IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

CELLCO PARTNERSHIP D/B/A VERIZON WIRELESS,
T-MOBILE USA, INC.,
AT&T SERVICES INC., AT&T MOBILITY LLC, AND AT&T CORPORATION
Petitioners,

v.

HEADWATER PARTNERS I LLC.
Patent Owner.

_____

U.S. Patent No. 9,198,042
Title: SECURITY TECHNIQUES FOR DEVICE ASSISTED SERVICES

_____

Inter Partes Review No.: IPR2024-00809

DECLARATION OF HENRY HOUH, Ph.D., UNDER 37 C.F.R. § 1.68 IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 9,198,042

Mail Stop: Patent Board
Patent Trial and Appeal Board
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

I. INTRODUCTION 4

II. BACKGROUND AND QUALIFICATIONS 7

III. MATERIALS CONSIDERED FOR THIS DECLARATION 16

IV. SUMMARY OF OPINIONS 16

V. OVERVIEW OF THE '042 PATENT, ITS PATENT FAMILY, AND ITS PROSECUTION HISTORY 17

A. Overview of the '042 Patent. 17

B. Overview of the Prosecution History of the '042 Patent 24

VI. LEVEL OF ORDINARY SKILL IN THE PERTINENT ART 25

VII. CLAIM CONSTRUCTION 26

VIII. UNDERSTANDING OF THE LAW 26

IX. SCOPE AND CONTENT OF THE PRIOR ART 29

A. Limont (EX-1004). 29

B. Wright (EX-1005) 37

C. Xu (EX-1016) 52

D. Polson (EX-1008) 60

E. Background Prior Art 72

1. Mobile Phone Policy Settings Reference Pearce (EX-1006) 72

2. Storing and Modifying Policies on Mobile Phones Reference Aarnos (EX-1007) 78

3. Hardware Enforced Protected Partition References Arm TrustZone Microprocessor Report (EX-1009) and Arm TrustZone Paper (EX-1010) 81

4. Encryption Protected Partition References (EX-1011) (EX-1014) (EX-1015) 89

5. Mobile Phones / Wearable Devices Implementing WWAN / WLAN Gateways (EX-1017) (EX-1018) (EX-1019) (EX-1020).....105

X. DETAILED UNPATENTABILITY ANALYSIS FOR THE '042 116

A. Ground 1: Challenged Claims 1, 2, and 6-18 Are Obvious In View of Limont combined with Wright and optionally Xu. 117

1. A POSA Would Have Been Motivated To Combine Limont, With Wright and Optionally Xu With A Reasonable Expectation Of Success. 118

2. Challenged Claims 1-2, 6-18 Are Disclosed By The Proposed Combination 131

a) Claim 1 131

Preamble: [*1.0] A method comprising:* 131

i. ***[1.1] receiving, over a service control link, a report from a wireless end-user device, the report comprising information about a device service state;*** 136

ii. ***[1.2] determining, based on the report, that a particular service policy setting of the wireless end-user device needs to be modified,*** 148

iii. ***[1.3] the particular service policy setting being stored in a protected partition of the wireless end-user device, the protected partition configured to deter or prevent unauthorized modifications to the particular service policy setting,*** 160

iv. ***[1.4] the particular service policy setting being associated with a service profile that provides for access by the wireless end-user device to a network data service over a wireless access network*** 196

v. ***[1.5] the particular service policy setting configured to assist in controlling one or more communications associated with the wireless end-user device over the wireless access network; and*** 206

vi. ***[1.6] in response to determining that the particular service policy setting needs to be modified, sending configuration information to the wireless end-user device over the service control link, the configuration information configured to assist in modifying or allowing modifications to the particular service policy setting.*** 208

b) Claim 2: *The method of claim 1, wherein the particular service policy setting assists in implementing a roaming control, a parental control, or an enterprise wireless wide-area network (WWAN) management control*.....211

c) Claim 6: *[6.0] The method of claim 1, further comprising: obtaining a service usage measure, the service usage measure accounting for the one or more communications associated with the wireless end-user device over the wireless access network; and:*..214

vii. **Claim 6.1:** ***based on the service usage measure, taking an action.***.....216

d) Claim 7: [7.0] The method of claim 6, wherein the service usage measure comprises a measure of a service usage activity....218

e) Claim 8: [8.0] The method of claim 6, wherein the action is to verify the service usage measure.....218

f) Claim 9: *[9.0] The method of claim 6, wherein the action is to quarantine or suspend the wireless end-user device*.....221

g) Claim 10: *[10.0] The method of claim 6, further comprising obtaining secondary information associated with the wireless end-user device, and wherein the action is to verify the service usage measure using the secondary information.*.....223

h) Claim 11: *[11.0] The method of claim 1, further comprising receiving, from the wireless end-user device, an integrity report configured to assist a network element in identifying an access control integrity violation.* 225

i) Claim 12: *[12.0] The method of claim 1, wherein the configuration information comprises at least a portion of the service profile.* 230

j) Claim 13: *[13.0] The method of claim 1, wherein the service control link is secured by an encryption protocol.* 233

k) Claim 14: *[14.0] The method of claim 1, wherein the device service state comprises a service profile setting, a service usage policy setting, or a device-assisted services (DAS) setting.* 236

l) Claim 15: [*15.0] The method of claim 1, wherein the device service state provides information about a user preference*. 238

m) Claim 16: *[16.0] The method of claim 1, wherein the device service state comprises information associated with an encryption key*. 242

n) Claim 17: *[17.0] The method of claim 1, wherein the device service state comprises an agent report, a service usage record, a transaction record, or an integrity report.* 245

o) Claim 18: *[18.0] The method of claim 1, wherein the device service state comprises user status information, device status information, application status information, a device location, or a device quality-of-service (QOS) state.* 248

B. Ground 2: The Challenged Claims Are Obvious Over Limont in combination with Wright and optionally Xu in further view of Polson. 250

1. Motivation To Include Polson In The Combination. 250

2. This Combination Renders Obvious Challenged Claims 3-5. 266

p) Claim 3: *[3.0] The method of claim 1, wherein the wireless end-user device is an intermediate networking device for forwarding traffic between a wireless wide-area network (WWAN) and a wireless local-area network (WLAN).* 266

q) Claim 4: *[4.0] The method of claim 1, wherein the wireless end-user device is an intermediate networking device comprising a cellular device, the intermediate networking device for forwarding traffic between the wireless access network and a second network.*

278

r) Claim 5: [5.0] The method of claim 1, wherein the wireless end-user device is an intermediate networking device, and the particular service policy setting assists one or more other end-user devices in communicating over the wireless access network via the intermediate networking device.....281

XI. SECONDARY CONSIDERATIONS DO NOT REBUT THE PRIMA FACIE CASE OF OBVIOUSNESS 288

XII. CONCLUSION.....289

HENRY H. HOUH.....292

Education.....292

Experience 292

Honors.....296

Patents and Patent Publications.....296

Trials, Testimony and Depositions.....298

Publications 303

Leadership, Activities and Interests 305

Petitioner's Exhibit List

Exhibit #	***Description***
1001	U.S. Patent No. 9,198,042 ("the '042")
1002	Prosecution history of the '042 ("'042 File History")
1003	Declaration of Petitioner's Expert Petitioners expert, Dr. Henry Houh
1004	U.S. Publication No. 2007/0006289 ("Limont")
1005	U.S. Publication No. 2004/0123153 ("Wright")
1006	U.S. Publication No. 2006/0183461 ("Pearce")
1007	U.S. Publication No. 2007/0288989 ("Aarnos")
1008	U.S. Publication No. 2007/0104169 ("Polson")
1009	Arm TrustZone Microprocessor Reports
1010	Arm TrustZone Papers
1011	U.S. Publication No. 2006/0112427
1012	U.S. Pat. No. 7,849,310
1013	Limont Prosecution History Excerpts (Application No. 11/171,850)

Exhibit #	***Description***
1014	U.S. Publication No. 2006/0224742A1
1015	U.S. Publication No. 2009/0265754
1016	U.S. Publication No. 2007/0061535 ("Xu")
1017	U.S. Pat. No. 8,064,417
1018	U.S. Pat. No. 7,672,695
1019	U.S. Pat. No. 7,881,267
1020	U.S. Publication No. 2008/0244018
1021	Plaintiff's Infringement Contention (Verizon case)
1022	Docket Control Order
1023	List of Related Applications

I, Henry Houh, Ph.D. hereby declare as follows:

I. INTRODUCTION

1. I have been retained as an expert witness on behalf of Cellco Partnership d/b/a Verizon Wireless, T-Mobile USA, Inc., AT&T Services Inc., AT&T Mobility LLC, and AT&T Corporation (collectively, "Petitioners") for the above-captioned Petition(s) for *Inter Partes* Review ("IPR") of claims 1-18 of U.S. Patent No. 9,148,042 ("the '042 patent") (the Challenged Claims). I am being compensated for my time in connection with this IPR at my standard consulting rate of $820 per hour. My compensation is in no way dependent on the outcome of this matter.

2. I have been asked to provide my opinions regarding whether the Challenged Claims are unpatentable as obvious. In preparing this declaration, I have reviewed the '042 patent, the file history of the '042 patent, and numerous prior art references from the time of the alleged invention.

3. In forming the opinions expressed in this declaration, I relied upon my education and experience in the relevant field of the art, and have considered the viewpoint of a person having ordinary skill in the relevant art, as of January 2009.

4. I understand that '042 claims priority through several applications with the earliest filed on January 28, 2009. My analysis as set forth below uses that date as the priority date of the '042 patent and the Challenged Claims.

5. My opinions directed to the unpatentability of the challenged claims are based, at least in part, on the following prior art publications:

Reference	Date of Public Availability
Limont, U.S. Patent Publication No. 2007/0006289	Limont published on January 4, 2007 from an application filed on June 30, 2005 ("Limont") (EX-1004). Limont is prior art under at least the pre-AIA version of 35 U.S.C. § 102(a), (b), (e), and (g). Limont is attached as Exhibit 1004 to the IPR.
Wright, U.S. Patent Publication No. 2004/0123153	Wright published on June 24, 2004 from an application filed on April 11, 2003 ("Wright") (EX-1005). Wright is prior art under at least pre-AIA version of 35 U.S.C.

	§ 102(a), (b) (e), and (g). Wright is attached as Exhibit 1005 to the IPR.
Xu, U.S. Patent Publication No. 2007/0061535	Xu published on March 15, 2007 from an application filed on September 12, 2005 ("Xu") (EX-1016). Xu is prior art under at least pre-AIA version of 35 U.S.C. § 102(a), (b) € and (g). Xu is attached as Exhibit 1016 to the IPR.
Polson, U.S. Patent Publication No. 2007/0104169	Polson published on March 15, 2007 from an application filed on September 12, 2005 ("Polson") (EX-1008). Polson is prior art under at least pre-AIA version of 35 U.S.C. § 102(a), (b) (e) and (g). Xu is attached as Exhibit 1008 to the IPR.

II. BACKGROUND AND QUALIFICATIONS

6. My background and expertise that qualify me as an expert in the technical issues in this case are as follows:

7. As indicated on my *Curriculum Vitae* attached as **Exhibit A**, I received a Ph.D. in Electrical Engineering and Computer Science from the Massachusetts Institute of Technology ("MIT") in 1998. I also received a Master of Science degree in Electrical Engineering and Computer Science in 1991, a Bachelor of Science Degree in Electrical Engineering and Computer Science in 1989, and a Bachelor of Science Degree in Physics in 1990, all from MIT.

8. During my college studies, I focused on communications and data networking. I took specialized courses including graduate courses in telecommunications networks, optical communications, and data networking. I, along with other graduate students in a networking research group, maintained both the computer workstations and the networking devices in the research group.

9. I also served as a teaching assistant for the Computation Structures core course a number of times. At the time, the course involved teaching computer architecture at a low level, and the laboratory component involved building a CPU from discrete components at the gate level and higher. When I was enrolled in this

course as an undergraduate student, I redesigned the hardware and software, including microcode and nanocode of this CPU, to achieve an average speed up of roughly thirty times. Based in part on this, I became a laboratory assistant, head laboratory assistant, and then a teaching assistant in my second term senior year, which is unusual in that teaching assistantships at MIT are normally reserved for graduate students. I further became head teaching assistant and also taught some recitation sections.

10. As part of my doctoral research at MIT from 1991-1998, I worked as a research assistant in the Telemedia Network Systems ("TNS") group at the Laboratory for Computer Science. The TNS group built a high-speed gigabit ATM network and applications which ran over the network, such as remote video capture (including audio), processing and display on computer terminals. In addition to helping design the core network components (such as the ATM switch), designing and building the high-speed ATM links, and designing and writing the device drivers for the interface cards, I also set up the group's web server, which at the time was one of the first several hundred web servers in existence. I used programmable logic devices, such as programmable array logic and field programmable gate arrays, and their software development environments, in the

design of these components. Our high-speed data network carried multimedia data including video and audio data within ATM cells.

11. The TNS group was the first group to initiate a remote video display over the World Wide Web. Vice President Al Gore visited our group in 1996 and received a demonstration of—and remotely drove—a radio-controlled toy car with a wireless video camera mounted on it; the video was encoded by TNS-designed hardware, streamed over the TNS-designed network and displayed using TNS-designed software. During this time, I also modified a web server to determine the location of client, and present different web pages depending on location.

12. I authored or co-authored twelve papers and conference presentations on our group's research. I also co-edited the final report of the gigabit networking research effort with Professor David Tennenhouse and Senior Research Scientist David Clark. David Clark is generally considered to be one of the fathers of the Internet Protocol and served as Chief Protocol Architect for the Internet. With its focus on networking, the group, including myself, set up and maintained the network and computer systems. These systems included the networking on the workstations and desktops, the distributed file system, desktops and workstations, setting up and maintaining the distributed file system (Network File System) and

the authentication system (Network Information Service, formerly known as Yellow Pages). Our system allowed users to log into any of the group's workstations using their username/password, which allowed that all of the user's files would be virtually mounted on that workstation as a networked home directory.

13.I defended and submitted my Ph.D. thesis, titled "Designing Networks for Tomorrow's Traffic," in January 1998. As part of my thesis research, I analyzed local-area and wide-area flows to show a more efficient method for routing packets in a network, based on traffic patterns at the time. My thesis also addressed real-time streamed audio and video. The network traffic that I analyzed was IP protocol traffic, including UDP and TCP.

14.I have been involved in Voice over Internet Protocol ("VoIP") technologies since 1997 and have specific experience in designing and testing VoIP networks.

15.From 1997 to 1999, I worked at NBX Corporation, which was acquired by 3Com Corporation in 1999. During this time, I was a Senior Scientist and Engineer working in IP Telephony. NBX delivered the world's first fully featured business telephone system to run over a data network, the NBX100. NBX was one of the first business phone systems to be configurable via a web interface. Users

and administrators had access to varying levels of configuration for the phone system.

16. As part of my work at NBX, I designed the core audio reconstruction algorithms for the telephones which depacketized the voice data and reconstructed the audio. In addition, I designed the voice data packet transmission algorithms. I created a system to capture and analyze network packets sent by devices in the NBX system for aid in testing and debugging. I also designed and validated the core packet transport protocol used by the phone system. In addition, I designed and oversaw the development of the underlying transport protocol used by the NBX100 phone system for reliable packet transport. That transport protocol is still used by the NBX100 system and its successors and is estimated to be used hundreds of millions of times daily. I wrote NBX's first demonstration IP software stack, which added the capability for utilizing the NBX100 phone system on an IP network. NBX first demonstrated a phone in the NBX100 system working over the Internet in 1998 at a trade show in Las Vegas. I was later the lead architect in designing NBX's next-generation highly scalable system, and, after NBX was acquired by 3Com, I did some work with 3Com's cable equipment division, including demonstrating a working NBX IP phone system over 3Com's cable

equipment infrastructure using an early version of DOCSIS at a trade show in 1999. The NBX100 was the market's leading business phone system to run on a data network for several years following its introduction. During that time, I became more familiar with the various standards relevant to Internet telephony as well as the problems which designers of commercial telephony operations were faced with in implementing VoIP.

17.I, along with two of NBX's founders, was awarded U.S. Patent No. 6,697,963 titled "Telecommunication method for ensuring on-time delivery of packets containing time-sensitive data," for some of the work we did while at NBX.

18.After NBX, I worked at Teradyne, a test tool company primarily focused on semiconductors. Teradyne had recently acquired Hammer, a company that specialized in load and functional testing for telecommunications systems. The Hammer product is well known as a telecom test tool. Teradyne spun out Hammer and several other internal divisions into an independent company called Empirix. I became Chief Technologist of the Hammer division of Empirix. Empirix was a leader in VoIP network testing and monitoring.

19. At Empirix, I laid out a new multi-year product vision for data network testing, secured internal funding for the effort, and led a team to deliver a new technology platform to the market in February 2001. This new product, PacketSphere, initially emulated network behavior so that wide-area VoIP connections could be tested in a lab. A later release allowed PacketSphere to generate high volumes of VoIP calls, including media streams, and to monitor the quality of VoIP voice streams. Later, the core technology was added to other Empirix products such as Empirix's Hammer XMS to monitor thousands of VoIP media streams in real time to determine their quality. PacketSphere was Empirix's most successful new platform introduction. Companies purchased the PacketSphere product to emulate an Internet Protocol network to see the effects of deploying their product on the Internet prior to launch. PacketSphere received several industry awards.

20. During my time at Empirix, I presented lectures on VoIP and data network testing to companies including Lucent Labs (formerly AT&T Bell Labs). I was also invited to present several guest lectures in a software engineering course at MIT. Since then, I have also participated twice as a unit lecturer (two weeks) in an experimental course that was taught by an Institute Professor (the highest award

that a MIT Professor can achieve) and sponsored by the Chairman of the MIT Corporation (MIT's board of trustees).

21.From 2004 to 2008, I was employed by BBN Technologies Corp., a technology research and development company located in Cambridge, Massachusetts. BBN Technologies is a world-renowned company with expertise in acoustics, speech recognition, and communications technology. BBN Technologies staff have pioneered many internetworking technologies and Internet applications, and built some of the world's largest government and commercial data networks.

22.My duties and responsibilities at BBN Technologies generally included commercialization of the technologies developed by BBN Technologies, which included spinning off companies and growing commercial businesses in-house. More particularly, I was involved in utilizing the award-winning AVOKE STX speech recognition technology to create the public audio/video search engine EveryZing (formerly known as PodZinger) which was spun out into a stand-alone company now known as RAMP, Inc. PodZinger won the 2006 MITX Technology Award for best Web 2.0 Application and was also named the 2006 Forbes Favorite Video & Audio Search Engine, beating out Google, Yahoo, and other companies.

After managing the creation of the initial prototype system, PodZinger built out a full streaming audio and video search solution when I was the Vice President of Operations and Technology there. I was also involved in the Boomerang Mobile Shooter Detection project as the Vice President of Engineering for the program. The Boomerang system was deployed to Iraq and Afghanistan, and was credited with saving many lives.

23.From 1989 to 1990, I worked at AT&T Bell Laboratories on optical computers. This work generated six peer-reviewed papers, and multiple U.S. and European patent applications in which I was named as a co-author or inventor. I also interned at AT&T Bell Laboratories in 1987 and 1988. Additional relevant experience in the field of optical computers is listed in my *Curriculum Vitae*.

24.I am a named inventor on several patents and published patent applications that are related to the VoIP technology including: U.S. Patent No. 6,967,963, entitled "Telecommunication Method for Ensuring On-time Delivery of Packets Containing Time- Sensitive Data"; U.S. Patent Application Publication No. 20020015387, entitled "Voice Traffic Packet Capture and Analysis Tool for a Data Network"; U.S. Patent Application Publication No. 20020016708, entitled "Method and Apparatus for Utilizing a Network Processor as Part of a Test

System"; U.S. Patent Application Publication No. 20020016937, entitled "Method and Apparatus for Utilizing a Network Processor as Part of a Test System"; and U.S. Patent No. 7,590,542, entitled "Method of Generating Test Scripts Using a Voice-Capable Markup Language."

25.[This paragraph left intentionally blank].

III. MATERIALS CONSIDERED FOR THIS DECLARATION

26.In addition to my general knowledge, education, and experience, I have considered all of the materials referenced in my declaration as well as the materials listed in **Exhibit B** in forming my opinions.

IV. SUMMARY OF OPINIONS

27.Based on my review of the '042 patent and its prosecution history, the other materials I have considered, and my knowledge and experience, my opinions are as follows. The prior art renders the claims obvious for the '042 patent as identified below.

28.In my analysis herein, I have considered the various disclosures (e.g., the '042 patent, the prior art, …) from the view of an person of ordinary skill in the art ("POSA") at the time of the invention, which I have also referenced as the "priority date" herein.

29.I have presented my opinion below regarding the challenged claims based on the following grounds:

Ground	Claims	Basis	Reference
1	1-2, 6-18	§ 103	Limont, Wright and optionally Xu
2	3-5	§ 103	Limont, Wright and optionally Xu with Polson

30.[This paragraph left intentionally blank].

V. OVERVIEW OF THE '042 PATENT, ITS PATENT FAMILY, AND ITS PROSECUTION HISTORY

A. Overview of the '042 Patent.

31.The application that became the parent '899 patent was filed May 23, 2013 as non-provisional application 13/901,466. The application that became the '042 patent (14/584,897) asserts itself to be a continuation of the parent '899 patent's application.

32.At a high level, the '042 patent is generally directed to "Methods and systems for receiving a report from an end-user device, the report comprising information about a device service state; determining, based on the report, that a

particular service policy setting of the end-user device needs to be modified, the particular service policy setting associated with a service profile that provides for access to a network data service over a wireless access network and configured to assist in controlling one or more communications between the end-user device and the wireless access network, the particular service policy setting stored in a protected partition configured to deter or prevent unauthorized modifications to the particular service policy setting; and, in response to determining that the particular service policy setting needs to be modified, sending configuration information to the end-user device, the configuration information configured to assist in modifying or allowing modifications to the particular service policy setting." EX-1001, Abstract.

33. The "Background of The Invention" states: "With the advent of mass market digital communications, applications and content distribution, many access networks such as wireless networks, cable networks and DSL (Digital Subscriber Line) networks are pressed for user capacity, with, for example, EVDO (Evolution-Data Optimized), HSPA (High Speed Packet Access), LTE (Long Term Evolution), WiMax (Worldwide Interoperability for Microwave Access), DOCSIS,

DSL, and Wi-Fi (Wireless Fidelity) becoming user capacity constrained. In the wireless case, although network capacity will increase with new higher capacity wireless radio access technologies, such as MIMO (Multiple-Input Multiple-Output), and with more frequency spectrum and cell splitting being deployed in the future, these capacity gains are likely to be less than what is required to meet growing digital networking demand. Similarly, although wire line access networks, such as cable and DSL, can have higher average capacity per user compared to wireless, wire line user service consumption habits are trending toward very high bandwidth applications and content that can quickly consume the available capacity and degrade overall network service experience. Because some components of service provider costs go up with increasing bandwidth, this trend will also negatively impact service provider profits." EX-1001, 1:47-2:3.

34. The '042 Title is "Security techniques for device assisted services." The '042 patent does not identify any specific problem that it seeks to solve nor does it characterize anything within its disclosure as solution.

35. As issued, the '042 patent includes 18 claims. I have been asked to opine on the Challenged Claims in my analysis, which I have included below:

1. A method comprising:

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

determining, based on the report, that a particular service policy setting of the wireless end-user device needs to be modified, the particular service policy setting being stored in a protected partition of the wireless end-user device, the protected partition configured to deter or prevent unauthorized modifications to the particular service policy setting, the particular service policy setting being associated with a service profile that provides for access by the wireless end-user device to a network data service over a wireless access network, the particular service policy setting configured to assist in controlling one or more communications associated with the wireless end-user device over the wireless access network; and

is in response to determining that the particular service policy setting needs to be modified, sending configuration information to the wireless end-user device over the service control link, the

configuration information configured to assist in modifying or allowing modifications to the particular service policy setting.

2. The method of claim 1, wherein the particular service policy setting assists in implementing a roaming control, a parental control, or an enterprise wireless wide-area network (WWAN) management control.

3. The method of claim 1, wherein the wireless end-user device is an intermediate networking device for forwarding traffic between a wireless wide-area network (WWAN) and a wireless local-area network (WLAN).

4. The method of claim 1, wherein the wireless end-user device is an intermediate networking device comprising a cellular device, the intermediate networking device for forwarding traffic between the wireless access network and a second network.

5. The method of claim 1, wherein the wireless end-user device is an intermediate networking device, and the particular service policy setting assists one or more other end-user devices in communicating over the wireless access network via the intermediate networking device.

6. The method of claim 1, further comprising:

obtaining a service usage measure, the service usage measure accounting for the one or more communications associated with the wireless end-user device over the wireless access network; and

based on the service usage measure, taking an action.

7. The method of claim 6, wherein the service usage measure comprises a measure of a service usage activity.

8. The method of claim 6, wherein the action is to verify the service usage measure.

9. The method of claim 6, wherein the action is to quarantine or suspend the wireless end-user device.

10. The method of claim 6, further comprising obtaining secondary information associated with the wireless end-user device, and wherein the action is to verify the service usage measure using the secondary information.

11. The method of claim 1, further comprising receiving, from the wireless end-user device, an integrity report configured to assist a network element in identifying an access control integrity violation.

12. The method of claim 1, wherein the configuration information comprises at least a portion of the service profile.

13. The method of claim 1, wherein the service control link is secured by an encryption protocol.

14. The method of claim 1, wherein the device service state comprises a service profile setting, a service usage policy setting, or a device-assisted services (DAS) setting.

15. The method of claim 1, wherein the device service state provides information about a user preference.

16. The method of claim 1, wherein the device service state comprises information associated with an encryption key.

17. The method of claim 1, wherein the device service state comprises an agent report, a service usage record, a transaction record, or an integrity report.

18. The method of claim 1, wherein the device service state comprises user status information, device status information, application status information, a device location, or a device quality-of-service (QOS) state.

36. [This paragraph left intentionally blank].

B. Overview of the Prosecution History of the '042 Patent

37. I have reviewed the prosecution history of the '042 patent in forming my opinions for purposes of this declaration.

38. Claims 1-18 received a first Office Action allowance with no prior art applied. The Examiner merely stated "the prior art, either alone or in combination, does not disclose Applicant's inventive claim language."

39. After the claims had been allowed on October 8, 2015, the applicant submitted additional prior art including sets of prior art on the next day including one set of 37 additional reference. In total, approximately 1000 references references were submitted during prosecution. I am unable to locate any discussion of these references by either the Examiner or the application in the prosecution history.

40. [This paragraph left intentionally blank].

VI. LEVEL OF ORDINARY SKILL IN THE PERTINENT ART

41.I have been advised that there are multiple factors relevant to determining the level of ordinary skill in the pertinent art, including the educational level of active workers in the field at the time of the invention, the sophistication of the technology, the type of problems encountered in the art, and the prior art solutions to those problems.

42.It is my opinion that a person having ordinary skill in the relevant art ("POSA") at the time of the invention would have been familiar with the changing of configuration settings of end-user devices to control access of the device to network data services, and storing those configuration settings in a protected partition as demonstrated by the prior art references and description in the State of the Art below.

43.A POSA would have gained knowledge of these concepts through a mixture of training and work experience, such as by having a Bachelor's degree in computer science and two years of experience; or by obtaining a Master's degree in computer science, but having only one year of experience.

44.[This paragraph left intentionally blank].

VII. CLAIM CONSTRUCTION

45.I understand that the parties in the related litigations have not exchanged proposed claim constructions or submitted claim construction briefing to the Court.

46.The prior art discussed below discloses the claim elements under any reasonable construction of the terms.

47.[This paragraph left intentionally blank].

VIII. UNDERSTANDING OF THE LAW

48.In expressing my opinions and considering the subject matter of the claims of the '042 patent, I am relying upon certain basic legal principles that have been explained to me. I have been informed by counsel that a patent claim is unpatentable as anticipated under 35 U.S.C. § 102 if each element of that claim is present either expressly or inherently in a single prior art reference. I have also been informed that, to be an inherent disclosure, the prior art reference must necessarily disclose the limitation, and the fact that the reference might possibly practice or contain a claimed limitation is insufficient to establish that the reference inherently teaches the limitation.

49.I have been informed that a claimed invention is unpatentable under 35 U.S.C. § 103, if the differences between the invention and the prior art are such

that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. I have also been informed by counsel that the obviousness analysis takes into account factual inquiries including the level of ordinary skill in the art, the scope and content of the prior art, and the differences between the prior art and the claimed subject matter.

50.I have been informed by counsel that the Supreme Court has recognized several rationales for combining references or modifying a reference to show obviousness of claimed subject matter. Some of these rationales include the following: (a) combining prior art elements according to known methods to yield predictable results; (b) simple substitution of one known element for another to obtain predictable results; (c) use of a known technique to improve a similar device (method, or product) in the same way; (d) applying a known technique to a known device (method, or product) ready for improvement to yield predictable results; (e) choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success; and (f) some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art

reference or to combine prior art reference teachings to arrive at the claimed invention.

51. Finally, I understand that secondary factors may be considered in an obviousness inquiry. I understand that these are also referred to as secondary considerations and may include evidence of long-felt need, failure of others, skepticism of those of skill in the art, licensing, commercial success, recognition in the industry, acquiescence, evidence of copying, and unexpected results. While these secondary considerations must be taken into account, they do not necessarily control the obviousness determination.

52. Moreover, for objective evidence of nonobviousness to be accorded substantial weight, I understand that the proponent of such evidence must establish a "nexus" between the evidence and the merits of the patent at issue. Specifically, I understand that the secondary consideration must be tied to the merits of the claimed invention of the patent at issue. Where the alleged secondary consideration results from something other than what is both claimed and novel, I understand that there is no nexus to the merits of the claimed invention and the secondary considerations are thus not indicative of nonobviousness. I also

understand that it is the patentee's burden to come forward with evidence that a nexus exists.

53. [This paragraph left intentionally blank].

IX. SCOPE AND CONTENT OF THE PRIOR ART

A. Limont (EX-1004).

54. Limont teaches "Enforcing device settings for mobile devices." Limont at Title. Like the '042 patent Limont teaches modifying policy settings on a mobile device based on configuration information sent from the mobile device to a computer server across a wireless network:

> The present invention extends to methods, systems, and computer program products for enforcing device settings for mobile devices. Generally, a computer system enforces appropriate mobile device settings (e.g., policy and/or configuration settings) prior to permitting a mobile device to access maintained data. The computer system receives a request from a mobile device. The computer system determines that current mobile device settings are not appropriate for accessing the maintained data. The computer system sends device settings, representing a new mobile device configuration that is appropriate accessing the maintained data, to the mobile device. The computer system receives an indication that the mobile device is

configured in accordance with the device settings. The computer system permits the mobile device to access the maintained data in response to receiving the indication that the mobile device is configured in accordance with the device settings.

