). Malek Decl. at ¶ 46.

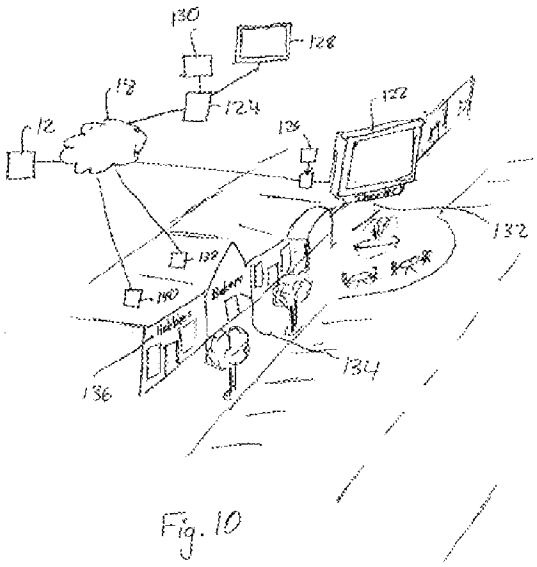


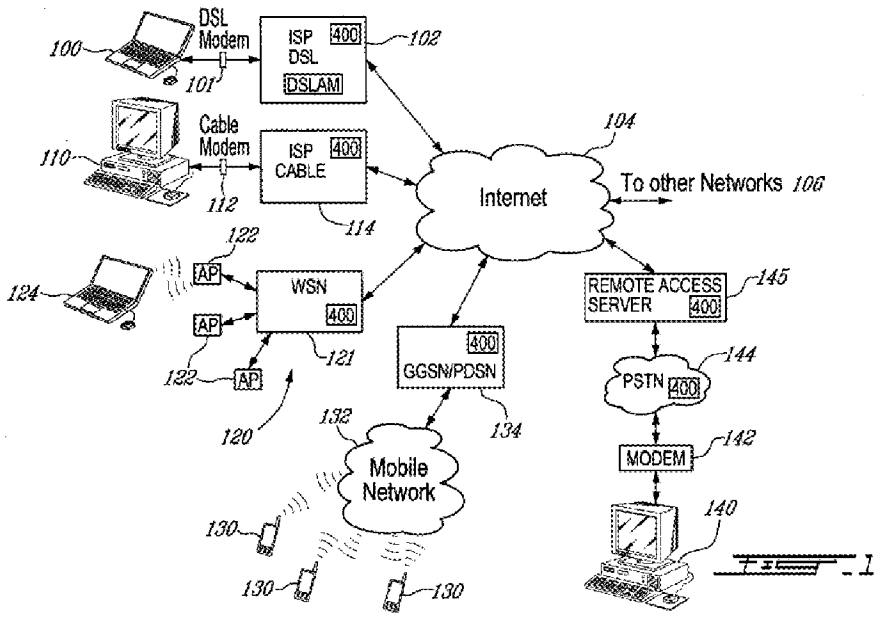
Fig. 10

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.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 33 of 114

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. Ex. D; Malek Decl. at ¶ 50. 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 ¶ 50; 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 ¶ 50; 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 ¶ 50; 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 ¶ 51. For instance, Fig. 3 shows that each data packet includes, in addition to a "payload"

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 34 of 114

(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):

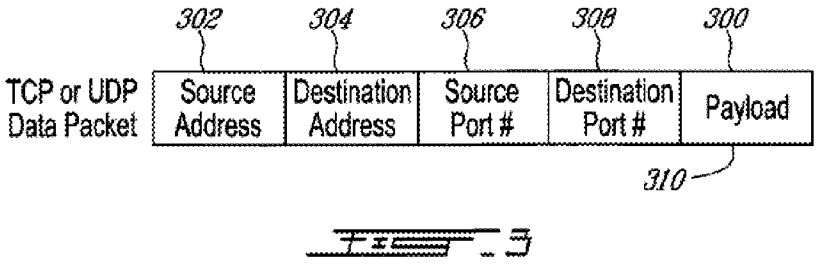


Fig. 3

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 ¶ 56. 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. *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 ¶ 57. 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 things, that as of at least 2003 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.*

[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.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 35 of 114

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:

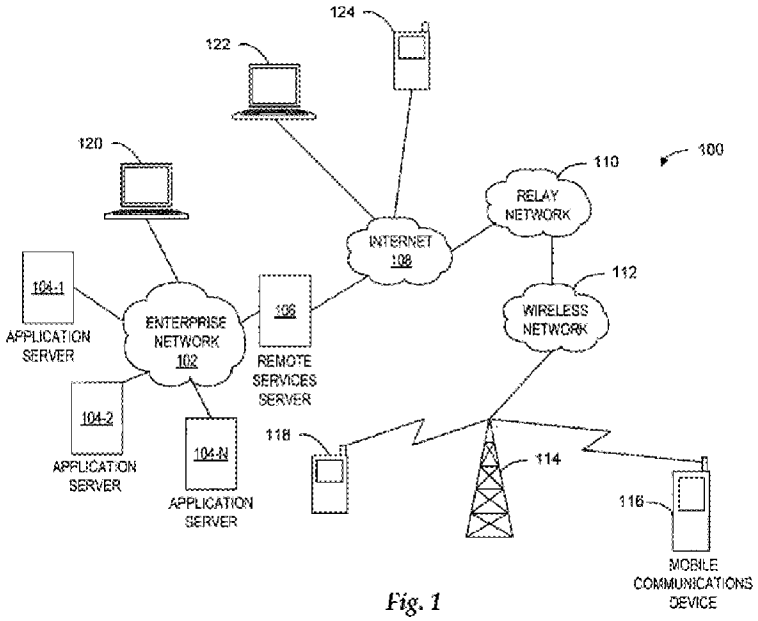


Fig. 1

Ex. K, Fig. 1; Malek Decl. at ¶ 52. 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 ¶ 52. 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 ¶ 102; 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. Ex. L, 1:41-51. The division of a component into rings is typically based on the degree or level of privilege. *Id.*, 1:51-53.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 36 of 114

7. U.S. Patent No. 7,184,554 ("*Freese*") (Ex. M)

Freese recognizes the need to manage mobile devices from a remote location in order to add, remove, or modify software. *Freese* discloses a Public Land Mobile Network (PLMN) 1 connected to wireless devices 2 and 4:

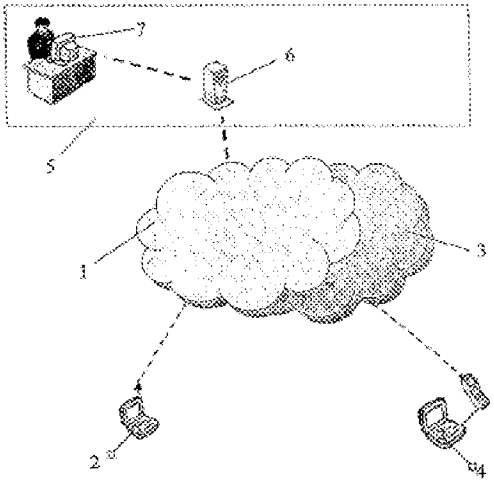


Figure 1

Ex. M, Fig. 1; Malek Decl. at ¶ 96. The network illustrated above in Fig. 1 also includes a "Management Centre" 5 that includes a "Management Server" 6 and "Management Console" 7. Ex. M, 3:18-35. This management centre manages mobile devices such as phones, PDAs, and laptops that are connected to a network. *Id.*, 1:6-10. A management agent program is stored on the end-user device to monitor the status of applications installed on the device and receive management instructions to manage applications accordingly. *Id.*, 1:24-40. This allows the device software architecture to be modified remotely by operators or authorized third parties, for instance to turn applications on or off by sending an appropriate management instruction to the end-user device. *Id.*, 1:46-57. "An important function of the management agent is that of reporting to the Management Centre 5" which "allows the Management Centre 5 to maintain an accurate record of the status of a mobile device." *Id.*, 4:33-38. This includes reported information such as "successful installation of a new application, or the failure of an instructed installation." *Id.* Control of software applications on the end-user device through the management centre can be, for instance, based on whether a license to the software is current or expired, turning the software on or off accordingly. *Id.*, 4:11-18. The management instructions sent from the management server to the end-user device are preferably cryptographically signed, demonstrating that the management server is secure. Malek Decl. at ¶ 96.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 37 of 114

8. U.S. Patent No. 6,085,098 ("*Moon*") (Ex. N)

Moon discloses automatically configuring settings of software applications on a portable device such as a smartphone based on geographic location. Ex. N, Abstract, 4:36-5:35; Malek Decl. at ¶ 100. For instance, settings need to be updated for phone dialer software or calendar software as geographic location of a user device (such as a mobile phone) changes. *Id.* 5:6-23.

9. U.S. Patent Pub. No. 2008/0215883 ("*Fok*") (Ex. O)

Fok describes techniques for "secure inter-application communication" in a "mobile operating environment." Ex. O, ¶¶ 36-37, 81, 106-108, Figs. 4 and 8-9. Fok uses a "round trip" concept where a "handshake" is established between a "primary application" and one or more "recipient" applications. *Id.*, ¶¶ 47-53, 96-102, 106-108, Figs. 7-10. Applications verify that another application is trusted during the handshake process using "a list of unique identifiers" associated with trusted applications installed on the mobile device. *Id.*, ¶¶ 48-50, 96, 101-102, 106, Figs. 8-9.

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 ¶ 105; 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 ¶ 105; 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 fewer messages to be sent and improved performance of the system. *Id.*

12. AU App. No. 2007200530 ("*Shenfield*") (Ex. U)

Just like the '320 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 ¶ 47; Ex. U, Fig. 1. *Shenfield* discloses the delivery and processing of push content communicated from a server to a mobile station. Malek Decl. at ¶ 47; Ex. U, Abstract. One such network is shown below in Figure 1:

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 38 of 114

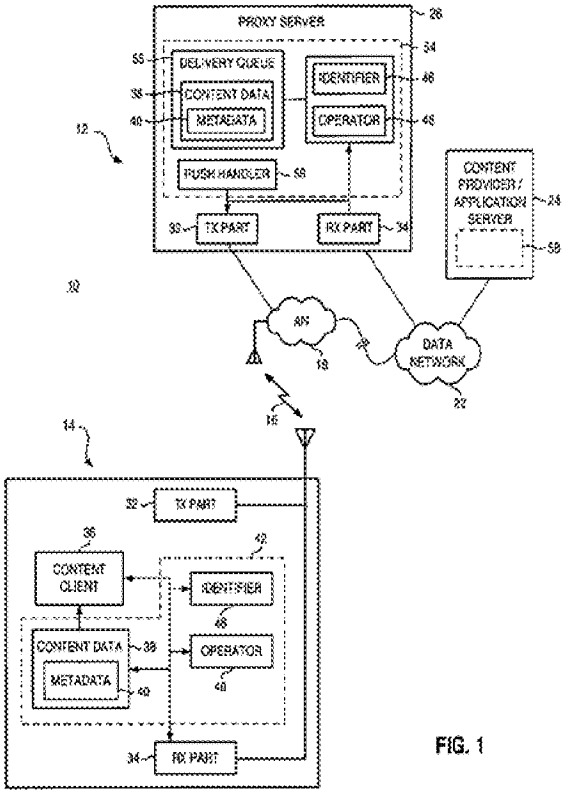


FIG. 1

Malek Decl. at ¶ 47; 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 ¶ 47. Notably, the proxy server can communicate content to multiple mobile stations and multiple applications (software components) within each mobile station. Malek Decl. at ¶ 47. 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 ¶ 48; Ex. U, ¶ 34. Figure 2, below, shows the communication layer that receives content pushed from the push handler of the proxy server.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 39 of 114

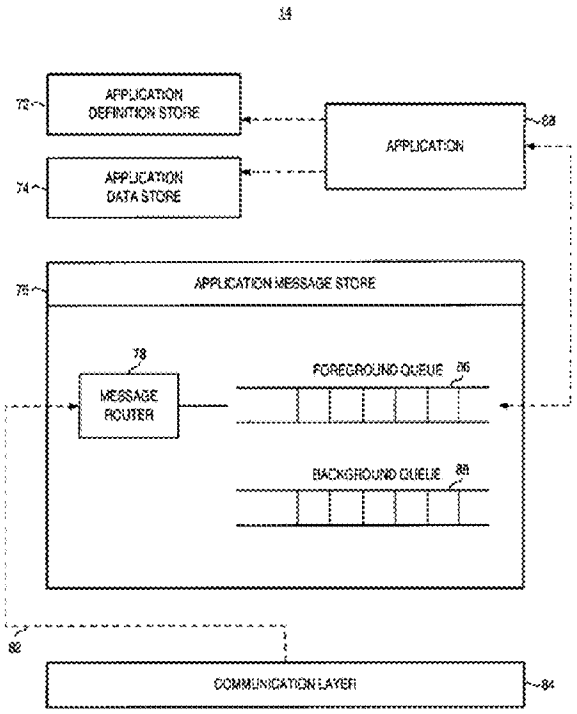


FIG. 2

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 ¶ 48; 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 ¶ 49; 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 ¶ 49; 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.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 40 of 114

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*) was presented to the Office during prosecution of the '350 Application or during any *inter partes* review proceeding.[4] While secondary references *Ellison* and *Fok* were relied on by Target and Amazon in support of their respective petitions for *inter partes* review of the '320 Patent, the grounds presented herein that rely in part on those references assert combinations that were not presented or considered in those petitions or any other *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, 10, 12-13, and 15-18 of the '320 Patent are anticipated by *Rittmaster*; (2) how claims 1-7, 10, 12-13, and 15-18 of the '320 Patent are obvious in view of *Rittmaster* and the knowledge of a PHOSITA (as evidenced by the *Distributed Systems* and/or *Computer Networks* textbooks); (3) how claims 1-7, 10, 12-13, and 15-18 of the '320 Patent are obvious in view of the combination of *Rittmaster* and *Shenfield*; (4) how claims 1-7, 10, 12-13, and 15-18 of the '320 Patent are obvious in view of the combination of *Rittmaster* and/or *Shenfield*, and *Klassen* and *Konstantinov*; (5) how claims 8-9 of the '320 Patent are obvious in view of the combination of *Rittmaster* (Grounds 1-4) and *Freese*; (6) how claim 11 of the '320 Patent is obvious in view of the combination of *Rittmaster* (Grounds 1-4) and *Freese* and/or *Moon*; (7) how claim 14 of the '320 Patent is obvious in view of the combination of *Rittmaster* (Grounds 1-4) and *Ellison*; (8) how claim 17 of the '320 Patent is obvious in view of the combination of *Rittmaster* and *Ellison* and/or *Fok*; and (9) how claim 18 of

[4] All of the references applied to independent claim 1 were, however, cited in *Ex Parte Reexamination* 90/015,831, in which a substantial new question of patentability was found as to very similar claims of U.S. Patent No. 9,615,192 on each of the prior art combinations cited.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 41 of 114

the '320 Patent is obvious in view of the combination of *Rittmaster* (Grounds 1-4) and *Coffee* and/or *Basso*.

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 time of the alleged invention of the '320 Patent 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) regarding patents in the same family as the '320 Patent. Ex. G. The court construed the terms "software components" and "device link agent" 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. Additionally, in *Headwter Rsch. LLC v. Amazon.com Serv's LLC, et al.*, No. 7:25-cv-00286-ADA (W.D. Tex.), while the court has not yet issued a Claim Construction Order, the parties completed *Markman* briefing on February 25, 2026 (Dkt. Nos. 40, 42). *See* Exs. V, W. The only term at issue is "fractionally shorter." *Id.*

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 42 of 114

1. "software components"

The term "software components" appears in claims 1, 4, and 15. Patent Owner has previously admitted that "software components" has a plain meaning to a skilled artisan in connection with related patents. Ex. G, p. 17. The court agreed and construed the term "software components" to be "components of software." *Id.* at pp. 17-18, 19. The broadest reasonable interpretation of "software components" is at least as broad as "components of software."

2. "device link agent"

While the term "device link agent" as contained in independent claim 1 and dependent claims 5, 6, 9, 11-17 has not been previously construed, the similar term "device messaging agent" as used in related U.S. Patent No. 9,198,117 (the "'117 Patent") to Raleigh was construed to mean "a piece of software on a mobile end-user device that performs certain messaging functions for other software." Ex. G p. 19. Similarly, the term "device agents" as used in related U.S. Patent No. 8,406,733 to Raleigh was construed to have the nearly identical definition of "a piece of software on the end-user device that performs certain functions for other software." The '117 Patent, the '733 Patent, and the '320 Patent share priority to the same four provisional applications and share the same disclosure. Ex. G, p. 1. While those definitions are not binding here, the meaning of "device link agent" should be at least as broad as those definitions.