55. Limont at Abstract.

56. Limont teaches configuring and updating policy settings for a wireless device based on information received from that device regarding the service state of the device. FIG. 3 illustrates an architecture for configuring and updating policy settings:

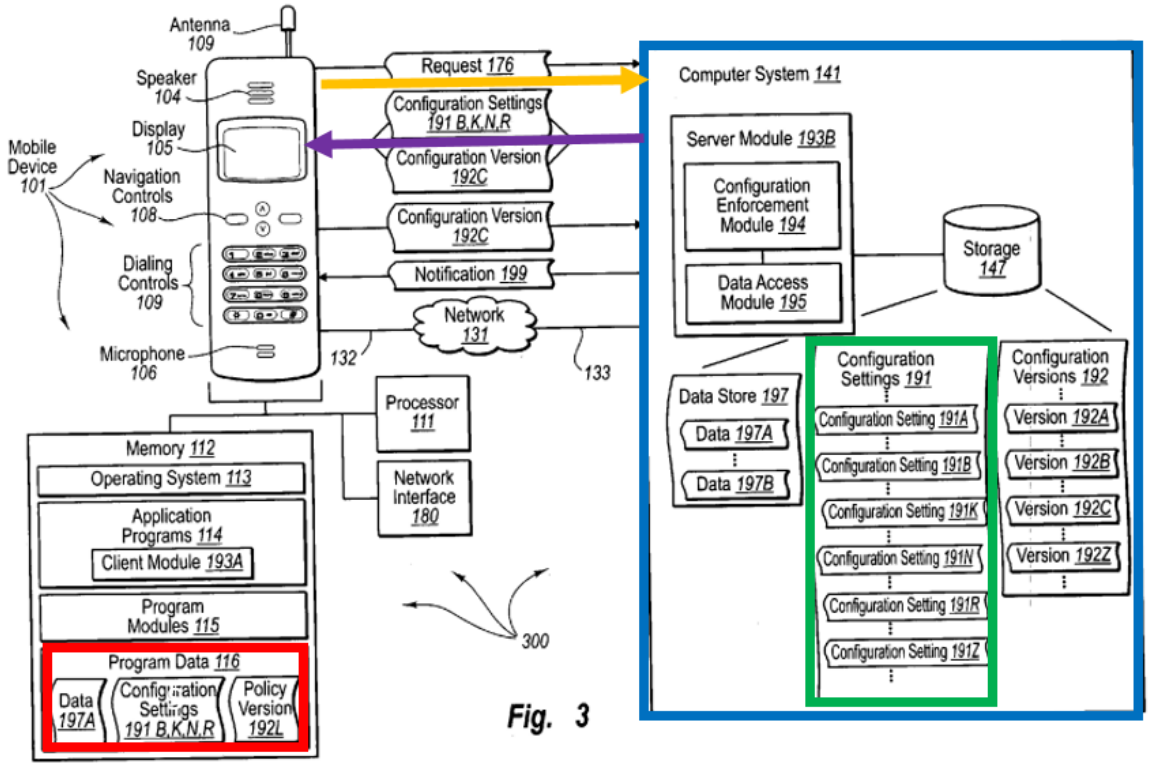


Fig. 3

57. EX-1004 FIG. 3.

58. Mobile device 101 may include client module 193A (*e.g.*, a Web browser for "displaying a Web page at display 105" (EX-1004, [0090]) to access data and retrieve maintained by server module 193B.

59. The server includes policy enforcement module 194 and data access module 195.

> Computer system 141 includes server module 193B (e.g., a Web server). Server module 193B fuirther [sic] includes policy enforcement module 194 and data access module 195. As depicted, configuration settings 191 includes configuration settings 191 include policy setting 191A, policy setting 191B, and policy setting 191Z. A series of two dots (a vertical ellipsis) between, before and after the expressly depicted configuration settings represents that other configuration settings can be included between, before and after the expressly depicted policy settings. Configuration settings can be name/value pairs. The name represents the name of a configuration setting and the value represents the value of the configuration setting. Configuration setting values can be of virtually any data type, such as, for example, Boolean, integer, floating point, string, character, enumerated, etc. Configuration settings can include: operating system settings, application program settings, hardware settings, allocated

> resource settings, network interface settings, wireless protocol settings, etc.

60. EX-1004, [0073].

61. Server module 193B interoperates with client programs (*e.g.*, client module 193A) to transfer data (*e.g.*, Web pages) to mobile device 101.

> Server module 193B can interoperate with client side programs (e.g., client module 193A) to transfer data (e.g., Web pages) to a mobile device. Thus, in response to a mobile device data request, policy enforcement module 194 can determine if a requesting mobile device's policy settings are appropriate for accessing data. For example, policy enforcement module 194 can determine if sufficient resources have allocated at a mobile device to receive a Web page, if a mobile device Web browser includes correct plug-ins for viewing content, if mobile device connection speed will permit a Web page to be downloaded in a reasonable amount of time, etc.

62. EX-1004, [0077].

63. Thus, in response to a mobile device data request for access to the web server, policy enforcement module 194 can determine if a requesting mobile device's policy settings are appropriate for accessing data. For example, policy enforcement module 194 can determine if sufficient resources have allocated at a mobile device to receive a Web page, if a mobile device Web browser includes

correct plug-ins for viewing content, if mobile device connection speed will permit a Web page to be downloaded in a reasonable amount of time, etc. EX-1004, [0077].

64.Configuration enforcement module 194 (in addition to user authentication and authorization modules) checks the device's configuration / policy settings and allowing access module 195 to access and either transfer the requested data or updated configuration settings (policies) to allow for such access. EX-1004, [0078], Abstract. Limont references the "configuration enforcement module" as "policy enforcement module" and "configuration settings" as "policy settings." EX-1004, [0077], [0083], [0055].

65.Limont's FIG. 4 illustrates a flow chart of a method for enforcing an appropriate mobile device configuration using the architecture of FIG. 3:

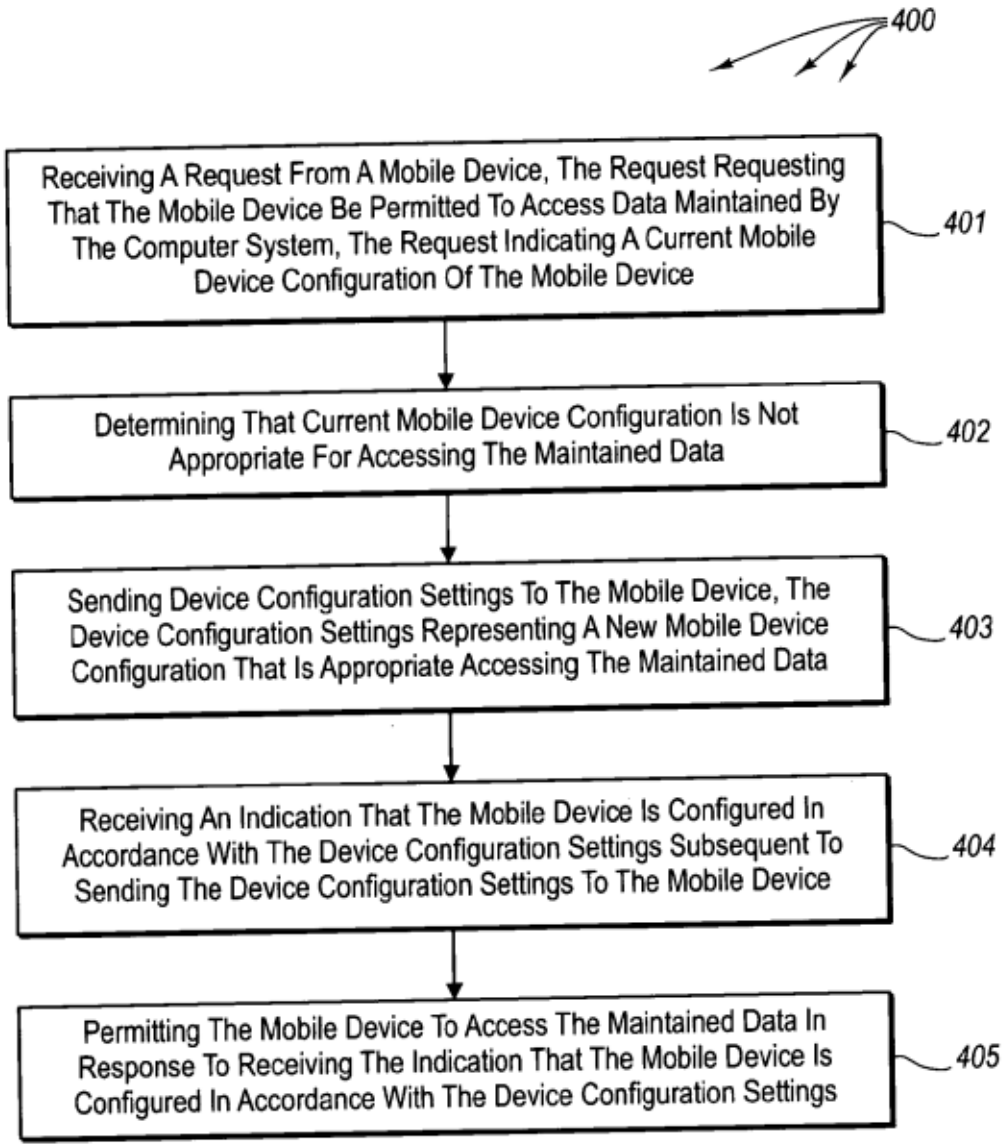


Fig. 4

66.EX-1004 FIG. 4.

67.Using the architecture shown in Limont's FIG. 3, method 400 in Fig. 4 shows the claimed updating of policies.

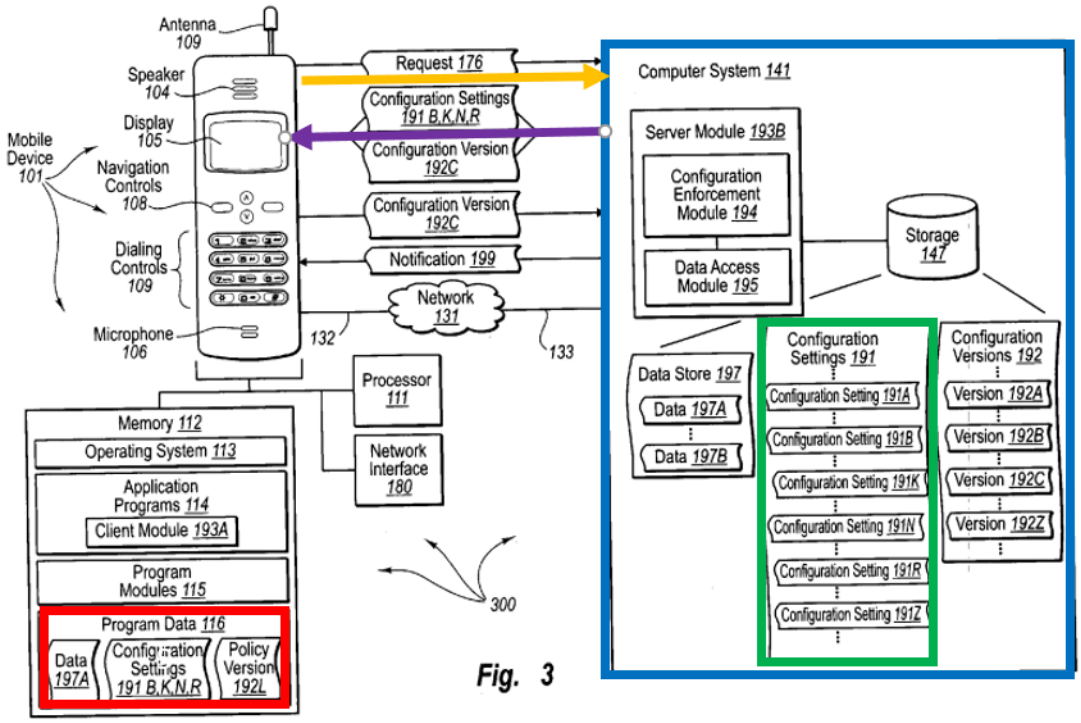


Fig. 3

EX-1004 FIG. 3.

68.In step 401, the mobile device sends request 176. Request 176 can include: (1) a current configuration version of the mobile device 101; (2) a data request, such as for a Web page; and / or (3) an express request for new configuration settings. EX-1004, [0080]. Configuration settings can include policy settings, operating system settings, application program settings, hardware settings,

allocated resource settings, network interface settings, wireless protocol settings, etc. EX-1004, [0073].

69. In step 402 (202), configuration enforcement module 193 determines whether the configuration setting in the request is appropriate to access the requested data. If so, then the data can be accessed. EX-1004, [0081-0082], [0070].

70. If the device's configuration setting is "inappropriate" for the data access, then the server sends modified settings to the mobile device (step 403 / 206). EX-1004, [0083]. For example, server module 193B can send configuration settings 191B, K, N, and R along with configuration version 192L to mobile device 101 in response to request 176 (a request). EX-1004, [0084]. Mobile device 101 can store implement configuration settings 191B, K, N, and R (potentially altering current configuration settings) to comply with configuration settings that are appropriate for accessing data maintained by server module 193B. EX-1004, [0086].

71. In step 405, the computer system 141 permits the mobile device to access the maintained data in response to receiving the indication that the mobile device is configured in accordance with the device configuration settings.

72. [This paragraph left intentionally blank].

B. Wright (EX-1005)

73. Wright teaches protecting data on mobile computing devices using various security tools. Wright explains that data stored on a mobile device is vulnerable to hackers even if that data was transmitted from a server using a secure trusted connection, such as a VPN.

> [0007] Traditional security architectures assume that the information assets being protected are 'tethered'—wired to a particular network infrastructure such as a company's network infrastructure. But mobile users can pick up valuable corporate information, such as that stored on their laptops, and walk away from the corporate network, and connect to other networks with different security policies. Users with laptops and mobile devices want to take advantage of wireless technologies, to connect wherever they are—at work, at home, in the conference room of another company, at the airport, a hotel, a highway or at the coffee shop on the corner. The mobile device's network environment is constantly changing as the user moves about. Each environment has different needs in terms of security. Each environment presents different challenges to protect the information on the mobile device while allowing access to e-mail, the Internet, and company Virtual Private Networks (VPNs).

> [0008] Personal firewalls are designed to deal with static environments. A personal firewall could be ideally suited for mobile users if users knew how to adapt their configuration for their particular mobile application. Unfortunately, security settings for one situation can compromise data security in another. The configuration of popular personal firewalls typically requires a level of expertise on how the technology actually works that average users do not possess. Additionally, personal firewalls don't protect against all 802.11 intrusions. For example, when a user configures a personal firewall off to surf the Internet through their wireless device, their files may be vulnerable to unauthorized malicious wireless attacks on their computer.
>
> [0009] Solutions which secure data in transit, for example a (VPN) connection, from a corporate server to a mobile client device do not protect the data once it is stored on the mobile device. For example, an executive could be retrieving sensitive files or emails from the corporate network, and the VPN will stop eavesdroppers from seeing the data in transit, but once the data is stored on the executive's remote device, hackers in the parking lot could break into the remote device and copy or maliciously alter the data. With the onset of new powerful mobile devices that can store corporate data, IT managers see their network perimeters having to extend to the new limits of these mobile wireless connections.

74. EX-1005, [0007-0009].

75. Wright describes client devices that have WLAN (802.11) and WWAN (GPRS, GSM, 3G) "wireless connections" that may have separate policies based on the particular type of network or network care.

> [0066] The illustrated system 201 embodiment in accordance with the present invention further comprises a security feature module 210 for determining whether one or more security features have an activity status of inactive or active in a communication session between the mobile device and another computer. An example of a security feature is a connection type of wired or wireless. In one example, this connection type may be indicated by the association of the port over which data is communicated with a *wireless* or wired network adapter or network interface card (NIC). In another example, this connection type may be indicated by the association of a local IP address with data communicated over a wireless or wired network adapter or network interface card (NIC). These classes or categories may be further subdivided into network classes subdivided further into types of wireless connections (e.g. 802.11, GPRS, GSM, 3G, etc.) and types of wired connections (e.g. modem, digital subscriber line (DSL), T1 line). In other embodiments, policies may be set based on particular features besides simply connection type. For example, a different security policy may be applied for different brands of NICs or particular classes (e.g. 802.3, 802.11a, 802.11b, GPRS, GSM) of NICs. Furthermore, different security policies may be assigned based

> on the operating system employed or the version of the operating system because different systems or versions provide different security features. Furthermore, different policies may be employed based on the security features (e.g. a firewall) provided by different types of network access points (NAP). Additionally, the presence or absence of upgraded NIC support for enhanced security protocols (e.g. 802.11i), or the presence or absence of security software such as virtual private network (VPN), or antivirus software, or intrusion-detection software may be the basis for setting different policies on a particular port, network adapter or data.

76. EX-1005, [0066]. See also [0045] (access network uses "a cellular base station providing network access through a General Packet Radio Services (GPRS) system, Global System for Mobile communication (GSM) system, third generation wireless 3G system or other kind of mobile wireless communication system.").

77. Wright confirms that the mobile devices can have multiple different network adapters that are classified by type including WWAN and WLAN network adapters:

> In a similar manner, the policy engine 832 may also determine 906 from the operating system the class (e.g. 802.11b, 802.3, 802.11a, 802.11 g, GSM, GPRS, 3G) **of the network adapters on the mobile device,** and assign 908 a value to an adapter class field in the adapter data object associated with each policy. Furthermore, the policy

> engine 832 may determine 910 from the operating system the hardware brand of the network adapters on the mobile device, and assign 912 a value to an adapter brand field in the adapter data object associated with each policy.

78. EX-1005, [0274].

79. Wright describes numerous devices with WLAN connections such as 802.11 connections. EX-1005, [0044] ("The notebook computer 122 and the personal digital assistant (PDA) 124 have a wireless connection to a wireless NAP 130, in this example an 802.11b connection through which they may communicate at the airport."); [0228] (using WEP encryption on 802.11 network).

80. Wright's claims also describe the different types of network adapters:

> 25. The system of claim 24 wherein at least one of the security features is a connection type of wired or wireless.
>
> 26. The system of claim 24 wherein at least one of the security features is a security software program.
>
> 27. The system of claim 24 wherein at least one of the security features is a network class.
>
> 28. The system of claim 27 wherein the network class is a type of mobile communications system.
>
> 29. The system of claim 28 wherein the type of mobile communications system is a type of wireless communications system.

> 30. The system of claim 29 wherein the network class is a Global System for Mobile Communications system.
>
> 31. The system of claim 28 wherein the network class is 802.3.
>
> 32. The system of claim 28 wherein the network class is 802.15.
>
> 33. The system of claim 28 wherein the network class is 802.16.
>
> 34. The system of claim 27 wherein the network class is a variation of 802.11.
>
> 35. The system of claim 27 wherein the network class is 3G.
>
> 36. The system of claim 27 wherein the network class is General Packet Radio Service.

81. EX-1005, claims 25-36.

82. Wright stores configuration information on a mobile device including the current version of the security policy software components for the mobile device, the current policy settings on the device, and attributes in accordance with those settings, for example, which ports are blocked.

> [0057] The remote diagnostics module 224 may also probe a particular client to verify its status. For example, client configuration information may be retrieved such as the current version of the security policy software components on the client device, the current policy settings on the device, and attributes in accordance with those settings, for example, which ports are blocked. This information may be stored for later assistance in a diagnostics situation or for use with a current diagnostics situation.

83. EX-1005, [0057].

84. Wright explains that one solution to the security issue identified above is to maintain the policy documents as XML documents to allow great flexibility in design, usage, and enhancement of policies. Using the flexibility of XML policy documents simplifies the complex problem of distributing and enforcing policies directed to program usage, network access, hardware restrictions, VPN access, data access, and many other policies. Wright explains that the policies can be protected from hacking by encryption or signatures (*i.e.*, XKMS, XMLDSIG, XMLENC, or proprietary encryptions). The policy is then enforced on the client by a process that can interpret the policy distributed by the enterprise. This approach allows a policy to be extensible and easily updated by the administrator. Also, the administrator can configure elements of the policy such that they are configurable by the user. EX-1005, [0270].

85. Wright's computer system acts as a server for a client mobile device. The server includes a policy management module that sets the permissions for the mobile device regarding the policies. Permissions typically relate to the allowable modification that may be made to a downloaded policy or software. EX-1005, [0078-0103].

86.For example, the policy management module determines whether the security information is to be encrypted. If it is to be encrypted, the policy is encrypted. Security policies may be included in XML documents which may themselves be encrypted.

> [0104] The policy management module 236 determines 309 whether the security information is to be encrypted. If not, the policy management module 236 stores 312 the security policy. If it is to be encrypted, the policy is encrypted 311. Similarly the policy management module 236 may also encrypted other types of security information such as software updates before they are stored. For example, the security policy may be stored as a data object in a memory 242 accessible via an internal enterprise network. In another example, security policies may be included in XML documents which may themselves be encrypted. In an alternate embodiment, the policy management module 236 may store the policy unencrypted, the policy distribution module 234 makes the determination of whether encryption applies to the policy or other security information, and the policy distribution module 234 encrypts the security information before distributing it. Additionally, in the embodiment of FIG. 2A, the policy management module 236 manages the one or more client devices for security purposes. One aspect of client management is that the policy management module 236 maintains 314 client management information for the mobile device and the one or more policies

> associated with it. The following list of information fields is an example of the types of information which may be included in client management information.
>
> [0105] User Name
>
> [0106] Group
>
> [0107] Connection state, which is one of:
>
> [0108] Connected
>
> [0109] Last connected time
>
> [0110] Never connected
>
> [0111] Policy for this user
>
> [0112] Policy version for this user
>
> [0113] Software version for this user
>
> [0114] Current enforcement mechanisms
>
> [0115] Diagnostic level, including diagnostic options available in the client settings
>
> [0116] Diagnostic information
>
> [0117] Auditing level
>
> [0118] Auditing information
>
> [0119] Locations Previously Detected

87. EX-1005, [0104-0119]. Furthermore, files stored on the mobile device may be encrypted.

> The administration of protection of data on a client mobile computing device by a server computer system such as within an enterprise network or on a separate mobile computing device is described.

> Security tools are described that provide different security policies to be enforced based on a location associated with a network environment in which a mobile device is operating. Methods for detecting the location of the mobile device are described. Additionally, the security tools may also provide for enforcing different policies based on security features. Examples of security features include the type of connection, wired or wireless, over which data is being transferred, the operation of anti-virus software, or the type of network adapter card.
>
> The different security policies provide enforcement mechanisms that may be tailored based upon the detected location and/or active security features associated with the mobile device. Examples of enforcement mechanisms are adaptive port blocking, file hiding and file encryption.

88. EX-1005 Abstract. See also EX-1005, [0177]

> [0260] One reason for requiring that all files created and/or modified in one of the specified locations is so that copies of sensitive files or data derived from the sensitive files are also protected. Specific mechanisms for protecting the files include file hiding and file encryption.

89. EX-1005, [0260].

90. Wright also describes using a secure trusted channel to provide the security policy for the server to the mobile device.

[0078] For illustrative purposes only, the method embodiments illustrated in FIGS. 3A and 3B are discussed in the context of the system embodiment of FIG. 2A. FIG. 3A illustrates a method for managing one or more security policies for the protection of data accessible by a mobile device based upon criteria in accordance with an embodiment of the present invention. In the system embodiment of FIG. 2A, the policy management module 236 defines 302 a security policy applicable to a client mobile device based upon criteria. One example of criteria is the location associated with the network environment in which the mobile device is operating. Other examples of criteria are the presence or the activity status of one or more security features. Of course, a combination of location and one or more security features may also form a criteria basis for defining a security policy. The policy management module 236 designates 304 one or more client devices associated with the policy. In one example, this association may be based on an entity or class to which the security policy is applicable. An example of an entity is a group with one or more members. An example of a member may be a user of the client mobile device. A policy may be set that is applicable to the group of all engineers in the software development department. Another example of a member is the mobile device itself. For example, the capabilities of different mobile devices may be the basis for classifying them into different groups. In a secure manner, the policy management module 236 provides 306 the one or more

designated client mobile devices with authorization information for use in contacting the server system securely. One example of authorization information is an encrypted token provided by the authorization module 232 to the mobile client device during a trusted connection between the two. An example of a trusted connection may be an internal connection behind the firewall of and within the internal network of the enterprise with which both the server system and the mobile client device system are associated. In one embodiment, an authority server within the firewall in the internal network provides the authorization information. When a client mobile device connects via the Internet, it interacts with one or more of the enterprise side servers external to the firewall. The client contacts the external servers to retrieve policies and instructions. The external servers also perform key/identity management, client disable methods (e.g. unmanaged mode) and policy persistence. The external servers communicate with the authority server through the firewall for client management information such as a key, a user, a group, and version information associated with a client mobile device system. In a similar manner, responsive to security information such as a policy or software being designated for encryption, the policy management module 236 provides 308 the designated client mobile device with cryptographic information which the client device can store and use to decrypt the security information. An example of cryptographic information is a key for use with a cryptographic authentication protocol. In one

> example, Microsoft® web keys may be used. The policy management module 236 sets 310 the permissions for the one or more associated mobile devices with respect to the one or more policies. In one aspect, permissions typically relate to the allowable modification that may be made to a downloaded policy or client software by the client mobile device. Permissions may be applied to various policies and to the criteria upon which policies are defined. For example, there may be permissions set for a policy, but permissions may also be set with respect to a location. Some examples of permissions specific to policies are as follows:

91. EX-1005, [0078].

92. A server's distribution module determines if the security policy has been designated to be encrypted. If so, then the security information is encrypted and distributed to the mobile device.

> [0128] FIG. 3B illustrates a method for distributing a security policy by a server computer system for the protection of data accessible by a mobile device in accordance with an embodiment of the present invention. In one embodiment, each of the client mobile devices sends a status request upon network access starting up to the server system. The status request provides information regarding the client mobile device, examples of which are authorization information, policies and their version numbers resident on the device, and diagnostic information. In the illustrative context of FIG. 2A, the authorization

> module 232 receives 322 the status request with authorization information from a client mobile device, and it determines 324 whether a communication exchange with this mobile device is authorized. If not, the status request is ignored 326 or an error message is sent 326. If the communication exchange is an authorized one, the policy distribution module 234 determines 328 if security information (e.g. a policy or software) applicable to the mobile client device has been updated since the last status request. If not, the status request is ignored 325 or a no update message is sent 325. Responsive to a new policy, a new version, or new software being available that is applicable to the requesting client device, the policy distribution module 234 distributes 327 the updated security information to the mobile device over the network (e.g. Internet) 204. In an alternate embodiment (not shown), the distribution module 234 determines if the information has been designated to be encrypted. If not, it distributes 327 the security information to the client device. If it is to be encrypted, the security information is encrypted and then distributed 327 to the client device.

93. EX-1005, [0128].

> [0264] One mechanism for encrypting the files is to simply mark them "encrypted" in their properties pages, and to rely on the file hiding feature (see above) to stop the files from being decrypted in an unauthorized location. Other versions may use the file-system filter to more effectively encrypt the files in a way that does not depend on the

operating system to prevent them from being decrypted in an unauthorized location.

[0265] Policies can have rules controlling the use of VPNs. For example, a rule can require that when the VPN is in use, all other ports are closed. This prevents hackers near the user from co-opting the user's device and coming in to the corporate network over the user's VPN connection. In one embodiment, a lightweight web-based VPN is used that allows traffic from selected applications (e.g., email) to be encrypted with Transport Layer Security (TLS).

[0266] In one embodiment, a VPN Lite 820 having a communication interface with the packet filter engine 818 establishes a TLS-encrypted, authenticated connection with the server, and then sends and receives traffic over this connection. The layered service provider 814 diverts the outgoing traffic from the application to a VPN client piece, and incoming traffic from the VPN client piece to the application.

[0267] In one implementation example in accordance with the present invention a layer is inserted into the Winsock environment, which opens up a Transport Layer Security (TLS) or Secure Socket Layer (SSL) socket to the VPN server, and tunnels all application network traffic through that connection to the VPN server. The applications are unaware that the VPN is active. The VPN has a very small footprint, since TLS is included in Windows.® In this example, using the Winsock Environment, all communication between client and server

> is routed through a secure channel. Unlike current clientless VPNs, all existing applications are supported

94. EX-1005, [0267]. See also EX-1005, Fig. 3A (elements 311, 312), Fig. 3C.

95. Wright also discloses a client diagnostics module that audits files, including the security policy to verify no corruption such as by modification by unauthorized users (*e.g.* checksum). EX-1005, [0068-0073]. A server's remote diagnostics module receives audit logs from a client and analyzes the audit information to check the integrity of the stored files. The remote diagnostic module may provide a repair to a problem in the client device, determine that a trend is occurring for the device, or determine that preventive maintenance is to be scheduled for the client device. EX-1005, [0055].

96. [This paragraph left intentionally blank].

C. Xu (EX-1016)

97. Xu is a patent assigned to Microsoft (like Limont). EX-1016, Cover page.

98. Xu provides for a secure environment to protect confidential data and applications.

> A processing unit for use in an electronic device includes standard instruction processing and communication interfaces and also includes functional capability in addition to or in place of those found in an

> operating system. A secure memory within the processing unit may contain a hardware identifier, policy data, and subsystem functions such as a secure clock, policy management, and policy enforcement. Data in functions within the secure memory are not accessible from outside the processing unit.

99. EX-1016, Abstract.

100. Xu identifies problems for mobile devices like mobile phones of security risks that could allow "hackers" to access confidential information including the ability to access confidential data across networks.

101.

> [0003] A processing unit with embedded system functions **provides a secure base for enforcing security and/or operating policies**, for example, for use in enforcing pay-per-use, pay-as-you-go, or other metered operation of an **electronic device such as a computer, cellular telephone, personal digital assistant, media player,** etc. The processing unit may include features and functional support found in most or all modern microprocessors and also support additional functions providing a hardware identifier, a tamper-resistant clock, and secure storage. Other functional capabilities such as a cryptographic unit, may be present as well.

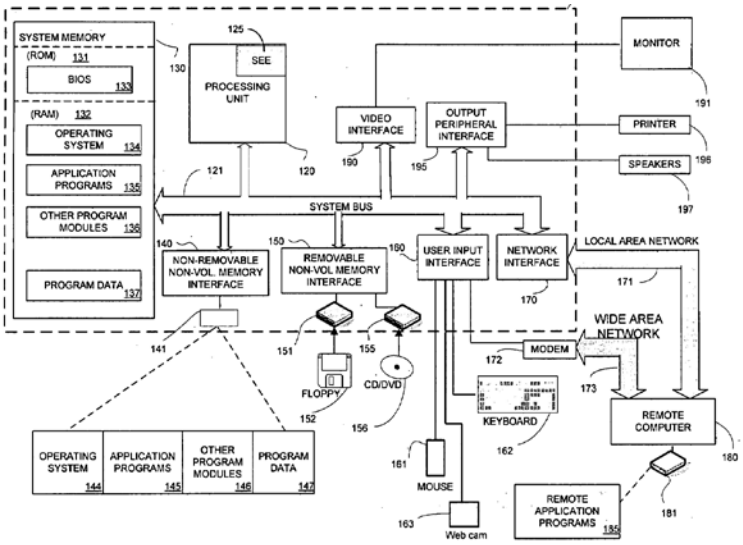
102. EX-1016, [0003].

103. Xu describes a device that communicates with servers over networks such as wired and wireless networks.

> FIG. 1 illustrates a network 10 that may be used to implement a pay-per-use computer system. The network 10 may be the Internet, a virtual private network (VPN), or any other network that allows one or more computers, communication devices, databases, etc., to be communicatively connected to each other. The network 10 may be connected to a personal computer 12 and a computer terminal 14 via an Ethernet 16 and a router 18, and a landline 20. On the other hand, the network 10 may be wirelessly connected to a laptop computer 22 and a personal data assistant 24 via a wireless communication station 26 and a wireless link 28. Similarly, a server 30 may be connected to the network 10 using a communication link 32 and a mainframe 34 may be connected to the network 10 using another communication link 36.

104. EX-1016, [0012]

105. Xu's Fig. 2 describes one of the network computers such as the server:



106. Xu's server component has known components operating in known fashions.

> [0013] FIG. 2 illustrates a computing device in the form of a computer 110 that may be connected to the network 10 and used to implement one or more components of the dynamic software provisioning system. Components of the computer 110 may include, but are not limited to, a processing unit 120, a system memory 130, and a system bus 121 that couples various system components including the system memory to the processing unit 120. The system bus 121 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. By way of example, and not limitation, such architectures include Industry Standard Architecture (ISA) bus, Micro Channel Architecture (MCA) bus, Enhanced ISA (EISA) bus, Video

> Electronics Standards Association (VESA) local bus, and Peripheral Component Interconnect (PCI) bus also known as Mezzanine bus.
>
> [0014] The processing unit 120 may be a microprocessor such as a microprocessor available from Intel, or others, as is known in the art. The processing unit may be a single chip or may be a multiple processor unit and may include associated peripheral chips (not depicted) or functional blocks (not depicted). Such associated chips may include pre-processors, pipeline chips, simple buffers and drivers, or may include more complex chips/chip sets such as the "Northbridge" and "Southbridge" chips known in some current technology computer architectures. The processing unit 120 may also include a secure execution environment 125, either on the same silicon as the microprocessor or as a related chip as part of the overall processing unit. The secure execution environment 125 and its interaction with the processing unit 120, or equivalent devices, is discussed in more detail below with respect to FIG. 3 and FIG. 4.