3. "wherein the period of the timer is fractionally shorter than a maximum data message interval"

As noted above, the Western District of Texas has not yet construed the term "wherein the period of the timer is fractionally shorter than a maximum data message interval." In its opening claim construction brief, Amazon argued that the entire limitation, and especially the term "fractionally shorter" is indefinite because "a POSITA would not be able to determine the scope and, in particular, the outer bounds of 'fractionally shorter' with reasonable certainty." Ex. V, p. 3 (citing *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 901 (2014)). In its responsive claim construction brief, Patent Owner asserts the "fractionally shorter" language is definite, and the language means "the message delivery trigger occurs *just before or immediately before* the message link is taken down." Ex. W, p. 2 (emphasis in original). But Patent Owner relies solely on extrinsic evidence, alleging that "numerous dictionary definitions" support its position "that 'fractional' means 'very small,' 'tiny,' or 'insignificant'" without acknowledging other dictionary definitions reproduced in Amazon's brief. *Id.*, p. 3; Ex. V, pp. 3-4.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 43 of 114

Even if Patent Owner is correct in the context of district court litigation, for the purpose of determining whether a substantial new question of patentability exists the USPTO must apply the *broadest* reasonable meaning to the claim language. The broadest reasonable interpretation must conform to the invention as set forth in the remainder of the specification. MPEP § 2111; 37 CFR § 1.75(d)(1). Here, neither the words "fractional" nor "fractionally" appear in the specification of the '320 Patent, and there is no discussion of a periodic timer being "shorter" than a maximum data message interval at all. Nevertheless, even assuming that the claim language requires that messages are designed to be sent shortly before a link to the server is terminated, claim 4 that contains this language is invalid for reasons discussed herein.

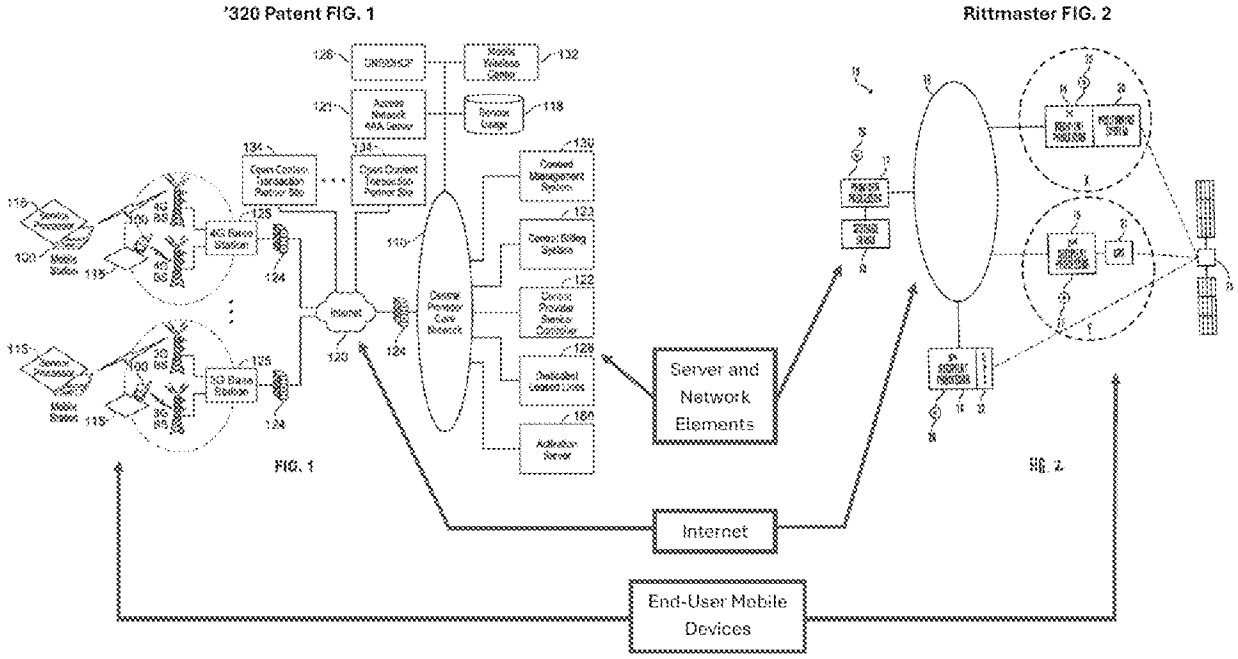
C. Ground 1: Claims 1-3, 5-7, 10, 12-13, and 15-18 are Anticipated by *Rittmaster*

Rittmaster discloses all elements of claims 1-3, 5-7, 10, 12-13 and 15-18 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 '320 Patent.

More specifically, all of the claims of the of the '320 Patent relate to networked system comprising (i) a network server system that includes a link interface to maintain links to end-user devices, a network interface to receive messages from network elements, and a message buffer system, and (ii) device link agents on respective end-user devices that maintain a secure link to the server's link interface, receive secure messages over that link, and cause messages with a unique identifier corresponding to a given software application to be delivered to that application. Malek Decl. at ¶ 53. Such a server system 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 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 '320 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 well-known and available at the time of the earliest effective filing date of the '320 Patent, as discussed in Ground 2.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 44 of 114

To better demonstrate the similarities between the system architectures of the '320 Patent and *Rittmaster*, an annotated comparison of Fig. 1 of the '320 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 (indicated by arrows labeled "End-User Mobile Devices"), communicating to a content provider server (indicated by arrows labeled "Server and Network Elements") through the Internet (indicated by arrows labeled "Internet"):



1. Claim 1

a. 1[PRE] *"A networked system comprising:"*

The preamble of claim 1 recites a "**networked system**." Like the '320 Patent, *Rittmaster* discloses a network including a server for providing message content that is linked to user devices. Malek Decl. at ¶ 54. Fig. 2 illustrates that the *Rittmaster* provider server 12 maintains links with any number of recipients (end-user devices 14, 15, 16):

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 45 of 114

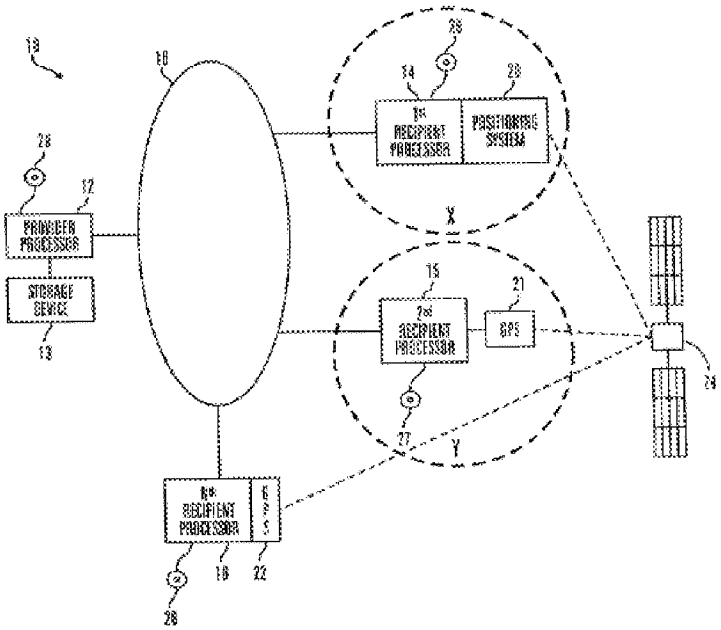


FIG. 2

Malek Decl. at ¶ 54; 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] ***"i) a network server system including a link interface to maintain a respective secure Internet data message link between the link interface and a respective device link agent on each of a plurality of wireless end-user devices,"***

Rittmaster discloses element 1[a] of the '320 Patent. As shown above, *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." Malek Decl. at ¶ 55; Ex. C, ¶ 42. The end-user devices may be "portable communication devices." Malek Decl. at ¶ 55; Ex. C, ¶¶ 126-27. *Rittmaster* does not outline specific software and protocols for sending and receiving messages but does state 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 ¶ 55; Ex. C, ¶ 42.

Rittmaster also explicitly describes a "secure internet data message link" because the server sends content "in an encrypted format." Malek Decl. at ¶ 55; 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, disclosing use of "a

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 46 of 114

secure Internet data message link" as recited in claim 1 of the '320 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." Ex. C, ¶ 42; Malek Decl. at ¶ 55. *Rittmaster* does, however, explicitly disclose a message link agent as in the '320 Patent and that software is responsible for maintaining a link, *e.g.*, through the Internet, between the link interface 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, 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 technique." Ex. C, ¶¶ 84-87. This corresponds to the "Device Link" 1691 shown in Fig. 24 of the '320 Patent, which serves to receive and decrypt messages before they are transported to the appropriate software program, as shown below:

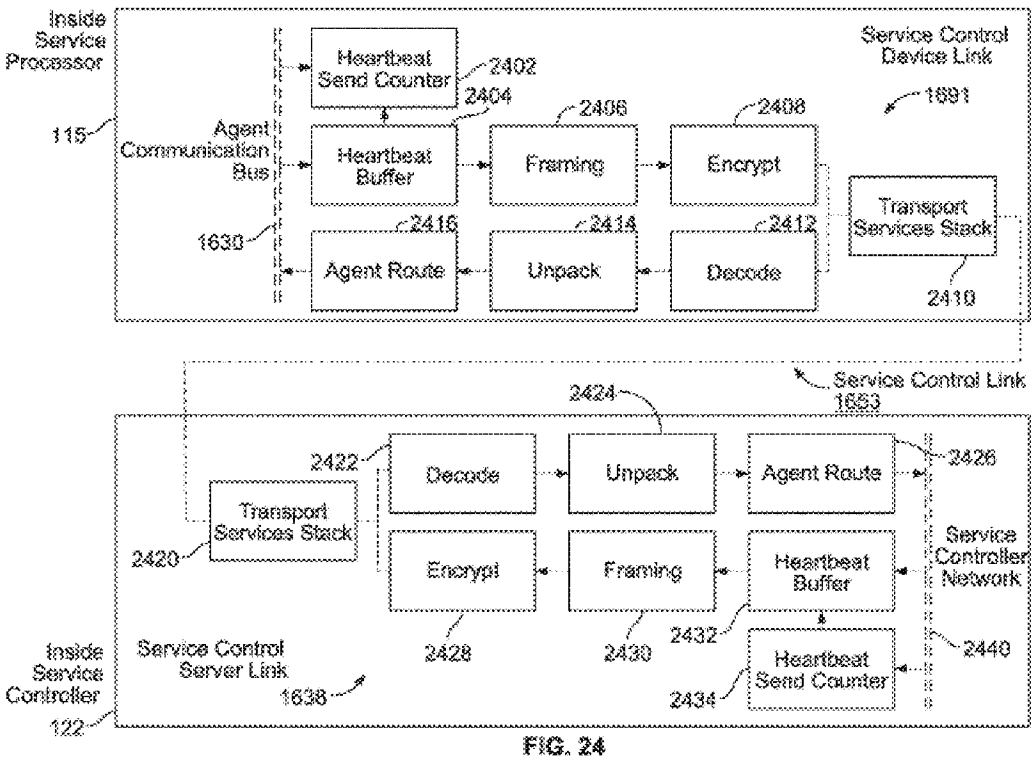


FIG. 24

Ex. A, Fig. 24; *see also* Ex. A, 90:52-64 (including "…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" Ex. C, ¶ 81.

Further, the '320 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 ¶ 64; 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 '320 Patent, and would further have recognized that a "link interface" at the server and "message link agent" on the end-user device would have been inherent (necessarily present) because that was the standard for communication over the internet. Malek Decl. at ¶ 64.

Rittmaster's disclosure of a device link agent on a user device is further described below in Section II.C.1.g. (claim element 1[f]). *Rittmaster's* disclosure of a respective secure message link maintained by the link interface is further described below in Section II.C.1.d. In short, however, communication over the Internet "would have inherently (necessarily) been between an interface (*e.g.*, a transport services stack) on the server and a link agent (*e.g.*, software program) on the mobile devices," as shown by basic textbooks such as *Distributed Systems*. Malek Decl. at ¶ 56; Ex. E, p. 584.

c. 1[b] *"each of the wireless end-user devices comprising multiple software components authorized to receive messages via the device link agent on that device;"*

Rittmaster further discloses element 1[b] of the '320 Patent. *Rittmaster* specifies that in some instances "the recipient processors comprise online user terminals, including, but not limited

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 48 of 114

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 ¶ 57; 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…." 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, which comprises "a hardware, firmware, software or hybrid decryption system for performing decryption operations in accordance with any suitable decryption technique." Ex. C, ¶¶ 84-87, Fig. 7. As discussed in the previous section, this performs the same functions as the "Device Link" shown in the '320 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 ¶ 57. *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.

d. 1[c] *"a network interface to receive messages from a plurality of network elements, for delivery to respective ones of the software components identified in the messages, each network element authorized to send messages via the link interface to one or more of the software components on one or more of the wireless end-user devices; and"*

Element 1[c] requires that the network-facing side of the server include an "interface" to receive messages from two or more "network elements," for delivery to specific software components that are identified in the messages. Malek Decl. at ¶ 58. This does little more than describe the basic manner in which messages were delivered from a network at the relevant time (January 2009), and how messages are still delivered today. *Id. Rittmaster* explicitly discloses

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 49 of 114

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 ¶ 58; Ex. C, ¶ 33. This necessarily includes an "interface" connecting the server to each suitable source, because communication through a secure Internet connection between a server and an end-user device (as in *Rittmaster*) broadly involves transmission of a message through a link from an interface on a server. Malek Decl. at ¶ 64. *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 time. Malek Decl. at ¶ 58; 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 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 ¶ 58. 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." Malek Decl. at ¶ 58; 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." Malek Decl. at ¶ 58; Ex. C, ¶ 125.

Messages from network elements may include, for instance, "promotional or advertisement information for a plurality of different establishments within the same shopping area." Malek Decl. at ¶ 58; 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." Malek Decl. at ¶ 58; 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. Malek Decl. at ¶ 58; Ex. C, ¶ 125.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 50 of 114

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 ¶ 58. 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, p. 340; Malek Decl. at ¶ 58. Including the address in the message ensures the message content is delivered to the appropriate software application. *Id.*

The message 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 Section I.C.4., 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 ¶ 58. This is verified by textbooks such as *Computer Networks*, 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, 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 also could be simultaneously limited by the server based on the user's geographic position. Ex. C, ¶ 112.

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 any 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 ¶ 59. For instance, Fig. 2 below illustrates a storage device 13

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 51 of 114

(*i.e.*, a memory) associated with the server 12, which may store messages prior to sending them to end-user devices:

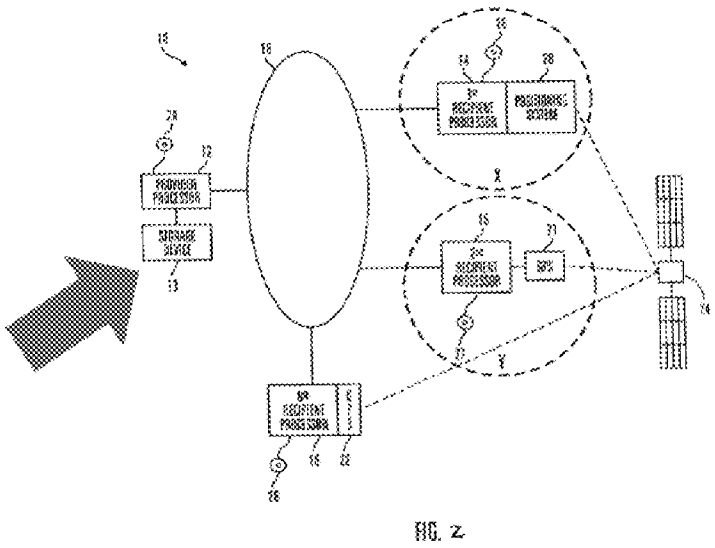


FIG. 2

Id.; Ex. C, Fig. 2 (annotated).

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. Malek Decl. at ¶ 60. 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 ¶ 60; 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 ¶ 60; Ex. C, ¶ 53. As such, the logic of the server determines in what region a particular user device is located. Malek Decl. at ¶ 60. *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 ¶ 60; Ex. C, ¶ 53.

Executing the foregoing logic results in buffering of messages to the end user until the system determines that the end-user device is located in an appropriate geographic region. Malek Decl. at ¶ 61 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

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 52 of 114

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 ¶ 61; Ex. C, ¶ 33. On the other hand, if the end-user device is located in a restricted region, messages are held until the device enters a non-restricted region. Advertisements from different establishments may be communicated to the provider server 12 "and stored in advance." Malek Decl. at ¶ 61; 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 ¶ 61; 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 ¶ 61; Ex. C, ¶¶ 120-21 Thus, *Rittmaster* explicitly discloses buffering content, and at a minimum buffering is involved in the storage and conditional transmission and display of content.

f. 1[e] ***"the logic to determine when one of a plurality of message delivery triggers for a 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 '320 Patent because providing content to an end-user device is dependent on one or more triggers. Malek Decl. at ¶ 62. 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 receipt of a message alone is not a trigger. *Id.*; Ex. C, ¶ 14. In addition, some 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. *Id.*, ¶ 14.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 53 of 114

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 the claim element 1[e] specifically requiring an "**asynchronous event with time-critical messaging needs**," a 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).[5] Malek Decl. at ¶ 63. This is consistent with the '320 Patent's disclosure, which 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 ¶ 63; Ex. A, 38:59-63. Furthermore, in litigation with Samsung on related patents having nearly identical specifications (including related U.S. Patent No. 9,615,192), 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 related '192 Patent, petitioner Samsung noted that the patent owner both (i) directly admitted that a message retrieval request from the user constitutes a message delivery trigger and (ii) 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)).

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**

[5] A PHOSITA would not only 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. The triggers of *Rittmaster* rely on the sending of information from the recipient to the network server, and, like the "transaction or service billing event" and "user requests" mentioned in the'320 Patent, 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.*

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 54 of 114

period, which a PHOSITA would understand to be a trigger with "time-critical messaging needs." Malek Decl. at ¶ 63; 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 ¶ 63; Ex. C, ¶ 66.

g. **1[f]** ***"upon determining that one of the message delivery triggers has occurred for the given one of the wireless end-user devices, the logic further to supply one or more messages comprising the buffered content for the given one of the wireless end-user devices 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; and"***

Rittmaster also discloses element 1[f] of claim 1 because, as discussed in the previous two sections, the system determines if certain criteria are met before sending messages from a memory of the server to the end-user device. 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 ¶ 64. 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 '320 Patent. Other possible triggers are receipt of a request within a given time period, verifying a minimum user age, or other suitable criteria. Malek Decl. at ¶ 64; Ex. C, ¶ 14.

h. **1[g]** ***"ii) the device link agents on the respective wireless end-user devices, each of the device link agents configured to maintain the respective secure Internet data message link over a wireless network to the link interface,"***

Rittmaster also discloses element 1[g] of claim 1. As explained above, *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." Malek Decl. at ¶ 65; Ex. C, ¶ 42. *Rittmaster* does not explicitly state that the secure link is maintained by a "device link agent" on the mobile devices over a wireless network to the "link interface" on the server, but a PHOSITA would have easily recognized that communication over the internet would have inherently been between a stack or interface on the server and a software program on the mobile devices. Malek Decl. at ¶ 65. Communication over the internet would have inherently involved the claimed "device link agents" maintaining the "secure Internet data message link" to the "link interface" by

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 55 of 114

virtue of using the widely known TLS and SSL protocols. *Id.*; Ex. E, p. 584. Further, under the broadest reasonable interpretation of this claim language, all that is required is that an element of the server of each end-user device is capable of maintaining a secure link with an element of the server, which is undoubtedly the case in *Rittmaster*. Therefore, communication over the Internet would have inherently involved the claimed "device link agents" maintaining the "secure Internet data message link" to the "link interface" by virtue of using the widely known TLS and SSL protocols. *Id.*

i. 1[h] "[each of the device link agents configured to] *receive secure Internet data messages from the network server system over the respective secure Internet data message link, including messages collected from multiple ones of the network elements and messages corresponding to multiple ones of the software components authorized to receive messages via the device link agent on that respective device,"*

Rittmaster also discloses element 1[h] of claim 1. *Rittmaster* 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…)." Malek Decl. at ¶ 66; Ex. C, ¶ 33. Messages from network elements may include, for instance, "promotional or advertisement information for a plurality of different establishments within the same shopping area." Malek Decl. at ¶ 66; 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." Malek Decl. at ¶ 66; Ex. C, ¶ 121. A PHOSITA would understand that mobile end-user devices such as laptops or phones each contain a plurality of software components each associated with a port number, and *Rittmaster* also identifies various types of content that may be received by those different software applications on the user device, such as video, movies, video games, or software. Malek Decl. at ¶¶ 57, 66. Thus, a PHOSITA would understand that *Rittmaster* discloses messages collected from multiple network elements and sent to multiple software components on end-user devices that are authorized to receive those messages.

j. 1[i] *"wherein at least a first subset of the secure Internet data messages contain both a unique identifier for a corresponding one of the software agents and data to be consumed by that software component, the data supplied from a respective network element corresponding to that software component, and"*

Rittmaster also discloses element 1[i] because messages sent by the server must necessarily be directed to the software agents and contain data to be consumed by the software components.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 56 of 114

That is simply how communications to laptops, cellular phones, and other computing devices is accomplished over the internet. Malek Decl. at ¶¶ 57-58. Specifically, as discussed in detail above, messages are routed to mobile devices over the internet using an identifier consisting of an IP address (identifying a specific device) and a port number (identifying a specific software location on the device). *Id.;* Malek Decl. at ¶ 67. The combination of IP address and port number in the message header is therefore a "unique identifier" because it is specific to one and only one copy of a software application – a copy of software located at a specific port on a specific device. *Rittmaster* also states that "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." Malek Decl. at ¶ 67; Ex. C, ¶ 125. This advertising information (data) from computers associated with the shopping establishments (network elements) would necessarily include an identifier for the specific user device and for the location of specific software necessary to display the advertising. Malek Decl. at ¶ 67. "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." *Id.*; Ex. C, ¶ 123. In other words, message content is delivered from the provider processor 12 in the form of a message sent to end-user devices, and every message from an online source delivered through *Rittmaster*'s network server (provider processor 12) to user devices necessarily would 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 was how all messages were already directed from provider servers to end-user devices (*e.g.,* in 3G or 4G networks) long prior to the '320 Patent. Malek Decl. at ¶ 67; *See*, *e.g.*, Ex. F, p. 340. The address is included in the message so that the message content is delivered to both the correct user device and the appropriate software application for that message type.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 57 of 114

k. 1[j] "[each of the device link agents configured to] *for software components that are authorized to access messages received via the device link agent, cause messages with a unique identifier corresponding to a given one of those software applications to be securely delivered to a software process corresponding to the given software component."*

Claim element 1[j] is disclosed because the provider processor 12 of *Rittmaster* delivers messages to end-user devices with multiple software applications such as cellular phones or laptops, and every message delivered through *Rittmaster*'s network server to end-user devices necessarily would 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 was already how messages were directed from provider servers to user devices at the relevant time prior to the '320 Patent. Malek Decl. at ¶¶ 57, 58, 57, and 68; Ex. F, p. 340. The messages must be received at a link agent responsible for maintaining a connection to the server and then would be distributed internally to the appropriate software program. The address is included in the message so that the message content is delivered from the software responsible for receiving incoming messages to the appropriate software application for that message type. Malek Decl. at ¶ 68. A software process is an operating system construct that contains a running program together with its own private address space, resources (such as memory mappings, file descriptors, and security credentials), and scheduling state. Malek Decl. at ¶ 68. In modern operating systems, software components/applications are executed through one or more such processes, and execution of the programs comprising a software component/application necessarily occurs within a software process managed by the operating system. Malek Decl. at ¶ 68.

2. Claim 2 – *"the message buffer system logic to determine, for each of the wireless end-user devices, when one of a plurality of message delivery triggers has occurred, at least one of the triggers for each given device specific to one or more states of that given device."*

Claim 2 depends from claim 1. *Rittmaster* clearly discloses a buffer system using a set of rules or logic to determine when one or more specific end-user devices are authorized to receive the message (e.g., such as end-user device "states" that include being located in a specific geographic region having previously sent a request to the server). Malek Decl. at ¶ 69. *Rittmaster* states that "a set of rules may be implemented, which depend upon the geographic information

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 58 of 114

(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 ¶ 69; Ex. C, ¶ 40. Further, *Rittmaster* states that in preferred embodiments, "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, under control of a routine of software 29 (as represented by step 22 in FIG. 3)." Malek Decl. at ¶ 69; Ex. C, ¶ 53. The determination of whether to send a message based on the geographic location of an end-user device is a "trigger…specific to one or more states of that given device" as required by claim 2. Malek Decl. at ¶ 69.

Rittmaster also discusses other triggers that are based on "states" of the end-user devices. Malek Decl. at ¶ 70. The '320 Patent discloses examples of device "states" such as online/offline, active and suspended, in that "[i]n some embodiments, a device is suspended based on inactivity, or the device is placed in a suspended service state or suspended account state," and "The device account and/or activation state can be re-activated when the device comes back online." Malek Decl. at ¶ 70; Ex. A, 125:20-43. Similarly, *Rittmaster* indicates that in some instances messages may only be triggered where an account associated with a particular device is in good standing, such as where "the content provider maintains an account record for pre-paid amounts" so that "the content provider may determine whether the user making the request has enough funds in the corresponding user account." Malek Decl. at ¶ 70; Ex. C, ¶ 114. Thus, *Rittmaster* discloses triggers based on device "states" in the same way as the '320 Patent and specifically as recited in claim 2.

3. Claim 3 – *"wherein one of the message delivery triggers is the expiration of a periodic timer."*

Claim 3 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 ¶ 71; Ex. C, ¶ 14. 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[f] and 1[g]. Malek Decl. at ¶ 71.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 59 of 114

4. Claim 5 – *"wherein one of the message delivery triggers is the receipt of a transmission on the respective secure Internet data 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 5 depends from claim 1 and is disclosed by *Rittmaster* because one possible trigger is the user requesting a product or service. Malek Decl. at ¶ 73; Ex. C, ¶¶ 74-76 and Fig. 6. In some embodiments, the end-user device sends information regarding the physical location of the user or advertising preferences to the network, leading to receipt of specific advertising content from the server. Malek Decl. at ¶ 73; Ex. C, ¶¶ 132-42.

5. Claim 6 – *"wherein one of the message delivery triggers is a heartbeat message generated by the given device link agent, or a request received from the given device link agent."*

Claim 6 depends from claim 1. A PHOSITA would understand claim 6 to mean that the user device periodically sends a request to the server, such as "pinging" the server with specific information with respect to a request. Malek Decl. at ¶ 74. *Rittmaster* discloses that 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." Malek Decl. at ¶ 74; Ex. C, ¶ 69. These multiple periodic communications issued from the end-user device would be a heartbeat message that acts as a trigger to cause delivery of content form the server to the user device that is issuing the heartbeat messages. Malek Decl. at ¶ 74.

6. Claim 7 – *"wherein one of the message delivery triggers is the receipt of a particular message from one of the network elements."*

Claim 7 depends from claim 1. Receipt of information from a network element is necessary for embodiments of *Rittmaster* where the server obtains information from network elements and then sends such information to user devices. Malek Decl. at ¶ 75. "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. In such an

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 60 of 114

embodiment, 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 ¶ 75; Ex. C, ¶ 121.

Furthermore, additional instructions from network elements to the server may 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 ¶ 75; 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.*

7. Claim 10 – *"wherein a second subset of the secure Internet data messages contain a user message from a network element, the user message intended for display on a user interface of a given one of the wireless end-user devices."*

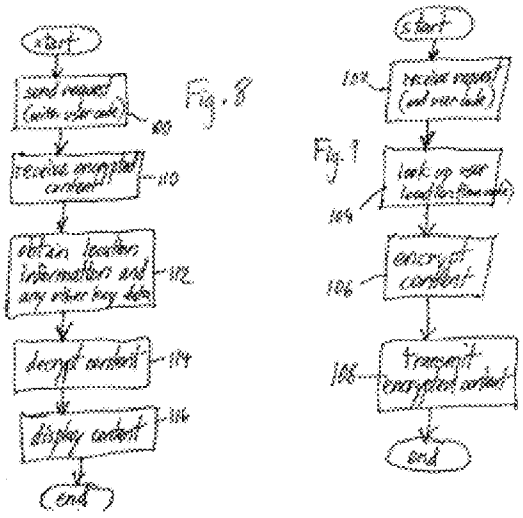
Claim 10 depends from claim 1 and is disclosed by *Rittmaster*, which states that "establishments may have communicated advertisement information to the provider processor 12 [server], from suitable computers 138 and 140 [network elements]" (Ex. C, ¶ 121) and then "each advertiser may control the general time at which the advertiser's message will be displayed, for example, by communicating instructions to the provider processor 12…from the advertiser's computer 138 or 140." Malek Decl. at ¶ 76; Ex. C, ¶ 124. *Rittmaster*'s end-user devices can include personal computers, portable communication devices, or vehicle-mounted computers which can have "user-operated input devices" such as a "touchscreen," thus disclosing that the user messages that are transmitted to the end-user devices can be "intended for display on a user interface." Malek Decl. at ¶ 76; Ex. C, ¶ 35-36. Even if "user message" is viewed to have a narrow meaning, even though the term does not appear in the '320 Patent's specification, in some cases the displayed message is a message intended to alert the user as to the status of a request or ability to receive certain content, for instance a "denied access" message that is displayed to the user on the device's screen in place of requested content. Ex. C, ¶ 73. Thus, at a minimum *Rittmaster* discloses a first

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 61 of 114

subset of messages relating to advertising and a second subset of messages relating to user alerts, satisfying claim 10.

8. Claim 12 – *"the link interface to encrypt messages identified for delivery to each given one of the wireless end-user devices to create secure Internet data messages, the device link agent on each given device further configured to decrypt the received secure Internet data messages for that device prior to delivering those messages to a respective software process."*

Claim 12 depends from claim 1, which is disclosed by *Rittmaster* because content from the network server is encrypted prior to transmission to end-user devices, and the content is decrypted upon receipt by end-user devices prior to delivery to specific software. Malek Decl. at ¶ 77. For instance, Figs. 8 and 9 illustrate the process of encrypting and decrypting messages. "FIG. 8 represents an example process carried out by a recipient processor [end-user device], while FIG. 9 represents an example process carried out by the content provider processor [server], as part of the same content communication transaction." Malek Decl. at ¶ 77; Ex. C, ¶ 89. These processes are shown below:



(Ex. C, Figs. 8 and 9). Once the end-user device makes a request (step 100), the server receiving the request (step 102) determines user location (step 104), and if the trigger is satisfied encrypts content (step 106) and transmits the encrypted content (step 108) to the end user device. The end-user device receives the encrypted content (step 110), and then decrypts (step 114) and displays the content (step 116). Malek Decl. at ¶ 77; Ex. C, ¶¶ 98-99. Encryption and decryption are accomplished by an encryption algorithm of the provider processor (server) (Ex. C, ¶ 97) and

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 62 of 114

"decryption module" 90 of the end-user device, respectively, which would qualify as a link interface and device link agent as claimed. Malek Decl. at ¶ 77.

9. Claim 13 – *"wherein the encrypted messages are transported to the device link agent using one or more of encryption on a transport services stack, IP (Internet Protocol) layer encryption, and tunneling."*

Claim 13 depends from claim 12. Communications in *Rittmaster* would have used IETF-standardized TLS, creating an encrypted channel at the transport layer (i.e., TCP) and thereby encrypting on the transport services stack. Malek Decl. at ¶ 78. *Rittmaster* expressly describes using one or more keys to encrypt content, which would necessarily include the payload of the message to be sent by the server. Malek Decl. at ¶ 78; Ex. C, ¶¶ 97-98. These keys, for instance, could be derived from location information and/or a user code. *Id.* Further, the '320 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 ¶ 78; Ex. A, 89:26-29. The *Computer Networks* textbook shows that the claimed layers of encryption were baseline knowledge to a PHOSITA at the relevant time, and further describes IPsec (IP Security), which was a popular secure communication protocol operating at the IP layer. Malek Decl. at ¶ 78; Ex. F, pp. 596-599.

10. Claim 15 – *"wherein the device link agent on a given one of the devices is further configured to receive, from one or more of the software components on that device, upload messages, each of the upload messages identifying a corresponding one of the network elements to which the device respective software component has requested delivery, the device link agent on that device transmitting the upload messages to the network message server over the respective secure Internet data message link, for delivery by the network message server to the respective identified network elements."*

Claim 15 depends from claim 1, and is disclosed by *Rittmaster* in multiple situations in which the end-user device provides information to the server. Malek Decl. at ¶ 79. For instance, geographic location and/or user preferences may be transmitted from the user to a provider computer. Malek Decl. at ¶ 79; Ex. C, ¶¶ 13-14 and 142. Advertiser computers (network elements) may access information regarding data transmitted from end-user devices in order to determine when advertising messages are to be sent. Malek Decl. at ¶ 79; Ex. C, ¶ 142. This would have involved the upload of the messages from the end-user device to the advertiser computers. Malek Decl. at ¶ 79. In the case of an advertising network, this would allow advertiser computers to be able to track which end-users are to receive specific types of message content and to determine

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 63 of 114

when a specific number of end-users are within a specified geographic area. *Id.* In one embodiment, *Rittmaster* discloses that "the provider processor issues a query or command to the requesting recipient computer to provide the user code" in response to which "the recipient computer communicates the user code to the provider processor," and the provider processor also "provide[s] the user code as part of or in association with the request for the content" sent to the network computer providing the content. Malek Decl. at ¶ 79; Ex. C, ¶¶ 96-97. Therefore, not only does the 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 form that element. Malek Decl. at ¶ 79. Further, "unlike current advertising modalities, but in accordance with embodiments of the invention, the selection of the commercial, promotional or informational content to include in the interleaved break(s) may be determined, in whole or part, by the physical location of the user." Malek Decl. at ¶ 79; Ex. C, ¶ 132. Therefore, the *Rittmaster* server may also deliver "upload messages" from specific software on a user device to a specified network element, such as by sending a message containing a user code or user preference to a computer associated with a specific establishment that provides content to users. Malek Decl. at ¶ 79.