107. EX-1016, [0003-0004].

108. Xu depicts its device (such as a cellular telephone, PDA or laptop) (EX-1016, [0012]) in Figure 3 with the secure memory 318.

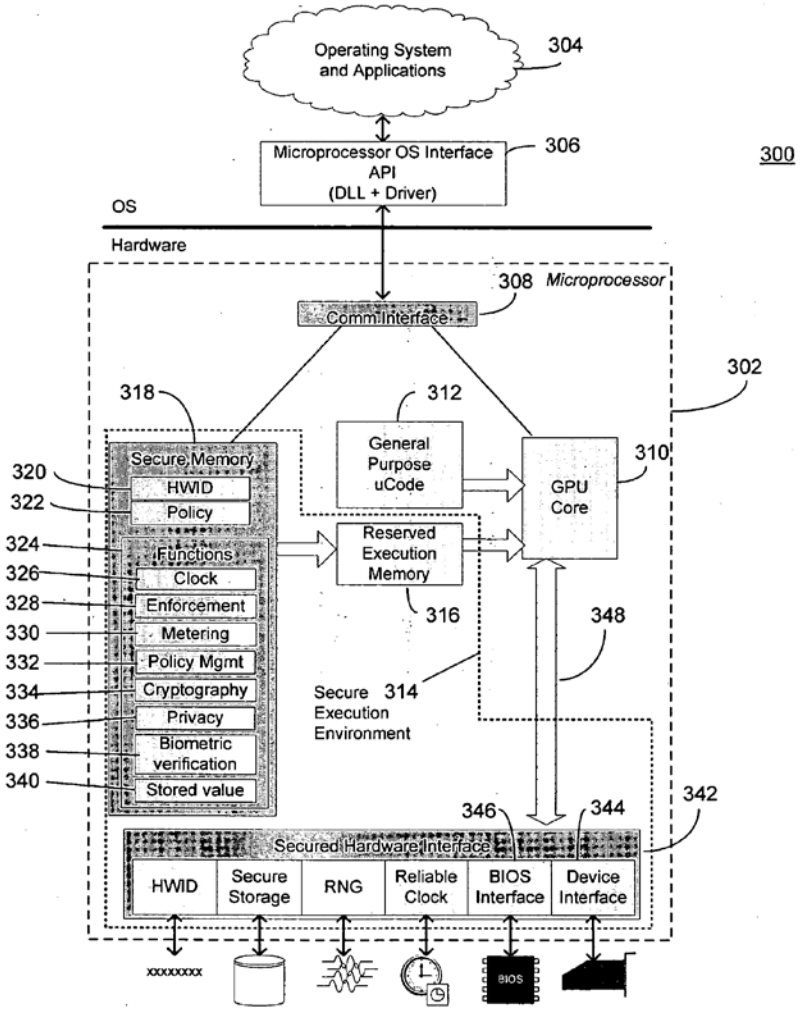


Fig. 3

109. EX-1016, Fig. 3. See EX-1016, [0021].

110. Figure 3 describes the secure execution environment provide by Xu.

111.

> [0022] A secure execution environment 314 may supplement the general processing capabilities provided by the GPU core and

microcode 310 312. The secure execution environment; 314 may include a reserved execution memory 316. The reserved execution memory 316 may provide a highly secure location for the execution of instructions having an elevated privilege level within the processing unit 302. This elevated privilege level of operation may allow the processing unit 302 to execute code that is not directly accessible from outside the processing unit 302. For example, a particular interrupt vector may set the processing unit 302 into secure operation, or instructions may be evaluated for content requiring secure resources. When operating in this elevated privilege mode, the processing unit 302 acts as a full subsystem and does not require any external assets, for example BIOS resources, program memory, or a TCM, to build a secure processing environment.

[0023] A secure memory 318 may store, in a tamper-resistant manner, code and data related to the secure operation of the computer 302. The communication interface 308 may determine which instructions entering the processor 302 should be directed to the secure memory 318, and subsequently for execution in the reserved execution memory 316. Data in the secure memory 318 may include an identification indicia or hardware identifier 320 and policy data 322 that may specify policy related operational directives such as metering, reporting, update requirements, etc. The secure memory 318 may also include code or data required to implement various functions 324. The functions 324 may include a clock 326 or timer

> implementing clock functions, enforcement functions 328, metering 330, policy management 332, cryptography 334, privacy 336, biometric verification 338, and stored value 340 to name a few.

112. EX-1016, [0023-0024].

113. Xu's secure environment can be used to enforce policies or "establish trust" to perform data access (such as updates) with computers across the network.

> Whether to meter and what specific items to measure may be a function of the policy 322 is implemented by the policy management function 332. A cryptography function 334 may be used for digital signature verification, digital signing, random number generation, and encryption/decryption. Any or all of these capabilities may be used to verify updates to the secure memory 318 or to established trust with an entity outside the processing unit 302 whether inside or outside of the computer 300.

114. EX-1016, [0025]. "Additional updates to the data in the secure memory 318 may be allowed only when specific criteria are met, for example, when the updates are verified by digital signature." EX-1016, [0034].

115. The secure memory stores policy management data:

> The secure memory 418 may include a hardware ID 420 and policy data 422 in addition to general purpose functions 424 that operate as discussed above with respect to FIG. 3, for example clock 426, enforcement 428, metering 430, policy management 432, and

> cryptography 434. Additionally, special-purpose functions such as privacy management 436, biometric verification 438, and stored value 440 may be present. The general purpose and special-purpose functions 424 are given by way of example and not limitation, as other functions are easily imagined by those of ordinary skill.

116. EX-1016, [0036].

117. Policy updates are communicated across the network and such updates may be verified prior to being installed in secure memory:

> 5. The processing unit of claim 1, wherein the communication interface provides data to an application program interface for communicating policy updates.
>
> 9. The processing unit of claim 1, further comprising software code stored in the tamper-resistant memory for implementing a cryptographic function, whereby a policy update is cryptographically verified before installation.

118. EX-1016, claims 5, 9.

119. [This paragraph left intentionally blank].

D. Polson (EX-1008)

120. Polson teaches a "gateway" between WWAN and LANs (both wireless and wireless) that enforces policies such as service agreements:

> A gateway adapted to establish a connection between itself and a WWAN, wherein the gateway has a WWAN interface adapted to receive data from and transmit data to the WWAN on behalf of devices of a LAN, is described herein. The gateway may further determine whether the WWAN interface is associated with a service agreement that provides for use of the gateway. If so, the gateway may operate the WWAN interface in accordance with the service agreement.

121. EX-1008, Abstract.

122. Polson defines "gateway" very broadly as any device that can forward data between the LAN (including WLAN) and WWAN networks:

> "[G]ateway" refers to any computing device capable of facilitating transmission of data from one or more LANS to one or more WWANs, and transmission of data from the one or more WWANs to the one or more LANS.

123. EX-1008, [0026]. For example, Polson's gateway establishes a forwarding link between a WWAN network (such as a cellular network) and a WLAN network (such as an 802.11 network). EX-1008, [0022-0023], [0051-0056].

124. Polson's "routing engine" performs the forwarding between networks.

> Additionally, gateway 108 comprises a routing engine coupled to a local networking interface and the socket, and adapted to transmit data received from one or more devices 102 of a LAN 104 to a recipient gateway device through a first WWAN 112, and selectively transmit data received from the recipient gateway device through the first WWAN 112 to the one or more devices 102 of the LAN 104, if a first WWAN interface 110 is removably received by a socket of the gateway, and transmit data received from the one or more devices 102 of the LAN 104 to a recipient gateway device through a second WWAN (not shown), and selectively transmit data received from the recipient gateway device through the second WWAN to the one or more devices 102 of the LAN 104, if the second WWAN interface is removably received by the socket.

125. EX-1008, [0020].

126. Polson's routing engine performs the forwarding based on policies.

> [0039] In various embodiments, the routing engine of gateway 108 may facilitate two-way transmission of data to and from the one or more LANs and to and from one or more WWANs. As mentioned above, capabilities of the routing engine may be affected by the results of the subscriber determination logic. That is, receipt from and transmission to a WWAN may be based on a service agreement between a user and a wireless service provider. Also, transmission of data from one device 102 of a LAN 104 to another device 102 of a second LAN is described in greater detail above.

[0040] When receiving data from a device 102 of a LAN 104 destined for a WWAN 112, the routing engine of gateway 108 may, in some embodiments, determine if the data received from the device 102 is a request for content from the WWAN 112, and may further determine if such content is cached in storage of gateway 108. If the content is cached, the routing engine may simply retrieve the requested content from the storage of gateway 108, and transmit the content to the device 102 of LAN 104 requesting the content. In such embodiments, no current connection to WWAN 112 is required. In one embodiment, if the subscriber determination logic has determined that the WWAN interface is not associated with a service agreement, the routing module may not provide the cached content.

[0041] If on the other hand the content is not cached, or the data received from device 102 of LAN 104 is not a request for content, the routing engine may, in various embodiments, compress the received data prior to transmitting it. By compressing the data, the routing engine may facilitate transmission of the data at a higher speed than might otherwise be achieved, especially given the typically low speeds at which data is transmitted across a WWAN. Such compression may be achieved through recourse to any compression algorithm known in the art, such as Huffman, Lempel-Ziv, or Venturi, or any combination of such algorithms.

[0042] In some embodiments, the routing engine of gateway 108 may determine whether the gateway 108 is connected to any gateway of

> any WWAN 112 before attempting transmission of data to the WWAN 112. In some embodiments, as mentioned above, the subscriber determination logic, rather than the routing engine of gateway 108, may make this determination. The gateway 108 may determine whether a connection exists by pinging an address of a WWAN 112 and listening for a reply. If no reply is received, the gateway 108 may wait some pre-determined time and try again. After a certain number of attempts have been met without success, the gateway 108 may, in some embodiments, buffer the data to be transmitted in some sort of data structure and continue on an intermittent basis to attempt connection to the WWAN 112. Once a connection has been achieved, the buffered data may then be transmitted to its appropriate destination.

127. EX-1008, [0039-0042].

128. Polson's gateway includes "portable" embodiments that may be carried by a user to allow for "teams of users" to use the WWAN / cellular connection by connecting to one of the WLAN interfaces.

> [0027] In some embodiments, gateway 108 may be adapted to be powered through a wall outlet, a vehicle power adapter, or an internal or external battery. Inclusion of the latter power supplies enables the gateway 108 to be used in portable settings. For example, teams of users may carry the gateway 108 in a briefcase or bag

129. EX-1008, [0027].

130. Polson's gateway creates what is now referenced as a wireless "hotspot" allowing WiFi devices to share a cellular connection. Such devices perform the primary function of Polson's device which is to forward data between a WLAN and WWAN connection. As I have noted herein (below), such hotspot devices in the form factor of mobile phones or "wearable" devices were well-known long prior to the 2009 priority date of the '042 Patent.

131. Polson's gateway also contains extensive ability to download and enforce policies from the cellular network that specify use of the WWAN and WLAN connections. As detailed below for claim 4, Polson identifies numerous different types of policies that the gateway can implement. The gateway may be "customized" with policies specific to a "large corporate user." EX-1008, [0037].

132. These policies are enforced by "subscriber determination logic" which can be software stored on persistent storage.

> [0029] In various embodiments, gateway 108 may include subscriber determination logic adapted to determine whether a WWAN interface 110 for accessing WWAN 112 is associated with a service agreement between a subscriber and the wireless service provider associated with WWAN 112. Once a connection is established with WWAN 112 (see below for further details on establishing the connection), the subscriber determination logic of gateway 108 may determine whether

the WWAN interface 110 being used is associated with a service agreement having one or more features specifying the terms for use of gateway 108. If the service agreement associated with the WWAN interface 110 permits use of gateway 108, then gateway 108 may operate the WWAN interface 110 in accordance with the service agreement, which may include providing connectivity to the applicable network according to the features of the service agreement and/or the policies of the wireless service provider. If the service agreement associated with the WWAN interface 110 does not permit use of the gateway 108, then gateway 108 may restrict WWAN 112 access. In one embodiment, more than one WWAN interface 110 may be available for use by gateway 108 to establish a WWAN 112 connection, and the subscriber determination logic of gateway 108 may further be adapted to determine service agreements, if any, for each WWAN interface 110. In one embodiment, gateway 108 may have and operate a plurality of WWAN interfaces 110, may determine service agreements for each interface 110, and, for each interface 110 associated with a service agreement, may operate the interface 110 in accordance with the service agreement.

[0030] Service agreement features and/or wireless service provider policies may restrict WWAN 112 access in any number of ways, including limitations on the number of simultaneous WiFi or Ethernet LAN 104 connections, the quality of service (e.g., of a suitable level to support Voice-over-IP), the throughput provided, the cumulative

bits per hour, day or month, port-forwarding, on-board VPN, etc. In cases where the WWAN interface 110 is not associated with a service agreement that includes access through gateway 108, gateway 108 may also block all WWAN 112 traffic.

[0031] In various embodiments, the subscriber determination logic of gateway 108 may facilitate a subscriber in altering their existing WWAN 112 access ability on attempting WWAN 112 access via gateway 108. In some such embodiments, the subscriber may be able to change their service agreement to one that allows for WWAN 112 access via gateway 108, or to purchase WWAN 112 access on another basis, e.g., a certain period of time, a certain quantity of bytes downloaded, etc. An example of a service agreement that does not permit use of gateway 108 may be a service agreement that envisions the subscriber only being able to use a single computer at a time to access the carrier's WWAN 112. Another example of a service agreement that doesn't permit a gateway 108 is one that's designed specifically for a phone. In a subset of such an example, the service agreement may permit use of gateway 108, but only in connection with a single computer at a time. Other examples may vary from the ones provided.

[0032] In some embodiments, the subscriber determination logic of gateway 108 may determine the existence of a service agreement and its features by the IP address assigned to the WWAN interface 110 by the wireless service provider. When gateway 108 connects to WWAN

> 112, gateway 108 may interrogate a server, such as a server of the wireless service provider, to determine what policies are associated with the WWAN interface 110's IP address. IP addresses may be categorized in any number of ways in relation to network accessibility. For example, some IP addresses may permit complete WWAN 112 access, while other IP addresses may have policies associated with them that may partially or completely restrict WWAN 112 connectivity.

133. EX-1008, [0029-0032]. See also EX-1008, [0020], [0033-0042], [0056-0058], claims 24-25.

134. Polson's gateway interacts with a wireless server provider (carrier) server to download new policies including, for example, policies that restrict or allow the LAN users to access the WWAN / cellular network.

> [0032] In some embodiments, the subscriber determination logic of gateway 108 may determine the existence of a service agreement and its features by the IP address assigned to the WWAN interface 110 by the wireless service provider. When gateway 108 connects to WWAN 112, gateway 108 may interrogate a server, such as a server of the wireless service provider, to determine what policies are associated with the WWAN interface 110's IP address. IP addresses may be categorized in any number of ways in relation to network accessibility. For example, some IP addresses may permit complete WWAN 112 access, while other IP addresses may have policies

associated with them that may partially or completely restrict WWAN 112 connectivity.

[0033] In one embodiment, where WWAN 112 is a GSM network, the subscriber determination logic of gateway 108 may base WWAN 112 connectivity on the Access Point Name (APN) assigned by the wireless service provider. For example, gateway 108 may provide unrestricted WWAN 112 access for one set of APNs, while providing restricted access for another set of APNs. For example, the "proxy" and "public" APNs on one wireless service provider's network may provide restricted WWAN 112 access (with potentially varying levels of restricted access), but the custom APNs may provide unrestricted access. In some embodiments, the unrestricted and restricted APNs may be configured on gateway 108, or the subscriber determination logic of gateway 108 may access a server, such as a server of the wireless service provider, for updated information about the policies associated with specific APNs. Other GSM network embodiments may incorporate different network access management methods.

[0034] In some embodiments, the subscriber determination logic of gateway 108 may determine an SIM, MIN or ESSID of the WWAN 112 connection and then interrogate a server associated with the gateway 108, or with the wireless service provider, to determine one or more features of the service agreement and/or policies of the wireless service provider based on the SIM, MIN or ESSID. WWAN 112 access restrictions may then be configured on gateway 108 based

on the one or more features of the service agreement, or based on one or more policies of the wireless service provider.

135. EX-1008, [0032-0034].

136.

[0078] In various embodiments, the gateway may then determine whether its WWAN interface is associated with a service agreement with a wireless service provider, block 806, the service agreement having one or more features outlining gateway usage benefits and restrictions. The gateway may determine the existence of the service agreement and one or more features of any such agreement in a number of ways. The gateway may inquire of a server, such as a server associated with the gateway or with a wireless service provider, as to the existence and features of a service agreement associated with one of a number of inputs, such as an IP address associated with a WWAN interface, an APN, a SIM, a MIN, a SSID, or a LAN user authentication. Exemplary features include a limitation on a number of simultaneous WiFi or Ethernet LAN connections of the gateway, a restriction associated with data ports, a quality of service, a throughput limitation, and a data transfer rate limitation. **In addition to providing the features of a service agreement, the server may also return one or more policies of the wireless service provider.** In one embodiment, the gateway may also facilitate a subscriber in altering the features of his/her service agreement, block 808.

137. EX-1008, [0078].

138. The gateway's interactions with the carrier's server allows the user to change / update their service plan – such as to allow for a LAN user to purchase additional WWAN services or upgrades.

> In various embodiments, the subscriber determination logic of gateway 108 may facilitate a subscriber in altering their existing WWAN 112 access ability on attempting WWAN 112 access via gateway 108. In some such embodiments, the subscriber may be able to change their service agreement to one that allows for WWAN 112 access via gateway 108, or to purchase WWAN 112 access on another basis, e.g., a certain period of time, a certain quantity of bytes downloaded, etc. An example of a service agreement that does not permit use of gateway 108 may be a service agreement that envisions the subscriber only being able to use a single computer at a time to access the carrier's WWAN 112. Another example of a service agreement that doesn't permit a gateway 108 is one that's designed specifically for a phone. In a subset of such an example, the service agreement may permit use of gateway 108, but only in connection with a single computer at a time. Other examples may vary from the ones provided.

139. EX-1008, [0031].

140. This is reflected in Polson's claims:

> 7. The method of claim 1, further comprising facilitating a user of one of the devices of the local area network in altering at least one of one

> or more features of the service agreement to allow the gateway to operate the wireless network interface to provide more or less wireless wide area network access.

141. EX-1008, claim 7.

> 19. The gateway of claim 15, wherein the logic is further adapted to facilitate a a user of one of the devices of the local area network in altering at least one of one or more features of the service agreement to allow the gateway to operate the wireless wide area networking interface to provide more or less wireless wide area network access.

142. EX-1008, claim 19.

143. [This paragraph left intentionally blank].

E. Background Prior Art

144. A number of additional other references demonstrate that all of the aspects of the claimed invention were well-known to a POSA long prior to the filing of the '042 patent.

1. Mobile Phone Policy Settings Reference Pearce (EX-1006)

145. U.S. Publication No. 2006/0183461 ("Pearce") (EX-1006) was filed on February 11, 2005 and published on August 17, 2006. Pearce is prior art to the '042 Patent under Section 102(a)(b)(e)(g).

146. It was known to use policy settings stored on a wireless device to control the operation of a wireless device including providing access to data networks, the type of communications permitted, the type of communication protocol used, the use of communications applications, and the identification of the wireless carrier.

147. For example, one prior art system (Pearce) provides a system and method of modifying policy settings in a wireless device.

> The present invention provides a system and method of modifying policy settings in an electronic device. An embodiment includes a plurality of access stations, each capable of wirelessly transmitting across a geographic region. A mobile electronic device, capable of roaming between regions is operable to establish a wireless link with the access stations. The device is owned by an office which sets communication policies determining through which access stations mobile device can place voice calls. This policy is stored on an office server as a database and periodically transmitted to the device as the device makes contact with the office server over the internet. Hence, the device maintains a copy of this policy database. When placing a voice call, the device first determines which access station is serving the region it is located in and then determines whether it is allowed to place a call through that access station using its policy database.

148. EX-1006, Abstract.

149. In Pearce, the wireless device maintains a database of the communication policy settings that is updated by the server in the office from time to time.

> [0040] By the same token, device 58 also includes CP database 122 that includes data corresponding to the information stored in CP database 118. The initial settings of CP database 122 are shown in Table II.
>
> TABLE II
>
> Example of a CP Database 122 of Device 58
>
> | Field 1 Access Station Identifier | Field 2 Policy for Voice Calls |
> |---|---|
> | AID1 | Allow Communication |
> | AID2 | Allow Communication |
> | AID3 | Allow Communication |
>
> Field 1 of database 122 corresponds to Field 2 of database 118, and Field 2 of database 122 corresponds to Field 3 of database 118. Because initially, when the user first acquires the device from office

62, device database 122 has the same content as the office database 118.

[0041] The policy, as described by CP database 118, is set by office 62 and updated by office 62 from time to time as needed. For example, office 62 may desire that device 58 should place wireless calls through network 50 only when a digital link is available between an access station 34 and device 50 to reduce the chances that the wireless portion of the call is intercepted. According to this policy office 62 would not want device 58 to connect to network 50 through access stations 34 2 or 34 3 since stations 34 2 34 3 only provide an analog link 42 2 42 3 based on AMPS which is highly susceptible to interception. Thus, policy database 118 would be updated to reflect the new policy as shown in Table III.

TABLE III

Example record of an Updated CP Database 118 of Office 62

Record # 1

Field 2

Field 1	Access	Field 3
Device	Station	Policy for
Identifier	Identifier	Voice Calls
555-555-	AID1	Allow
5555	Communication	
AID2	Disallow	
Communication		

AID3 Disallow Communication

> Notice that Field 3 associated with AID2 has been changed to "Disallow Communication" to reflect the new policy that device 58 should not connect to network 50 through access station 34 2.

150. EX-1006, [0040-0042].

151. The policies can control the ability of the wireless device to access various types of networks based on a variety of different policy considerations:

> [0009] The policy can permit one type of service to be performed in one specific region, while disallowing another type of service in the same specific region.
>
> [0010] The policy can disallow communications in a particular region if the communications within the region are conducted over an insecure link, or are otherwise insecure.
>
> [0011] The policy can disallow communications in a particular region if the communications within the region are conducted over an insecure link, or are otherwise insecure.
>
> [0012] The policy can disallow the communications in at least one of the regions if a financial cost for conducting the communications exceeds a predefined threshold.

152. EX-1006, [0009-0012].

153. Further, the policy can allow specific communications such as voice calls, web browsing, e-mails, etc. EX-1006, [0060], [0008].

154. Pearce's mobile device can use multiple different WLAN (802.11) and WWAN (CDMA, AMPS, GSM, GPRS) connections.

> The links can include wireless links that can be based on one or more of CDMA, OFDM, AMPS, GSM, GPRS, bluetooth, infra-red and 802.11.

155. EX-1006, [0013], claim 15, [0067], [0035].

156. Pearce describes known methods for encrypting links and teaches that such encryption provides "inherently more secure links."

> Digital links 42 based on GSM offer enhanced security over analog links 42 based on AMPS. Interception and reconstruction of a digital link involves more highly specialized and expensive equipment than an analog link. Moreover, digital links 42 can be encrypted using methods such as stream ciphers, resulting in an encrypted communication between device 50 and access station 34. In this embodiment link 42, is a digital link, whereas links 42 2 and 42 3 are analog links. As such, link 42 1 is inherently more secure then links 42 2, and 42 3.

157. EX-1006, [0035].

158. [This paragraph left intentionally blank].

2. **Storing and Modifying Policies on Mobile Phones Reference Aarnos (EX-1007)**

159. U.S. Publication No. 2007/0288989 ("Aarnos") (EX-1007) was filed on June 9, 2006 and published on December 13, 2007. Aarnos is prior art to the '042 Patent under Section 102(a)(b)(e)(g).

160. Aarnos teaches that it was known in the prior art that policies could be stored on a mobile phone and subsequently modified. For example, in one prior art system (Aarnos), before a stored policy could be modified, an electronic signature or key is verified in order to determine whether and what extent the modification is in fact authorized to modify the existing policy.

> [0023] The developed software component and the corresponding policy update script are then combined, in Step 103 into a deployment (or installation) package for deployment on the device. The deployer (or party responsible for creating the deployment package and providing it to the electronic device, which may or may not be the software developer), in Step 104 signs the package (i.e., incorporates a digital signature, such as a private key, with the package). The signature will be used to verify whether and to what extent the signer (i.e., the deployer) is authorized to modify the electronic device security policy; thus providing increased security to the policy updating process. In one exemplary embodiment, different parties

may be provided with different levels of authorization. For example, where one party may have authorization to make wholesale modifications to the existing security policy, other parties may have only restricted access.

[0024] The deployment or installation package, including the software component, the policy update script and the signature, is then provided to the device in Step 105. In one exemplary embodiment, this step is performed where the user of the electronic device initiates the download of the software component over a network, such as a wide area network (WAN), or the like. Alternatively, the software component may be pushed to the electronic device. As one of ordinary skill in the art will recognize, the software component may be transmitted via any number of mechanisms, including, for example, over Bluetooth, a USB cable, infrared, or even a multimedia card (MMC), without departing from the spirit and scope of exemplary embodiments of the present invention.

[0025] Regardless of how the deployment package is received by the electronic device (in Step 106), upon receipt, installation of the deployment package begins (Step 107). In one exemplary embodiment, at the commencement of the installation process, the deployer's signature is verified in order to determine, as stated above, whether and to what extent the party transmitting the deployment package is in fact authorized to modify the existing security policy of the mobile device (Step 108). Assuming the signature is verified and

> that the deployer is authorized (based on the existing electronic device security policy), in Step 109, the policy update script is processed in order to effect the modifications to the security policy that are described by or included in the policy update script.

161. EX-1007, [0023-0025]. This type of verification process is also used to provide different levels of authorization --for example, one party may have authorization to make wholesale modifications to the existing policy, and other parties may have only restricted access. EX-1007, [0023]. See also EX-1007, [0021-0028] describing the "Method of Updating Electronic Device Security Policy."

162. Aarnos also teaches a mobile device (e.g., "cellular telephone, PDA, PC, laptop, pager") that operates with both WWAN (EX-1007, [0021] and WLAN functionality.

> More particularly, the mobile station can be capable of operating in accordance with any of a number of second-generation (2G), 2.5G and/or third-generation (3G) communication protocols or the like. Further, for example, the mobile station can be capable of operating in accordance with any of a number of different wireless networking techniques, including Bluetooth, IEEE 802.11 WLAN (or Wi-Fi®), IEEE 802.16 WiMAX, ultra wideband (UWB), and the like.

163. EX-1007, [0045]

164. [This paragraph left intentionally blank].

3. **Hardware Enforced Protected Partition References Arm TrustZone Microprocessor Report (EX-1009) and Arm TrustZone Paper (EX-1010)**

165. Prior to the '042, many companies had developed (and deployed) hardware-based approaches to providing protected partitions of memory on mobile devices that were configured to deter or prevent unauthorized modification. A POSA at the time of the invention would have known from the prior art that critical data, such as policies, would be beneficially stored in protected memory partitions to prevent unauthorized access that could include hardware-based techniques to provide the protections.

166. Providing protected partitions of memory that restricted access to critical data was well-known and pervasive in mobile devices by the 2009 Priority Date. Schemes for protecting memory included both hardware controls and encryption. For example, Arm's "TrustZone" technology was patented starting in 2003.

167. For example, in August 2003, the publication Microprocessor Reports published an article entitled "ARM Dons Armor TrustZone Security Extensions Strength ARMv6 Architecture." (EX-1009) ("TrustZone MPR).

168. TrustZone MPR noted the need for secure computing and specifically targeted mobile devices and noted that "wireless networking" created the potential for "intrusions"

> ARM's target applications are smartphones, handheld computers, and any embedded system likely to suffer from the malicious hackers who are expanding their attention beyond PCs. Wireless networking and field-upgradable software are opening new doors for intrusions, yet the typical embedded system has fewer system resources to spare for security measures than a PC has.:

169. EX-1009 at 1. As noted, TrustZone implementations were expected by 2004 and in products by 2005 – long prior to the 2009 priority date of the '042 Patent. EX-1009, at 1.

170. TrustZone provides "hard-wired" protected partitions:

> A key feature of TrustZone is that the extensions are hard wired into the microprocessor core, … A better approach is to chisel the basic security features into the processor's logic and minimize the amount of software that needs to be secure. The fewer doors and windows there are, the fewer the opportunities for break-ins.

171. EX-1009, at 1.

172. TrustZone implements secured memory partitions to protect data.

> The secure monitor doesn't necessarily have to flush the instruction cache, data cache, TCM, or any other memory when switching contexts, because TrustZone divides those structures into secure and nonsecure partitions. The caches, memory-management unit (MMU), and translation lookaside buffer (TLB) have additional tag bits—S-bit tags—to keep track of those partitions. Only a secure process can access a secure memory partition or cache line. Any attempt by a nonsecure process to access the restricted cache lines or memory will generate a cache miss and/or external abort, as if the program had tried to access nonexistent memory.
>
> Although secure partitioning makes parts of the caches off-limits to nonsecure processes, the secure cache lines aren't actually locked (unless the programmer explicitly locks them). New data from a secure or nonsecure process can evict old data from the secure cache lines as part of the cache's normal behavior.
>
> Scratchpad memory isn't organized into lines like a cache, so a system that uses TrustZone must dedicate separate TCMs for secure and nonsecure data. The ARMv6 architecture allows up to four TCMs, and developers can partition a single physical block of on-chip SRAM into multiple logical TCMs. Partitions can vary in size at run time, though it may be undesirable for one process to dynamically allocate resources that another process may need. ARM expects the secure

> monitor and its scratchpad memory to reside in a secure TCM—partly for its own protection, and partly so the monitor's response latencies are predictable.
>
> By maintaining separate partitions in caches and memory, and by strictly enforcing access privileges for those partitions, TrustZone can eliminate a back door commonly exploited by malicious programs. An untrusted program shouldn't be able to substitute its own instructions or data to seize control of the system or corrupt the output.

173. EX-1009, at 2.

174. The Arm MPR notes that similar technology is being developed for many other microprocessors:

> However, it is possible to add similar extensions to the configurable microprocessor cores licensed by ARC International, MIPS Technologies, and Tensilica, or even to add custom extensions that go well beyond TrustZone. For instance, ARC has instruction extensions for the ARCtangent-A5 processor that accelerate any protocols using DES or 3DES encryption, such as IPSec (Internet Protocol Security), SSL (Secure Sockets Layer), TLS (Transport Layer Security), and encrypted PPP (Point-to-Point Protocol). In addition, ARC recently announced two new security packages, IPShield and ARCprotect. IPShield adds IPSec to ARC's licensable TCP/IP stack for ARCtangent-A5, ARM, MIPS, ColdFire, and Power- PC processors.

> ARCprotect uses the DES extension and about half a dozen other custom instructions to accelerate IPShield on the ARCtangent-A5

175. EX-1009, at 4.

176. Arm published white papers in 2004 describing "TrustZone: Integrated Hardware and Software Security System." EX-1010 ("TrustZone Whitepaper")

177. The TrustZone Whitepaper both notes the need for such protections in "mobile applications" and Arm's solution. EX-1010, at 1. TrustZone was partitioned into protected and unprotected worlds including memories. EX-1010 at 6 (Diagram). TrustZone was useful for cryptography and encryption. EX-1010 at 5.

> Together, the integrated hardware-software TrustZone solution provides a number of key security features, including: platform identification and authentication, identity, key and certificate management, low-level cryptography, I/O access control, safe data storage, smart card access and code/integrity checking.

178. EX-1010, at 5.

> The Security Module and the TrustZone-optimized software feature an independent and certifiable secure framework. It has exclusive access to dedicated protected memory, dedicated persistent storage, SIM card, crypto-accelerators and a possible trusted user Interface. By

> way of security services, it provides integrity checking (SIMLock, IMEI protection, secure boot), access control, secure storage and cryptography services. Future services may include frameworks for DRM, digital signature and e-banking.