11. Claim 16 – *"the device link agent on the given device further configured to buffer one or more of the upload messages for transmission to the network message server at a time selected by a heartbeat mechanism."*

Claim 16 depends from claim 15, and is disclosed by *Rittmaster* in at least 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." Malek Decl. at ¶ 80; Ex. C, ¶ 69. Receipt of these multiple periodic requests uploaded to the server from an end-user device would be a heartbeat mechanism that acts as a trigger to cause delivery of content from the server to the user device issuing the heartbeat messages. Malek Decl. at ¶ 80. A PHOSITA also would

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 64 of 114

understand this to mean that messages are buffered by the end-user device until they are ready to be transmitted at predetermined periodic intervals. *Id.*

12. Claim 17 – *"at least a given one of the devices further comprising a secure interprocess communication service separately secured from the secure Internet data message link, the device link agent for the given device causing messages to be securely delivered to a software process by initiating delivery of each such message on the secure interprocess communication service."*

Claim 17 depends from claim 1. Although *Rittmaster* does not disclose how messages are distributed within the end-user device itself, a PHOSITA would know that the "device link agent" would deliver messages to identified software on the same device. Malek Decl. at ¶ 81. In view of *Rittmaster's* disclosure of a "decryption module," transmission of messages to applications on the end-user device would be separately secured from the secure Internet data message link. *Id.*

13. Claim 18 – *"wherein at least one of the secure Internet data messages comprises multiple identifier/data pairs."*

Claim 18 depends from claim 1. To the extent that this claim indicates that a single message contains two or more payloads each associated with an identifier, this claim is disclosed in view of *Rittmaster* alone. Malek Decl. at ¶ 82. *Rittmaster* describes this element by discussing an embodiment where 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 comprise information, such as promotional or advertisement information for a plurality of different establishments within the same shopping area." Malek Decl. at ¶ 82; 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.*

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 1-7, 10, 12-13, and 15-18

To the extent one might argue that protocol-level details such as a "transport services stack" or "device link agent" are not strictly inherent in *Rittmaster*, 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

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 65 of 114

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 (i) a direct acknowledgement that missing protocol-level details would have been obvious and (ii) 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 hardware and network communication details such as those discussed in widely-available prior art textbooks.

1. Claim 1

a. 1[PRE] *"A network server system comprising:"*

As discussed above, 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 ¶ 54.

b. 1[a] *"i) a network server system including a link interface to maintain a respective secure Internet data message link between the link interface 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 ¶ 55. To the extent, however, that specific protocols for sending or receiving messages are considered 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 ¶ 55. This is especially true in view of *Rittmaster*'s invitation to use "communication interfacing" that was "well known in the art." Malek Decl. at ¶ 55; Ex. C, ¶ 42.

In addition, to the extent *Rittmaster* is considered to lack an explicit disclosure of the secure Internet data message link existing between a "link interface" on the server and a "device link agent" on the mobile devices, a PHOSITA would have found it obvious to provide the link between an interface (e.g., transport services stack) on the server and a link agent (e.g., software program) on the mobile devices. Malek Decl. at ¶ 56. Likewise, even if a "secure" Internet data message

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 66 of 114

link between the link interface 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)[6]. *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 ¶ 56. The *Distributed Systems* textbook explains the importance of maintaining a secure communication link between server and client devices on the Internet. *See Distributed Systems*, Ex. E, p. 584; Malek Decl. at ¶ 56. *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:

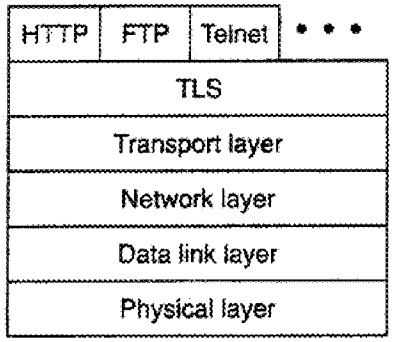


Figure 12-22. The position of TLS in the Internet protocol stack.

Ex. E, p. 584; Malek Decl. at ¶ 56. 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 and a software program on client devices. Malek

[6] 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.

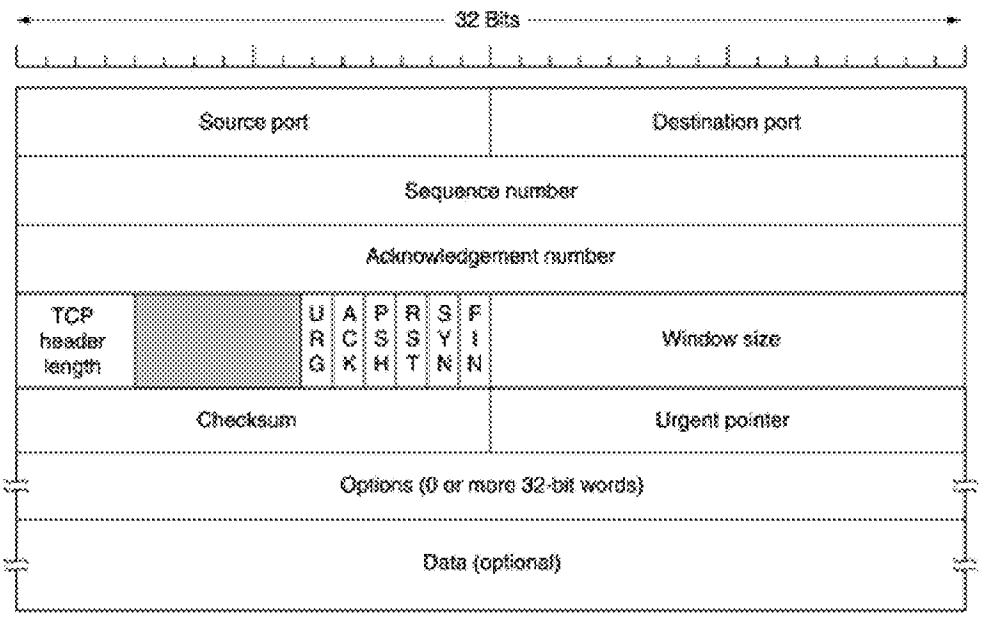
Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 67 of 114

Decl. at ¶ 56. 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.* Messages are directed over a secure link to a network layer of the recipient device, referred to by the '320 Patent as a "device link agent." Malek Decl. at ¶ 65; Ex. E, p. 584. A PHOSITA would have found it extremely obvious prior to the critical date of the '320 Patent to employ the foregoing protocols to maintain a secure connection between a network interface and a mobile device link agent because having a secure connection of this type 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.*

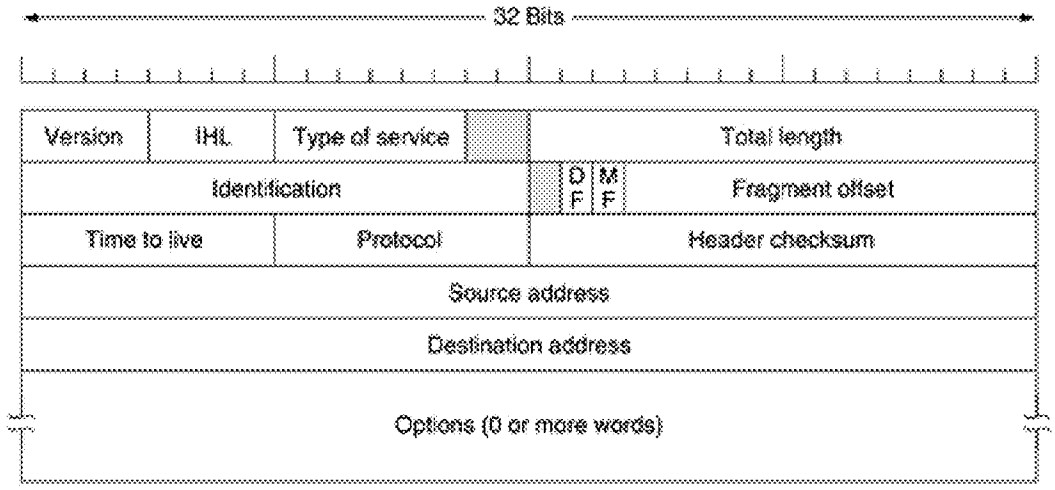
c. 1[b] *"each of the wireless end-user devices comprising multiple software components authorized to receive messages via the device link agent on that device;"*

Rittmaster also discloses claim 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 ¶ 57. 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 ¶ 57. 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). *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, p.340; Malek Decl. at ¶ 57. 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.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 68 of 114



Ex. F, p. 410; Malek Decl. at ¶ 57. 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, pp. 329-330; Malek Decl. at ¶ 57.



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] *"a network interface to receive messages from a plurality of network elements, for delivery to respective ones of the software components identified in the messages, each network element authorized to send messages via the link interface to one or more of the software components on one or more of the wireless end-user devices; and"*

Rittmaster discloses claim element 1[c]. *See supra* Section II.C.1.d. This element requires that the network-facing side of the server include a "network interface" to receive messages from two or more "network elements," for delivery to specific software components that are identified in the messages. Malek Decl. at ¶ 58. This does little more than describe the basic manner in which all messages were delivered to a server from networked 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…)." 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 ¶ 58. These establishment-owned computers coupled to the network are inherently authorized to send messages via the link interface to one or more software components on a wireless end-user device because *Rittmaster's* system is able to send advertising content from the networked computers to end-user devices such as cellular phones through the network server. 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 ¶ 58. *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 ¶ 58. "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; Malek Decl. at ¶ 58.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 70 of 114

Even if *Rittmaster* were considered not to expressly or inherently disclose the elements of 1[c], 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. Malek Decl. at ¶ 58. 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 ¶ 58. Ex. F, 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 ¶ 55.

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 any of the wireless end-user devices,"*

Rittmaster discloses claim 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 ¶ 59. 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 ¶ 59. *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 process), 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 ¶¶ 60 - 61; 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,

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 71 of 114

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 ¶ 60; Ex. C, ¶ 53. 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 he requested product or service." Malek Decl. at ¶ 61; Ex. C, ¶ 56

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 ¶ 61. 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 ¶ 61; 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 ¶ 61; 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 ¶ 61. 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 ¶ 61; Ex. F, p. 408.

f. **1[e]** ***"the logic to determine when one of a plurality of message delivery triggers for a 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 claim element 1[e] for the reasons discussed above in Ground 1. *See supra* Section II.C.1.f.; *see also* Malek Decl. at ¶¶ 62-63. 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

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 72 of 114

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 ¶ 62; 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 ¶ 61; Ex. C, ¶ 56. All of the foregoing triggers require more than receipt of a message.

While *Rittmaster* primarily discusses geographic location, additional triggers are also 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 ¶ 62; 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 merely 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).[7] Malek Decl. at ¶ 63. Further reinforcing the time-criticality of

[7] This is consistent with how the patent owner appears to have interpreted the term, because the '320 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 ¶ 63; 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 related 9,615,192 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 ¶ 63; Ex. H (Samsung

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 73 of 114

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 ¶ 63; 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 ¶ 63; Ex. C, ¶ 66.

g. 1[f] *"upon determining that one of the message delivery triggers has occurred for the given one of the wireless end-user devices, the logic further to supply one or more messages comprising the buffered content for the given one of the wireless end-user devices 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; and"*

Rittmaster discloses claim element 1[f] for the reasons discussed above. *See supra* Section I.C.1.g.; *see also* Malek Decl. at ¶ 64. As discussed above relative to element 1[f], messages are sent when the logic determines that one or more 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 device link agent on one of a plurality of end-user devices. *See supra* Section I.C.1.g.

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 '320 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. 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, p. 28 ("Layer n on one machine carries on a conversation with layer n on another machine"). It would have been obvious to incorporate such well-known network features given *Rittmaster's* suggestion to incorporate communication interfacing well known in the art.

Reply Brief in IPR2024-00010, Paper 16 at p. 4); see also Malek Decl. at ¶ 63; Ex. I (PO Response Brief in IPR2024-00010, Paper 12) and Malek Decl. at ¶ 63; 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 9,615,192 patent.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 74 of 114

h. 1[g] *"ii) the device link agents on the respective wireless end-user devices, each of the device link agents configured to maintain the respective secure Internet data message link over a wireless network to the link interface,"*

Rittmaster discloses claim element 1[g] for the reasons discussed above. *See supra* Section II.C.1.h.; *see also* Malek Decl. at ¶ 65. *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." Malek Decl. at ¶ 65; Ex. C, ¶ 42. While *Rittmaster* does not explicitly state that the secure link is maintained by a "device link agent" on the mobile devices over a wireless network to the "link interface" on the server, those skilled in the art would have easily recognized that communication over the Internet would have inherently (necessarily) been between an interface on the server and a device link agent on the mobile devices. Malek Decl. at ¶ 65. Therefore, communication over the Internet inherently would have involved the claimed "device link agents" maintaining the "secure Internet data message link" to the "link interface" by virtue of using the widely known TLS and SSL protocols. *Id.*; Ex. E, p 584. Even if it could be argued that a network could have been operated without the foregoing protocols, and to the extent *Rittmaster* is considered to not necessarily involve a secure connection, a PHOSITA would have found it extremely obvious to have a secure connection between a link interface on the server and a mobile device link agent that is maintained long enough to send and/or receive messages because having such a secure connection was standard and broadly recognized as superior to an unsecured connection. Malek Decl. at ¶ 65 At a minimum, at the relevant time it would have been viewed as unusual not to have a secure connection to a network. *Id.*

i. 1[h] *"[each of the device link agents configured to] receive secure Internet data messages from the network server system over the respective secure Internet data message link, including messages collected from multiple ones of the network elements and messages corresponding to multiple ones of the software components authorized to receive messages via the device link agent on that respective device,"*

Rittmaster discloses claim element 1[h] for the reasons discussed above. *See supra* Section II.C.1.i.; Malek Decl. at ¶ 66. *Rittmaster* 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…)." Malek Decl. at ¶ 66; Ex. C, ¶ 33. *Rittmaster* further states that messages from network elements may include, for instance, "promotional or advertisement information for a plurality of

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 75 of 114

different establishments within the same shopping area." Malek Decl. at ¶ 66; 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." Malek Decl. at ¶ 66; Ex. C, ¶ 121. For the reasons discussed above, a PHOSITA would have understood that mobile end-user devices such as laptops or phones each contain a plurality of software components each associated with a port number, and *Rittmaster* also identifies various types of content that may be received by those different software applications on the user device, such as video, movies, video games, or software. Malek Decl. at ¶ 66. Advertisements and other information from computers 138 and 140 are "messages collected from multiple ones of the network elements" and the different formats of these messages indicates that they are "messages corresponding to multiple ones of the software components authorized to receive messages via the device link agent on that respective device," Therefore, a PHOSITA would understand that *Rittmaster* discloses messages collected from multiple network elements and send to multiple software components authorized to receive those messages. *Id.*

j. 1[i] *"wherein at least a first subset of the secure Internet data messages contain both a unique identifier for a corresponding one of the software agents and data to be consumed by that software component, the data supplied from a respective network element corresponding to that software component, and"*

Rittmaster discloses claim element 1[i] for the reasons discussed above. *See supra* Section II.C.1.j.; Malek Decl. at ¶ 67. However. even if *Rittmaster* were considered not to expressly or inherently disclose this limitation, a PHOSITA would have recognized that it would have been extremely obvious to implement standard message formats for communication through servers over the Internet at the relevant time, which would have included those features. *Id.* 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 "[t]ogether, these **ports serve to identify** the processes using the connection on both ends." (emphasis added) Malek Decl. at ¶ 67. *See* Ex. F, p. 340. In fact, *Rittmaster* explicitly suggests using this type of "communication interfacing" that was "well known in the art," and therefore did not include basic details of its messaging system because they were so well-known in the art. Malek Decl. at ¶ 55; Ex. C, ¶ 42.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 76 of 114

k. 1[j] "[each of the device agents configured to] *for software components that are authorized to access messages received via the device link agent, cause messages with a unique identifier corresponding to a given one of those software applications to be securely delivered to a software process corresponding to the given software component.*"

Rittmaster discloses the final claim 1 element 1[j] for the reasons discussed above. *See supra* Section II.C.1.k.; Malek Decl. at ¶ 68. As discussed above in Section II.D.1.j., every message from an online source delivered through *Rittmaster*'s network server (provider processor 12) to user devices necessarily would 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 ¶ 68; *see, e.g.*, Ex. F, p. 340. For instance, it was textbook knowledge that "[e]ach outgoing TCP message contains both a source port and a destination port" and that "[t]ogether, these ports serve to identify the processes using the connection on both ends." (emphasis added) Malek Decl. at ¶ 67. *See* Ex. F, p. 340. This would therefore be a unique identifier to a specific software process located on a specific end-user device. The address is included in the message so that the message content is delivered from the software responsible for receiving incoming messages to the appropriate software application for that message type. Malek Decl. at ¶ 68. A PHOSITA would have recognized that it would have been extremely obvious to implement standard message formats for communication through servers over the Internet and within user devices that were routinely employed at the relevant time, which would have included those features. *Id.* Moreover, *Rittmaster* explicitly suggests implementing such "communication interfacing" that was "well known in the art," and therefore did not include basic details of its messaging system because they were so well-known in the art. Malek Decl. at ¶ 55; Ex. C, ¶ 42. In addition, a PHOSITA would have understood that, for a message to be delivered to a software component or software application, the message must ultimately be delivered to one of the software processes implementing that component or application. Malek Decl. at ¶ 68. A software process is an operating system construct that contains a running program together with its own private address space, resources (such as memory mappings, file descriptors, and security credentials), and scheduling state. *Id.* In modern operating systems, software components/applications are executed

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 77 of 114

through one or more such processes, and execution of the programs comprising a software component/application necessarily occurs within a software process managed by the operating system. *Id.*

2. Claim 2 – *"the message buffer system logic to determine, for each of the wireless end-user devices, when one of a plurality of message delivery triggers has occurred, at least one of the triggers for each given device specific to one or more states of that given device."*

Claim 2 depends from claim 1, and its subject matter is disclosed by Rittmaster for reasons discussed above. *See Supra* Section II.C.2. *Rittmaster* clearly discloses a buffer system using a set of rules or logic to determine when one or more specific end-user devices are authorized to receive the message, such as by virtue of the user being located in a specific geographic region, the server receiving a request from a user, or the server receiving an instruction from a networked content provider. Malek Decl. at ¶ 69-70; Ex. C, ¶¶ 40, 53, and 114.

3. Claim 3 – *"wherein one of the message delivery triggers is the expiration of a periodic timer."*

Claim 3 depends from claim 1. This additional element is disclosed in *Rittmaster*, as explained in Section II.C.3., *supra*. *Rittmaster* discloses prohibition or allowance of transmission of messages based on recurring events such as time, day, week, etc. Malek Decl. at ¶ 71; Ex. C, ¶ 14. 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 ¶ 71; Ex. C, ¶ 69-70. These periodic transmissions of location and/or time are trigger events. Malek Decl. at ¶ 71.

4. Claim 4 – *"wherein the period of the timer is fractionally shorter than a maximum data message interval beyond which the Internet data message link to the given device is taken down."*

Claim 4 depends from claim 3 and adds that messages are designed to be sent shortly before a link to the server is terminated. Malek Decl. at ¶ 72. 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

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 78 of 114

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, ¶¶ 69-70. Otherwise, the location and/or time information would not be transmitted. Sending the message shortly prior to closing of the link would have been obvious because it would conserve resources and minimize security risks in comparison to leaving the link open indefinitely after the necessary information had been communicated.

5. Claim 5 – *"wherein one of the message delivery triggers is the receipt of a transmission on the respective secure Internet data 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 5 depends from claim 1. As discussed in Section II.C.4., *supra*, *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 ¶ 73; Ex. C, ¶¶ 74-76 and Fig. 6. For instance, 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 ¶ 73; Ex. C, ¶¶ 8-9. As another example, the end-user device can send information regarding the physical location of the user or advertising preferences to the network, leading to receipt of specific advertising content as discussed in detail above in connection with claim 1. Malek Decl. at ¶ 73; Ex. C, ¶¶ 132-42.

6. Claim 6 – *"wherein one of the message delivery triggers is a heartbeat message generated by the given device link agent, or a request received from the given device link agent."*

Claim 6 depends from claim 1 and, asdiscussed in Section II.C.5., *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 ¶ 74. The device link agent is the software responsible for sending signals from the end-

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 79 of 114

user device, and would therefore be generating the heartbeat message. To the extent that *Rittmaster* is considered to not disclose any aspect of this claim, a PHOSITA would have found the claim obvious because it is at most a trivial variation of *Rittmaster's* disclosure and there are limited options for generating *Rittmaster's* heartbeat message. *Id.*

7. Claim 7 – *"wherein one of the message delivery triggers is the receipt of a particular message from one of the network elements."*

Claim 7 depends from claim 1, and this added element is disclosed by *Rittmaster* for the reasons discussed in Section II.C.6., *supra*. *See also* Malek Decl. at ¶ 75. 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 ¶ 75; 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 ¶ 75; Ex. C, ¶ 124. These instructions from the advertiser computer (network element) trigger sending of a message stored at the server. *See* Malek Decl. at ¶ 75. 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]." Malek Decl. at ¶ 75; Ex. C, ¶ 125.

8. Claim 10 – *"wherein a second subset of the secure Internet data messages contain a user message from a network element, the user message intended for display on a user interface of a given one of the wireless end-user devices."*

Claim depends from claim 1. This additional element is disclosed by *Rittmaster* for the reasons discussed in Section II.C.7., *supra*. *See also* Malek Decl. at ¶ 76. *Rittmaster* states that "establishments may have communicated advertisement information to the provider processor 12 [server], from suitable computers 138 and 140 [network elements]" (Ex. C, ¶ 121) and 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…from the advertiser's computer 138 or 140 [network element]" (Ex. C, ¶ 124). Malek Decl. at ¶ 76. The end-user devices of *Rittmaster* can include "personal computers (PCs), portable communication devices (such as portable telephones, personal digital assistants, or other portable information units), or vehicle-

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 80 of 114

mounted computers" which can have "user-operated input devices" such as a "touchscreen," and thus *Rittmaster* discloses that the user messages (such as advertising) that are transmitted to the end-user devices can be "intended for display on a user interface" as recited in claim 10. *Id.*; Ex. C, ¶ 35-36. Even if "user message" is interpreted to have a narrow meaning, even though the term does not appear in the '320 Patent's specification, in some cases the displayed message is a message intended to alert the user as to the status of a request or ability to receive certain content, for instance a "denied access" message that is displayed to the user on the device's screen in place of requested content. Ex. C, ¶ 73. Thus, *Rittmaster* discloses a first subset of messages relating to advertising and a second subset of messages relating to user alerts, as recited in claim 10.

9. **Claim 12 – *"the link interface to encrypt messages identified for delivery to each given one of the wireless end-user devices to create secure Internet data messages, the device link agent on each given device further configured to decrypt the received secure Internet data messages for that device prior to delivering those messages to a respective software process."***

Claim 12 depends from claim 1. *Rittmaster* discloses this additional element for the reasons discussed above in Section II.C.8., *supra*. *See also* Malek Decl. at ¶ 77. For instance, Figs. 8 and 9 illustrate the process of encrypting and decrypting messages. Malek Decl. at ¶ 77. The server encrypts content (step 106) and transmits the encrypted content (step 108), and the end-user device receives the encrypted content (step 110), decrypts the content (step 114), and displays the content (step 116). Malek Decl. at ¶ 77; Ex. C, ¶¶ 98-99 and Figs. 8-9. Encryption and decryption are accomplished by an encryption algorithm of the provider processor (server) (Ex. C, ¶ 97) and "decryption module" 90 of the end-user device, respectively, which would qualify as a link interface and device link agent as claimed. Malek Decl. at ¶ 77. Even if Rittmaster is considered to not disclose the subject matter of claim 12, a PHOSITA would have found it obvious to configure the link interface of the server to encrypt messages and configure the device link agent of the end-user device to decrypt messages, because those are the elements of the respective devices responsible for sending and receiving messages. Malek Decl. at ¶ 77

10. **Claim 13 – *"wherein the encrypted messages are transported to the device link agent using one or more of encryption on a transport services stack, IP (Internet Protocol) layer encryption, and tunneling."***

Claim 13 depends from claim 12. *Rittmaster* discloses this element for the reasons above. *See supra* Section II.C.9.; Malek Decl. at ¶ 78. At a minimum transporting encrypted messages using a transport services stack, IP (Internet Protocol) layer encryption, and/or tunneling was

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 81 of 114

extremely well-known to any PHOSITA prior to the critical date of the '320 Patent, 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 '320 Patent does. Malek Decl. at ¶ 78; Ex. F, 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 ¶ 79; Ex. F, pp. 602-603.

11. Claim 15 – *"wherein the device link agent on a given one of the devices is further configured to receive, from one or more of the software components on that device, upload messages, each of the upload messages identifying a corresponding one of the network elements to which the device respective software component has requested delivery, the device link agent on that device transmitting the upload messages to the network message server over the respective secure Internet data message link, for delivery by the network message server to the respective identified network elements."*

Claim 15 depends from claim 1. *Rittmaster* discloses this element for the reasons above. *See supra* Section II.C.10.; Malek Decl. at ¶ 79. *Rittmaster* identifies multiple situations in which the end-user device provides information to the server. Malek Decl. at ¶ 79. For instance, geographic location and/or user preferences may be transmitted from the user to a provider computer. *Id.*; Ex. C, ¶¶ 13-14 and 142. Information regarding data transmitted from user-devices may be accessed by advertiser computers (network elements) in order to determine when advertising messages are to be sent. Malek Decl. at ¶ 79; Ex. C, ¶ 142. This would have involved upload of the messages from the end-user device to the advertiser computers, or it would have been at least obvious to do so. In the case of an advertising network, this would allow advertiser computers (e.g., computers associated with a restaurant or bakery) to be able to track which end-users are to receive specific types of message content and to determine when a specific number of end-users are within a specified geographic area. Malek Decl. at ¶ 79. *Rittmaster* also discloses that in one embodiment, "the provider processor issues a query or command to the requesting recipient computer to provide the user code" in response to which "the recipient computer

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 82 of 114

communicates the user code to the provider processor," and the provider processor also "provide[s] the user code as part of or in association with the request for the content" sent to the network computer providing the content. *Id.*; Ex. C, ¶¶ 96-97. Thus, not only does the 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 inputting a user code in an application which then sends the user code through a device link agent to a specific network element when content is requested from that element. Malek Decl. at ¶ 79. Further, "unlike current advertising modalities, but in accordance with embodiments of the invention, the selection of the commercial, promotional or informational content to include in the interleaved break(s) may be determined, in whole or part, by the physical location of the user." *Id.*; Ex. C, ¶ 132. 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, restaurant, store, etc.). Malek Decl. at ¶ 79.

12. Claim 16 – *"the device link agent on the given device further configured to buffer one or more of the upload messages for transmission to the network message server at a time selected by a heartbeat mechanism."*

Claim 16 depends from claim 15, and is disclosed by *Rittmaster* for the reasons above. *See supra* Section II.C.11.; Malek Decl. at ¶ 80. For instance, *Rittmaster* discloses that 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." Malek Decl. at ¶ 80; Ex. C, ¶ 69. It would at least have been obvious for a PHOSITA to configure the device link agent to buffer messages because that is the component responsible for sending messages and would allow for the most accurate timing. *Id.* Buffering by an upstream component could introduce unintended delays in message timing. *Id.*

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 83 of 114

13. Claim 17 – *"at least a given one of the devices further comprising a secure interprocess communication service separately secured from the secure Internet data message link, the device link agent for the given device causing messages to be securely delivered to a software process by initiating delivery of each such message on the secure interprocess communication service."*

Claim 17 depends from claim 1. *Rittmaster* discloses this element for the reasons above. *See supra* Section II.C.12.; Malek Decl. at ¶ 81. A PHOSITA would know that the "device link agent" would deliver messages to identified software on the same device, and although *Rittmaster* does not disclose how messages are distributed within the end-user device itself, it would have been obvious to securely deliver messages on "a secure interprocess communication service separately secured from the secure internet data message link." Malek Decl. at ¶ 81. A PHOSITA would have found it obvious to include a secure interprocess communication service so that communication of information between device components does not compromise security as information is transmitted between the secure device link agent and the secure execution environment. *Id.*

14. Claim 18 – *"wherein at least one of the secure Internet data messages comprises multiple identifier/data pairs."*

Claim 18 depends from claim 1. *Rittmaster* discloses this element for the reasons above. *See supra* Section II.C.13.; Malek Decl. at ¶ 82. 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 would have been at least obvious in view of *Rittmaster*. Messages sent through *Rittmaster's* server states can include "promotional or advertisement information for a plurality of different establishments within the same shopping area." Malek Decl. at ¶ 82; 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 ¶ 82; 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 ¶ 82; Ex. E, p. 344. A PHOSITA would understand that two independent data elements (e.g., advertisements), each having a data payload and identifier, could be assembled

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 84 of 114

into a single message in order to allow for better handling of a high number of messages. Malek Decl. at ¶ 82.

E. Ground 3: The Combination of *Rittmaster* and *Shenfield* Renders Obvious Claims 1-7, 10, 12-13, and 15-18

To the extent that *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* ("*Shenfield*," (Ex. U)). Malek Decl. at ¶ 106. *Shenfield* was filed on February 7, 2007, and published September 6, 2007, more than one year prior to the earliest claimed priority for the '320 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 ¶ 106; Ex. U, Fig. 1. For example, 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.*; Ex. U ¶36. It would have been obvious at the time of the claimed invention of the '320 Patent 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 ¶ 106. 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 network-level and device-specific details not explicitly disclosed. *Id.*

Shenfield discloses a network similar to those of the '320 Patent and *Rittmaster* for sending messages from content providers (24) to a variety of mobile end-user devices (14) through a network part (12, such as proxy server 26):

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 85 of 114

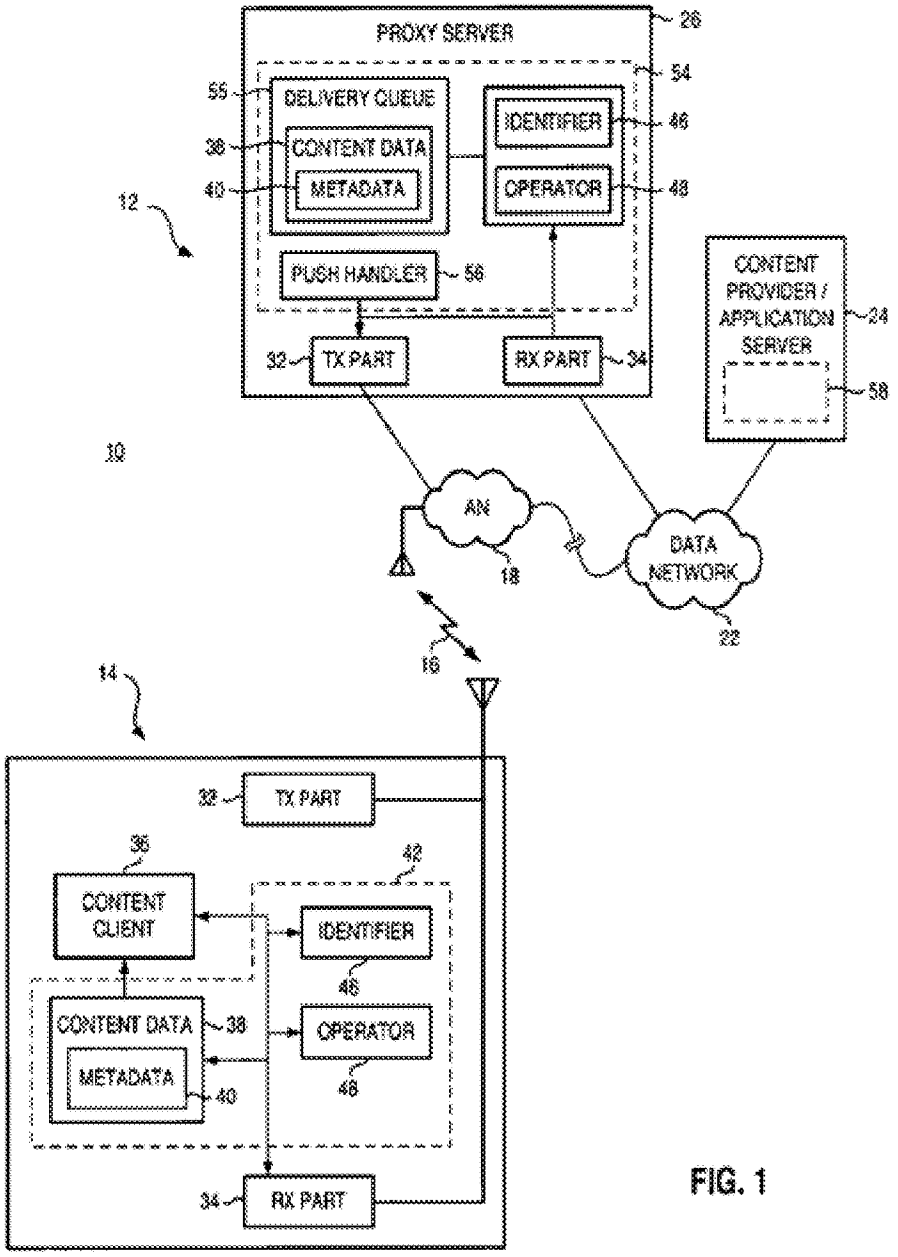


FIG. 1

Ex. U, Fig. 1; Malek Decl. at ¶ 100. As illustrated above, *Shenfield* discloses a Proxy Server (26) linking a plurality of network elements (Data Network 22 including content provider server 24) to a plurality of mobile communications devices (including mobile device 14) through an Access Network 18 (e.g., the Internet) that is not connected to the Data Network, just like the '320 Patent and *Rittmaster*. *Shenfield* discloses the delivery and processing of push content communicated to a mobile station of a communication system. Malek Decl. at ¶ 100; Ex. U, Abstract.