179. EX-1010, at 7.

180. Arm filed patents describing the TrustZone technology starting in 2003. For example, U.S. Pat. No. 7,849,310 was filed in 2002 in Great Britain and in 2003 in the U.S (EX-1012) ("Watt") It published in August 5, 2004 as U.S. Publication No. 2004/0153672. Watt is prior art to the '042 Patent under Section 102(a)(b)(e)(g)

181. Watt teaches a processor allowing for "Switching between secure and non-secure processing modes." EX-1012, Title.

182. A data processing system including a processor operable in a plurality of modes and in either a secure domain or a non-secure domain. The system includes at least one secure mode being a mode in the secure domain, at least one non-secure mode being a mode in the non-secure domain, and a monitor mode. When the processor is executing a program in a secure mode the program has access to secure data which is not accessible when the processor is operating in a non-secure mode. Switching between the secure and non-secure modes takes place

via the monitor mode and the processor is operable at least partially in the monitor mode to execute a monitor program managing switching between the secure and non-secure modes.

183. EX-1012, Abstract.

184. Watt identifies the problem of protecting data applications from "hacking." EX-1012, 1:13-42.

185. Watt's solution arises because "it will be desirable to provide an improved technique for seeking to retain the security of such secure data contained within the memory of the data processing apparatus." EX-1012, 1:49-52.

186. Watt teaches a hardware-enforced mechanism that will "define the part of the memory that is to be protected as secure memory." EX-1012, 45:58-59.

187. Watt teaches "Access To Secure and Non-Secure Memory":

> Access to Secure and Non-secure Memory
> As described with reference to FIG. 1, the data processing apparatus has memory, which includes, inter alia, the TCM 36, cache 38, ROM 44, memory of slave devices and external memory 56. As described with reference to FIG. 37 for example, memory is partitioned into secure and non-secure memory. It will be appreciated that there will not typically be any physical distinction between the secure memory regions and non-secure memory regions of the memory at the time of

> fabrication, but that these regions will instead be defined by a secure operating system of the data processing apparatus when operating in the secure domain. Hence, any physical part of the memory device may be allocated as secure memory, and any physical part may be allocated as non-secure memory.

188. EX-1012, 20:43-62.

189. In such systems, [t]he memory protection unit is managed by the secure operating system … defining the partitions between the secure memory and the non-secure memory." EX-1012, 39:64-67.

190. Watt provides extensive details of the secure partition and environment with regard to the techniques used to secure the memory. EX-1012, 37:23-50:17. These techniques include a "partition checker 222" which ensures that the secure memory partitions are protected from unauthorized access.

191. Effectively, Watt teaches the type of secure environment technology that the later Xu reference uses for its policy storage and enforcement and other activities as described for Xu below.

192. [This paragraph left intentionally blank].

4. **Encryption Protected Partition References (EX-1011) (EX-1014) (EX-1015)**

193. A POSA at the time of the invention would have known from the prior art that critical data, such as policies, would be beneficially stored in protected memory partitions to prevent unauthorized access that could include encryption techniques to provide the protections.

194. For example, U.S. 2006/0112427 was filed on priority date of August 27, 2002 and published on May 25, 2006 (Shahbazi) (EX-1011). Shahbazi is prior art to the '042 Patent under Section 102(a)(b)(e)(g).

195. Shahbazi teaches "Enterprise-wide security system for computer devices." EX-1011, Title.

196. In particular, Shahbazi teaches protections for mobile devices using profiles and policies.

> A system and method for securing data in mobile devices includes a computing node and a plurality of mobile devices. A node security program executed in the computing node interfaces with a device security program executed at a mobile device. The computing node is responsible for managing the security based on a node security profile interpreted by a node security program executed in the computing node. A device discovery method and arrangement also detects and

> locates various information about the mobile devices based on a scan profile.

197. EX-1011, Abstract.

198. Shahbazi notes the need for data protections for mobile devices and details some of the known techniques for such protections.

> [0004] As society continues to adopt handheld devices as a standard computing platform and applications become more powerful with the standardization of wired and wireless computing, security threats to data stored in these types of mobile devices have become a serious concern and have created a heightened awareness and increased need for security. In fact, the U.S. Air Force Research Laboratory (AFRL), which develops some of the government's most advanced technologies, is crafting a policy to deal with security risks for data stored in mobile devices.
>
> [0005] Various types of security software incorporating different data security encryption standards have been used in the past for securing network, desktop, laptop and PDA environments. On such suit of software is called Trusted Mobility Suite™ offered by Trust Digital™, which is used to set access control, encryption, and other parameters and push them to such mobile devices as Palm Pilot™, Pocket PC™, Blackberry™ or Symbian OS devices to protect against fraud and theft, sabotage, malicious hacking and other adverse exposure caused by data compromise. For example, at a network

level, PDASecure™ Virtual Private Network provides secure communication among mobile devices or between mobile devices and routers and servers. Mobile DesktopSecure™ is a security and encryption software designed to protect files, data, applications, databases, directories, or an entire hard drive. It is also used to push security profiles containing defined security policies from a server to protect laptops and desktops within a network. Generally, Trusted Mobility Suite™ implements security using a graphical user interface (GUT) that allows administrators and users to secure all or selected applications. In this way, the users and administrators can selectively secure application(s) from unwanted and unauthorized access.

[0006] Trusted Mobility Suite™ manages data security for mobile devices at different levels. At a higher server level Trusted Mobility Server™ deploys, manages, and secures networks containing mobile devices using a centralized management solution. A policy-profile editor is used to set security parameters for groups of users based on defined security policies. At a lower device level PDASecure™ encrypts the data on the mobile device itself and offers-security management for those devices through the Trust Mobility Server. Once insalled [sic] on a mobile device, PDASecure™ provides for universal integration with all available mobile devices on the network, without the requirement for moving data into separate, secured applications. Also, Trusted Mobility Software Development Kit™ allows software developers to incorporate Trust Digital's Mobility

> Framework, comprising security, encryption, and centralized rule-based management technologies into their products, for mobile/PDA users.

199. EX-1011, [0005-0006]. Notably, even as of its 2002 filing, Shahbazi noted the known techniques for protecting mobile device data included "security, encryption, and centralized rule-based management technologies … for mobile/PDA users."

200. Shahbazi teaches that the mobile devices include security parameters in their profiles to prevent hacking including through encryption.

> In contrast with the node security profile 208, which sets the computing node security parameters, the device security profile 206 sets the security parameters for the devices 104 and 124, as interpreted by the device security programs 204. The device security parameters include encryption preferences, global (device) password, local (application or resource) password, access control to applications and resources, access control to the device, integrity protection against hackers and traps, file encryption options, port protection, communication protection (i.e., send and receive), ability to use wireless connections like Wi-Fi, 802.11, Bluetooth, controlling the content of the device like restricting installing of some applications, etc.

201. EX-1011, [0046]. See EX-1011, [0079] (noting that parameters of "IsFileEncrypted" or "Encryptfile").

202. As with other references herein, Shahbazi contemplates that its mobile devices will have WLAN and WWAN connections. EX-1012, [0046] ("Wi-Fi, 802.11").

203. Shahbazi's target mobile devices included mobile phones.

> Recent advances in hardware and communication technologies have brought about the proliferation of powerful mobile devices ranging from notebook computers to much smaller personal digital assistants (PDAs) that operate over wired and wireless networks. These mobile devices (also known as handheld devices) operate on various platforms, such as palm computing platform, Windows CE, etc. Other types of mobile devices include paging and messaging devices, laptop computers, data-capable smart phones, etc. These devices can provide users with network access connectivity, which allows users to be quickly notified of changing events, and provide them with the resources necessary to respond even when in transit. In this way, users can be given the power to access mission critical information in quick and reliable manner. For example, data generated by client applications running on a wide variety of mobile devices may be transported over networks having various access protocols and wired and wireless links. One such protocol is Transmission Control

> Protocol/Internet Protocol (TCP/IP), which is designed to connect computer systems that use different operating systems and network technologies. Many popular network applications have been built directly on top of the TCP over the past decade, maling [sic] TCP/IP a de-facto network access protocol standard.

204. EX-1011, [0002].

205. U.S. 2006/0224742A1 was filed on February 28, 2006 and published on October 10, 2005 ("Shahbazi II") (EX-1014). Shahbazi II is prior art to the '042 Patent under Section 102(a)(b)(e)(g).

206. Shahbazi II teaches (similar to other references including Wright) that administrators had the capability and rights to quickly define that any or all of the data on the mobile device may be encrypted including protections for "lost & stolen" devices – which matches Limont's concern about such devices.

> Device Policy [0124] Once a mobile device 10, such as, a PDA or Smartphone, has been allowed to access data from the enterprise or corporate network, there are a number of options to control what peripherals and resources the device can use based on security administrator concerns about accidental or malicious data exposure.
> [0125] Depending on the platform and the device type, the table below provides a representative example of the types of peripherals and resources that can be restricted.

Device Policy v1	This set of policy features describes the access rights and restrictions relating to non-software functions and peripherals.
Peripheral and Port Restrictions	This feature provides a listing of all peripheral and port capabilities of the device type and enables the administrator to allow access, prevent access based on approved device white list
Time Restrictions	This feature enables the administrator to set specific day of week and time period restrictions on accessing the device. When the device is out of range of acceptable time periods the appropriate message should be displayed.

[0126] Lost & Stolen Devices

Lost & Stolen Devices	This set of policy features helps eliminate data theft and also provides a set of parameters should devices become lost or stolen.
Idle Lock	This policy feature describes the amount of idle time that transpires before the Power on Password screen is displayed. This time may be more or less than the idle time power down on the device. In any event, if the idle lock time has transpired or the device goes to sleep itself, the system will display the Power On Password before the device

	can be used further.
Sync Inactivity Lock/Wipe	This policy feature describes the amount of time that transpires without an data processing or synchronization activity happening on the device that transpires before additional actions are taken by the device based on the policy.
Password Failure	This describes the number of tries a user is allowed to enter a password before additional action (Lock or Wipe) is taken.
Enable Forgot Password	This allows an administrator to choose from a group of pre-determined set of questions which the user must answer in order to re-set the password in question. Based on the questions selected as part of the policy, a user will be prompted to answer these questions as part of either the initial start up process on the device or immediately following the next successful login if it is part of an updated policy. An option to access this is available on the Power Up Password screen.
Wipe Password	This password is designed to enable the user to select a password to self destruct the device and all its data. If selected as part of a policy, the user will be prompted to enter the wipe password

	during the initial startup up process on the device or immediately following the next successful login if it is part of an updated policy.
Remote Unlock (1× challenge)	This option should be displayed on the Power-On Password Screen and enables the user to read the administrator a long number and then have the administrator read back a long number as well to unlock the device. This should accessible [sic] from the Power on password screen as well as instances where the device has been lock (idle or activity locks) where the action is to lock and not wipe the device.

[0127]

The preferred embodiment further provides on-the-fly encryption capabilities and operability that maximizes user compliance and minimizes data theft and loss. An administrator has rights to quickly define the type of information and databases (All, PIM, Specific *.ext and/or designated databases), or even the entire device, to be encrypted. This ensures that the data is always encrypted on the mobile device 10 and that only "Trusted" applications can access the data. This eliminates the threat of worms, viruses, Trojan horses and unapproved applications recklessly or maliciously accessing important

information. These same encryption capabilities can also be applied to storage peripherals such as SD cards; again with no user interaction and no need to create special files or folders. Finally, this approach is application, device and network agnostic and therefore is even natively compatible with all enterprise sync vendors and sync methods ((PC sync, device-initiated, IP Push).

Encryption Preferences	This option enables the user to select the target file types or other data options that should be encrypted as part of a given policy. The specific algorithm and encryption key are managed at a global level.

ALGORITHM	FIPS-Validated	NON-FIPS
Triple DES	X	
AES	X	
SHA1	X	
HMAC-SHA1	X	
RNG	X	
Twofish		X
Blowfish		X
RC4		X
TEA		X
XOR		X
MD5		X

[0128]

The storage module 24 provides the capability and operability to encrypt data on removable storage media on one type of mobile device (e.g., Pocket PC) and move the data on that storage device for processing on one or more other types of devices (e.g., laptop, Palm, desktop). The data remains protected throughout the moves and is able to be decrypted and utilized on each of the devices to which the media is moved. The storage module 24:

[0129] Provides portable data encryption

[0130] Facilitates easy transfer of information between mobile device 10 and PC 11 a

[0131] Enables other authorized users to open stored files and view/modify contents on different platforms and operating systems

[0132] Works on PDAs and SmartPhones, as well as laptop, tablet and desktop PCs Network interface module 26 includes a wireless firewall. It provides a small footprint (only about 150 Kb of memory), and provides the following functionality:

[0133] Enable/disable and change security settings without re-booting the device

[0134] Multiple security profiles, default policy, rules customization based on specific settings and time restrictions as well as direction of data flow (inbound or outbound)

[0135] Security logs

[0136] Supports rules for TCP, UDP, and IP, as well as ICMP events.

[0137] Host blocking and content filter

> The administrator also has several options available to them both at policy creation and at any time moving forward based on a policy group or individual user including:
>
> [0138] Force Password Change at Next Logon
>
> [0139] Re-Set Power-On Password
>
> [0140] Re-Set Wipe Password

207. EX-1014, [0127-0140].

208. Like many of the other references herein, Shabazi II allows for policy updates across networks to mobile devices.

> One configuration for the systems and methods of the present invention leverages the PC Agent 28 for software distribution, policy distribution and updates, registration process and non-device specific remote services. Distribution can be accomplished during synchronization via a USB port or wireless connection.

209. EX-1014, [0141].

210. Shahbazi II identifies and uses a large number of policies and, like Wright, uses XML to distribute those policies. EX-1014, [0144-0147].

211. Shabazi II describes a desired goal (like Wright and Limont) to allow administrators to update and distribute policies to mobile users with wireless communications. EX-1014, [0012-0013].

212. U.S. 2009/0265754 was filed on April 17, 2008, published on November 22, 2009 ("Hinds") (EX-1015). Hinds is prior art to the '042 Patent under Section 102(a)(e)(g).

213. Hinds expressly teaches storing policies as encrypted on mobile devices:

> [0053] In an embodiment, enforcement policy 230 is stored in an encrypted state on mobile device 120. As an example, policy server 130 may encrypt enforcement policy 230 created by administrator 102 before it is provided to mobile device 120. Encryption of enforcement policy 230 may prevent user 150 from modifying enforcement policy 230.
>
> [0054] In an embodiment, not intended to limit the invention, enforcement policy 230 is encrypted using FIPS 140-2 compliant encryption. FIPS 140-2 is known to persons skilled in the art and is a U.S. government computer security standard used to accredit cryptographic modules. Some of the cryptographic algorithms used are triple DES (3DES) and advanced encryption standard (AES). However, the invention could alternatively employ any well known encryption algorithm process or technique.

214. EX-1015, [0053-0054].

215. The stored polices are decrypted when retrieved from memory:

> [0075] In step 504, enforcement device driver 240 decrypts mobile device settings included in encrypted enforcement policy 230. As an example, such settings may be set by an administrator 102 to control access to resources associated with mobile device 102.
>
> [0076] In step 506, enforcement device driver 240 stores decrypted mobile device settings in memory associated with mobile device 120.
>
> [0077] In step 508, enforcement device driver 240 uses decrypted mobile device settings in enforcement policy 230.

216. EX-1015, [0076-0077]

217. As with other references, Hinds expressly teaches that its devices may have WLAN (WiFi) and WWAN (Cellular) connections and that the mobile device may enforce policies based on those network types.

> [0034] Enforcement policy 230 may include information regarding resources on a mobile device that can be controlled by administrator 102. Furthermore, enforcement policy 230 may describe how features of mobile device 120 may be set, configured or disabled. Exemplary resources or features that may be controlled by enforcement policy 230, include, but are not limited to:
>
> [0035] 1. Cellular Network Connections
>
> [0036] 2. Internet Connections and Security Configuration
>
> [0037] 3. Infrared Ports
>
> [0038] 4. WiFi Connections
>
> [0039] 5. Microphones

[0040] 6. Device Cameras

[0041]

7. Device Memory Expansion Slots

[0042] 5. Device USB Connectivity

[0043] 9. Device Bluetooth Connectivity

[0044] 10. Owner Information for Device

[0045] 11. Email and Text Messaging Configuration

[0046] Additionally, enforcement policy 230 may control or enforce internet controls 250, messaging configuration 252, network connection 254, camera device 256, Bluetooth device 258 and external data store 270.

[0047] Internet controls 250 may include controls which may regulate access to certain sites on the Internet or control a manner in which mobile device 120 connects to the Internet or other networks.

[0048] Messaging configuration 252 may include information on how messages are transmitted and received by mobile device 120. For example, messaging configuration 252 may prevent user 150 from sending messages to a certain group of users associated with network 110.

[0049] Network connection 254 may include one or more connections used by mobile device 120 to access network 110. Enforcement policy 230, for example, may prevent user 150 from accessing network 110 by controlling or restricting access to network connection 254.

218. EX-1015, [0034-0049].

219. Hinds also teaches that its mobile devices receive policies across the wireless network from servers:

> [0031] Mobile device 120 may receive enforcement policy 230 from policy server 130 over network 110. Enforcement policy 230 could also be pre-installed, manually installed or installed through any other method. As an example, not intended to limit the invention, mobile device 120 may receive enforcement policy 230 from policy server through a message transmitted using the short messaging service (SMS). SMS is known to persons skilled in the art as a method to transmit short messages to mobile devices across wireless networks.

220. EX-1015, [0031]

221. Thus, as shown by the references above, before the 2009 priority date of the '042 Patent, a POSA would have understood and known that there was a need for protected partitions of memory storing policy data and that one known solution was to provide for encryption of the memory storing confidential data including policies.

222. [This paragraph left intentionally blank].

5. **Mobile Phones / Wearable Devices Implementing WWAN / WLAN Gateways (EX-1017) (EX-1018) (EX-1019) (EX-1020)**

223. Before the 2009 priority date of the '042 Patent, a POSA would have known that there were known techniques and technologies to allow for a gateway between WWAN and WLAN networks to forward data between those networks and to be in the form factor of a mobile phone or a wearable mobile devices. Such devices were widely described in patents including the patents referenced below.

224. U.S. Pat. No. 8,064,417 was filed on November 4, 2008, published on July 16, 2009, and issued on November 22, 2011 ("Maki") (EX-1017). Maki is prior art under at least 102(a)(e)(g).

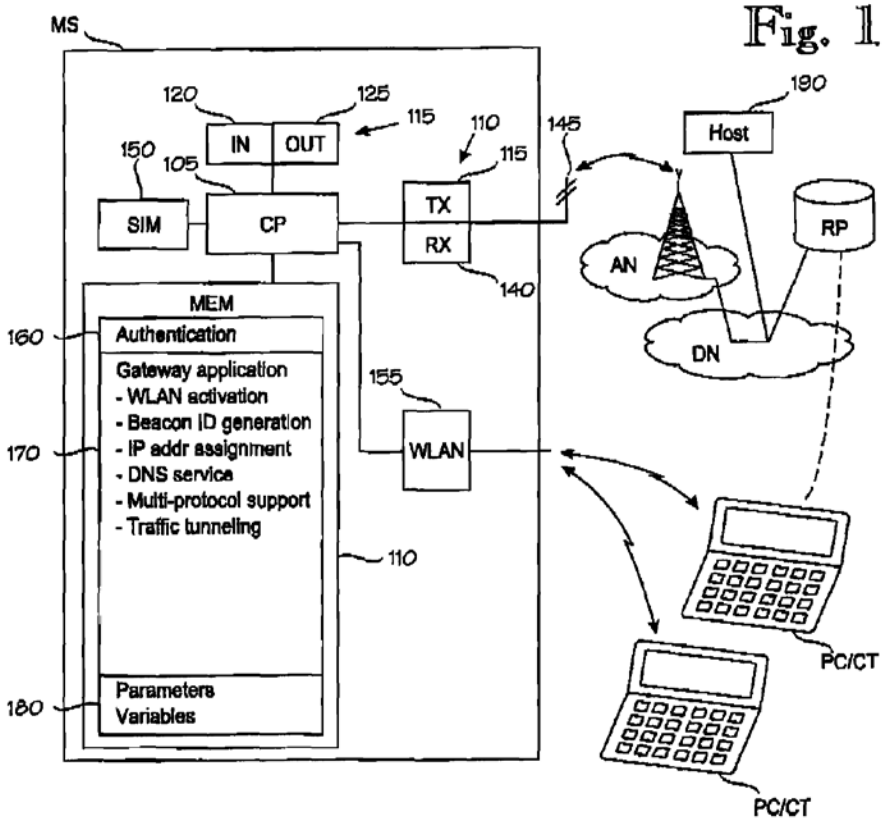
225. Maki teaches a "Mobile WLAN Gateway." EX-1017 at Title. Maki teaches forwarding data between a WLAN and "broadband connection."

> A technique for operating a mobile station as wireless local-area network (WLAN) gateway. The mobile station is provided with a gateway application to control the following operations: activating the WLAN means as a WLAN base station capable of communicating with at least one WLAN terminal over a WLAN network; creating a network identified for the WLAN base station; assigning an internet protocol address for the at least one WLAN terminal; resolving domain name service (DNS) queries in cooperation with an external

DNS service system; assigning at least one port number for each protocol supported by the gateway application; and tunneling internet traffic between the at least one WLAN terminal and an internet host over the broadband connection.

226. EX-1017, Abstract.

227. Maki shows a "MS" (mobile station) acting to forward data between a WLAN 155 and a WWAN using antenna 145:



228. The access network is "typically a broadband-capable mobile communication network." A POSA would understand such a disclosure to include

a WWAN network because such mobile communication networks provided wireless wide-area networking.

229. The MS (mobile station) forwards data between the WLAN and WWAN networks. 4:44-5:67.

230. U.S. Pat. No. 7,672,695 was filed on December 6, 2005, and issued on March 2, 2010 ("Rainnie") (EX-1018). Rainnie is prior art under section 102(a)(e)(g).

231. Rainnie teaches a "Wearable Access Point." EX-1018, Title.

232. Rainnie acts as a WLAN/WWAN gateway to forward / route data between the two networks:

> A portable access point comprises a wireless LAN transceiver that selectively establishes a plurality of Ethernet wireless links with a plurality of wireless client devices, respectively. A wireless WAN transceiver establishes an Ethernet data connection with an Internet Service Provider (ISP), receives and forwards Ethernet data packets from at least one of said wireless client devices to said ISP and receives and forwards Ethernet data packets from said ISP to said one of said wireless client devices. A routing device routes Ethernet data packets between said wireless LAN transceiver and said wireless WAN transceiver. A control module controls operation of said wireless LAN transceiver and said wireless WAN transceiver. A first

storage device stores operating system and application instructions for said control module.

233. EX-1018, Abstract.

234. Wainnie's wearable access point has a WWAN and WWLAN transceivers.

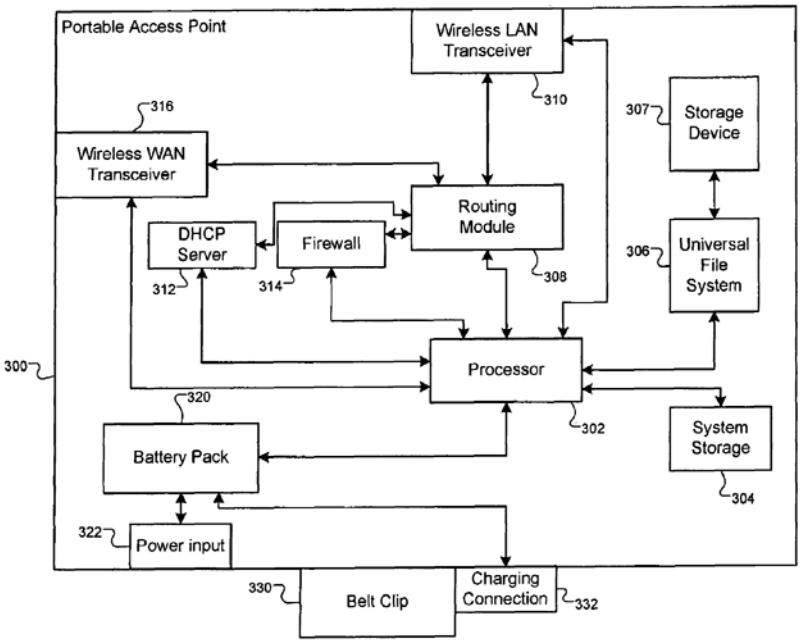


FIG. 4

235. EX-1018, Fig. 4. It can also be implemented in "phone" format:

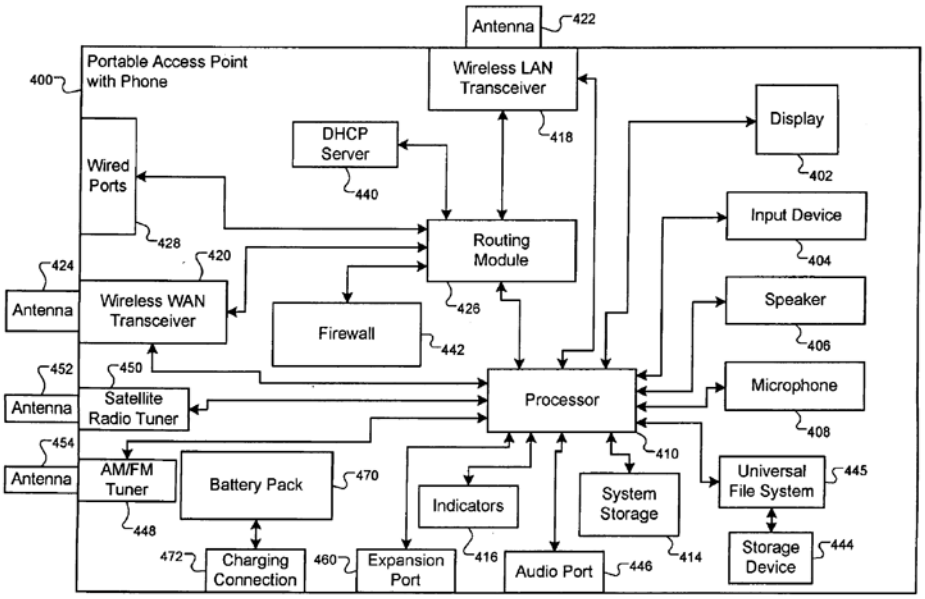


FIG. 5

236. EX-1018, Fig. 5.

237. Rainnie describes a "portable access point" throughout.

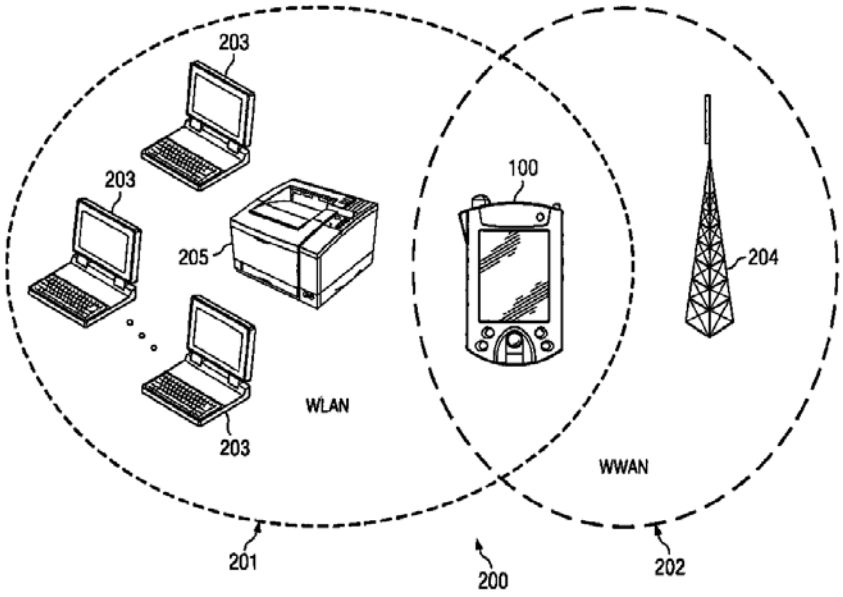
238. Rainnie's WLAN/WWAN gateway "may be a mobile telephone, a PDA, or any other battery-powered device" and / or may "attach to a user's belt via a belt clip." EX-1018, 7:17-23. See also EX-1018, 2:25 ("A belt clip permits wearing of the portable access point."); 4:26, 6:28-30 (all describing small form factor that can be worn and/or carried in a briefcase.

239. Rainnie's WWAN/WLAN gateway implements a firewall that allows it to enforce protections for the devices attached to it. EX-1018, 4:27-30, 6:15-18,

7:7-15. It would be obvious to a POSA that the firewall would enforce policies related to network action in light of Rainnie's disclosures.

240. U.S. Pat. No. 7,881,267 was filed on June 4, 2004, published as US 2005/0286476 on December 29, 2005 and issued on February 1, 2011 ("Crosswy") (EX-1019). It is prior art under section 102(a)(b)(e)(g) (including the published version of it).

241. Crosswy depicts a mobile phone / PDA acting as a WWAN / WLAN gateway:



242. EX-1019, Fig. 4.

243. Crosswy's mobile WLAN/WWAN gateway may be implemented in various portable forms including PDA to facilitate data transfers between various WWAN and WLAN networks:

> Referring now to the drawings, FIG. 1A depicts portable computing device 100 according to representative embodiments. Portable computing device 100 includes processor 101, wireless wide area network (WWAN) interface(s) 102, and wireless local area network (WLAN) interface(s) 103. Suitable commercially available WWAN interfaces include, but are not limited to, GPRS interfaces, code division multiple access (CDMA) 1×RTT interfaces, CDMA 1×EVDO interfaces, 802.16 (WiMax) interfaces, wireless broadband interfaces, and the like. Suitable commercially available WLAN interfaces include, but are not limited to, 802.11b interfaces, 802.11a interfaces, 802.11g interfaces. For the purposes of the following description, the term WLAN is also used to refer to other communication mechanisms possessing limited communication ranges, e.g., personal area Bluetooth networks, personal area Ultra Wideband (UWB) networks, and/or the like.
>
> Portable computing device 100 may be implemented in the form of a personal digital assistant (PDA), a notebook computer, or other portable computing platform. Suitable commercially available PDAs that comprise WWAN and WLAN interfaces include iPAQ™ Pocket PCs available from Hewlett-Packard Company,

244. EX-1019, 2:42-61. See Figs. EX-1019, 1A, 1B.

245. Crosswy's WLAN/WWAN PDA gateway facilitates routing between the different networks (forwarding).

> Furthermore, portable computing device 100 provides gateway functionality to other wireless communication devices within the established WLAN. Specifically, portable computing device 100 receives packets from the wireless communication devices in the WLAN and routes the packets to resources available via the Internet using the WWAN. Portable computing device 100 provides other communication functionality to facilitate the routing of packets such as network address translation (NAT), dynamic host configuration protocol (DHCP), firewall functionality, virtual private networking (VPN) functionality, content filtering functionality, and/or the like.

246. EX-1019, 3:34-45.

> FIG. 2 depicts communication system 200 according to one representative embodiment. Communication system 200 comprises portable computing device 100. Portable computing device 100 is established within a cell or service area of WWAN 202. Portable computing device 100 communicates with resources on the Internet using WWAN infrastructure 204.
>
> Portable computing device 100 acts as an access point for WLAN 201 to thereby provide an access point that is neither fixed in location (i.e., is portable) nor relies on wireline links for wide area communications.

> Furthermore, portable computing device 100 may authenticate or otherwise limit which devices may communicate within WLAN 201 to establish a private network. Wireless devices 203 within WLAN 201 may be implemented using a variety of computing devices such as desktop computers, laptop computers, personal digital assistants, and/or the like. Wireless devices 203 may include integrated WLAN interfaces or removable WLAN cards. Wireless devices 203 may communicate with resources available on the Internet by routing packets through portable computing device 1100. Wireless devices 203 may communicate with each other using the wireless management functionality of portable computing device 100. Alternatively, wireless devices 203 may communicate with shared resources (e.g., printer 205) using the wireless management functionality of portable computing device 100.

247. EX-1019, 3:58-4:16.

248. U.S. Publication No. 2008/0244018 was filed on March 27, 2007 and publish on October 2, 2008 ("Chen") (EX-1020). It is prior art under section 102(a)(e)(g).

249. Chen describes a "personal communication gateway" used to forward data between WWAN (GSM, 3G) or WLAN networks. EX-1020, [0002], [0076] ("Additionally the user terminal may comprise a radio interface 505 (shown with

dashed line) for connecting to wireless communication networks, such as WLAN, GSM, 3G and satellite communication networks,").

250. Chen teaches its gateway in the form of a laptop computer.

> FIG. 1 shows a schematic picture of a system according to an embodiment of the invention. The system comprises a user terminal 101 and a laptop computer 102 operating as a personal communication gateway (PCG). The user terminal and the laptop computer are connected through a Bluetooth connection 103. Additionally or alternatively, the connection between the user terminal and the personal communication gateway may be through some other personal area network or near field connection, such as for example USB (Universal Serial Bus). By using Bluetooth or some other wireless near field communication technology one achieves that the user may maintain mobility. The laptop may alternatively be a desktop computer or even another user terminal, for example. The laptop 102 has a broadband connection to a multimedia service network 104. The multimedia service network may comprise IMS (IP Multimedia Subsystem) and/or internet application services. Further the system comprises other communicating parties 105 connected to the multimedia service network. Physical connection to the multimedia service network (from the laptop 102 and/or the other communicating parties 105) is through a communication network. The communication network may be for example internet or a proprietary

> communication network, and it may comprise fixed line or wireless connections or a suitable combination of them. The other communicating party may be for example another user terminal, computer, server or service reachable through the multimedia service network.

251. EX-1020, [0045].

252. Chen's device is a gateway that forwards communications between the two networks.

> The laptop 102 acts as a proxy or a gateway to provide multimedia communication between the other communicating party 105 and the user terminal 102. The multimedia communication may be for example MIM (multimedia instant messaging), PIM (personal information management), SMS, MMS, voice/video calls, media (e.g. photo/video/music) sharing, file transfer, mobile phone call forwarding and so forth.

253. EX-1020, [0046].

254. Thus, as noted in each of the references above, a POSA would have recognized that gateways between networks such as a WWAN and WLAN could be implemented in a form factor of a small, portable devices such as a PDA, mobile phone, or laptop.

255. [This paragraph left intentionally blank].

X. DETAILED UNPATENTABILITY ANALYSIS FOR THE '042

256. For the '042, I have been asked to provide an opinion as to whether Challenged Claims 1-2, 6-18 are obvious over the Limont in view of Wright and optionally with Xu (Ground 1) and whether Challenged Claims 3-5 are obvious over the Limont in view of Wright and optionally with Xu in view of Polson (Ground 2).

257. As part of my obviousness analysis, I have considered the scope and content of the prior art, described above and below. Additionally, I considered whether any differences between the alleged invention and the prior art are such that the subject matter, as a whole, would have been obvious to a person having ordinary skill in the art at the time of the alleged invention. I have also considered the level of ordinary skill in the pertinent art in performing my analyses.

A. Ground 1: Challenged Claims 1, 2, and 6-18 Are Obvious In View of Limont combined with Wright and optionally Xu.

258. As detailed below, Limont in combination with Wright and optionally Xu, discloses, or renders obvious, Challenged Claims 1, 2 and 6-18 and thus renders these claims unpatentable.[1]

259. Limont provides extensive details regarding a system for receiving information including policy / configuration information from a mobile device, determining if that policy information needs to be modified to allow access to requested data, and sending the updating policy to the mobile device to allow access to data that has been request.

260. Limont shows two related and overlapping embodiments. The first is in Figures 1 and 2 with specific details in EX-1004, [[0038-0071]. The second embodiment is in Figures 3 and 4 with specific details in EX-1004, [[0072-0091]. I note that Limont's claim 1 recites the steps in Figure 4 and Limont's claim 9 recites the steps in Figure 2.

[1] As used herein, "discloses" includes that the reference's disclosure renders obvious to a POSA.

261. I rely upon both for what a POSA would understand from Limont. Much of the content is overlapping and related including [0001-0037]. Fig. 5 shows an exemplary embodiment for operating Limont's server. EX-1004, [0092-0099].

262. [This paragraph left intentionally blank].

1. A POSA Would Have Been Motivated To Combine Limont, With Wright and Optionally Xu With A Reasonable Expectation Of Success.

263. A POSA would be motivated to combine Limont with Wright and optionally Xu with a reasonable expectation of success.

264. Limont and Xu are assigned to the same company (Microsoft) which is a known leader in the field of computer technology, software and policy enforcement. Wright is assigned to Apple – another known leader in this field. Collectively, I will reference the combination of them as the "Proposed Combination."

265. All three references pertain to the same general subject matter of the management and update of secure data, including policies, on client devices. As detailed in the substance below, each reference: (1) describes a mobile device that enforces policies; (2) describes the ability to modify / update those policies from a server over a wireless connection.

266. Limont and Wright have heavily overlapping and complementary disclosure reflecting that each of these references identify the problem of securing updates to traveling users. Compare EX-1004, [0005-0014] (citing, for example, concerns about "sales personnel and executives may frequently be out of the office on business travel and while traveling may need access to corporate data" from different physical locations) with EX-1005, [0005-0010] (citing concerns about "Users with laptops and mobile devices want to take advantage of wireless technologies, to connect wherever they are—at work, at home, in the conference room of another company, at the airport, a hotel, a highway or at the coffee shop on the corner" and personnel "in transit" that might be hacked).

267. In light of the above, a POSA would have been motivated to consider, and combine, references from leading well-known companies in this field, that describe the same general technology (policy enforcement and updates), and identify the same problem that is being addressed by their disclosure.

268. Reflecting this heavy overlap in their disclosures, in the prosecution of Limont, the Examiner cited Wright extensively and repeatedly. EX-1013, 0000140-141, 000145-146.

269. Related to the current subject, the Examiner held that Wright disclosed a significant portion of Limont's teachings that are discussed below to invalidate the Challenged Claims. For example, the Examiner held that Wright discloses both of Limont's steps 401 and 402:

> Wright discloses a system and method for protecting data accessible by a mobile device, the system and method having:
>
> **an act of receiving at the computer system** (i.e. server system) **a request** (i.e. status request) **from the mobile device, the request requesting that the mobile device be permitted to access the data maintained by the computer system, the request indicating a current mobile device configuration of the mobile device and including a configuration version corresponding to the current mobile device configuration** (0128, lines 5-10)**;**
>
> **an act of determining that the current mobile device configuration is not appropriate for accessing the maintained data, wherein the act of determining that the current mobile device configuration is not appropriate for accessing the maintained data comprises an act of comparing the configuration version included in the received request to one or more configuration versions stored at the computer system representing appropriate configurations for accessing the maintained data** (0047, lines 13-16, 23-27; 0128, lines 17-25; 0139, lines 1-2; 0140, lines 1-2; 0141, lines 1-2)**.**

270. EX-1013, 000229-230.

271. The Examiner also determined that Wright disclosed Limont's step 202 cited in the invalidity discussion below:

Wright discloses:

determining that the current policy settings at the mobile device are not appropriate for accessing the data maintained by the computer system, wherein determining that the current policy settings at the mobile device are not appropriate for accessing the data maintained by the computer system comprises comparing the policy version included in the received data command to one or more policy versions stored at the computer system representing appropriate policy settings for accessing the maintained data (0047, lines 13-16, 23-27; 0128, lines 17-25; 0139, lines 1-2; 0140, lines 1-2; 0141, lines 1-2)**;**

notifying the mobile device that the current policy settings are not appropriate for accessing the maintained data (0128, lines 21-25)**;**

receiving a policy request from the mobile device, the policy request requesting policy settings that are appropriate for accessing the maintained data (0144, lines 1-4; 0145, lines 1-4)**;**

notifying the mobile device that access to the maintained data has been permitted (0128, lines 17-21; 0281, lines 14-18)**.**

272. EX-1013, 000147-148.

273. As quoted above, Limont's Examiner noted that Wright disclosed large portions of Limont's claims.

274. As detailed below, Limont's steps 401, 402, and 202 are cited to disclose element [1.1] and [1.2] of the Challenged Claims.

275. Regardless of whether the Examiner's determinations were correct, the Examiner's repeated citations to Wright in Limont's prosecution show the heavy overlap between Limont and Wright. Such an overlap would have motivated a POSA to consider and combine the two references.

276. The Examiner's citation is also heavy evidence that a POSA would have considered these two references together.

277. Furthermore, when viewing a first reference, a POSA would have considered the other references cited in the prosecution of the first reference because the prosecution exhibits a determination that someone that is likely a POSA themselves (or close in qualifications) considered the references to be so closely related that one might have invalidating disclosure for the other.

278. Beyond the demonstrated heavy overlap, a POSA would be motivated to combine Wright's teachings of protecting policies into Limont's mobile devices. Limont is directed to a method of configuring and enforcing policy settings for a wireless device based on information received from the wireless device regarding its service state.

279. Both Limont and Wright identify data security as a critical issue. EX-1004, [0004-0015], EX-1005, [0005-0010].

280. Both Limont and Wright identify that wireless users present specific security challenges. Limont teaches that "[c]omputer systems operating in a wired networking environment are to some extent inherently more secure than computer systems operating in a wireless networking environment." EX-1004, [0005-0006]. A wired environment allows for specific types of data security mechanism that "limit data access based on the physical location, domain, and/or electronic address of a computer system." These wired-environment mechanisms allow the administrator to "lock down" the computer system for secure updates of critical information. Such critical information includes "encryption" information such as algorithms and keys, as well as password and PIN information that allow remote network access. EX-1004, [0007-0009], [0047]. Wright contains an analogous teaching:

> [0005] This application relates to the field of security of data accessible by mobile devices. Mobile devices are using wired and wireless technologies to access networks at work, at home, or in public 'hot spots.' Those same mobile devices have documents, spreadsheets, e-mail, and other files with valuable company information if not valuable personal information in them.

[0006] The availability of wired and wireless network access points (NAP) allow mobile devices like laptop computers and personal digital assistants (PDAs) to enable users today to be more mobile, providing access to corporate networks, e-mail, home networks and the Internet from anywhere. With the advent of the IEEE 802.11 standard for wireless communication, and other popular wireless technologies, software products that protect against unwanted access to information stored on mobile devices and corporate servers is highly desirable.

[0007] Traditional security architectures assume that the information assets being protected are 'tethered'—wired to a particular network infrastructure such as a company's network infrastructure. But mobile users can pick up valuable corporate information, such as that stored on their laptops, and walk away from the corporate network, and connect to other networks with different security policies. Users with laptops and mobile devices want to take advantage of wireless technologies, to connect wherever they are—at work, at home, in the conference room of another company, at the airport, a hotel, a highway or at the coffee shop on the corner. The mobile device's network environment is constantly changing as the user moves about. Each environment has different needs in terms of security. Each environment presents different challenges to protect the information on the mobile device while allowing access to e-mail, the Internet, and company Virtual Private Networks (VPNs).

281. EX-1005, [0005-0007].

282. Both Limont and Wright identify the problem that users want flexible access through new wireless technologies. Limont identifies the issue that "users typically desire available and flexible access to their data regardless of location and/or the type of computer system that will be used to access the data." EX-1004, [0010]. This "flexible access" requires that users that are "out of the office on business travel" have "access to corporate data." EX-1004, [0010]. However, the "flexible access" for travelers presents the risk and problem that "hackers or other malicious users" may access the data. EX-1004, [0012]. As quoted above, Wright correspondingly notes that "Users with laptops and mobile devices want to take advantage of wireless technologies, to connect wherever they are—at work, at home, in the conference room of another company, at the airport, a hotel, a highway or at the coffee shop on the corner." EX-1005, [0007].

283. Both Limont and Wright identify the problem that "hackers" could access data on a stolen / lost device that the hackers acquire. Limont identifies that "[w]ireless access can be particularly problematic" because there is an "increased risk of loss or theft" of mobile devices which hackers may use to access secure data. EX-1004, [0013]. Limont highlights the importance of securing the data on

the mobile device by teaching that "[i]f a specified number of incorrect PIN entries are detected, the mobile device can initiate a local wipe of memory contents." EX-1004, [0048]. An administrator may also order a "remote wipe" to protect the data. EX-1004, [0047-0049]. Wright teaches:

> Solutions which secure data in transit, for example a (VPN) connection, from a corporate server to a mobile client device do not protect the data once it is stored on the mobile device. For example, an executive could be retrieving sensitive files or emails from the corporate network, and the VPN will stop eavesdroppers from seeing the data in transit**, but once the data is stored on the executive's remote device, hackers in the parking lot could break into the remote device and copy or maliciously alter the data**. With the onset of new powerful mobile devices that can store corporate data, IT managers see their network perimeters having to extend to the new limits of these mobile wireless connections.

284. EX-1005, [0009].

285. After identifying these problems, both Limont and Wright proposed the solution of secure updates for the mobile devices to protect the policies.

286. In light of both Limont's and Wright's teachings on data security and identified issues discussed above, a POSA would have recognized that it was important to prevent "malicious users" from accessing critical data on mobile

devices if those devices were lost or stolen (as identified in both Limont and Wright).

287. Moreover, because policies on the device may include confidential information used for remote access, such as encryption algorithms, keys, and the user's password and PIN, a POSA would have recognized that such policy information needed be protected on the mobile devices or "locked down" to not only protect the data on the device, but to also protect the corporate data stored in the server from being accessed by unauthorized users using lost or stolen credentials (including the use of a lost or stolen device to access such data).

288. As noted below, Limont provides an architecture which satisfies the identified need of allowing corporate administrators the ability to update and modify policies over wireless connections – used, for example, to manage traveling users. Wright provides a similar architecture (as exemplified by Limont's Examiner repeatedly rejecting Limont's claims over Wright).

289. Limont does not expressly state the configuration settings for the mobile device should be stored in a protected partition. However, both Wright and Limont identify the problem of devices being physically accessed (either lost or stolen) by hackers. Given this problem, a POSA would have recognized that, in

addition to performing updates wirelessly, a corporate administrator had a need to be able to secure the information on a device after it had been updated.

290. A POSA would have recognized that one form of data protection for the data on a device would be a protected partition of memory that included additional protections to prevent access by a "malicious user" (hacker) that has acquired physical access to the device. A POSA would have recognized that such protected memory would have beneficially improved the data security issues identified by Limont and Wright by further protecting the critical mobile device data from unauthorized access.

291. Moreover, such a protected partition ensures that only the administrator (and not corporate users) can access, and modify, critical portions of data used for remote access. Thus, it provides protection against both "malicious users" and unauthorized (or inadvertent) modifications made by authorized users.

292. Wright provides a specific solution to this problem identified by both Wright and Limont by encrypting (or "hiding") the information in the memory of the mobile device as detailed below. A POSA would have recognized such encryption as one of the alternatives for providing protections for the portions of

memory containing confidential data such as the policies in light of the disclosures and problems identified in both Wright and Limont discussed herein.

293. A POSA also would have been motivated to consider Wright's teaching because it solves Limont's problem of protecting updated policy settings transmitted to a mobile device operating outside the corporate "wired environment." Wright discloses that the policy settings can be kept in a schema or document in XML format which can then be encrypted and sent to the mobile device as being encrypted during the transmission also. A POSA would have understood that such encryption provides an extra level of security for the traveling users using, for example, public wireless networks such as WiFi (802.11) access points as identified in both Limont and Wright.

294. Further, Wright discloses auditing the policy settings stored on the mobile device to determine the integrity of the data, *e.g.*, whether it has been corrupted (such as by the "malicious users" identified in Limont). In light of Limont's teaching that an administrator may want to remotely wipe the mobile device memory, Wright's auditing ability allows corporate administrators to have additional information (and notice) regarding any malicious or inadvertent modification to the policy memory – thus allowing the corporate administrator to

repair the problem (as noted in Wright) by updating policies or to wipe the memory to force a policy update as described in Limont.

295. A POSA would be motivated to modify Limont's teachings of storing policy settings on the mobile device by encrypting the policy settings as taught by Wright to prevent unauthorized access to the stored data, and further auditing the stored data. A POSA would be motivated to do so because unauthorized access to the data would: (1) allow a "malicious user" access to the either the confidential data on the device and/or policy settings on the device which permit remote access (thus allowing the "malicious user" access to the corporate data); and (2) allow even an "authorized" user to change the policy setting (either intentionally or inadvertently) to provide access to networks to which the user did not have access, potentially avoid billing charges, and use resources (*e.g.*, network bandwidth) to which the user is not entitled.

296. A POSA would have a reasonable expectation of success of the modification as it is a software solution which uses known encryption techniques for their intended purpose – securing the stored data. Moreover, Limont already provides the hardware and software to implement and use encryption algorithms and encryption keys because such encryption procedures are already performed on

the device for other reasons. EX-1004, [0009], Fig.1 (processor 111, memory 112), [0040].

297. Using Wright's encryption techniques with Limont's system is merely the application of well-known operations (encryption), operating on known components (processors with encryption algorithms and memory), for their known and intended purposes (to encrypt and therefore protect the data stored in memory).

298. Because Xu reflects an alternative and complementary method of protection, I have discussed the motivation to incorporate Xu with Limont and Wright with a reasonable expectation of success is addressed in the claim element for which Xu is cited (element [1.3] below).

299. [This paragraph left intentionally blank].

2. Challenged Claims 1-2, 6-18 Are Disclosed By The Proposed Combination.

a) Claim 1

Preamble: [*1.0] A method comprising:*

300. Whether or not the preamble is limiting, Limont discloses this element in combination with Wright and/or Xu as detailed below.

301. For example, Limont's "FIG. 4 illustrates an example flow chart of a method for enforcing an appropriate mobile device configuration prior to

permitting a mobile device to access maintained data." EX-1004, [0026]. Figure 4 details the steps of one of Limont's embodiments.

302. I note that the steps in Fig. 4 correspond to "the method comprising" recited in Limont's claim 1.

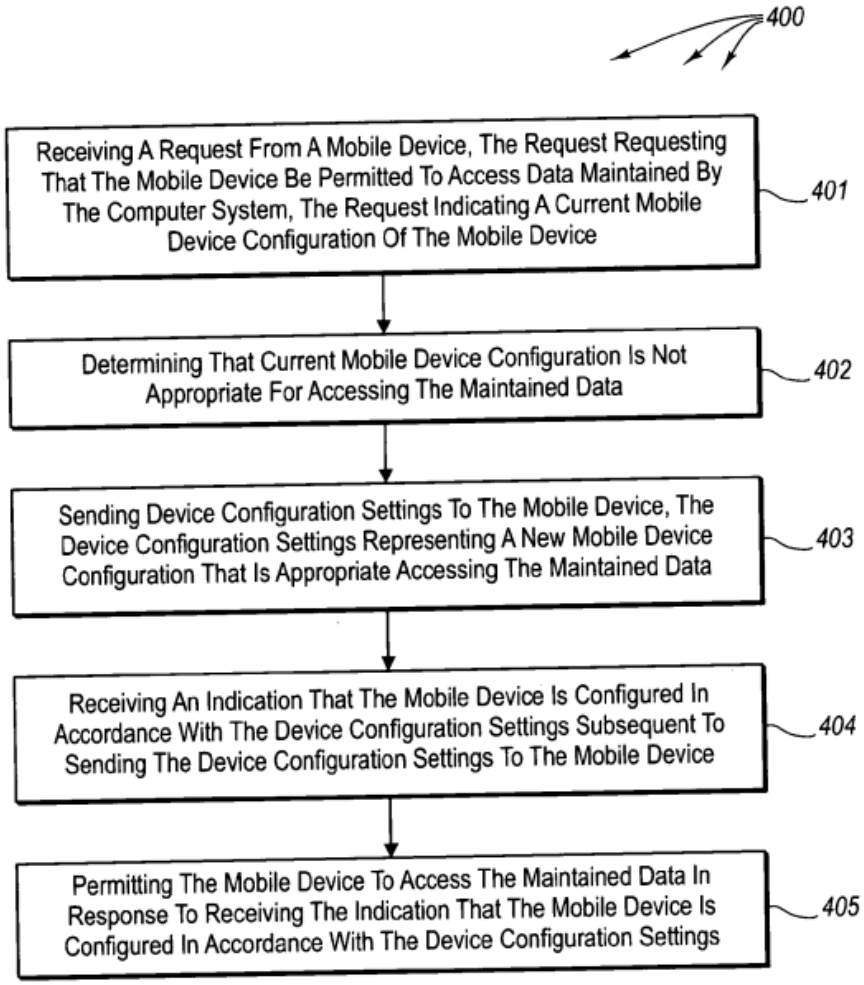


Fig. 4

EX-1004, FIG. 4.

303. Limont's Annotated FIG. 3 illustrates an architecture for performing the method of FIG. 4. FIG. 3 below has been annotated to highlight some of the aspects described in FIG. 4 related to the acts occurring between Limont's mobile device 101 and computer system 141.

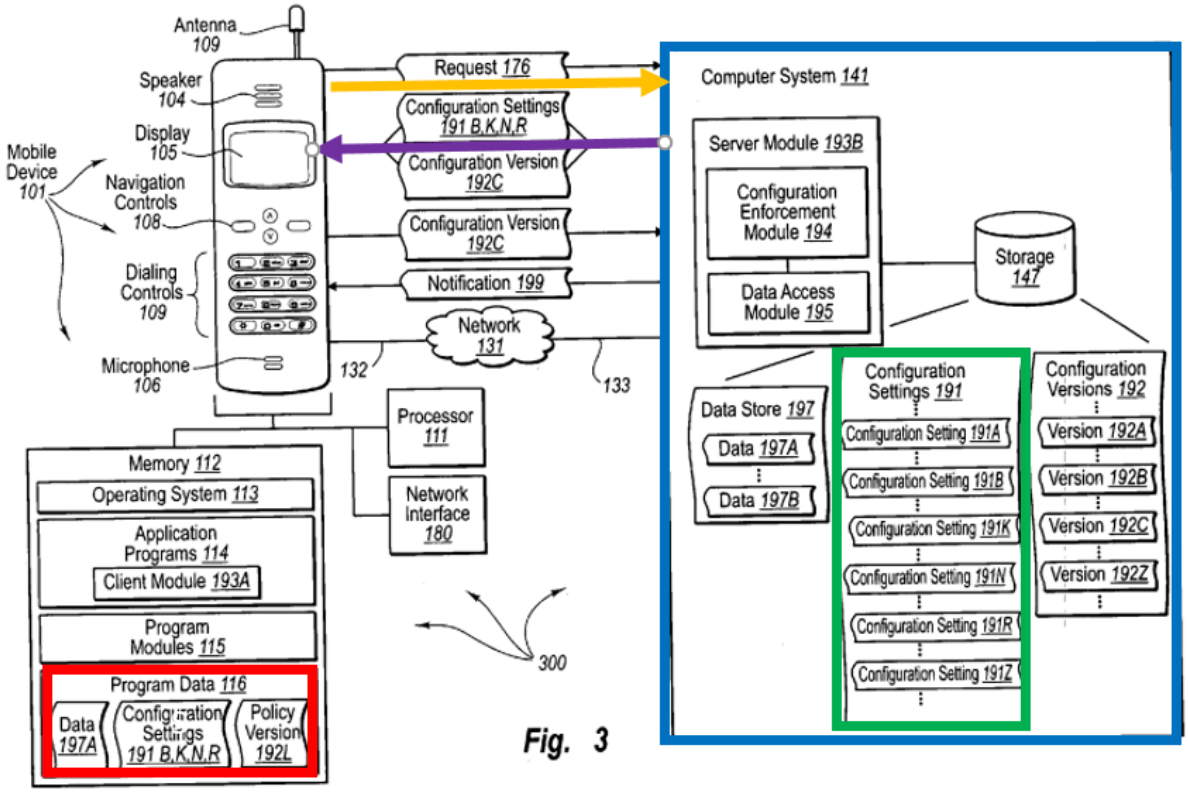


Fig. 3

EX-1004 FIG. 3. *See also* EX-1004, FIGs. 1, 2.

304. As noted above, Limont's Figures 1 and 2 show a related embodiment effectively teaching the same method (at least for purposes of invalidity).

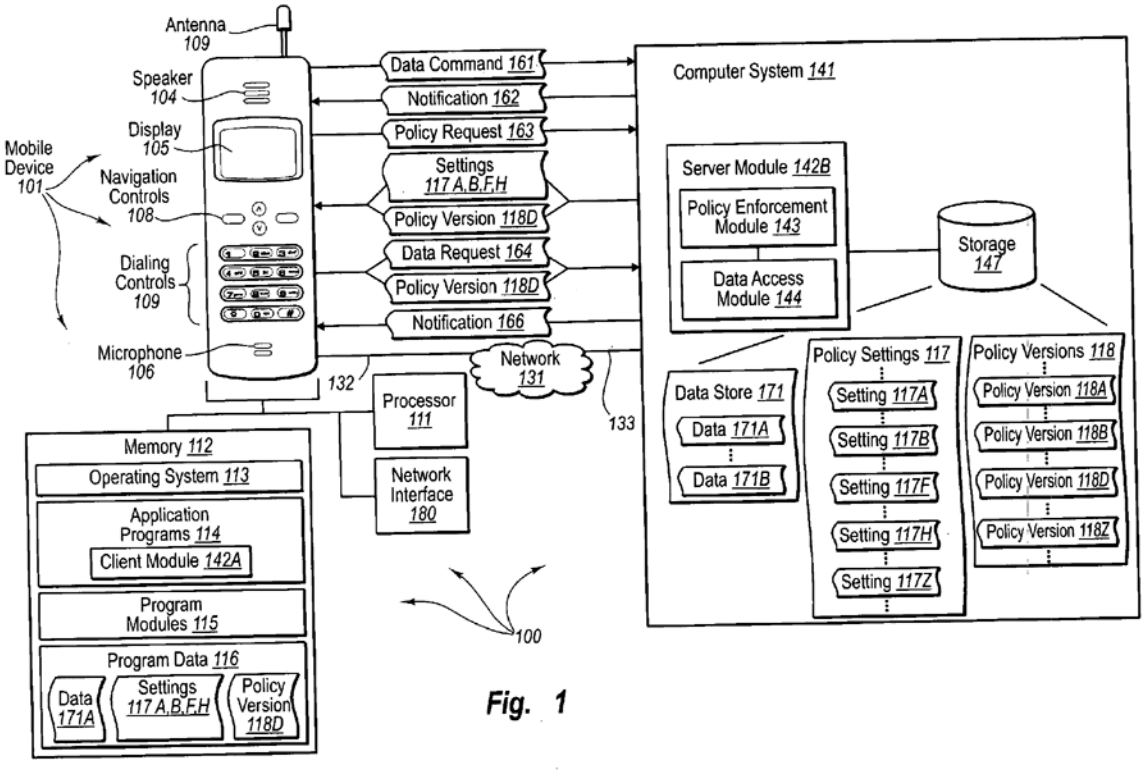


Fig. 1

305. EX-1004, Fig. 1.

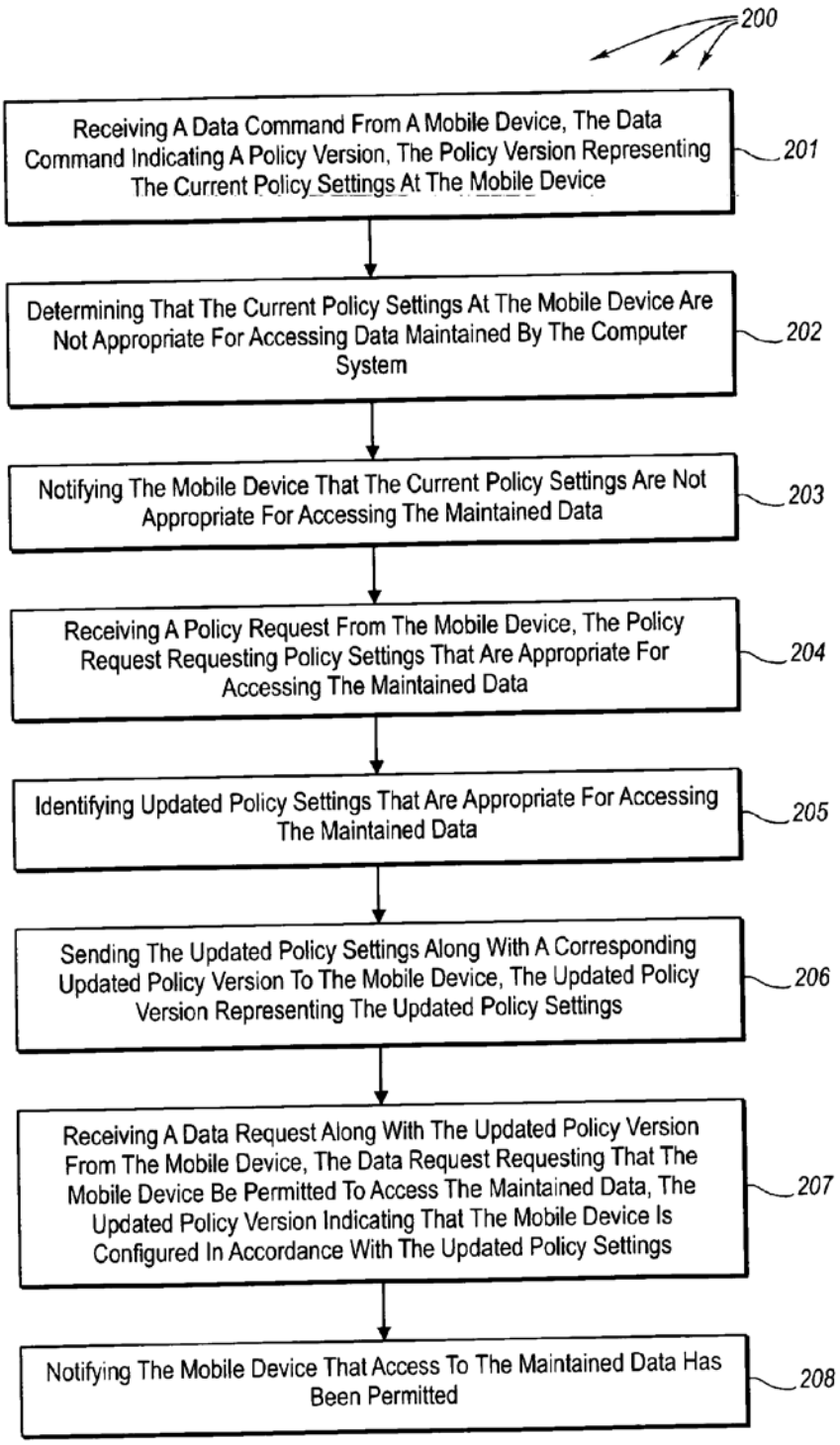

200
Receiving A Data Command From A Mobile Device, The Data Command Indicating A Policy Version, The Policy Version Representing The Current Policy Settings At The Mobile Device
201
Determining That The Current Policy Settings At The Mobile Device Are Not Appropriate For Accessing Data Maintained By The Computer System
202
Notifying The Mobile Device That The Current Policy Settings Are Not Appropriate For Accessing The Maintained Data
203
Receiving A Policy Request From The Mobile Device, The Policy Request Requesting Policy Settings That Are Appropriate For Accessing The Maintained Data
204
Identifying Updated Policy Settings That Are Appropriate For Accessing The Maintained Data
205
Sending The Updated Policy Settings Along With A Corresponding Updated Policy Version To The Mobile Device, The Updated Policy Version Representing The Updated Policy Settings
206
Receiving A Data Request Along With The Updated Policy Version From The Mobile Device, The Data Request Requesting That The Mobile Device Be Permitted To Access The Maintained Data, The Updated Policy Version Indicating That The Mobile Device Is Configured In Accordance With The Updated Policy Settings
207
Notifying The Mobile Device That Access To The Maintained Data Has Been Permitted
208

Fig. 2

306. EX-1004, Fig. 2.

307. The specific details of how the acts in Figures 2 and 4 (as operated by the architectures in Figures 1 and 3) correspond to the elements of the '042 claims are detailed in the elements below.