1. Claim 1

a. 1[PRE] *"A network server system comprising:"*

Rittmaster and *Shenfield* both disclose a "networked system" because, as discussed above, they disclose a server for providing message content from various sources to linked user devices. Malek Decl. at ¶ 106-107. In particular, *Shenfield* discloses a network similar to those of the '320 Patent and *Rittmaster* for sending messages from content providers (24) to a variety of mobile end-user devices (14) through a network part (12, such as proxy server 26):

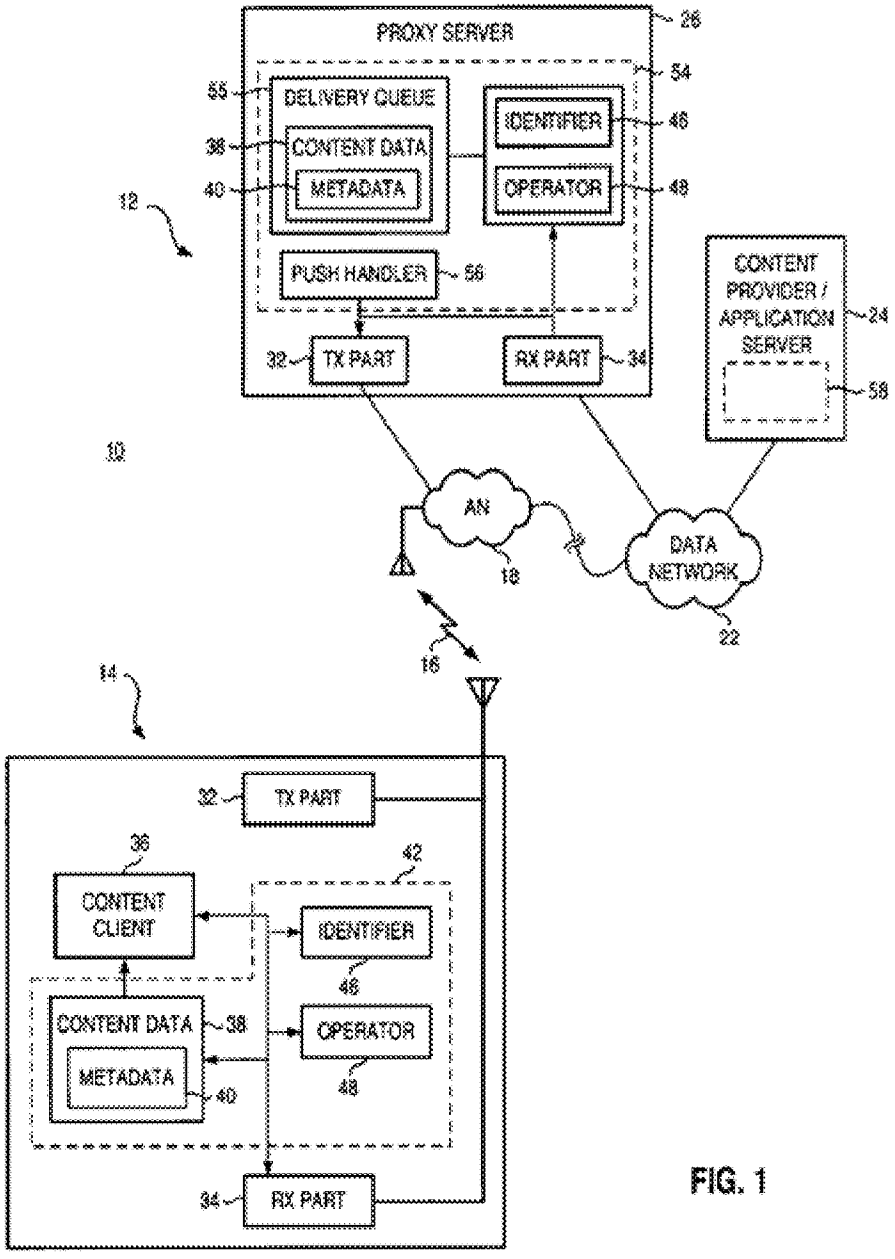


FIG. 1

Ex. U, Fig. 1; Malek Decl. at ¶ 107-108. As illustrated above, *Shenfield's* Proxy Server (26) links a plurality of network elements (Data Network 22 including content provider server 24) to a plurality of mobile communications devices (including mobile device 14) through an Access Network 18 (e.g., the internet) that is not connected to the Data Network, just like the '320 Patent and *Rittmaster*. Malek Decl. at ¶ 107. *Shenfield* discloses the delivery and processing of push content communicated to a mobile station of a communication system. Malek Decl. at ¶ 107; Ex. U, Abstract.

b. 1[a] "*i) a network server system including a link interface to maintain a respective secure Internet data message link between the link interface 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* Sections II.C.1.b. and II.D.1.b.; Malek Decl. at ¶ 109. 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 ¶ 109. To the extent *Rittmaster* is considered not to disclose details of how its link interface 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 found it obvious to implement details from the similar network of *Shenfield*, including a communication layer 84 of each end-user device (i.e., device link agent) that receives messages sent by the transmission part 32 of the server (i.e., link interface), for ultimate distribution to the message store 76 of the appropriate application on the mobile device based on the incoming message's application identification. Malek Decl. at ¶ 109; Ex. U ¶ 69. Implementing this feature of Shenfield's messaging system into *Rittmaster* to make a functional network would have required nothing but routine skill, and a PHOSITA would have been motivated to do so by at least *Rittmaster's* explicit suggestion to use "communication interfacing" that was "well known in the art" because it was not necessary to describe such basic details. Malek Decl. at ¶¶ 106-110; Ex. U, ¶ 4269. *Shenfield* notes that a communication link is intended to be 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." Malek Decl. at ¶ 109; Ex. U, ¶ 47.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 88 of 114

c. [1b] "*each of the wireless end-user devices comprising multiple software components authorized to receive messages via the device link agent on that device;*"

Rittmaster discloses end-user devices such as portable telephones, personal digital assistants, and personal computers. Malek Decl. at ¶ 110; Ex. C, ¶ 35. To the extent *Rittmaster* is considered not to disclose details such as the end-user devices (e.g., portable phones, portable digital assistants, or portable computers) having contained multiple software components on each device authorized to receive messages via a device link agent on that device, it would have been obvious to utilize *Rittmaster*'s network with mobile devices having multiple applications capable of receiving messages such as those described in *Shenfield*. Malek Decl. at ¶ 110. *Shenfield* discloses that "[t]he proxy server 26 interacts with…mobile stations, such as the mobile station 14, and the applications resident thereat." Malek Decl. at ¶ 110; Ex. U, ¶ 36. These multiple applications may all be associated with the same processor or have their own processor. Malek Decl. at ¶ 110; Ex. U, ¶ 71. *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." Malek Decl. at ¶ 110; Ex. U, ¶ 34. 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. Malek Decl. at ¶ 110. Further, 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 there are multiple content clients (applications) and that the content clients are authorized to receive and process information delivered from the communication layer (device link agent) so that the communication layer can place a given message in the message store of content client that is determined to be "appropriate" for each message. Malek Decl. at ¶ 110; Ex. U, ¶ 69. 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 queueing messages and updating/modifying them so that users of *Rittmaster*'s system do not receive outdated advertisements or other content. Malek Decl. at ¶ 110. Fig 2 of *Shenfield* shows the interaction of communication layer 84 and the message store 76 of one of the plurality of applications on the mobile station 14:

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 89 of 114

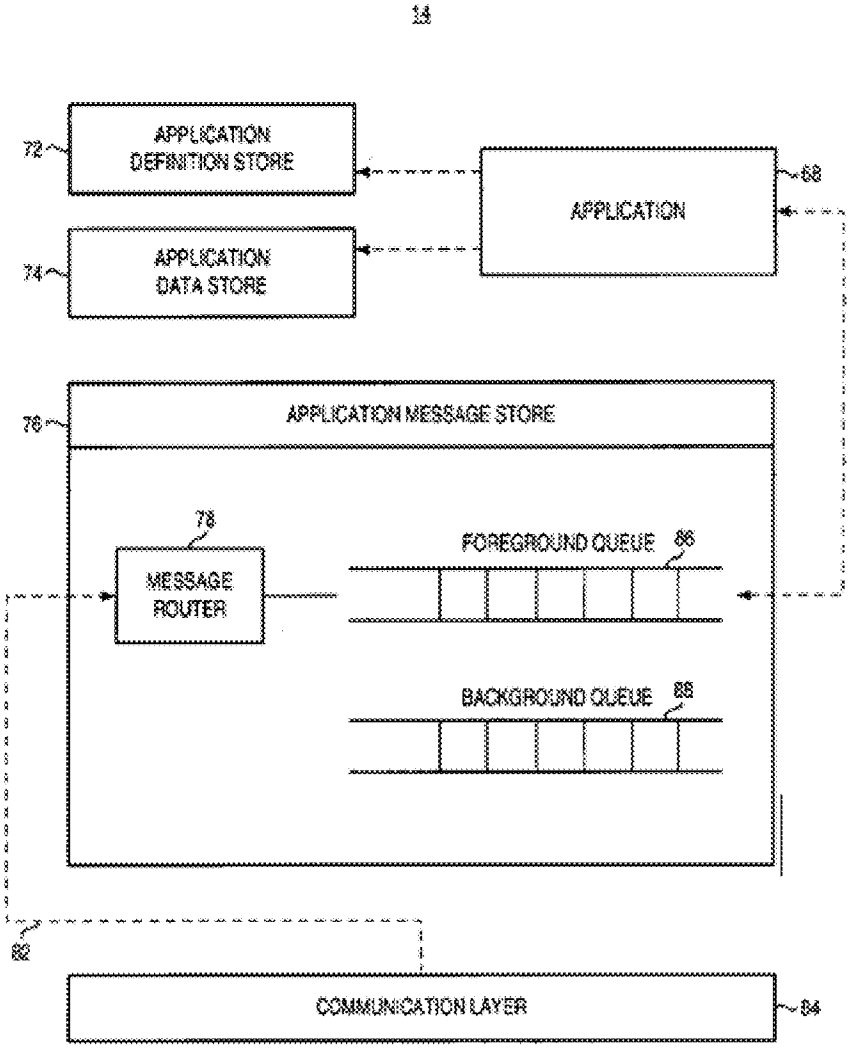


FIG. 2

Ex. U, Fig. 2.

d. 1[c] "*a network interface to receive messages from a plurality of network elements, for delivery to respective ones of the software components identified in the messages, each network element authorized to send messages via the link interface to one or more of the software components on one or more of the wireless end-user devices; and*"

This element requires that the network-facing side of the server include a "network interface" to receive messages from two or more "network elements," for delivery of that content to specific end-user devices by including data for and an identification of authorized software. Malek Decl. at ¶ 111. This does little more than describe the basic manner in which all messages

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 90 of 114

were delivered from a network at the relevant time. Malek Decl. at ¶ 111. 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* Sections II.C.1.d. and II.D.1.d.; Malek Decl. at ¶ 111. *Shenfield* likewise discloses a proxy server 26 that interfaces with a receives messages from an application server 24 for delivery to mobile devices, and such details would have been obvious to implement in *Rittmaster* for the reasons discussed above in order to create a functional network. Malek Decl. at ¶ 111. *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 ¶ 111. *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 ¶ 111.

At a minimum, 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 because both *Rittmaster* and *Shenfield* disclose transmitting message data from network elements to a server and ultimately to user devices and Shenfield provides technical details regarding how a messaging system such as Rittmaster operates. Malek Decl. at ¶ 111. *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 ¶ 111. 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. Malek Decl. at ¶ 111. Even if *Shenfield* is considered to not necessarily require the messages from the content

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 91 of 114

provider server to include destination application information, it would have been an obvious and trivial difference for such information to be included in the message from the content provider sent to the proxy server rather than appending that information to a message at the server level. *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 any of the wireless end-user devices,"*

Rittmaster alone discloses or renders obvious claim element [1d] including a message buffer system including memory and logic for reasons discussed above. *See supra* Sections II.C.1.e. and II.D.1.e.; Malek Decl. at ¶ 112. 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 ¶ 112. 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 and 40; Malek Decl. at ¶ 112. *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 ¶ 112. It would have been obvious to implement the features of *Shenfield* into the buffer of *Rittmaster* in order to avoid delivering outdated content. Malek Decl. at ¶ 112.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 92 of 114

f. 1[e] *"the logic to determine when one of a plurality of message delivery triggers for a 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* alone discloses or renders obvious claim 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* Sections II.C.1.f. and II.D.1.f.; Malek Decl. at ¶ 113. *Rittmster* 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." Ex. C, ¶ 14; Malek Decl. at ¶ 113. Alternatively, the 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 ¶ 113. *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 ¶ 113. These messages are two different triggers that cause messages to be released from a buffer (queue). Malek Decl. at ¶ 113. "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 ¶ 113. "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 the release of messages from a queue as determined by the server, such as timing ("scheduled deliver") 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

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 93 of 114

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 for the given one of the wireless end-user devices, the logic further to supply one or more messages comprising the buffered content for the given one of the wireless end-user devices 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; and"*

As discussed above, *Rittmaster* alone discloses and renders obvious claim element [1f]. *See supra* Sections II.C.1.g. and II.D.1.g. Both *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. Malek Decl. at ¶ 114. *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 ¶¶ 64 and 114. *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. Malek Decl. at ¶114 The combination of *Rittmaster* and *Shenfield* would therefore necessarily include logic to supply messages comprising buffered content for delivery on the secure message link maintained between the link interface and a device link agent on wireless end-user devices. *Id.* While the above claim language suddenly begins to refer to the link interface of the server as a "transport services stack" without explanation, this does not make the claim non-obvious. *Id.* The '320 Patent itself admits that its "Transport Services Stack" provides "**basic** transport services" and can be "**implemented with standard secure or open Internet networking protocols, such as TLS or TCP**." Ex. A, 89:29-36 (emphasis added); Malek Decl. at ¶ 114. As noted in Sections II.C.1.g. and II.D.1.g., a PHOSITA would 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) or at least obvious because that was standard for communication over the Internet. *See* Ex. F, p. 28. Malek Decl. at ¶ 114.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 94 of 114

h. 1[g] *"ii) the device link agents on the respective wireless end-user devices, each of the device link agents configured to maintain the respective secure Internet data message link over a wireless network to the link interface,"*

As discussed above, *Rittmaster* alone discloses or renders obvious claim element [1g]. *See supra* Section II.C.1.h. and II.D.1.h.; Malek Decl. at ¶ 115. *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 ¶ 115. *Rittmaster* does not disclose specific technical protocols at the code level for sending or receiving messages, but 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 know that common messaging protocols at the time (e.g., TLS) would be employed in such a system, and thus that a "secure Internet data message link" would be maintained by a "link interface" and "device link agents" on the various end-user devices (such as cellular phones, personal digital assistants, or laptops). Malek Decl. at ¶ 115. To the extent that there is any doubt that *Rittmaster* discloses communication from a link interface on the server and device link agents on end-user mobile devices, a PHOSITA would have implemented details from the similar network of *Shenfield*, including a communication layer 84 of each mobile device that maintains a link to the server and receives messages sent through that link, for distribution to the message store 76 of the appropriate application on the mobile device based on the incoming message's application identification. Malek Decl. at ¶ 115; Ex. U, ¶ 69. *Shenfield* also notes that a link is maintained between the server and end-user devices. Malek Decl. at ¶ 115; Ex. U, ¶ 47. Therefore, the combination of *Rittmaster* and *Shenfield* would have this feature.

i. 1[h] "[each of the device link agents configured to] *receive secure Internet data messages from the network server system over the respective secure Internet data message link, including messages collected from multiple ones of the network elements and messages corresponding to multiple ones of the software components authorized to receive messages via the device link agent on that respective device,"*

As discussed above, *Rittmaster* alone discloses or renders obvious claim element [1h]. *See supra* Sections II.C.1.i. and II.D.1.i.; Malek Decl. at ¶ 116. This element requires that the "device link agents" receive messages from the server over the "secure Internet data message link," and

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 95 of 114

that the messages include messages collected from multiple "network elements," the messages corresponding to authorized software components on a mobile device. Malek Decl. at ¶ 116. *Rittmaster* discloses this limitation by describing advertisements from multiple advertisers that are connected to the server through the Internet so that the advertisements may be delivered by the server to a plurality of end-user devices, as discussed above in Sections II.C.1.i. and II.D.1.i.To the extent *Rittmaster* is considered not to disclose details of a device link agent on a device which receives messages corresponding to multiple software components on the user device authorized to receive the data received via the device link agent on that device, *Shenfield* makes this feature clear by disclosing multiple content provider computers/servers (network elements) interfacing with the proxy server to deliver messages to one of a plurality of mobile stations. Malek Decl. at ¶ 116; Ex. U, ¶¶ 32-36. A PHOSITA would have had a clear motivation to implement the protocol-level details of the similar network of *Shenfield* into *Rittmaster*'s system. Malek Decl. at ¶ 116. *Shenfield* discloses a proxy server 26 that receives messages from a plurality of application servers 24 for delivery to mobile devices, and such details would have been obvious to implement in *Rittmaster* for the reasons discussed above. Malek Decl. at ¶ 116.

j. 1[i] *"wherein at least a first subset of the secure Internet data messages contain both a unique identifier for a corresponding one of the software agents and data to be consumed by that software component, the data supplied from a respective network element corresponding to that software component, and"*

As discussed above, *Rittmaster* alone discloses or renders obvious claim element [1i]. *See supra* Section II.C.1.j. and II.D.1.j. *Rittmaster*'s system is designed to communicate messages to specific mobile devices, and those messages would necessarily need to be processed by a specific software application on those devices, and therefore the messages would have contained both an IP address and a port number that in combination act as a unique identifier addressing the message to a specific software application located at a specific virtual location on a specific end-user device. Malek Decl. at ¶ 117. To the extent *Rittmaster* is considered not to disclose details of sending messages that include data for an 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 *Shenfield* (Ex. U). Malek Decl. at ¶ 117. *Shenfield* explicitly discloses that "[e]ach incoming message to the device contains an application identification and a message identification" and that the communication layer 84 of the communication device 14 "uses the application identification to place the message in the

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 96 of 114

appropriate message store 76" of one of multiple software components. Malek Decl. at ¶ 117; Ex. U, ¶ 69. A PHOSITA would have had a clear motivation to implement protocol-level details of *Shenfield* in *Rittmaster* to create a functional system where messages, which necessarily include data to be consumed by a software component, are directed to the appropriate software component by the application identification. Malek Decl. at ¶ 117.

k. 1[j] "[each of the device link agents configured to] *for software components that are authorized to access messages received via the device link agent, cause messages with a unique identifier corresponding to a given one of those software applications to be securely delivered to a software process corresponding to the given software component.*"

The final element of claim 1 [1j] would have been obvious for all of the reasons above. *See supra* Section II.C.1.k, II.D.1.k, and II.E.1j.; Malek Decl. at ¶ 118. The combination of *Rittmaster* and *Shenfield* would have unique identifiers (i.e., application identifications) used by the device link agent (communication layer) of each device to securely deliver messages to the message router associated with the appropriate software component. Malek Decl. at ¶ 118; Ex. U, ¶¶ 68-69, Fig. 2. As explained repeatedly above, both *Rittmaster* and *Shenfield* have messages with unique identifiers targeting a specific software application, and this was the basic manner in which messages were delivered over a network well prior to the '320 Patent. *Rittmaster*'s system would necessarily have contained both an IP address and a port number that in combination act as a unique identifier, causing the message to be delivered to a specific software application located at a specific virtual location on a specific end-user device. Malek Decl. at ¶ 117. *Shenfield* is the same but explicitly discloses that "[e]ach incoming message to the device contains an application identification and a message identification" and that the communication layer 84 of the communication device 14 "uses the application identification to place the message in the appropriate message store 76" of one of multiple software components. Malek Decl. at ¶ 117; Ex. U, ¶ 69. At a minimum, a PHOSITA would have had a clear motivation to implement protocol-level details of *Shenfield* in *Rittmaster* to create a functional system where messages, which necessarily include data to be consumed by a software component, are directed to the appropriate software component by the application identification. Malek Decl. at ¶ 117. The software components to which messages are intended to be delivered in *Rittmaster* and *Shenfield* are by definition authorized to access messages received via the device link agent within the meaning of claim 1.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 97 of 114

2. Claim 2 – *"the message buffer system logic to determine, for each of the wireless end-user devices, when one of a plurality of message delivery triggers has occurred, at least one of the triggers for each given device specific to one or more states of that given device."*

As discussed above, in Sections II.C.2. and III.D.2., *Rittmaster* discloses the types of triggers disclosed in the '320 Patent such as device "states" like online/offline, active, and suspended. Malek Decl. at ¶ 119; Ex. A, 125:20-43. Additionally, *Shenfield* also discloses triggers specific to one or more states of the end-user device. For instance, *Shenfield* states that the proxy server "mediates subscription and notification work flows between the content provider and the mobile station" and provides "temporary storage of content when a mobile station is out of communication range." Malek Decl. at ¶ 119; Ex. U, ¶ 36.