308. [This paragraph is left intentionally blank].

i. ***[1.1] receiving, over a service control link, a report from a wireless end-user device, the report comprising information about a device service state;***

309. Limont discloses this element.

310. As illustrated in Annotated FIG. 3 below, Limont's computer system 141 (blue) receives a "request" (gold) from mobile device 101 (*receiving a report from a wireless end-user device*).

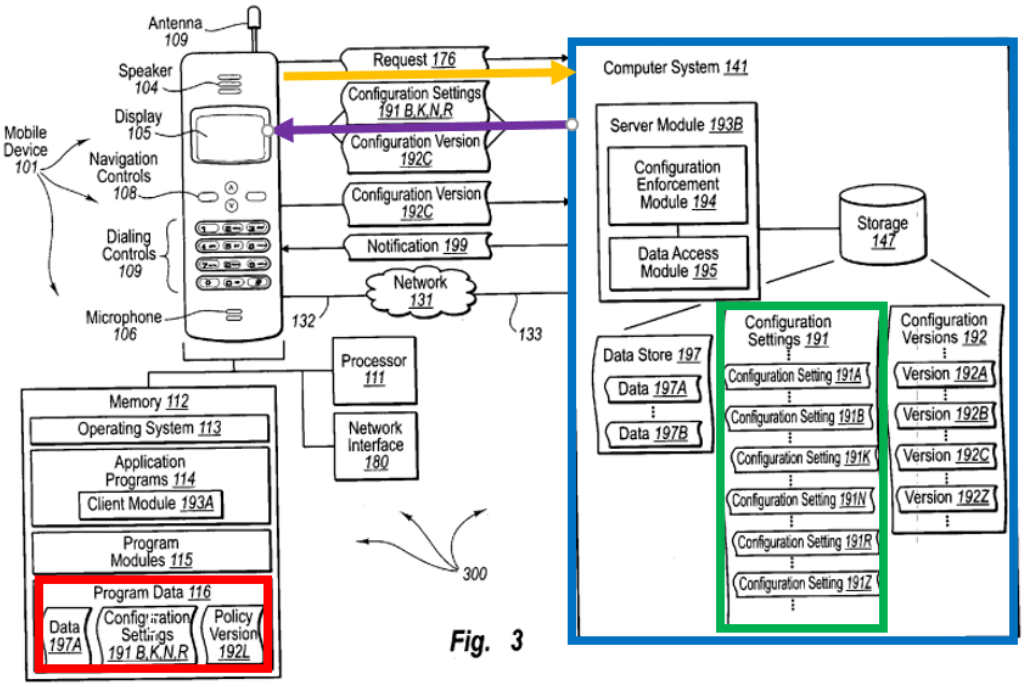
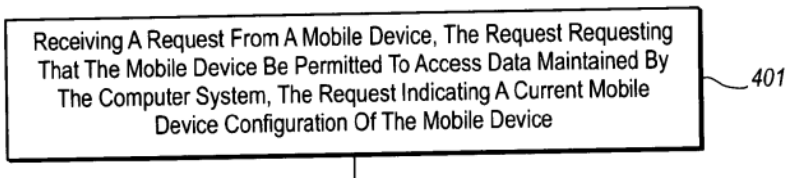


Fig. 3

311. The request corresponds to the claimed *report*.

312. Limont's Figure 4 describes: "receiving a request from a mobile device, the request requesting that the mobile device be permitted to access data maintained by the computer system, the request indicating a current mobile device configuration of the mobile device." (Fig. 4, step 401; claim 1).



313. EX-1004 FIG. 4, step 401.

314. As taught by Limont, the "request" in Figure 4 can include different pieces of data as described in [0080-0081]:

> [0080] Method 400 includes an act of determining that current mobile device configuration is not appropriate for accessing the maintained data (act 401). For example, mobile device 101 (client 193A) can send request 176 to computer system 141. Request 176 can indicate a **configuration version representing the one or more of the current configuration settings of mobile deice 101**. Computer system 141 can receive request 176 from mobile device 101. Request 176 can be a **request for data,** such, as, for example, a Web page request. Alternately, request 176 **can be a provision request** expressly requesting appropriate configuration settings.
>
> [0081] A request **may or may not expressly include a configuration version**. Lack of an expressly included configuration version can indicate that a mobile device has yet to implement and/or does not support remote configuration.

315. Limont's "configuration version representing one or more of the current configuration setting" is *information about a device service state* of mobile device 101 for the reasons explained below.

316. I note that the embodiment in Figures 1 and 2 contains a similar disclosure of information sent from the mobile device to the server computer. In particular, Figure 2 recites:

> receiving a data command from a mobile device, the data command indicating a policy version, the policy version representing the current policy settings at the mobile device;
>
> …
>
> receiving a policy request from the mobile device, the policy request requesting policy settings that are appropriate for accessing the maintained data;

317. EX-1004, Fig. 2, claim 9.

318. Figure 1 shows that the "data command" in Fig. 2, step 201 and the "data request 164 / policy version 118D" are received by the server from the mobile device.

319. The "data command" in Figures 1 and 2 has effectively the analogous information as the "request" described above for Figures 3 and 4 as detailed in [0058-0059].

> [0058] Method 200 includes an act of receiving a data command from a mobile device, the data command indicating a policy version, the policy version representing the current policy settings at the mobile device (act 201). For example, mobile device 101 (client module 142A) can send data command 161 to computer system 141. Computer system 141 can receive data command 161 from mobile device 101. Data command 161 can be a request for data, such as, for example, a sync or folder sync command. Alternately, data command

> 161 can be provision command expressly requesting appropriate policy settings.
>
> [0059] A data command may or may not expressly include a policy version. Lack of an expressly included policy version can indicate that a mobile device has yet to implement and/or does not support policies.

320. EX-1004, [0058-0059]. Paragraph 0030 shows the same information ("The computer system receives a data command from a mobile device. The data command indicates a policy version representing the current policy settings at the mobile device….").

321. Similarly, as shown in Figure 1, the server receives "data request 164 / policy version 118D" which is also the claimed request. This is explained in paragraphs [0067-0069]:

> [0067] Method 200 includes an act of receiving a data request along with the updated policy version from the mobile device, the data request requesting that the mobile device be permitted to access the maintained data, the updated policy version indicating that the mobile device is configured in accordance with the updated policy settings (act 207). For example, mobile device 101 (client module 142A) can send data request 164 along with policy version 118D to computer system 141. Computer system 141 can receive data request 164 along with policy version 11 8D from mobile device 101. Data request 164 can be a request to access data 171A.

> [0068] Policy enforcement module 143 can determine, for example, through comparison to known appropriate policy versions, that policy version 118D represents policy settings that are appropriate for accessing data 171.
>
> [0069] Method 200 includes an act of notifying the mobile device that access to the maintained data has been permitted (act 208). For example, server module 142B can send notification 166 to mobile device 101. Notification 166 can indicate to mobile device 101 that policy enforcement module 143 has permitted access to data 171A. Data request 164 along with policy version 118D (a request) and notification 166 (a response) can be corresponding messages in a request/response protocol, such as, for example, HTTP.

322. EX-1004, [0067-0069].

323. Thus, in each of these "receiving" actions, the mobile device has transmitted ""configuration version representing one or more of the current configuration setting" / "policy version, the policy version representing the current policy settings at the mobile device (act 201)."

324. Limont's "configuration version" / "policy version" is *information about a device service state* of mobile device 101.

325. The '042 Patent broadly recites the "device service state." That term includes "types of information used to properly measure and/or control the device

services" as well as "information reported from the device and received or derived outside the device that is required to adequately define the actions needed from the service controller to maintain proper DAS system operation." EX-1001, 18:5-11.

326. Limont's "configuration settings" include "policy settings … operating system settings, application program settings, hardware settings, allocated resource settings, network interface settings, wireless protocol setting, etc." EX-1004, [0073].

327. Limont's "Policy settings can include: a Personal Identification Number ("PIN") lock activation setting, a minimum PIN length setting, a PIN format setting (e.g., alphanumeric or numeric), a number of PIN failures permitted before performing a local wipe setting, a number of PIN failures after which an override "passcode" must be entered setting, a force wipe on next connection to server setting, a client application version setting, a protocol version setting, a protocol commands allowed setting, a custom application permitted setting, a time interval for enforcing compliance setting, a remote wipe enabled setting, and a require policy check setting." EX-1004, [0047].

328. Limont's "configuration settings" and "policy settings" correspond to the disclosure in the '042 Patent for "device service state" which can include

current service usage policy settings, current DAS settings, device status information, application status information, or other state and/or settings information as well as "types of information used to properly measure and/or control the device services" as well as "information reported from the device and received …that is required to adequately define the actions needed from the service controller to maintain proper DAS system operation." EX-1001, 17:46-18:11. Each of the policies in Limont describes "information used to properly … control the device services" and / or "is required to adequately define the actions needed … to maintain proper" operation of Limont's system to access data. That is the entire purpose of the identified settings (to provide the basis for the ability to manage policies, including modifying as necessary, to allow for access to services such as email and web services and to control the device (by measuring characteristics such as memory, connection speed, plug-ins…) and its ability to operate to properly process and display the requested information.

329. For example, Limont's configuration settings / policy settings "required to adequately define the actions needed from the service controller to maintain proper [] system operation" because those settings are checked by

Limont's server to allow for data access to specific types of data provided by various network services as detailed below.

330. Similarly, Limont's configuration settings / policy settings provide "the types of information used to properly measure and/or control the device services" because, for example, they provide information about "if sufficient resources have allocated at a mobile device to receive a Web page, if a mobile device Web browser includes correct plug-ins for viewing content, if mobile device connection speed will permit a Web page to be downloaded in a reasonable amount of time, etc." EX-1004, [0077], [0086].

331. "Device service state" is defined broadly and encompasses the configuration settings / policy settings on the mobile device. Claim 1 recites that "*the report comprising* ***information about*** *a device service state*." The configuration version / policy version are "information about" the device service state because they are "information about" the current device configuration settings / policy settings.

332. Limont's information between the mobile device and server is shown in both Figures 1 and 3 as being on "communication links 132, 133" across

"network 131." In the '042, "a service control link … is used for communication between the" device and server. EX-1001, 7:28-32, 4:33-37; Fig. 1.

333. Limont's communication links 132, 133 in FIGs. 1 and 3 show *a service control link*) because they are the communication path that allows Limont's wireless end-user device to communicate with the computer system.

> [0038] FIG. 1 illustrates an example of a computer architecture 100 that facilitates enforcing policy settings of mobile devices. Depicted in computer architecture 100 is mobile device 101 and computer system 141. Mobile device 101 is connected to network 131, such as, for example, a Local Area Network ("LAN"), a Wide Area Network ("WAN"), or even the Internet, via communication link 132. Similarly, computer system 141 connected to network 131 via communication link 133. Thus, mobile device 101, computer system 141, and other network connected computer systems (not shown) can exchange data via network 131. Accordingly, mobile device 101 and computer system 141, as well as other connected computer systems, can create message related data and exchange message related data (e.g., Internet Protocol ("IP") datagrams and other higher layer protocols that utilize IP datagrams, such as, Transmission Control Protocol ("TCP"), Hypertext Transfer Protocol ("HTTP"), Simple Mail Transfer Protocol ("SMTP"), etc.) over network 131.

334. EX-1004, [0038].

335. Communication links 132 and 133 include using one or more different wireless protocols (e.g., GPRS, GSM, etc.) which shows that the communication can be *over a wireless access network*.

> [0043] Communication link 132 logically represents that mobile device 101 is connected to network 131. Communication link 132 abstracts the actually physical representation of the connection from mobile device 101 to network 131. The actual physical representation can include communication through one or more intermediate network devices and can include communication in one or more different protocols. At least a portion of the actual physical representation can include wireless communication using **wireless protocols (e.g., GPRS, GSM, etc. to a mobile telephone server provider**)

336. EX-1004, [0043]

> [0056] Communication link 133 logically represents that computer system 141 is connected to network 131. Communication link 133 abstracts the actually physical representation of the connection from computer system 141 to network 131. The actual physical representation can include communication through one or more intermediate network devices and can include communication in one or more different protocols. **At least a portion of the actual physical representation can include wireless communication using wireless protocols**.

337. EX-1004, [[0056].

338. GSM is a wireless protocol used for wireless access networks. GSM is an acronym for "Global System For Mobile" communications. It is a body of standards and protocols that allow interoperability for mobile devices and mobile networks to exchange information / data to allow for wireless communications. "GPRS" is an acronym for "General Packet Radio Service." The "radio" in the name denotes that GPRS is generally understood to represent a wireless communication access network / system. GPRS is designed to be packet oriented (analogous to the IP protocol used for the Internet).

339. Thus, by disclosing that communications links 132, 133 can include "wireless protocols" and giving the specific examples of GSM and GPRS, Limont discloses (or renders obvious) that the communications are "over a service control link" to provide "access … over a wireless access network."

340. I also note that both Figures 1 and 3 in Limont show a "mobile device" (in the form that would be recognized as a "mobile phone") with an "antenna." Even without the express disclosures above, a POSA would understand such disclosure to include (including rendering obvious) that the mobile device uses a wireless access network to communicate data with the servers shown in Figures 1 and 3.

341. Thus, Limont discloses, including rendering obvious, this claim element.

342. [This paragraph is left intentionally blank].

ii. ***[1.2] determining, based on the report, that a particular service policy setting of the wireless end-user device needs to be modified,***

343. Limont discloses this element.

344. As I detailed above for element 1.1, Limont's mobile device sends to the service a report (in the forms I have identified above) that indicates the various "configuration settings" or "policy settings" currently on the mobile device.

345. Limont's computer system 141 (shown in Figures 1 and 3) uses the configuration version / policy version received from to mobile device to determine whether the device's settings need to be modified to allow for the access to the data that the mobile device is requesting.

346. Limont details this determination for both the Figures 1 / 2 embodiment and the Figures 3 / 4 embodiment. Limont shows that the server (part of computer system 141 in Figures 1 and 3) may "compare" the configuration version in the report (as detailed above) to other configuration versions ("*based on the report*") to determine that the "version" in the request does not permit the

desired access of data on the server and therefore needs to be modified ("*determining, based on the report, that a particular service policy setting of the wireless end-user device needs to be modified*").

> [0080] … Request 176 can indicate a configuration version representing the one or more of the current configuration settings of mobile device 101. Computer system 141 can receive request 176 from mobile device 101 … request 176 can be a provision request expressly requesting appropriate configuration settings….
>
> [0082] Method 400 includes an act of determining that current mobile device configuration is not appropriate for accessing the maintained data (act 402). For example, configuration enforcement module 193 can compare a configuration version included in request 176 to other configuration versions (e.g., included in configuration versions 192) that are appropriate for accessing data (e.g., Web pages in data store 197) maintained by server module 193B (e.g., a Web server). When the included configuration version does not match any other appropriate configuration version, configuration enforcement module 194 determines that the configuration settings of mobile device 101 are inappropriate for accessing data maintained by server module 193B. If no configuration version was included, policy enforcement module 193 can be default determine that the configuration settings of mobile device 101 are inappropriate for accessing data maintained by server module 193B.

> [0083] In response to detection of an inappropriate configuration, configuration enforcement module 143 can **identify configuration settings**, such as, for example, 191B, K, N, and R that are appropriate for accessing data maintained by server module 193B….

347. EX-1004, [0080-0083]. See also EX-1004, claim 1.

348. The Figure 1 / 3 embodiment contains the same "determination"

349.

> [0060] Method 200 includes an act of determining that the current policy settings at the mobile device are not appropriate for accessing data maintained by the computer system (act 202). For example, policy enforcement module 143 can compare a policy version included in data command 161 to other policy versions (e.g., included in policy versions 118) that are appropriate for accessing data (e.g., electronic mail messages and folders in data store 171) maintained by server module 142B (e.g., an electronic mail server). When the included policy version does not match any other appropriate policy version, policy enforcement module 143 determines that the policy settings of mobile device 101 are inappropriate for accessing data maintained by server module 142B. If no policy version was included, policy enforcement module 143 can be default determine that the policy settings of mobile device 101 are inappropriate for accessing data maintained by server module 142B.

[0061] Method 200 includes an act notifying the mobile device that the current policy settings are not appropriate for accessing the maintained data (act 203). For example, server module 142B can send notification 162 to mobile device 101 to notify mobile device 101 that its current policy settings are inappropriate for access data maintained by server module 142B.

[0062] Data command 161 (a request) and notification 162 (a response) can be corresponding messages in a request/response protocol, such as, for example, HTTP. In some embodiments, notification 162 is configured to include an HTTP 5xx (e.g., 512) response code indicating that the server could not fulfill the request (i.e., data command 161).

[0063] Method 200 includes an act of receiving a policy request from the mobile device, the policy request requesting policy settings that are appropriate for accessing the maintained data (act 204). For example, mobile device 101 (client module 142A) can send policy request 163 to computer system 141. Computer system 141 can receive policy request 163 from mobile device 101. Policy request 163 can be an initial request for policy settings, can be a request sent in response expiration of a time interval, can be a request sent in response to a notification of new policy settings, or can be a request sent after a period of exception for a user has expired.

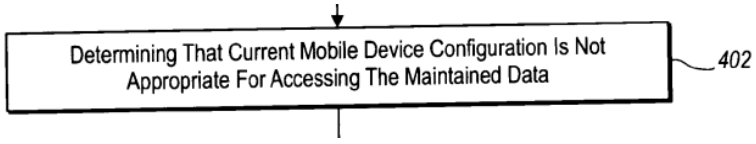
[0064] Method 200 includes an act of identifying updated policy settings that are appropriate for accessing the maintained data (act

> 205). For example, policy enforcement module 143 can identify that settings 117A, B, F, and H are appropriate for accessing data maintained by server module 142B. Settings 117A, B, F, and H can correspond to any of the previously described policy settings.
>
> [0065] Method 200 includes an act of sending the updated policy settings along with a corresponding updated policy version to the mobile device, the updated policy version representing the updated policy settings (act 206). For example, server module 142B can send settings 117A, B, F, and H along with policy version 118D to mobile device 101. Policy request 163 (a request) and settings 117A, B, F, and H along with policy version 118D (a response) can be corresponding messages in a request/response protocol, such as, for example, HTTP.

350. EX-1004, [0060-0065], Fig. 2, claim 9, [0045-0053].

351. Thus, by determining that the existing settings are not appropriate and identifying the "updated" settings that would be appropriate (in both embodiments above), the server has performed the act of "*determining, based on the report, that a particular service policy setting of the wireless end-user device needs to be modified*."

352. Limont depicts this activity in Figures 4 and 2.



353. EX-1004 FIG. 4, step 402. See also EX-1004, FIG. 2, steps 202, 205, claim 9.

354. The mobile device is attempting to "access maintained data" on the server through its various requests to the server.

355. "FIG. 4 illustrates an example flow chart of a method 400 for enforcing an appropriate mobile device configuration prior to permitting a mobile device to access maintained data." EX-1004, [0079].

> [0089] Method 400 includes an act of permitting the mobile device to access the maintained data in response to receiving the indication that the mobile device is configured in accordance with the device configuration settings (act 405). For example, configuration enforcement module 194 can permit mobile device 101 to access data 197A. Server module can subsequently send notification 199 to mobile device 101. Notification 199 can indicate to mobile device 101 that configuration enforcement module 194 has permitted access to data 197A. Data request configuration version 192L (a request) and notification 199 (a response) can be corresponding messages in a request/response protocol, such as, for example, HTTP.

356. EX-1004, [0089].

357. The Figures 1 / 2 embodiment also shows the mobile device seeks to access data.

> [0060] Method 200 includes an act of determining that the current policy settings at the mobile device are not appropriate for accessing data maintained by the computer system (act 202). For example, policy enforcement module 143 can compare a policy version included in data command 161 to other policy versions (e.g., included in policy versions 118) that are appropriate for accessing data (e.g., electronic mail messages and folders in data store 171) maintained by server module 142B (e.g., an electronic mail server). When the included policy version does not match any other appropriate policy version, policy enforcement module 143 determines that the policy settings of mobile device 101 are inappropriate for accessing data maintained by server module 142B. If no policy version was included, policy enforcement module 143 can be default determine that the policy settings of mobile device 101 are inappropriate for accessing data maintained by server module 142B.

358. EX-1004, [0060]. See also Fig. 4 (step 405), Fig. 2 (steps 207-208)

359. Limont's requested server data can only be accessed by the mobile device with the "appropriate" configuration / policy settings as detailed above.

360. Thus, a determination that the current settings are "inappropriate for accessing data maintained by the server" (to which the mobile device seeks access) is a determination that the mobile device's configuration settings (policies) "*need[]*

to be modified" to allow the desired access – particularly when combined with a further determination that identifies the specific correct settings for such access.

361. The claim recites "***a particular service policy setting***" for which the determination of the need for modification is made. Limont's determination evaluates the existing "policy settings" (as reflected by Limont's reference to both of 'configuration settings" and "policy settings") to determine the modification.

362. Limont's "configuration settings" includes policy settings, and Limont uses these terms interchangeably.

> Computer system 141 includes server module 193B (e.g., a Web server). Server module 193B fuirther [sic] includes policy enforcement module 194 and data access module 195. As depicted, configuration settings 191 includes configuration settings 191 include policy setting 191A, policy setting 191B, and policy setting 191Z. A series of two dots (a vertical ellipsis) between, before and after the expressly depicted configuration settings represents that other configuration settings can be included between, before and after the expressly depicted policy settings. Configuration settings can be name/value pairs. The name represents the name of a configuration setting and the value represents the value of the configuration setting. Configuration setting values can be of virtually any data type, such as, for example, Boolean, integer, floating point, string, character, enumerated, etc. Configuration settings can include: operating system

> settings, application program settings, hardware settings, allocated resource settings, network interface settings, wireless protocol settings, etc.

363. EX-1004, [0073].

364. For example, Limont's "configuration enforcement module" 194 can be referred to as "policy enforcement module" 194 and "configuration settings" can correspond to "policy settings."

> Server module 193B can interoperate with client side programs (e.g., client module 193A) to transfer data (e.g., Web pages) to a mobile device. Thus, in response to a mobile device data request, **policy enforcement module 194** can determine if a requesting mobile device's policy settings are appropriate for accessing data. For example, policy enforcement module 194 can determine if sufficient resources have allocated at a mobile device to receive a Web page, if a mobile device Web browser includes correct plug-ins for viewing content, if mobile device connection speed will permit a Web page to be downloaded in a reasonable amount of time, etc.

365. EX-1004, [0077] (using "policy enforcement module 194"). The very next paragraph uses the term interchangeably:

> Configuration enforcement module 193 can interoperate with one or more of an authentication module, authorization modules, and policy enforcement module of server module 193B (not shown) to reduce the

> likelihood of inappropriate data access. When configuration settings are appropriate (and, for example, a user is authenticated and authorized and policy settings are appropriate), data access module 195 accesses requested data and transfers requested data to the requesting mobile device. On the other hand, when configuration settings are inappropriate (and even if a user is authenticated and authorized and policy requirements are appropriate), **configuration enforcement module 194** can access appropriate configuration settings and transfer the appropriate configuration settings to the requesting mobile device.

366. EX-1004, [0078] (using "configuration enforcement module 194").

367. The same is true about the interchangeable reference to "configuration settings" and "policy settings."

> [0083] In response to detection of an inappropriate configuration, configuration enforcement module 143 can identify **configuration settings**, such as, for example, 191B, K, N, and R that are appropriate for accessing data maintained by server module 193B. **Configuration settings** 191B, K, N, and R can correspond to any of the previously described **policy settings**.

368. EX-1004, [0083].

369. Given Limont's interchangeable references, the claimed "service policy setting" is shown by the evaluation and modification of the configuration /

policy settings in Limont. S*ee also* EX-1004, [0045], [0055], [0060], [0064], [0088-0089] (all describing the use of "policy enforcement module" with respect to policy settings and/or configuration settings).

370. Limont's disclosures fit within the meaning of "service policy settings" in the '042 Patent. I note that the term "service policy settings" is used in the '042 Patent specification only a single time:

> In some embodiments, the only mechanism for modifying any program elements executing inside the protected DAS partition 114 is through the service control link so that only the service controller 122 may modify the operation or service policy settings for the agents located in the service measurement and/or service control execution partition.

371. EX-1001, 7:54-63. The '042 specification also does reference "policy settings for the various service plans":

> In some embodiments, a policy control server 154 stores policy settings for the various service plans that can be implemented on the device, and communicates the appropriate policy settings to the appropriate device DAS agents

372. EX-1001, 8:26-30. However, the specification does not provide any specific information on these policy settings for various service plans.

373. Limont discloses numerous examples of the configuration / policy settings that would correspond to service policy settings. For example, Limont's configuration / policy settings include "operating system settings, application program settings, hardware settings, allocated resource settings, network interface settings, wireless protocol settings, etc." EX-1004, [0073]. Network interface settings and wireless protocol settings disclose, including rendering obvious, such service policy settings because those settings define the particular aspects of the service across the wireless network. Moreover, as detailed below for element 1.4, the settings in Limont also are specific to various network services (e.g., email, Web) for which Limont's policy / configuration settings must be appropriate to be able to access the data across the network from the server.

374. That Limont discloses, including rendering obvious, the claimed determination of "needs to be modified" is also reflected by Limont's actual modification of the policy / configuration settings that occurs by Limont sending new settings (when needed) (e.g., modifying the mobile device settings) to allow for the requested access. This is discussed in detail in element 1.6. As detailed therein, Limont's "configuration settings" (policy settings) are sent from computer system 141 in steps 405, 206 for modifying the mobile device's configuration to

permit the desired access to the server data (*a particular service policy setting … needs to be modified*) of the mobile device (*the wireless end-user device*). EX-1004, [0085], [0089], [0065], Fig. 4 (steps 403, 405); Fig. 2 (steps 205, 206).

375. Thus, Limont discloses this element.

376. [This paragraph left intentionally blank].

iii. ***[1.3] the particular service policy setting being stored in a protected partition of the wireless end-user device, the protected partition configured to deter or prevent unauthorized modifications to the particular service policy setting,***

377. Limont in view of Wright and optionally Xu discloses this limitation.

378. Limont's mobile device 101 stores data, for example, configuration settings 191B, K, N, and R and configuration version 192L in program data 116 (**red**) for subsequent access (*the particular service policy setting being stored in a [] partition … the wireless end-user device*).[2] EX-1004, [0086], Annotated FIG 3.

379. As shown in FIG. 3 below (and in FIG. 1), the mobile device includes a "memory 112" that is shown with different data stored therein, including storage for different data / programs

[2] As noted in [1.2], the "configuration settings" and "version" encompass policies.

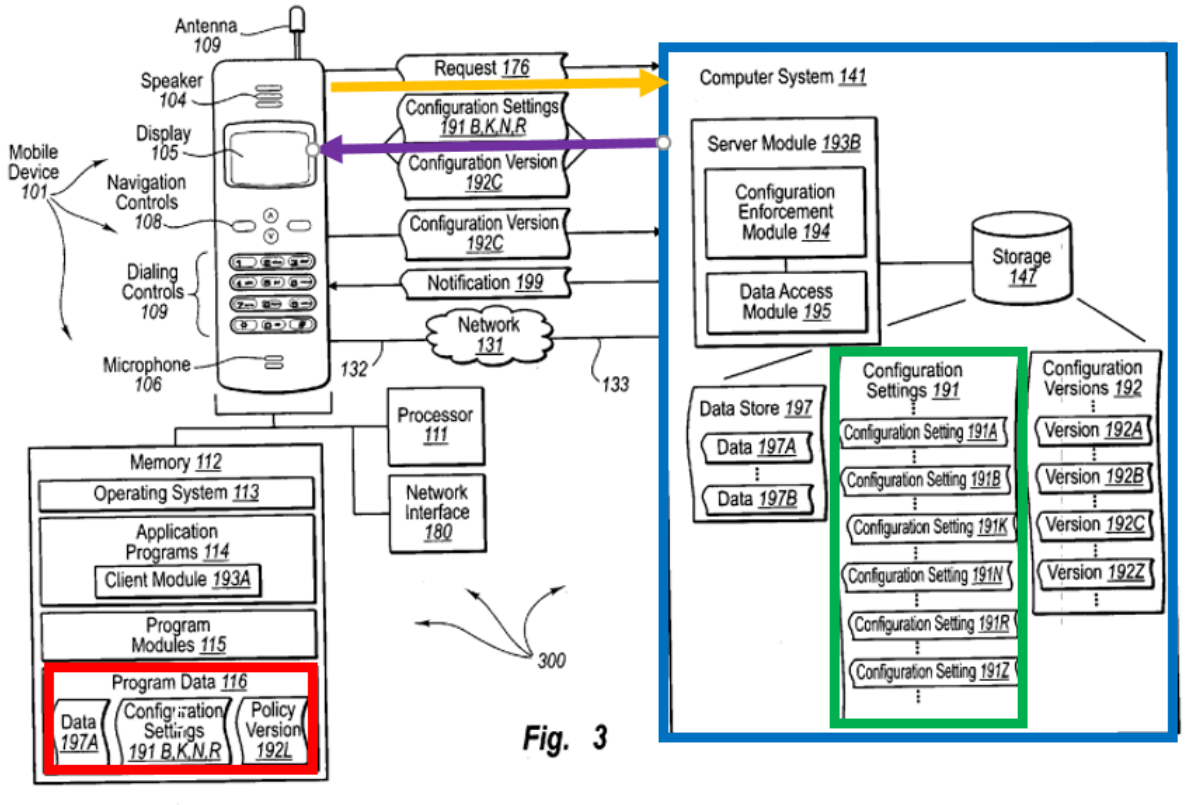


Fig. 3

380. EX-1004, FIG. 3.

The memory 112 generally represents a wide variety of volatile and/or non-volatile memories and may include types of memory previously discussed. However, the particular type of memory used in the mobile device 101 is not important to the present invention. Program code means comprising one or more program modules may be stored in memory 112. The one or more program modules may include an operating system 113, one or more application programs 114, program modules 115, and program data 116.

381. EX-1004, [0040]. The memory stores many different types of data.

> Generally, mobile device 101 can store data, such as, for example, electronic mail messages, Web pages, documents, policy settings, policy versions, configuration settings, configuration versions, etc. in memory 112. Mobile device 101 can utilize client side programs, such as, for example, client module 142A (e.g., an electronic mail client) to access data from a server (e.g., an electronic mail server).

382. EX-1004, [0044].

383. Analogous to Figure 3, Figure 1 depicts memory 112 with the program data partition storing "Data 171A," "[policy] Settings 117 A,B,F,H," and "Policy Version 118D." *See also* EX-1004, [0045-0053] (describing various policy settings and versions).

384. Thus, Limont's disclosure includes, or renders obvious that the mobile device has a "partition" that stores the recited "*service policy setting*" (actually, multiple settings).

385. Limont does not expressly disclose that this partition is a "*protected partition ... configured to deter or prevent unauthorized modifications*" to the stored data. However, Wright and, optionally, Xu, show that a partition on a mobile device that is "protected."

386. As described in the Motivation to Combine Section above, a POSA would be motivated to modify Limont's teachings to encrypt or hide the

configuration settings as taught by Wright to deter or prevent unauthorized changes to the settings of the mobile phone.

387. Wright provides such a memory partition in at least two ways: through encrypting and/or "hiding" policies stored on the mobile device.

388. Wright identifies "security information" that may be encrypted that includes policies transmitted from the server to the mobile device. Security information includes policies.

> [R]esponsive to security information such as a policy or software being designated for encryption, the policy management module 236 provides 308 the designated client mobile device with cryptographic information which the client device can store and use to decrypt the security information. An example of cryptographic information is a key for use with a cryptographic authentication protocol. … permissions typically relate to the allowable modification that may be made to a downloaded policy or client software by the client mobile device.…
>
> For illustrative purposes only, the method embodiments illustrated in FIGS. 3A and 3B are discussed in the context of the system embodiment of FIG. 2A. FIG. 3A illustrates a method for managing one or more security policies for the protection of data accessible by a mobile device based upon criteria in accordance with an embodiment of the present invention. In the system embodiment of FIG. 2A, the

policy management module 236 defines 302 a security policy applicable to a client mobile device based upon criteria. One example of criteria is the location associated with the network environment in which the mobile device is operating. Other examples of criteria are the presence or the activity status of one or more security features. Of course, a combination of location and one or more security features may also form a criteria basis for defining a security policy. The policy management module 236 designates 304 one or more client devices associated with the policy. In one example, this association may be based on an entity or class to which the security policy is applicable. An example of an entity is a group with one or more members. An example of a member may be a user of the client mobile device. A policy may be set that is applicable to the group of all engineers in the software development department. Another example of a member is the mobile device itself. For example, the capabilities of different mobile devices may be the basis for classifying them into different groups. In a secure manner, the policy management module 236 provides 306 the one or more designated client mobile devices with authorization information for use in contacting the server system securely. One example of authorization information is an encrypted token provided by the authorization module 232 to the mobile client device during a trusted connection between the two. An example of a trusted connection may be an internal connection behind the firewall of and within the internal network of the enterprise with which both

the server system and the mobile client device system are associated. In one embodiment, an authority server within the firewall in the internal network provides the authorization information. When a client mobile device connects via the Internet, it interacts with one or more of the enterprise side servers external to the firewall. The client contacts the external servers to retrieve policies and instructions. The external servers also perform key/identity management, client disable methods (e.g. unmanaged mode) and policy persistence. The external servers communicate with the authority server through the firewall for client management information such as a key, a user, a group, and version information associated with a client mobile device system. In a similar manner, responsive to security information such as a policy or software being designated for encryption, the policy management module 236 provides 308 the designated client mobile device with cryptographic information which the client device can store and use to decrypt the security information. An example of cryptographic information is a key for use with a cryptographic authentication protocol. In one example, Microsoft® web keys may be used. The policy management module 236 sets 310 the permissions for the one or more associated mobile devices with respect to the one or more policies. In one aspect, permissions typically relate to the allowable modification that may be made to a downloaded policy or client software by the client mobile device. Permissions may be applied to various policies and to the criteria upon which policies are defined.

> For example, there may be permissions set for a policy, but permissions may also be set with respect to a location. Some examples of permissions specific to policies are as follows:

389. EX-1005, [0078];

390. The encryption of the policies is related to certain "permissions" set for those policies which is a separate form of "protection" creating a "protected partition." Wright lists exemplary "permissions" which "permissions typically relate to the allowable modification that may be made to a downloaded policy." EX-1005, [0078].

> [0079] Ability to see the tray icon
>
> [0080] Ability to shut down the service
>
> [0081] Ability to go to unmanaged mode
>
> [0082] Ability to go to self-managed mode
>
> [0083] Ability to change to a different policy server, or get a policy from another server in the same enterprise
>
> [0084] Ability to not pull down new policies when they are available
>
> [0085] Ability to get software updates directly from a vendor
>
> [0086] Ability to launch the settings application
>
> [0087] Ability to modify visual settings
>
> [0088] Ability to modify feedback levels
>
> [0089] Ability to see/modify server-defined global objects (for each type of object)

[0090] Ability to create new global objects (for each type of object)

[0091] Ability to see/modify global objects in the policy (for each type of object)

[0092] Ability to change the global objects used in the policy (for each type of object)

[0093] Ability to remove adapters from the policy.

[0094] Some examples of permissions specific to locations are as follows:

[0095] Ability to manually switch to a location

[0096] Ability to override a location.

[0097] Ability to manually switch to a different location

[0098] Ability to change enforcement mechanisms.

[0099] In one embodiment, in setting the permissions, for flexibility, a permission setting or a level of identification for each of the permissions may also be set. Some examples of these possible settings or levels are as follows:

[0100] Modifiable: The user has permission to modify the setting freely.

[0101] Recommended: The user has permission to modify the setting, but the application will recommend the policy's default.

[0102] Mandatory: The user does not have permission to modify the setting.

[0103] Hidden: The user does not have permission to view or modify the setting.

391. EX-1005, [0079-0103], [0280-284].

> [P]olicy distribution module 234 distributes security information to the one or more client mobile devices. … Examples of security information are versions of existing policies, policies, or software.

392. EX-1005, [0051]. The various protections are set and enforced by the "policy setting module:"

> In this embodiment, the layer manager 206 has a communication interface, for example a software interface or buffers for storing parameters, to a location detection module 208. The layer manager 206 forwards network parameters to the location detection module 208. The location detection module 208 detects or determines the location associated with the current network environment based upon criteria defined in a downloaded policy from the server system 200. In this example, the policy setting module 212 receives, installs and updates the security information including security policies and/or software updates received from the policy management module 236 via the policy distribution module 234 over the network connection 204. The policy setting module 212 may define criteria or if permissions set by the policy management module 236 allow, supplemental policy definitions or customization of policy definitions based upon user input processed by the mobile device user interface module 218. Similarly, if operating in a standalone mode not under the control of the server system, the policy setting module 212 defines

> an aspect of a policy such as location criteria or security features criteria based upon user input processed by user interface module 218.

393. EX-1005, [0061].

394. Wright thus discloses "protected partitions" through: (1) storing encrypted security information (policies); (2) the ability to "hide" the policy file and (3) "permissions" for policies. EX-1005, [0014], [0103], [0262], [0280-0284]. Each of these mechanism will "deter or prevent unauthorized modifications" to the stored data such as policies.

395. Wright details policies broadly including many aspects of those policies which would be known to a POSA. Such "aspects of" policies include:

> Defining policies includes the creation of policies and the modification of policies. Examples of aspects of a policy includes specification of rules and permissions (e.g. policy override), defining one or more locations associated with network environments, defining or identifying security features to be monitored, ports to be monitored, network services to be monitored, applications to be monitored, enforcement mechanisms to be put in place for a particular policy, level identification for a policy or policy aspect for flexibility (optional, recommended, mandatory, invisible), and feedback (e.g. custom error messages) to alert an administrator via a user interface screen using the server system 200 of certain conditions or to alert a client device user via a user interface screen of certain conditions.

396. EX-1005, [0048].

397. Wright also teaches specific examples of a user might define and configure the policies:

> [0180] FIG. 5B illustrates a graphical user interface example illustrating a method for defining criteria with respect to environmental network parameters or characteristics to define a location in accordance with an embodiment of the present invention. In the embodiment of FIG. 2A, the policy management module 236 may receive from the user interface module 240 a user-selected name for a location to be defined via such a graphical user interface as this illustrated example. A user-provided description may also be received for this location via the illustrated interface. In one example, the network parameters are defined based upon user input received from user interface module 240 for each location to be defined. For additional locations in which the client user is allowed to define a location associated with a network environment of if the device is operating in a standalone mode, responsive to a selection of a button indicating the user wants the location to be defined, a "Stamp" button in this embodiment, one or more network parameters are determined. In the example in the context of FIG. 2B, responsive to the "Stamp" request, the policy setting module 212 requests a snapshot of the current network environment parameters which it receives in the example of FIG. 2B from the layer manager 206. Examples of

network parameters are identifications of network services such as Gateways, Domain Name System (DNS) Servers, (Dynamic Host Control Protocol) DHCP and Domain servers. Other examples include identifications for Windows® Internet Naming Service (WINS) servers. Alternatively, the policy management module 236 may receive the "stamped" network parameters from the policy setting module 212 or the location detection module 208 on the client device after a snapshot has been taken in order to define locations.

[0181] FIG. 5C illustrates a graphical user interface example displaying the network services identified in a network snapshot in further illustration of the method example described in FIGS. 5B, 5D, 5E and 5F. In the example in the context of FIG. 2A, the policy management module 236 directs the user interface module 240 to display the types of servers which the user interface module 240 causes to be displayed in such an interface as the illustrated example of FIG. 5C. The displayed user interface example of FIG. 5C illustrates by check marks user input that has been received via an input device identifying those services selected for further configuration.

[0182] FIG. 5D illustrates a graphical user interface example for configuring parameters associated with one of the selected network services, in this example Gateway services, of the method example described in FIGS. 5B, 5C, 5E and 5F in accordance with an embodiment of the present invention providing for further

configuration of the selection of services. FIG. 5D presents an example user interface for configuring a "Gateway Service Definition." In this embodiment, the service definition specifies the specific servers that provide network service for this location. In this example, for each service provider entry, a service definition may be defined by a service identifier having a value of a NETBIOS name such as "NET-GATEWAY" or an IP address. In the example in the context of FIG. 2A, a service identifier designation is received by the policy management module 236 from the user interface module 240. In the illustrated example of FIG. 5D, the service identifier designation indicates whether or not a particular service identifier provided by a service provider during location detection in operation of the mobile device must match this service identifier by a "Yes" or a "No" input designation. The policy management module 236 stores the service identifiers and their corresponding service identifier designations so that they are associated with the location being defined.

[0183] FIG. 5E illustrates another graphical user interface example for configuring parameters associated with one of the selected network services, in this example Domain Name System (DNS) Servers, of the method described in FIGS. 5B, 5C, 5D and 5F in accordance with an embodiment of the present invention providing for further configuration of the selection of services. In this example, the parameter associated with each of these identified servers is an IP

> address, and user input designates by "Yes" or "No" whether the IP Address is a parameter to be associated with the location associated with this network environment.
>
> [0184] FIG. 5F illustrates an example user interface for indicating a minimum number of network services or service providers to be present within the network environment for a valid location identification in continuing illustration of the example of a method in accordance with the present invention illustrated in FIGS. 5B, 5C, 5D, and 5E. In the example in the context of FIG. 2A, the minimum number is received by the user interface module 240 and forwarded to the policy management module 236. This minimum number may include the number of service providers whose service identifiers must match plus a number of service providers whose identifiers may optionally match according to a user defined criteria. These one or more network parameters identifying the location are stored in a data object (e.g. look-up table) in memory 242 for the associated client device. Similarly, they may be stored in a data object in resident memory 220, particularly for locations defined by the client system 201.

398. EX-1005, [0180-0184] See also Figs. 5B-5F (referenced above).

399. Wright shows these features in Figure 2B (which shows the mobile device, mobile client computer system 201).

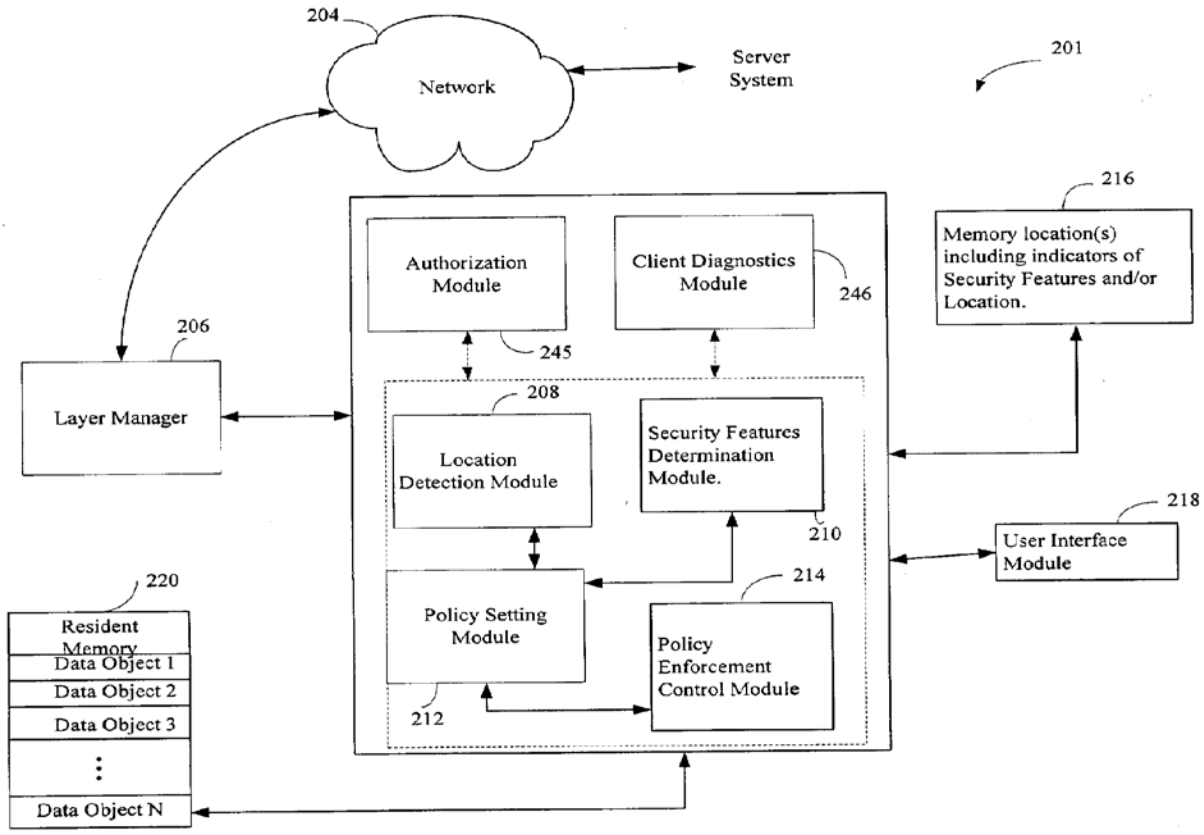


FIG. 2B

400. EX-1005, Fig. 2B, [0046]. The "memory 220" is the "protected partition."

> [0047] The system embodiment 200 **protects data accessible by the mobile device** that may be resident (See FIG. 2B, 220) …. Examples of such data may include security policies, corporate data, group files indicating the organization of personnel into various groups, client device management data, and diagnostic information related to the

mobile devices or computers internal to the corporate network. As is apparent, these are examples of information valuable to a company.

401. EX-1005, [0047].

[0058] FIG. 2B illustrates a **system 201 for protecting data accessible by a mobile device** based on a location associated with a network environment in which the mobile device is operating in accordance with an embodiment of the present invention. Additionally, the system 201 in FIG. 2B illustrates a system for determining and enforcing security policies based upon the activity status of a security feature in a communication session between the mobile device and another computer. The illustrated system embodiment 201 comprises a location detection module 208, a policy setting module 212, security features determination module 210, a policy enforcement control module 214, a layer manager 206, a user interface module 218, memory location(s) 216, an authorization module 245, and a client diagnostics module 246. T**he system 201 protects data accessible by the mobile device that may be in resident memory 220 on the device** or be data 242 accessible over a network 204. In this illustrated example, each of these modules has a communication interface or is communicatively coupled to each of the other modules. **Resident memory 220 may be accessed by one or more of these modules**.

[0059] ….

> [0060] The layer manager 206 has a communication interface to one or more modules 208, 210, 212, 214, 245, 246. A layer manager 206 processes network traffic which may include inbound data (e.g. 242, FIG. 2A) accessible over a network and outbound copies of data objects from resident memory 220. In this embodiment, the layer manager 206 processes information in one or more layers of a model for communications between computers in a network. An example of such a model is the Open Systems Interconnection (OSI) data communications model. The seven layers of the OSI model are the physical layer, the data-link layer, the network layer, the transport layer, the session layer, the presentation layer, and the application layer. Another example is the layered Internet Protocol stack. It is represented as four layers including the subnetwork layer, the Internet layer, the transport layer, and the application layer.

402. EX-1005, [0058-0060].

403. The cryptographic data may be stored in memory 220.

> Responsive to it being determined 335 that new security information, for example a policy, software, or a message, is available, the new security information is downloaded 337. The client policy setting module 212 determines 338 if the security information is encrypted 338. If so, the security information is decrypted 340 using cryptographic information stored in memory (e.g. 220) that was previously downloaded in a secure session within the enterprise's internal network. For example, on the server side, a SHA1 hash of the

file is performed, and the result is appended to the file. In this example, the file data is encrypted with the key for example using the Advanced Encryption Standard (AES). On the client side, a hash is performed with the key, and a comparison of the result made.

404. EX-1005, [0131].

405. Memory 220 specifically stores policies:

[0176] Security policies may be stored as data objects accessible over a network 242 in FIG. 2A or in resident memory 220 in FIG. 2B. In another example, security policies may be stored as XML documents. A security policy may have associated with it or be associated with more than one location or security feature. For example, a security policy may be defined as a container having an object type of "location" and a data object type of "security feature." In one example, the "location" data object has attributes of "security features" and rules defining the policy associated with the location type. One example in which the security feature of adapter type is included in the location data type definition is illustrated below

[0177]

Policy

Locations

Location (list)

Adapters

Wired Adapter

Wireless Adapter

> Permissions
>
> Rules
>
> File Encryption
>
> .....
>
> In the illustrated example, network adapters are generalized into the two categories of wired and wireless and when the policy is put into action on the mobile device, whatever adapters exist on the mobile device inherit the properties of these two prototype adapters in the policy object.

406. EX-1005, [0176-0177].

407. The policies regarding encryption and hiding are applied to the files stored in memory 220.

> In the event 1002 that a request is received 1024 for a file, the policy engine 832 determines 1026 whether the current policy allows access to this file. As defined in the embodiment of FIG. 8, the file rules 812 may define this aspect of the current policy. The file may be located in resident memory (see 220) or be accessible over a network (see 242). Responsive to a determination that the current policy allows access to this file, the policy engine 832 determines 1030 further whether only an encrypted version of the file is allowed to be accessed. Again, in FIG. 8, the file rules 812 may define this aspect of the current policy. Responsive to a determination that only an encrypted file is allowed to be accessed, the file filter 824 allows access to 1032 an encrypted

> copy of the file. Responsive to a determination that encryption of the file is not required, the file filter 824 allows access to 1034 an unencrypted copy of the file. Responsive to a determination that the current policy does not allow or prohibits access to this file, the policy engine 832 hides 1028 the file. The file may be hidden in various ways known to those of ordinary skill in the art. Examples include sending a notification that the file was not found instead of the file descriptor.

408. EX-1005, [0280].

409. Thus, Wright teaches a specific "protected partition" corresponding to this claim element.

410. For the proposed combination, for at least the stored policies, Limont's memory 112 would be implemented as is described for Wright's memory 220 (including, as necessary, Wright's modules that provide the encryption / decryption capabilities and controls). Such a combination would merely be the use of known components (e.g., memory and processors implementing encryption) to perform known operations (e.g., encrypting memory information and decrypting as authorized) to achieve a known and predictable result (that only authorized users can access and modify the protected data in the memories).

411. Wright's disclosure includes several aspects that mirror Limont and further bolster the motivation to combine.

412. For example, Wright addresses the same issue identified by Limont in that the mobile device's "location" may impact the need for a "security policy" that protects the data (by encryption or hiding as per a policy). EX-1005, [0014]. A POSA would have been further motivated to combine Wright's solution for protecting data with Limont's architecture because this location-based protection fits Limont's concerns about accessing data from various locations. For example, Wright allows protection for Limont's data when the mobile user is accessing data from locations that may be known to be either secure, or not secure.

413. Thus, Wright provides a solution for the problems identified in Limont of: (1) unauthorized access to secure data (such as policies) on a mobile device; (2) allowing an administrator to lock down the policies on the mobile device; and (3) allowing an administrator to remotely administer / update policies wirelessly. Wright's solution is to provide for the encryption of secure data on the mobile device (and the ability for the administrator to authorize access to the encrypted data and the ability to add permissions that specify the rights to modify

or not modify depending on the level of authorization and factors such as the location). EX-1005, Figs. 2B, 3C; [0131-0132].

414. Wright's use of encryption to provide a "*protected partition of the wireless end-user device*" is consistent with the disclosure of the '042 Patent where the protected partition that stores policies is "the memory protection function includes encrypting traffic to and from memory so that only authorized device program elements possess the counterpart encryption capability to access the memory." EX-1001, 9:27-30. The "counterpart encryption capability" in the '042 Patent corresponds to the permissions specified in Wright which allow for different programs within Wright's mobile device to decrypt and or view (e.g., not hidden) the stored data such as policies.

415. Thus, Wright's disclosure of memory storing encrypted policies teaches, or renders obvious, the claimed "*the particular service policy setting being stored in a protected partition of the wireless end-user device*." If PO argues that the "protected partition" requires functionality beyond "storing" data, then Wright's "protected partition" would include the components and modules in Fig. 2B (along with the processor and buses) used to perform encryption / decryption.

EX-1005, Figs. 2B, 3C; [0131], [0047], [0051], [0062]. These components in Wright were detailed above.

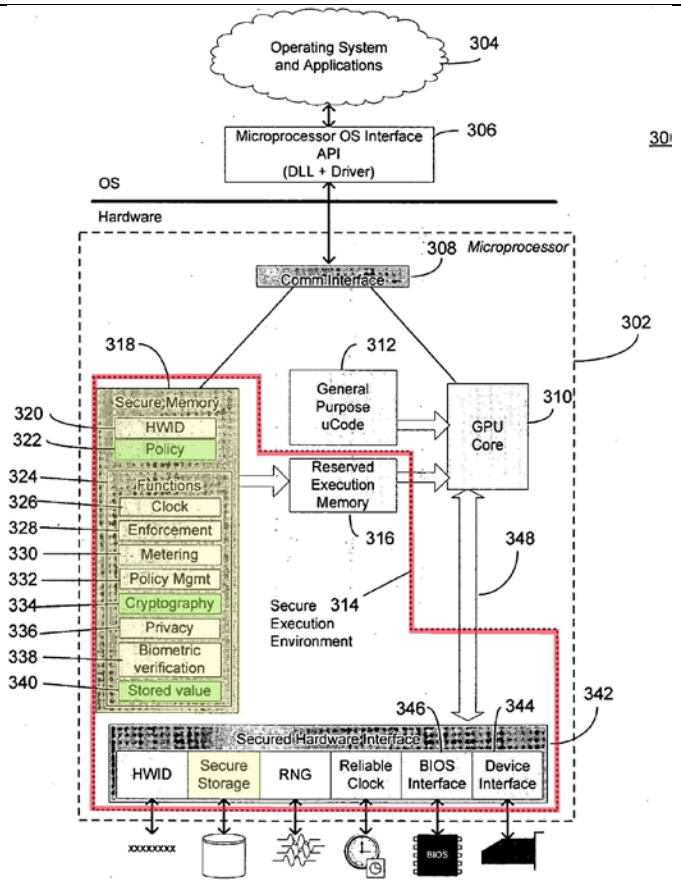
416. Moreover, as detailed above, Wright's "*protected partition"* is *"configured to deter or prevent unauthorized modifications to the particular service policy setting*" because the encryption (and hiding) prevents unauthorized users from modifying the policies stored in Wright's encrypted memory. EX-1005, [0078-0104], [0229-0230], [0259-0264], [0280-0284], [0048]. I have detailed above for Wright's memory 220 how the data therein is protected by the encryption capabilities.

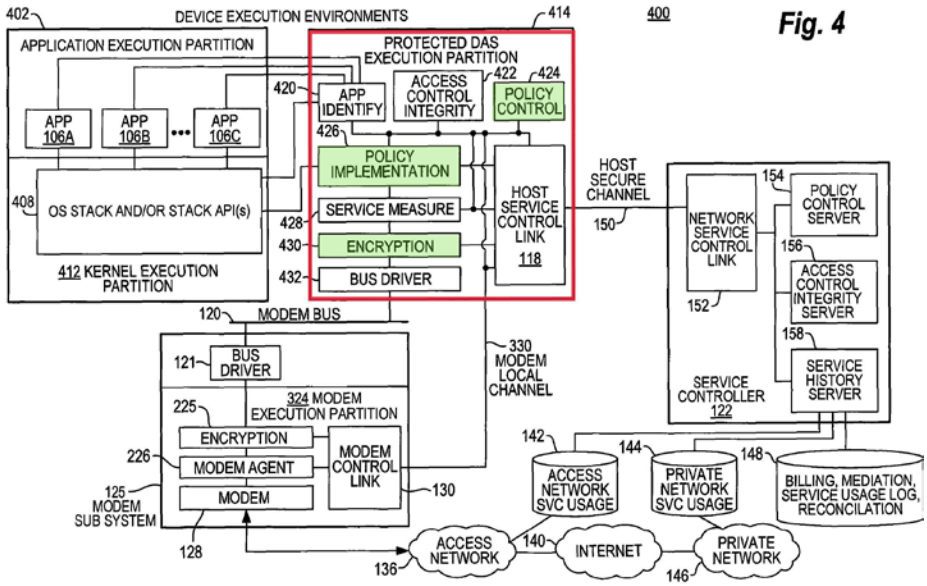
417. A POSA would have understood that the data stored in the memory disclosed in Limont (such as policy settings) should be encrypted (or "hidden") to further limit access to the stored data in the system which "reduce[s] the likelihood of a compromised device or a device with noncompliant policy setting being able to access data" as expressly taught by Wright and would be confident of its success, as discussed in the Motivation to Combine section above. EX-1004, [0071]. Wright's techniques deter or prevent unauthorized access. As noted in both Limont and Wright, such unauthorized access is known to be undesirable. Thus, by adding Wright's protection techniques (described above), a POSA would

have understood that Limont's system would benefit through the additional protections and the deterring / prevention from access by the "malicious" actors referenced in Limont as detailed above.

418. The '042 Patent describes an embodiment in which the "protected partition" appears to be implemented using known techniques to provide "secure execution environments" for certain critical data and programs. If the "*stored in a protected partition*" claim term requires that the partition be "secure execution environment" as depicted in Fig. 4 of the '042 patent (as shown below) or specific hardware controls, then Xu supplies such a secure execution environment.

419. As shown below, the '042 patent largely copies the relevant secure execution environment functionalities disclosed by Xu of policy control / management and encryption in which the "secure" environment in each allows for storage / evaluation of policies and also allows for the storage and evaluation of encryption information and algorithms within the secure environment.

Xu Fig. 3	Operating System and Applications 304 Microprocessor OS Interface API (DLL + Driver) 306 OS Hardware 308 Microprocessor Comm Interface 302 318 312 Secure Memory HWID Policy Functions Clock Enforcement Metering Policy Mgmt Cryptography Privacy Biometric verification Stored value 320 322 324 326 328 330 332 334 336 338 340 General Purpose uCode GPU Core 310 Reserved Execution Memory 316 348 Secure Execution Environment 314 346 344 342 Secured Hardware Interface HWID Secure Storage RNG Reliable Clock BIOS Interface Device Interface xxxxxxx BIOS

'042 Fig. 4	

420. Xu focuses on a secure execution environment to protect various pieces of critical data and programs from unauthorized access using hardware controls. The secured memory specifically stores the policies:

> A processing unit for use in an electronic device includes standard instruction processing and communication interfaces and also includes functional capability in addition to or in place of those found in an operating system. A secure memory within the processing unit may contain a hardware identifier, policy data, and subsystem functions such as a secure clock, policy management, and policy enforcement. Data in functions within the secure memory are not accessible from outside the processing unit.

421. EX-1016, Abstract.

> A processing unit with embedded system functions provides a secure base for enforcing security and/or operating policies, for example, for use in enforcing pay-per-use, pay-as-you-go, or other metered operation of an electronic device such as a computer, cellular telephone, personal digital assistant, media player, etc. The processing unit may include features and functional support found in most or all modern microprocessors and also support additional functions providing a hardware identifier, a tamper-resistant clock, and secure storage. Other functional capabilities such as a cryptographic unit, may be present as well. The result is a processing unit that is not reliant on any outside components, particularly operating system software, a trusted computing module (TCM), or secure-boot BIOS to establish the basis for computer capable of being operated in compliance to a usage policy.

422. EX-1016, [0003].

423. The secure memory is "tamper resistant" which corresponds to the requirement that the protected partition "deter or prevent unauthorized" access.

> [0022] A secure execution environment 314 may supplement the general processing capabilities provided by the GPU core and microcode 310 312. The secure execution environment; 314 may include a reserved execution memory 316. The reserved execution memory 316 may provide a highly secure location for the execution of instructions having an elevated privilege level within the processing

> unit 302. This elevated privilege level of operation may allow the processing unit 302 to execute code that is not directly accessible from outside the processing unit 302. For example, a particular interrupt vector may set the processing unit 302 into secure operation, or instructions may be evaluated for content requiring secure resources. When operating in this elevated privilege mode, the processing unit 302 acts as a full subsystem and does not require any external assets, for example BIOS resources, program memory, or a TCM, to build a secure processing environment.
>
> [0023] A secure memory 318 may store, in a tamper-resistant manner, code and data related to the secure operation of the computer 302. The communication interface 308 may determine which instructions entering the processor 302 should be directed to the secure memory 318, and subsequently for execution in the reserved execution memory 316. Data in the secure memory 318 may include an identification indicia or hardware identifier 320 and policy data 322 that may specify policy related operational directives such as metering, reporting, update requirements, etc. The secure memory 318 may also include code or data required to implement various functions 324. The functions 324 may include a clock 326 or timer implementing clock functions, enforcement functions 328, metering 330, policy management 332, cryptography 334, privacy 336, biometric verification 338, and stored value 340 to name a few.

424. EX-1016, [0023].

425. Xu's "secure memory" stores policies "in a tamper resistant manner" and thus, is "***configured to deter or prevent unauthorized modifications***" to the stored policies because the "tamper resistant" functionality is configured to deter modifications. "For example, [Xu's protected] policy may not be 'spoofed' by replacing a policy memory section of external memory." EX-1016, [0032].

426. For example, "By reallocating system memory 134 to the secure execution environment 314, the system memory 134 is essentially made unavailable for user purposes" thus deterring or preventing unauthorized access. EX-1016, [0024].

427. The proposed combination implements Limont's portions of memory 112 including portions of "data storage 116" in Xu's secure memory. The stored information includes at least Limont's policy information on the mobile device (EX-1004, elements 117-118, 191-192) (which corresponds assigned to "policy data 322" although it may include any data in "data storage 116."). The secure memory would also include any of the other aspects of Limont's memory 112 needed for the policies.

428. Xu's secure environment also provides the functionality to execute Wright's encryption algorithms using cryptography function 334. The

"cryptography function 334 may be used for digital signature verification, digital signing, random number generation, and encryption/decryption." EX-1016, [0025].

429. Xu's "policy" management includes numerous different policies. For example, Xu states:

> [0029] In operation, a designated interrupt may be processed by the communication interface 308 causing data or one or more functions to be loaded from the secure memory 318; to the reserved execution memory 316. The GPU 310 may execute from the reserved execution memory 316 to implement the function. In one embodiment, the functions 324 available may supplement or replace standard functions available in the operating system 134. When configured in this manner, a corresponding operating system 134 will only operate when paired with processing unit 302. Carrying this concept to another level, another embodiment of the processing unit 302 may be programmed to trap external operating system functions unless executed from the reserved execution memory 316. For example, attempts to allocate memory by the external operating system 134 may be denied or redirected to internally stored functions. When configured in this manner, only an operating system specifically configured for processing unit 302 will operate correctly. In yet another embodiment, policy data 322 and policy management functions 332 may test operating system 134, application program

135, and hardware parameters to ensure that authorized software and hardware is present.

[0030] In one embodiment, the computer 300 boots using a normal BIOS startup procedure. At a point when the operating system 134 is being activated, the processing unit 302 may load the policy management function 332 into reserved execution memory 316 for execution to configure the computer 300 according to the policy data 322. The configuration process may include allocation of memory, processing capacity, peripheral availability and usage as well as metering requirements. When metering is to be enforced, policies relating to metering, such as what measurements to take, for example, by CPU usage or over a period of time, may be activated. Additionally, when usage is charged per period or by activity, a stored value balance may be maintained using the stored value function 340. When the computer 300 has been configured according to the policy 322, the normal boot process may continue by activating and instantiating the operating system 134 and other application programs 135. In other embodiments the policy may be applied to different points in the boot process or normal operation cycle.

[0031] Should non-compliance to the policy be discovered, the enforcement function 328 may be activated. A discussion of enforcement policy and actions may be found in co-pending application U.S. patent application Ser. No. 11/152,214. The enforcement function 328 may place the computer 300 into an

> alternate mode of operation when all attempts to restore the computer to compliance with the policy 322 fail. For example, in one embodiment, a sanction may be imposed by reallocating memory from use as system memory 130 and designating it as secure memory 318. Since secure memory 318 is not addressable by outside programs including the operating system 134, the computer's operation may be restricted, even severely, by such memory allocation.
>
> [0032] Because the policy and enforcement functions are maintained within the processing unit 302, some typical attacks on the system are difficult or impossible. For example, the policy may not be "spoofed" by replacing a policy memory section of external memory. Similarly, the policy and enforcement functions may not be "starved" by blocking execution cycles and their respective address ranges.