3. Claim 3 – *"wherein one of the message delivery triggers is the expiration of a periodic timer."*

Claim 3 depends from claim 1. This added element is disclosed in *Rittmaster*, as discussed above in Sections II.C.2. and II.D.2., 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 ¶ 120. 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." *Id.*; Ex. C, ¶ 14.

4. Claim 4 – *"wherein the period of the timer is fractionally shorter than a maximum data message interval beyond which the Internet data message link to the given device is taken down."*

Claim 4 depends from claim 3 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 Sections II.D.4. *See also* Malek Decl. at ¶ 72 and 121.

5. Claim 5 – *"wherein one of the message delivery triggers is the receipt of a transmission on the respective secure Internet data 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 5 depends from claim 1 and further requires 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

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 98 of 114

in part. This is disclosed in, or obvious in view of, *Rittmaster* for the reasons discussed above in Sections II.C.4 and II.D.5., 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.5.; Malek Decl. at ¶ 122.

6. Claim 6 – *"wherein one of the message delivery triggers is a heartbeat message generated by the given device link agent, or a request received from the given device link agent."*

Claim 6 depends from claim 1. This would have been recognized by a PHOSITA as being disclosed in, or obvious in view of, *Rittmaster*, as discussed in Sections II.C.5. and II.D.6. above, 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." Malek Decl. at ¶ 123; Ex. C, ¶ 69. Receipt of these multiple periodic requests issued from the server would be a heartbeat message that acts a trigger to cause delivery of content from the server to the user device issuing the heartbeat messages. Malek Decl. at ¶ 123.

7. Claim 7 – *"wherein one of the message delivery triggers is the receipt of a particular message from one of the network elements."*

Claim 7 depends from claim 1 and recites that, in addition to the elements of claim 1, one of the message delivery triggers is receipt of a particular message from one of the network elements, which is shown in, or obvious in view of, *Rittmaster*. *See supra* Sections II.C.6. and II.D.7. 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. 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

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 99 of 114

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. Likewise, *Shenfield* discloses that push messages to users can be triggered by the content provider. Ex. U, ¶ 6. 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.

8. Claim 10 – *"wherein a second subset of the secure Internet data messages contain a suer message from a network element, the user message intended for display on a user interface of a given one of the wireless end-user devices."*

Claim 10 depends from claim 1. *Rittmaster* discloses or renders obvious this element for the reasons discussed above. *See supra* Section II.C.7. and II.D.8. In addition, *Shenfield* discloses that messages are delivered and displayed on a user device. Malek Decl. at ¶ 127; Ex. U, ¶¶ 7 and 22.

9. Claim 12 – *"the link interface to encrypt messages identified for delivery to each given one of the wireless end-user devices to create secure Internet data messages, the device link agent on each given device further configured to decrypt the received secure Internet data messages for that device prior to delivering those messages to a respective software process."*

Claim 12 depends from claim 1. *Rittmaster* discloses or renders obvious this claim for the reasons discussed above. *See supra* Sections II.C.8. and II.D.9. *Rittmaster* contemplates encryption by the server of content from network elements and decryption of the encrypted content prior to delivery to one or more of the plurality of user devices. Malek Decl. at ¶ 129. This feature would have been obvious to implement in the combination of *Rittmaster* and *Shenfield* in order to increase security. Malek Decl. at ¶ 129.

10. Claim 13 – *"wherein the encrypted messages are transported to the device link agent using one or more of encryption on a transport services stack, IP (Internet Protocol) layer encryption, and tunneling."*

Claim 13 depends from claim 12. *Rittmaster* discloses this claim for the reasons discussed above. *See supra* Section II.C.9. and II.D.10. At a minimum, this would have been obvious to implement in the combination of *Rittmaster* and *Shenfield* in order to increase security.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 100 of 114

11. Claim 15 – *"wherein the device link agent on a given one of the devices is further configured to receive, from one or more of the software components on that device, upload messages, each of the upload messages identifying a corresponding one of the network elements to which the device respective software component has requested delivery, the device link agent on that device transmitting the upload messages to the network message server over the respective secure Internet data message link, for delivery by the network message server to the respective identified network elements."*

Claim 15 depends from claim 1. This element would have been obvious in view of *Rittmaster* for the reasons discussed above and therefore would be present in a combination of *Rittmaster* and *Shenfield*. *See supra* Sections II.C.10 and II.D.11. Like *Rittmaster*, *Shenfield* discloses providing content based on a user request. Ex. U, ¶ 4; Malek Decl. ¶ 132. 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. ¶ 132. Both of these scenarios would have involved identification of the relevant content provider from which content is requested and transmission of the upload messages through the device link agent responsible for communicating with the server. 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.

12. Claim 16 – *"the device link agent on the given device further configured to buffer one or more of the upload messages for transmission to the network message server at a time selected by a heartbeat mechanism."*

Claim 16 depends from claim 15. This element would have been obvious in view of *Rittmaster* for the reasons discussed above and therefore would be present in a combination of *Rittmaster* and *Shenfield*. *See supra* Sections II.C. 11. And II.D.12.; Malek Decl. ¶ 133.

13. Claim 17 – *"at least a given one of the devices further comprising a secure interprocess communication service separately secured from the secure Internet data message link, the device link agent for the given device causing messages to be securely delivered to a software process by initiating delivery of each such messages on the secure interprocess communication service."*

Claim 17 depends from claim 1. This element would have been obvious in view of *Rittmaster* for the reasons discussed above and therefore would be present in a combination of *Rittmaster* and *Shenfield, and either Fok or Ellison*. *See supra* Section II.C. 12. And II.D.13.; Malek Decl. ¶ 134.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 101 of 114

14. Claim 18 – *"wherein at least one of the secure Internet data messages comprises multiple identifier/data pairs."*

Claim 18 depends from claim 1. This element would have been obvious in view of *Rittmaster* for the reasons discussed above and therefore would be present in a combination of *Rittmaster* and *Shenfield*. *See supra* Section II.C.13. and II.D.14.; Malek Decl. ¶ 135. Claim 17 also would have been obvious for the reasons discussed below in Ground 9.

F. Ground 4: The Combination of *Rittmaster*, *Klassen*, and *Konstantinov* Renders Claims 1-7, 10, 12-13, and 15-18 Obvious.

Rittmaster discloses or makes obvious all of the elements of claim 1 and dependent claims 2-7, 10, 12-13, and 15-18 for the various reasons explained above in Grounds 1 and 2 (Sections II.C. and II.D. above). To the extent *Rittmaster* is considered to lack explicit disclosure of certain software-level details such as messages that include a unique identifier for a software application or a link interface or network interface, a PHOSITA would have looked to other prior art references that do explicitly describe the basic protocol-level elements of such networks. Malek Decl. at ¶ 83. 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 in order to supplement its disclosure. *Id.*

To the extent there is any doubt that *Rittmaster* discloses communication from a network interface to device link agents on end-user mobile devices (claim element 1[a]), a PHOSITA would have simply implemented details from the similar network of *Klassen*, which includes a mobile device with a device link agent having 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:

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 102 of 114

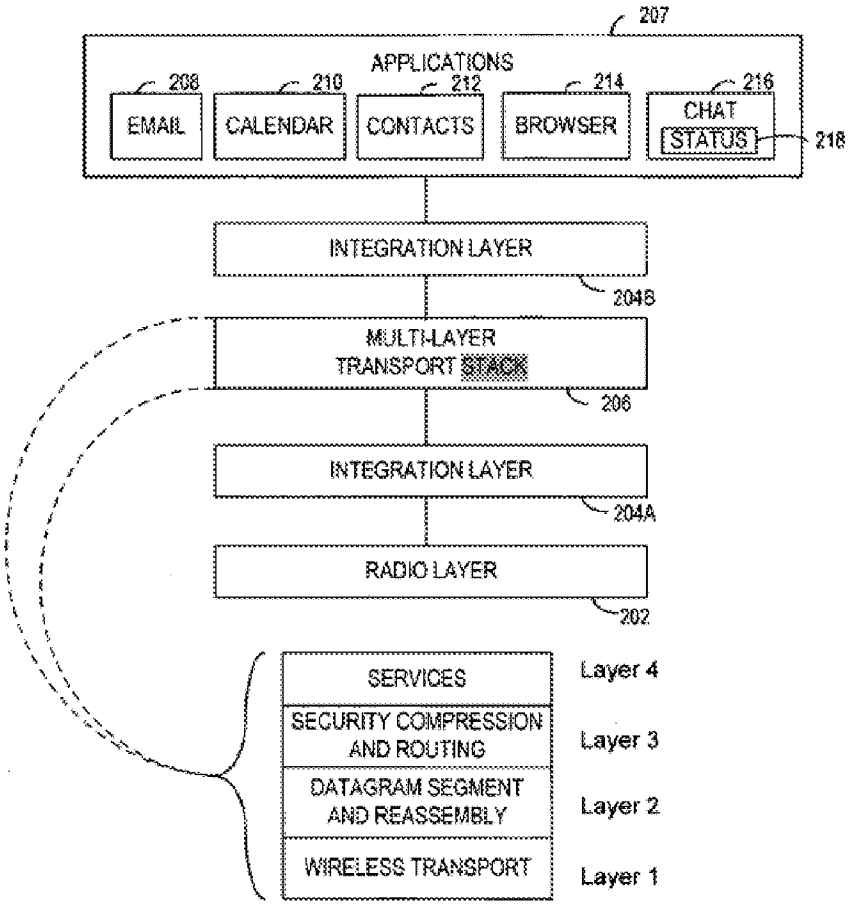


Fig. 2

Malek Decl. at ¶ 85-86; 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 ¶ 85-86.

It also would have been obvious in view of the *Rittmaster/Klassen* combination to have the network-facing side of the server include a "network interface" to receive messages from two or more "network elements," for delivery of that content to specific end-user devices by including data for and an identification of authorized software, as recited by claim element 1[c]. Malek Decl. at ¶ 87. Likewise, *Klassen* would have made it obvious to include multiple network elements through its disclosure of a remote services server 106 that receives messages from a plurality of

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 103 of 114

application servers (104-1 through 104-N) for delivery to mobile devices, as recited by claim element 1[b]. *Id.* These details would have been obvious to implement in *Rittmaster* for the reasons discussed above. *Id.*

Further, in addition to *Rittmaster's* ample disclosure of buffering messages and using triggers to determine when messages are sent, *Konstantinov* also discloses buffering of messages upon certain conditions and would have been obvious to combine with *Rittmaster* in order to scramble certain messages if the server logic determines that the requester is unauthorized, as recited by claim elements 1[d]-1[f]. Malek Decl. at ¶ 88. *Konstantinov* specifically mentions delaying data packets by transferring them into a buffer, as recited by claim element 1[d]. *Id.*; Ex. D, ¶ 42.

To the extent that there is any doubt that *Rittmaster* discloses or makes obvious messages that include a unique identifier and data to be consumed by the software component to which the message is sent as recited in claim element 1[i], *Konstantinov* expressly discloses addressing messages to one of a plurality of user devices from a server by utilizing both an IP address and a port number for each device, acknowledging that both the content provider and the plurality of potential recipients (*e.g.*, end-user devices) have a plurality of software agents identified by port number. Malek Decl. at ¶ 93; *See, e.g.*, Ex. D, ¶ 39. This identifier is unique in that it is unique to one particular instance of a software program, i.e., the specific software application located at a specific port number of a particular device. Malek Decl. at ¶ 93. A PHOSITA would have been motivated to combine *Konstantinov* with *Rittmaster* at the time of the alleged invention of the '320 Patent due to *Konstantinov*'s great detail as to messaging protocol and because it describes security measures to delay data packets according to certain rules in order to diminish the quality of illegitimate data traffic. Malek Decl. at ¶ 96; Ex. D, ¶ 33. Fig. 3 of *Konstantinov* below illustrates that each data packet includes a "payload" (data provided from a source device to be consumed by the destination application) and addressing information identifying "destination address" (i.e., recipient device IP address) and "destination port #" (i.e., port number identifying the virtual location on the recipient device at which a specific software application is located):

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 104 of 114

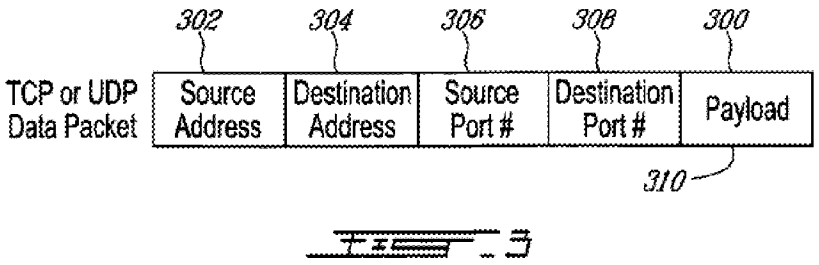


Fig. 3

Ex. D, Fig. 3 and ¶ 39.

Dependent claims 2-7, 10, 12-13, and 15-17 would have been obvious for the same reasons discussed above in at least Ground 2. *See Sections Supra* Sections II.D.2 through II.D.14.

G. Ground 5: The Combination of *Rittmaster* (as in any of Grounds 1-4) and *Freese* Renders Obvious Claims 8-9

1. Claim 8 – *"further comprising a secure server to store a secure authorization list, the secure authorization list indicating the authorized software components and the authorized network elements that are allowed to communicate using the network server system."*

Claim 8 depends from claim 1. While *Rittmaster* does not explicitly mention use of a secure server to store a secure authorization list identifying authorized software components and authorized network elements, other prior art discloses separate secure servers to maintain information regarding the status of software applications on mobile devices and capable of tracking and managing related permissions required for those software applications to communicate over the network with other elements of the network. Malek Decl. at ¶ 96. For instance, U.S. Patent No. 7,184,554 to Freese et al. ("*Freese*") (Ex. M) discloses a management system allowing remote control of permissions and other aspects of user devices. It would have been obvious to layer a management system of the type disclosed in *Freese* on top of the trigger-based communication network of *Rittmaster* because both systems relate to the same types of networks and devices and *Freese's* management system would conveniently allow third parties to adjust authorizations of devices and applications on those devices based on location and/or based on subscription status. Malek Decl. at ¶ 96. The combination of these references would have been straightforward to those skilled in the art, implementing known techniques to achieve a predictable result. *Id.*

Freese discloses a Public Land Mobile Network (PLMN) 1 connected to wireless devices 2 and 4 as shown below:

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 105 of 114

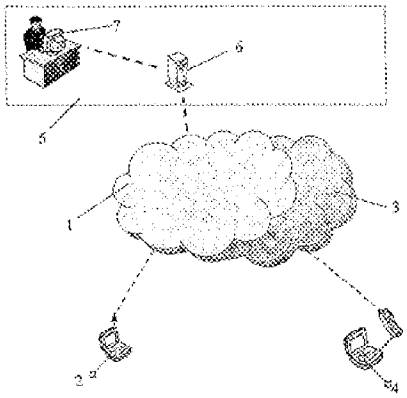


Figure 1

Ex. M Fig. 1; the above network also includes a "Management Centre" 5 that includes a Management Server 6 and Management Console 7. Ex. M, 3:18-35; Malek Decl. at ¶ 96. This Management Centre 5 manages mobile devices such as phones, PDAs, and laptops that are connected to a network, just like the end-user devices of *Rittmaster*'s network. Ex. M, 1:6-10; Malek Decl. at ¶ 96. A management agent program is stored on the end-user device to monitor the status of applications installed on the device and receive management instructions to manage applications accordingly. Ex. M, 1:24-40. This allows the device software architecture to be modified remotely by operators or authorized third parties, for instance to turn applications on or off by sending an appropriate management instruction to the end-user device. Ex. M, 1:46-57; Malek Decl. at ¶ 96. As *Freese* explains, "[a]n important function of the management agent is that of reporting to the Management Centre 5" which "allows the Management Centre 5 to maintain an accurate record of the status of a mobile device." Ex. M, 4:33-38. This includes reported information such as "successful installation of a new application, or the failure of an instructed installation." *Id.* Given that this record (i.e. list) of the status of applications/devices is stored by the Management Centre, it would have been obvious to store the list either on the Management Server or Management Controller that make up the Management Centre. Malek Decl. at ¶ 96. *Freese* also notes that control of software applications on the end-user device through the Management Centre could be based on whether a license to the software is current or expired, turning the software on or off accordingly. Ex. M, 4:11-18. The management instructions sent from the Management Server to the end-user device are preferably cryptographically signed, demonstrating that the Management Server is secure. Malek Decl. at ¶ 96. Thus, just as in claim 8, *Freese* shows a secure authorization list indicating authorized software components and authorized network elements that are allowed to communicate using the network server system.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 106 of 114

Id.; Ex. M, 2:41-49. It would have been obvious to layer a management system of the type disclosed in *Freese* on top of the trigger-based communication network of *Rittmaster* because both systems relate to the same types of devices (mobile end-user devices such as cellular phones, PDAs, and laptops) and *Freese's* management system would conveniently allow third parties to turn device-based applications on and off depending on whether they are allowed to receive content from certain providers (i.e. network elements) in certain regions and/or based on whether they are currently subscribed to an applicable service. Malek Decl. at ¶ 96. The implementation of the two systems would have been straightforward to those skilled in the art, implementing known techniques to achieve a predictable result. *Id.*

2. Claim 9 – *"further comprising the respective device link agent on each wireless end-user device receiving access authorization information from the secure server, the access authorization indicating, respectively for each wireless end-user device, the software components authorized to receive messages via the device link agent on that device."*

Claim 9 depends from claim 8, which would have been obvious for the reasons discussed above. The features of claim 9 also would have been obvious in view of *Rittmaster* in combination with *Freese*. Malek Decl. at ¶ 97. Each user device connected to *Rittmaster's* network would have had a device link agent to receive incoming communications and route them to the appropriate software application as described above in connection with claim 1. *Freese* allows the device software architecture to be modified remotely by operators or authorized third parties, for instance to turn applications on or off by sending an appropriate management instruction to the end-user device. Ex. M, 1:46-57; Malek Decl. at ¶ 97. When adding the *Freese* management system to *Rittmaster's* network, which would have been a straightforward combination of the two prior art disclosures, management instructions would be sent to the device link agent and then communicated within the end-user device to turn a software application on or off depending on existing permissions because the purpose of a device link agent is to receive all incoming messages and distribute them to the appropriate software application on the end-user device. Malek Decl. at ¶ 97. In other words, a message would be received by the device agent from the secure management server indicating whether one or more software applications should be "on" or "off," indicating whether they are currently authorized to receive communications from network elements. *Id.* For at least these reasons, the combination of *Rittmaster* and *Freese* teaches a respective device link agent on each wireless end-user device receiving access authorization information from the secure server, the access authorization indicating, respectively for each wireless end-user device, the

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 107 of 114

software components authorized to receive messages via the device link agent on that device, just as in claim 9. Malek Decl. at ¶ 97; Ex. M, 2:41-49. This combination of prior art elements would have been obvious because both *Rittmaster* and *Freese* relate to networks for the same types of devices (mobile end-user devices such as cellular phones, PDAs, and laptops), and *Freese's* management system would have been added to *Rittmaster*'s network to conveniently allow third parties to turn device-based applications on and off using communications to the device link agent of individual end-user devices. Malek Decl. at ¶ 97. The implementation of the two systems would have been straightforward to those skilled in the art, implementing known techniques to achieve a predictable result. *Id.*

H. Ground 6: The Combination of *Rittmaster* (as in any of Grounds 1-4) and *Freese* and/or *Moon* Renders Obvious Claim 11

1. Claim 11 – *"wherein one of the software components on a given one of the wireless end-user devices is a policy control agent, and the data to be consumed by the policy control agent comprises service settings and/or configuration information for the given device."*

Claim 11 depends from claim 1. The '320 Patent does not limit the "policy agent" to a particular type of software, but identifies various potential functions of such agents, including "download management." Malek Decl. at ¶ 99; Ex. A, 49:14-19. *Rittmaster* describes that "[i]n preferred embodiments, if access is allowed (in step 38), 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 ¶ 99; Ex. C, ¶ 56. At a minimum, it would have been obvious to have policy control messages sent through *Rittmaster*'s server cause service setting or configuration changes to the end-user device in order to permit access to data files and/or computer programs sent to the end-user device in view of additional prior art. Malek Decl. at ¶ 99-100. For instance, analogous prior art patents such as *Freese* disclose installing a "management agent" program on a wireless device of the type used in *Rittmaster* in order to receive management instructions from a remote "management center" so that the management agent can manage applications on the device accordingly. Ex. M, Abstract; Malek Decl. at ¶ 100. The management agent may "control and enforce policies on the wireless device" such as security policies, encryption, and/or permitted connections. Malek Decl. at ¶ 100; Ex. M, 2:45-49. Those skilled in the art would have recognized at the time of the claimed invention of the '320 Patent that in view of *Rittmaster*'s disclosure of differing requirements for accessing content in different geographic systems, it would be beneficial

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 108 of 114

to use the same geolocation-based trigger system to automatically change security settings (including connectivity and/or encryption settings) in order to enhance security in locations where the user device is more at risk or where required by local wireless systems and/or local regulations. Malek Decl. at ¶ 100. In addition to updating device settings based on location, it would have been obvious in view of *Freese* to update device settings based on other status indicators, such as whether or not the user has an up-to-date license to use certain features or applications. Malek Decl. at ¶ 100. *Freese* suggests that the management agent that it discloses "allows operators and software vendors to maintain control over who may use their software…in an extremely flexible manner," such as where "users may be charged a license fee for a fixed time period add, after that time has expired and the user has not renewed the license, the software in the user's device may be inhibited" or where "the management agent proceeds to update the virus signature database in the memory of the device" when the management center makes an update to anti-virus software available. Malek Decl. at ¶ 100; Ex. M, 4:11-32. The management agent disclosed by *Freese* can receive messages from a server (Ex. M, 3:53-65), and therefore it would require no more than ordinary and routine skill to adapt *Rittmaster*'s server system to send instructions to a management agent on the device. Malek Decl. at ¶ 100.

Alternatively, it would have been obvious at the time of the claimed invention of the '320 Patent to implement a policy control agent in view of U.S. Patent No. 6,085,098 to *Moon et al.* ("*Moon*"), which discusses automatically configuring settings of software applications on a portable device such as a smartphone based on geographic location. Malek Decl. at ¶ 100; Ex. N, Abstract and 4:36-5:24. For example, settings need to be updated for phone dialer software or calendar software as geographic location of a user device (such as a mobile phone) changes. Malek Decl. at ¶ 100; Ex. N, 5:6-23. It would have been obvious to modify the server in *Rittmaster* to make such automatic configurations of settings to end-user devices based on communicated geographic location of those devices in order to enable or optimize use of message content sent from the server to the recipient end-user devices. Malek Decl. at ¶ 100. A PHOSITA would have recognized that, at the time of the claimed invention of the '320 Patent, system updates, including system settings and software configurations, were routinely made to user devices through servers prior to the time that the applications that led to the '320 Patent were filed, and it would have been obvious to configure *Rittmaster*'s server to provide such updates. *Id.*

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 109 of 114

I. Ground 7: The Combination of *Rittmaster* (as in any of Grounds 1-4) and *Ellison* Render Obvious Claim 14

1. Claim 14 – *"wherein the device link agent on a given device executes in a secure execution environment, and at least one of the software components on that device executes outside of the secure execution environment."*

Claim 14 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 ¶ 102. It would have been obvious at the time of the claimed invention of the '320 Patent 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* (Ex. L) or similar prior art references in order to divide applications between secure and unsecure operating environments. This would have been an obvious optimization and prioritization of security resources, at the time of the claimed invention of the '320 Patent, 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 ¶ 8102.

The '320 Patent discloses in passing that all software may be stored in secure memory, that software may be stored in encrypted form in secure memory, and executing all software and communications within a secure execution environment, hardware environment, and/or protected memory space. Ex. A, 43:32-37. The '320 Patent does not appear to suggest that there is any advantage to having some software components outside of a secure execution environment while other components are within a secured environment. Malek Decl. at ¶ 102. However, protecting some but not all software of a device in a secure environment was known at the time of the claimed invention of the '320 Patent, 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 ¶ 102. For instance, the *Ellison* reference discloses a method to protect a subset of a software environment. Malek Decl. at ¶ 102; 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 ¶ 102; Ex. L, 2:41-51. The division of a component into rings is typically based on the degree or level of privilege. Malek Decl. at ¶ 102; *see also* Ex. L, 2:51-53. It would have been obvious to a PHOSITA at the time of the claimed invention of the '320 Patent 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

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 110 of 114

the teachings of *Ellison* or similar prior art references in order to divide applications between secure and unsecure operating environments. Malek Decl. at ¶ 102.

J. Ground 8: The Combination of *Rittmaster* (as in any of Grounds 1-4) and *Fok* and/or *Ellison* Render Obvious Claim 17

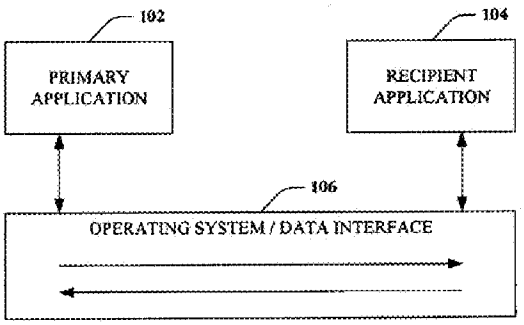
1. Claim 17 – *"at least a given one of the devices further comprising a secure interprocess communication service separately secured from the secure Internet data message link, the device link agent for the given device causing messages to be securely delivered to a software process by initiating delivery of each such message on the secure interprocess communication service."*

Claim 17 depends from claim 1. Claim 17 would have been obvious in view of *Rittmaster* (Grounds 1 or 2), or *Rittmaster* in combination with *Shenfield* (Ground 3) and/or *Klassen/Konstantinov* (Ground 4), in further combination with U.S. Patent Pub. No. 2008/0215883 to *Fok et al.* ("*Fok*," Ex. O)[8]. Malek Decl. at ¶ 104 and 134. *Fok* describes techniques for "secure interapplication communication" in a "mobile operating environment." Malek Decl. at ¶ 104; Ex. O, ¶¶ 36-37, 81, 106-108, and Figs. 4 and 8-9. *Fok* uses a "round trip" concept where a "handshake" is established between a "primary application" and one or more "recipient" applications. Malek Decl. at ¶ 104; Ex. O, ¶¶ 47-53, 96-102, 106-108, and Figs. 7-10. Applications verify that another application is trusted during the handshake process using "a list of unique identifiers" associated with trusted applications installed on the mobile device. Malek Decl. at ¶ 104; Ex. O, ¶¶ 48-50, 96, 101-102, 106, and Figs. 8-9.

Even if "secure interprocess communication service" is understood to require more than secure communication between two processes on the same device, *Fok* describes an interprocess communication (IPC) service where an operating system provides the data interface between applications. Malek Decl. at ¶ 104. For instance, Fig. 1 of *Fok* below shows the operating system providing an interface that mediates communication between two processes, the primary application 102 and recipient application (104):

[8] Fok is prior art under 35 U.S.C. § 102(e) (pre-AIA) and appears to be supported by both of the provisional applications to which it claims benefit.

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 111 of 114



Ex. K, ¶ 46 & Fig. 1; Malek Decl. at ¶ 104. The handshake can be initiated by the primary application 102 by sending a handshake request that includes at least a unique identifier of the primary application 102 or a random number generated for the handshake or both. Malek Decl. at ¶ 104; Ex. K, ¶ 48. Typically, an operating system (106) can require certain standards to be met for applications designed to execute on the operating system, such as a list of unique identifiers of trusted primary applications. *Id.* The recipient application 104 could then use such a list to verify that a received handshake request is sent by an application authorized to make the request, which would then cause the recipient application 104 to trust and engage in communication with such an application. *Id.* Notably, *Fok* states that subsequent to receiving the handshake response the trusted applications can exchange data, including requests that can include data within the request itself (*i.e.* send a message that includes a payload), although pointers identifying data in shared memory could alternatively be used. Malek Decl. at ¶ 104; Ex. K, ¶ 53. Thus *Fok* contemplates mapping an application identifier in a message to a software process corresponding to the application identifier and forwarding application data in the message itself to the software process via a secure interprocess communication service. Malek Decl. at ¶ 104.

Combining *Rittmaster* and *Fok* would have been obvious to a PHOSITA at the time of the claimed invention of the '320 Patent because it would have been a matter of combining prior art elements according to known methods to yield predictable results, and there would have been a reasonable expectation of success because *Fok*'s interprocess system is for use in the types of mobile devices (e.g., laptops and mobile phones) described in *Rittmaster*. Malek Decl. at ¶ 104. *Rittmaster* acknowledges that computers and communication interfacing are well known in the art and therefore not described therein in detail, and a PHOSITA would have looked to other prior art such as *Fok* in order to determine how to handle interprocess communications within the end-user

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 112 of 114

devices. Malek Decl. at ¶ 104. The teachings of *Fok* would be added to the end-user devices of *Rittmaster* without affecting how the mobile end-user devices communicate with the network, and as a result the secure interprocess communication service of *Fok* would be separately secured from the secure Internet data message link between the end-user device of *Rittmaster* and the associated server. Malek Decl. at ¶ 104.

Claim 17 also would have been obvious in further view of *Ellison* (Ex. L), which discloses a method to protect a subset of a software environment and providing a hierarchy, or "rings," dividing hardware and software components designed to perform dedicated tasks within an operating system. Malek Decl. at ¶ 104; Ex. L, Abstract, 2:41-51. The division of a component into rings is typically based on the degree or level of privilege. *Id.*; *see also* Ex. L, 2:51-53. Not only would it have been obvious to a PHOSITA at the time of the claimed invention of the '320 Patent to divide the memory of an end-user device of *Rittmaster* into such rings based on the sensitivity of particular applications as in *Ellison*, a PHOSITA also would have found it obvious to include a secure interprocess communication service so that communication of information between device components does not compromise security as information is transmitted between the secure device link agent and the secure execution environment. Malek Decl. at ¶ 104.

K. Ground 9: The Combination of *Rittmaster* (as in any of Grounds 1-4) and *Coffee* and/or *Basso* Render Obvious Claim 18

1. Claim 18 – *"wherein at least one of the secure Internet data messages comprises multiple identifier/data pairs."*

Claim 18, which depends from claim 1, specifies that two or more payloads, each having an identifier, may be sent in a single message. Malek Decl. at ¶ 105. *Rittmaster* describes this element for the reasons discussed above in Sections II.C.13., II.D.14., II.E.14, and II.F. To the extent *Rittmaster* is found not to disclose all the features of claim 18, a PHOSITA, at the time of the claimed invention of the '320 Patent, would have been motivated to look to *Coffee* to remedy such deficiencies. More specifically, a PHOSITA would have understood 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 identifier, in order to reduce throughput problems by bundling small messages into larger, less frequent messages. Malek Decl. at ¶ 105; Ex. S, ¶¶ 117-119. Similarly, the *Basso* reference discloses that multiple messages to be sent form a network processor may be bundled into a single message to

Headwater Research LLC
Ex. 2017, IPR2026-00106
Page 113 of 114

reduce the number of messages and improve performance. Malek Decl. at ¶ 105; Ex. T, Abstract. A PHOSITA, at the time of the claimed invention of the '320 Patent, would have combined message bundling as in *Coffee* or *Basso* with the system of *Rittmaster* in order to enhance throughput by reducing the number of messages sent to a single end-user device. Malek Decl. at ¶ 105.

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 '320 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 1-18 of the '320 Patent unpatentable, thereby raising substantial new questions of patentability regarding these claims. *ex parte* reexamination should be commenced, and claims 1-18 should be found invalid.

Respectfully submitted,

FITCH, EVEN, TABIN & FLANNERY LLP

Dated: April 15, 2026

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

120 South LaSalle Street
Suite 2100
Chicago, Illinois 60603
(312) 577-7000
(312) 577-7007 (fax)
Attorney for Requester
Walmart Inc.