430. EX-1016, [0029-0032].

431. Such policies overlap with, and augment, those types of policies discussed above as being present in Wright and Limont. Moreover, Xu's secure memory does not have any particular aspects that would preclude other types of policies from beneficially taking advantage of the protections allowed to Xu's articulated policies.

432. Indeed, Xu teaches that the cryptographic function is used for policy updates and to secure such policy updates. "A cryptography function 334 may be used for digital signature verification, digital signing, random number generation,

and encryption/decryption. Any or all of these capabilities may be used to verify updates to the secure memory 318 or to established trust with an entity outside the processing unit 302 whether inside or outside of the computer 300." EX-1016, [0025]. "Additional updates to the data in the secure memory 318 may be allowed only when specific criteria are met, for example, when the updates are verified by digital signature" (such as policy updates). EX-1016, [0034]. See also Xu's claim 9. Such techniques fit squarely with Wright's described techniques for encrypting and verifying updates and also solve Limont's stated problem of updates over unknown (and possibly untrusted) networks such as wireless networks when corporate users travel outside the office.

433. As discussed in the state of the art sections above, it was long known to provide protected partitions of memory to securely store sensitive data on mobile devices. Moreover, different techniques were known to prove the desired protections. These techniques include hardware techniques to secure memory, encryption techniques to prevent unauthorized access, and combinations thereof.

434. A POSA would be motivated to implement Xu's secure environment on Limont's mobile device incorporating Wright's encryption functionality. A POSA would recognize that Xu was assigned to the same source (Microsoft) as

Limont and that both Microsoft (Limont and Xu) and Apple (Wright) were leaders in the data policy management field. All three references provide complementary solutions for updating and protecting data, including specifically policies, for mobile devices.

435. For example, Limont provides the basic architecture for updating the mobile user's policies to allow for access to various corporate network services across networks such as wireless networks. Wright focuses on the mechanics of protecting such updates – both while in transit over communications networks and after it is received at the mobile device. Xu, similar to Wright, focuses on enhanced protection of the confidential policy data on the mobile device and provides further protections for the policy updates including a mechanism for securely verifying such updates.

436. Xu's secure environment addresses Limont's concern regarding "malicious users" accessing confidential information if "a mobile phone [is] lost or stolen" by controlling the device at boot-up. EX-1004, [0013]; EX-1016, [0030]. The secure environment also beneficially stores the encryption keys referenced in Limont for confidential communication, including policy updates – which Wright also describes as being encrypted in memory.

437. A POSA would also have been motivated by Xu's ability to augment Wright's encryption functionality using Xu's secure environment. For example, Wright's usage of "cryptographic information which the client device can store and use to decrypt the security information" to protect "keys" and "cryptographic authentication protocols" for protecting files, software and policies benefits from Xu's secure environment which protects such cryptographic algorithms and keys from unauthorized access. EX-1005, [0078], EX-1016, [0025-0026]. As detailed above, Wright teaches encrypting policy updates and Xu beneficially augments that teaching by allowing for cryptographic verification of such updates and to "establish trust" to outside entities (such as Limont and Wright's server) to perform such updates "between client and server … through a secure channel." EX-1016, [0025], EX-1005, [0267]. Thus, Xu beneficially increases Limont's and Wright's protections for traveling users at risk of having their devices lost and stolen and which devices may need to be updated with new policies in unsecure environments using wireless channels.

438. A POSA would have a reasonable expectation of success in the combination. Xu's secure environment provides the functionality to implement storage and encryption as described in Limont and Wright. The combination is

merely well-known functionality (hardware protecting memory and programs in a secure environment) operating in its known and predictable manner (to execute instructions to access secure data only under conditions to protect the data) to achieve a known and predictable result (the storage of data and the execution of instructions on a microprocessor). As noted above in the state of the art, such secure environments were known at least going back to 2003 when Arm filed its TrustZone patents.

439. I noted that the '042 Patent does not describe any improvement to known techniques for such "protected partitions" but rather relies upon the knowledge of a POSA. For example, the '042 Patent states:

> In some embodiments, protection of the device assisted service agents/functional elements to protect the functions that perform the device assisted functions is provided with a protected execution partition on the CPU (Central Processor Unit), APU (Auxiliary Processor Unit), or another hardware based processor. For example, such hardware protected execution capabilities in the CPU, APU, or other processor can be combined in some embodiments with either OS software functions or other native mode software functions to create secure program execution partitions as described herein.

440. EX-1001, 5:21-31. See also EX-1001, 6:23-7:27. While the '042 Patent describes and uses the "protected partition" as it was already known in the

art, the '042 Patent does not describe any particular improvement. Rather, the '042 Patent is using a known techniques for providing secure memory and is using those techniques for known data such as policy data. 3:13-46.

441. Thus, the combination herein discloses this element or renders it obvious.

442. [This paragraph left intentionally blank].

iv. ***[1.4] the particular service policy setting being associated with a service profile[3] that provides for access by the wireless end-user device to a network data service over a wireless access network***

443. Limont this element.

444. In Limont's system:

> [0041] Mobile device 101 is connectable to networks, such as, for example, an office-wide or enterprise-wide computer network, an intranet, and/or the Internet. Mobile device 101 can wirelessly exchange data with external sources, such as, for example, remote computer systems and/or application databases over such a network. Mobile device 101 includes network interface 180 that can, when

[3] The '042 Patent specification does not recite the term "service profile" or even "profile."

> appropriate, interoperate with antenna 109 to receive data from external sources and/or transmit data to external sources.

445. EX-1004, [0041].

446. Thus, Limont teaches the "access by the wireless end-user device to [data] over a wireless access network."

447. As discussed above for elements 1.1 and 1.2, Limont also discloses a configuration version (*service profile*) as a set of data including one or more configuration settings (*service policy setting*). EX-1004, [0075], [0045-0053] (describing various policy settings and versions).

448. I note that the '042 Patent does not use the terms "profile" or "service profile" in any place except the claims and the Abstract (which was added in the 2013 filing of the application leading to the '042 patent).

449. For purposes of the '042 Patent, a "service profile" would encompass at least Limont's (and Wright's, and Xu's) identification of a collection of settings that make up the "profile." Thus, Limont's "configuration version" / "policy version" corresponds to such a profile because they indicate, identify, and represent a group of one or more policy settings / configuration settings. EX-1004, [0053], [0075]. This is discussed for elements 1.1 and 1.2 above. The individual

policy settings within the identified group correspond to the service policy settings for the reasons discussed also in 1.2.

450. Limont also discloses the configuration / policy settings of the mobile device (*wireless end-user device*) can include a **network interface**, and **wireless protocol settings**." EX-1004, [0087]. Limont's communication links may use wireless protocols (e.g., GPRS, GSM, etc.) *over a wireless access network*. EX-1004, [0043], [0056]. This disclosure renders obvious that the settings allow / facilitate communications over wireless access networks (such as GPRS or WLANs).

451. Thus, a POSA would have understood that this "access" along with the network interface and wireless protocol settings is encompassed by *service policy settings that provides for access … to a* network *data service over a wireless access network* because the network interface controls the transmission / reception of data from the mobile device, and the wireless protocol specifies the format of the data wireless transmitted over the wireless access network to the mobile device. This is an example of the settings that provide access to a network data service.

452. Limont describes several forms of additional services with distinct accessed data corresponding to the "*network* data *service*" including email servers and web page servers.

453. For example, Limont's server module 193B on a computer system could be an electronic mail server, or a web server that communicates with the mobile device using protocols including TCP/IP and other higher layer protocols, Hypertext Transfer Protocol ("HTTP"), Simple Mail Transfer Protocol ("SMTP), etc.) over network 131 (*access by the wireless end-user device to a network data service)*. EX-1004, [0038].

> [0045] Computer system 141 includes server module 142B (e.g., **an electronic mail server)** and storage 147. Server module 142B further includes policy enforcement module 143 and data access module 144. Generally, storage 147 can store data, such as, for example, electronic mail messages, Web pages, documents, policy settings, policy versions, configuration settings, configuration versions, etc. For example, storage 147 can store policy settings 117 representing a group of policy settings that mobile devices can implement. As depicted, policy settings 117 include setting 117A, setting 117B, setting 117F, setting 117H, and setting 117Z. A series of two dots (a vertical ellipsis) between, before and after the expressly depicted

> policy settings represents that other policy settings can be included between, before and after the expressly depicted policy settings.

454. EX-1004, [0045].

455. [0073] Computer system 141 includes server module 193B (e.g., a Web server). Server module 193B fuirther [sic] includes policy enforcement module 194 and data access module 195. As depicted, configuration settings 191 includes configuration settings 191 include policy setting 191A, policy setting 191B, and policy setting 191Z. A series of two dots (a vertical ellipsis) between, before and after the expressly depicted configuration settings represents that other configuration settings can be included between, before and after the expressly depicted policy settings. Configuration settings can be name/value pairs. The name represents the name of a configuration setting and the value represents the value of the configuration setting. Configuration setting values can be of virtually any data type, such as, for example, Boolean, integer, floating point, string, character, enumerated, etc. Configuration settings can include: operating system settings, application program settings, hardware settings, allocated resource settings, network interface settings, wireless protocol settings, etc.

456. EX-1004, [0073].

457. Moreover, as discussed above in [1.2] and [1.3], Limont's policies are intended to allow "*for access by the wireless end-user device to a network data service*" providing the data on / from the server. EX-1004, Fig. 4, step 405; [0055]; [0078], [0085-0089], [0090] ("policy enforcement" is a "requirement" to access "data 197A"), claims 1-20 (reciting "access" to data), Fig. 2, step 208, [0069-0070] (allowing data access).

458. Limont's policies can be specific to different services' (such as email and web pages) data in "data store" 191 / 171 because those policies are evaluated to allow for access to the specific data being requested. EX-1004, [0076];

459. For example, email is one type of specific data service for which the policies are evaluated for appropriateness specific to that service:

> [0060] Method 200 includes an act of determining that the current policy settings at the mobile device are not appropriate for accessing data maintained by the computer system (act 202). For example, policy enforcement module 143 can compare a policy version included in data command 161 to other policy versions (e.g., included in policy versions 118) **that are appropriate for accessing data (e.g., electronic mail messages and folders in data store 171)** maintained by server module 142B (e.g., **an electronic mail server**). When the included policy version does not match any other appropriate policy version, policy enforcement module 143

> determines that the policy settings of mobile device 101 are inappropriate for accessing data maintained by server module 142B. If no policy version was included, policy enforcement module 143 can be default determine that the policy settings of mobile device 101 are inappropriate for accessing data maintained by server module 142B.

460. EX-1004, [0060-0068].

461. For example, Limont teaches policies that are specific to a "network data service" in the form of an HTTP web data service:

> [0082] Method 400 includes an act of determining that current mobile device configuration is not appropriate for accessing the maintained data (act 402). For example, configuration enforcement module 193 can compare a configuration version included in request 176 to other configuration versions (e.g., included in configuration versions 192) that are **appropriate for accessing data (e.g., Web pages in data store 197) maintained by server module 193B (e.g., a Web server).** When the included configuration version does not match any other appropriate configuration version, configuration enforcement module 194 determines that the configuration settings of mobile device 101 are inappropriate for accessing data maintained by server module 193B. If no configuration version was included, policy enforcement module 193 can be default determine that the configuration settings of mobile device 101 are inappropriate for accessing data maintained by server module 193B.

> [0083] In response to detection of an inappropriate configuration, configuration enforcement module 143 can identify configuration settings, such as, for example, 191B, K, N, and R that are appropriate for accessing data maintained by server module 193B. Configuration settings 191B, K, N, and R can correspond to any of the previously described policy settings.

462. EX-1004, [0082-0083].

> [0089] Method 400 includes an act of permitting the mobile device to access the maintained data in response to receiving the indication that the mobile device is configured in accordance with the device configuration settings (act 405). For example, configuration enforcement module 194 can permit mobile device 101 to access data 197A. Server module can subsequently send notification 199 to mobile device 101. Notification 199 can indicate to mobile device 101 that configuration enforcement module 194 has permitted access to data 197A. Data request configuration version 192L (a request) and notification 199 (a response) can be corresponding messages in a request/response protocol, such as, for example, HTTP.
>
> [0090] If other access requirements are satisfied (e.g., authentication, authorization, and policy enforcement), mobile device 101 can subsequently access data 197A. Mobile device 101 can then store data 197A for subsequent use by client module 193A, such as, for example, displaying a Web page at display 105.

> [0091] Accordingly, embodiments of the present invention can be used to reduce the likelihood of a device with inappropriate configuration settings being able to access data. For example, configuration enforcement manager 1 93B can potentially prevent the download of data to an in appropriate configured mobile device. Preventing the download of data that can not be appropriately processed conserves network bandwidth and systems resources.

463. EX-1004, [0089-0091].

464. Those policies can information specific to various services (e.g., web services):

> Server module 193B can interoperate with client side programs (e.g., client module 193A) to transfer data (e.g., Web pages) to a mobile device. Thus, in response to a mobile device data request, policy enforcement module 194 can determine if a requesting mobile device's policy settings are appropriate for accessing data. For example, policy enforcement module 194 can determine if sufficient resources have allocated at a mobile device to **receive a Web page,** if a mobile device **Web browser includes correct plug-ins** for viewing content, if mobile device connection **speed will permit a Web page** to be downloaded in a reasonable amount of time, etc.

465. EX-1004, [0077].

> [0054] As depicted, data store 171 includes data 171A and 171B. Different data portions can represent different types of data. For

> example data 171A can be electronic mail messages and data 171B can be Web pages. Alternately, different data portions can represent similar or the same type of data but for different users. For example data 171A can be electronic mail messages for user A and data 171B can be electronic mail messages for a different user B.
>
> [0055] Server module 142B can interoperate with client side programs (e.g., client module 142A) to transfer data (e.g., electric mail messages) to a mobile device. Thus, in response to a mobile device data request, policy enforcement module 143 can determine if a requesting mobile device's policy settings are appropriate for accessing data. Policy enforcement module 143 can interoperate with authentication and/or authorization modules of server module 142B (not shown) to reduce the likelihood of inappropriate data access. When policy settings are appropriate (and, for example, a user is authenticated and authorized), data access module 144 accesses requested data and transfers requested data to the requesting mobile device. On the other hand, when policy settings are inappropriate (and even if a user is authenticated and authorized), policy enforcement module 143 can access appropriate policy settings and transfer the appropriate policy settings to the requesting mobile device.

466. EX-1004, [0054-0055]; FIGs. 1-4.

467. Limont's server module 193B interoperates with programs on the mobile device client (*e.g.,* client module 193A) to transfer data (*e.g.,* Web pages and email data) to mobile device 101.

468. As detailed in 1.1 and 1.2 above, policy enforcement module 194 determines if a requesting mobile device's policy settings are appropriate for accessing data specific to a service and modifies those settings as necessary for access. EX-1004, [0077].

469. Thus, a POSA understood that server module 193 (or 142) provides *access to a network data service over a wireless access network* because it is allowing access by the mobile device to the specific network data services such as the web page server and email server.

470. Thus, Limont discloses this element.

471. [This paragraph left intentionally blank].

v. ***[1.5] the particular service policy setting configured to assist in controlling one or more communications associated with the wireless end-user device over the wireless access network; and***

472. Limont this element.

473. As discussed in [1.2], [1.3] and [1.4] above, Limont's server 142 / 193 evaluates the configuration / policy settings (*particular service policy setting*) to

determine if those policies allow for access to specific data requested from the service. The policy settings are modified (if needed) to be appropriate to access the requested server data with the request and exchanges of information including the provision (or not providing) of the requested data being the claimed *one or more communications associated with the wireless end-user device over the wireless access network*").

474. The server's evaluation of whether the device's settings are "appropriate to access the data" determines ("*control[s]*") whether the server communicates the requested data back to the mobile device and therefore "*the particular service policy setting"* is *"configured to assist in controlling one or more communications*." The policy settings (the specific settings that are either initially resident on the mobile device or the ones that are modified) are configured to assist the control because those settings (either individually or collectively) control the evaluation of whether, and when, the data is accessed and communicated back to the mobile device as requested.

475. Furthermore, as detailed in element 1.4, Limont's policy settings can be specific to different types of communications such as e-mail and HTTP web

service. Thus, the "particular" setting controls the communication of the requested data (and certainly "assists in controlling" that communication).

476. Additionally, Limont discloses that implemented configuration settings can also alter the current configuration for a network interface, and wireless protocol settings, at the mobile device which is a separate form of "*control one or more communications associated with the wireless end-user device over the wireless access network*." EX-1004, [0073], [0087]. For example, the specific network interface settings and wireless protocol settings can be used to define the specific network paths (such as different networks) as well as the parameters for that communication such as by controlling the speed of the communication path. They also "assists in controlling" the communication by providing the parameters to interact with the wireless network effectuating the communication.

477. Thus, Limont discloses this element.

478. [This paragraph left intentionally blank].

vi. ***[1.6] in response to determining that the particular service policy setting needs to be modified, sending configuration information to the wireless end-user device over the service control link, the configuration information configured to assist in modifying or allowing***

modifications to the particular service policy setting.

479. Limont this element.

480. Limont discloses this limitation as detailed in [1.2], [1.3], and [1.4]. Element 1.1 discusses Limont's the *service control link.* Limont discloses *determining that the particular service policy setting needs to be modified* as discussed in [1.2], [1.3] above.

481. As shown in Figure 3:

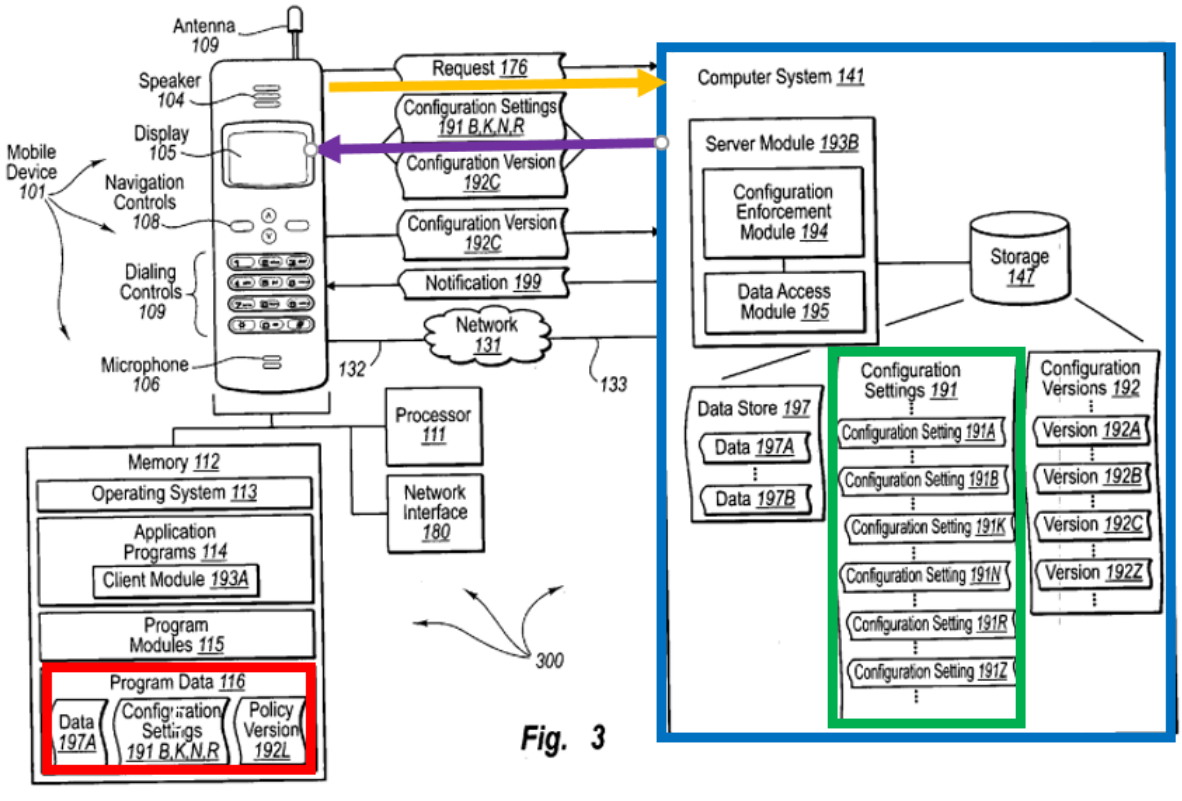


Fig. 3

482. Limont sends modified device configuration (policy) settings to the mobile device (purple) (*sending configuration information to the wireless end-user device*). EX-1004, Fig. 3; Fig. 1 (transmission of "settings 117" and "Policy Version 118D"); [0065].

483. After being sent the modified configuration settings, "[m]obile device 101 can implement settings 117A, B, F, and H (potentially altering current policy settings) ["*configured to assist in modify or allowing modification to the particular service policy setting*"] to comply with policy settings that are appropriate for accessing data maintained by server module 142B." EX-1004, [0066]. *See also* EX-1004, [0065], [0086-0087], claim 6.

484. The device configuration setting represents a modified mobile device configuration that is appropriate to access the maintained data on the server as detailed in elements 1.2 and 1.4 above. See EX-1004, [0084-0089], Fig. 4 [step 403].

485. The *configuration information* for the configuration / policy settings (sent to the mobile device) to allow access the network data service (such as web pages or email) on the server and for the network interface and the wireless protocol setting is discussed in claim element 1.4 above.

486. Thus, Limont discloses this element.

487. [This paragraph left intentionally blank].

b) Claim 2: *The method of claim 1, wherein the particular service policy setting assists in implementing a roaming control, a parental control, or an enterprise wireless wide-area network (WWAN) management control.*

488. Limont discloses this limitation.

489. Element 1.2 discusses Limont *particular service policy setting*. For example Limont's configuration / policy settings 191B, K, N, and R (*the particular service policy setting*) can correspond to any of the previously described policy settings as well as "[t]he current configuration of one or more of an operating system an application program, hardware, allocated resources, a network interface, and wireless protocol settings, at the mobile device." EX-1004, [0083], [0085], [0087], [0073].

490. A POSA would have understood that configuration / policy settings related a network interface or wireless protocol can *assist in implementing roaming control*. For example, the ability to control (via policies) the wireless protocol

settings allows for control of roaming by preventing (or allowing) access to specific wireless protocols and the specific networks (either home or roaming). Such wireless protocol settings may provide identification of available networks on which the device may roam as well as the information necessary to connect to such networks (such as authentication information).

491. Similarly, because one of Limont's articulated evaluation "if mobile device connection speed will permit a Web page to be downloaded in a reasonable amount of time," (EX-1004, [0077]), the updated policy settings provided by the server that make the device settings appropriate to access the data (web data) may include updates to the settings that allow for "roaming" on faster networks (or to return to a home network if that is faster). For example, the settings may specify that that mobile device should switch to a different "network interface" or a different "wireless network protocol" such as a WLAN network interface (or protocol) to have the proper download speed to load the web page (and therefore access the data). This specification of faster network would be encompassed by the claimed "roaming control" because it allows for switching between different wireless access networks. EX-1001, 3:62-63.

492. Moreover, Limont specifically identifies (as a problem solved by Limont) the inability of system "administrators" to control the configuration of mobile devices – particularly to protect sensitive information that may be "private." EX-1004, [0006-0015]. Furthermore, given that Limont includes the ability for an authority figure (e.g., "administrator") to oversee individual with less access privilege (e.g., users), a POSA would have found it obvious that Limont's system assists in implementing a "parental control" in which an analogous authority figure (parent) oversee individuals with less access privileges (children). By 2009, a POSA would have understood that an administrator effectively stands in the same position over the corporate users as a parent stands over children when it comes to controlling the usage of devices owned by the corporation (e.g., the family / parents). Parental controls are thus just an obvious variant of the corporate administrator controls.

493. Limont's mobile device connects to networks such as "a Local Area Network ('LAN'), a **Wide Area Network ('WAN')**, or the Internet" using "wireless protocols (e.g., GPRS, GSM, etc….)." EX-1004, [0034], [0038], [0043], [0056]. Those networks include "an **office-wide** or **enterprise-wide computer network**, an intranet, and/or the Internet." EX-1001, [0041]. Therefore, Limont's

managed network expressly includes an "enterprise-wide" wide-area networks. As noted above, one of Limont's goals was to allow an administrator to effectively update and control policies throughout the organization.

494. Thus, a POSA understood that a mobile device having configuration settings that can be used to modify the hardware, network interface, allocated resources, and wireless protocol settings to connect wirelessly through the internet or other wide area network can be used to *assist in implementing enterprise wireless wide-area network (WWAN) management control* for the corporate wireless mobile devices managed by the "administrator" and therefore teaches, or renders obvious this element as well.

495. [This paragraph left intentionally blank].

c) Claim 6: *[6.0] The method of claim 1, further comprising: obtaining a service usage measure, the service usage measure accounting for the one or more communications associated with the wireless end-user device over the wireless access network; and:*

496. Limont discloses this limitation.

497. Limont's settings can be based on "if mobile device connection speed will permit a Web page to be downloaded in a reasonable amount of time" and the mobile will "verify download speed" (*obtaining a service usage measure*). EX-1004, [0073], [0077], [0086]. To be able to make the determination of "if" a download occurs in a "reasonable amount of time," and in order to "verify download speed," the system is necessarily obtaining a measurement of the download speed, rate and/or bandwidth because the "reasonable time" comparison and/or verification of download speed would require such information.

498. As detailed above for element 1.5, these measurements *account[] for the one or more communications associated with the wireless end-user device over the wireless access network*) because those communications being requested, controlled, and serviced (perhaps after a communication modifying the settings) are the communications across the wireless network between the server and the mobile device. EX-1004, [0077], Figs. 1-4. These communications include, for example, the communications on which the connection speed is evaluated as well as the communication of data which is desired (and evaluated against the connection speed for the determination of a "reasonable time.").

499. Wright's client diagnostic modules (detailed in claim 11) provide "usage" logs to the server which correspond to this claim element because those logs reflect express measurements made about the service between the mobile device and servers (such as the communications transmitted updated / encrypted policies, data, and applications.). EX-1005, [0220], [0225] ("network service usage" information]; [0270] (referencing service usage measurements such as "program usage, network access… VPN access, data access…]).

vii. **Claim 6.1:** ***based on the service usage measure, taking an action.***

500. Limont's mobile devices verify the speed (*service usage measure*). The system takes four separate *actions based on the service measure* and whether the measure is "appropriate" for the requested data: (1) if the measure is inappropriate, then the server prevents the data transfer and then modifies the settings (both *actions*); and (2) if appropriate, the server allows / makes the transfer and notifies the mobile (both *actions*). EX-1004, Fig. 4, [0086], [0091], [0061], [0077-0078]. These actions are "based on the" speed measurement because the server takes different actions resulting from an evaluation of the verified speed

against the download speed necessarily to transmit a file in a reasonable amount of time.

501. At a very minimum, Limont's disclosures above would render this claim obvious. One of the reasons that systems take measurements of services (such as the speed of a connection) is to take some action on those speed. Absent such an action, the measurement is merely unnecessary overhead that may impact system performance. Thus, the fact that Limont and Wright disclose the taking of such measurements would render obvious to a POSA to take an action based on that measurement because that would be the typical use case for such measurements.

502. Wright's diagnostic modules perform diagnostic *actions based on* the usage logs as detailed in claim 11, *infra*. EX-1005, [0046], [0052-0059], [0068-0077], [0220]. These actions include repair, running security tests, requesting additional information, sending additional software or policies, and "prob[ing]" a client device for more inforamtion.

503. The '042 Patent copies Limont in identifying a "service usage measure[]" as "projected traffic demand [and] application usage … reported to the

servers for the purpose of provisioning the right amount of data bandwidth … to the device." EX-1001, 13:59-14:2.

504. [This paragraph left intentionally blank].

d) Claim 7: [7.0] The method of claim 6, wherein the service usage measure comprises a measure of a service usage activity.

505. Limont and Wright each disclose this limitation for the reasons discussed for Claim 6 where the *service usage activity* is downloading data (Limont) or "network usage" (Wright). See claim 6 above.

506. The measurement, for example, is the speed in Limont and the "network service usage" in Wright.

507. [This paragraph left intentionally blank].

e) Claim 8: [8.0] The method of claim 6, wherein the action is to verify the service usage measure.

508. As discussed for Claim 6, Limont's "actions" including preventing or allowing the transfer of data, updating the settings and notifying the device. EX-1004, [0078], [0091]. Limont further discloses that one way to determine whether the configuration settings are inappropriate (or appropriate) and/or to comply with

the modified settings is to verify the download speed (*verify the service usage measure*). EX-1004, [0086].

509. Wright's "remote diagnostics module 224 [discussed below for claim 11] may also probe a particular client to verify its status" including "policy settings on the device, and attributes in accordance with those settings, for example, which ports are blocked." EX-1005, [0057]. Wright's diagnostic module also orders "audits" and receives "audit logs" (including the results of "tests") which a POSA would understand to render obvious the verification of measurements service usage in light of Wright's policies specifying network usage and data access. EX-1005, [0054], [0068], [0076-0077], [0104-0123], [0138], [0269].

510. For example, Wright describes the "it is verified whether the indications of the installation of the network interface cards (NICs) is accurate" (EX-1005, [0073]) which corresponds go Limont's settings and determinations related to the "network interface" (of which the NIC is one). EX-1004, [0040-0041], [0073], [0085], [0087].

511. Thus, for example, Limont's settings might reflect the existence or installation of a particular network card (which is a measurement of network service usage because the absence or presence of such a card reflects either the

capability or lack thereof of such network service usage) and Wright's teaching is a policy that verifies such existence. A POSA would understand it to be obvious to verify the existence as the action in response to a determination using the settings that a particular network card (or other software such as plug-ins) is needed to allow for access to Limont's maintained data.

512. Wright describes numerous other verification related to network service usage measurements including verifying whether particular network services are available and being used, verifying the parameters of the network service usage stack (EX-1005, [0202]).

513. Similarly, Wright describes that "several network characteristics" may be 'verified" based on the policy assessment. EX-1005, [0210]. These include verification of the site being used, location of usage, the MAC address of the access points being used. EX-1005, [0210]. These are all measurements of service usage activities as per claim 6 because they measure an aspect of the service usage (e.g., location of the service usage) and then take action to verify it.

514. Wright also describes the actions to verify that the applications, protocols, and VPN used for service usage are enabled or running. EX-1005, [0238-0240]. These are all measurements of service usage activities (because the

applications, protocols, and VPN reflect such usage) and actions taken to verify that usage.

515. Based on service usage measurements, Wright describes the ability to verify files, checksums, and registry entries. EX-1005, [0069-0071]. It would be obvious to perform such verifications based on network service usage logs returned to the server to allow for the server to perform its repair actions as described in claim 11 below.

516. [This paragraph left intentionally blank].

f) Claim 9: *[9.0] The method of claim 6, wherein the action is to quarantine or suspend the wireless end-user device*

517. Limont discloses this limitation.

518. Limont discloses preventing the download of data (*action is to suspend*) to an inappropriately configured mobile device (*wireless end-user device*) as detailed in [1.2], [1.3], [1.4]. EX-1004, [0091]. For example, after Limont's system measures the connection speed, it may quarantine or suspend the device by not allowing or preventing the transfer of the requested data. Limont specifically contemplates such action and the benefits of such a quarantine or suspension:

> Accordingly, embodiments of the present invention can be used to reduce the likelihood of a device with inappropriate configuration settings being able to access data. For example, configuration enforcement manager 193B can potentially prevent the download of data to an inappropriate [sic] configured mobile device. Preventing the download of data that can not be appropriately processed conserves network bandwidth and systems resources.

519. EX-1004, [0091]. "Download of data" that cannot be appropriately processed includes attempts to download data for which the connection speed is too slow to meaningfully use that data. Thus, in that situation, suspending that specific request conserves resources.

520. Limont also discloses a "wipe" action which a POSA would recognize as quarantining or suspending the device because the "wiping" would remove the information needed to access data including, for example, credentials such as usernames, passwords … that are used to access the corporate data through corporate servers. EX-1004, [0047-0049], [0071]. Thus, for example, if a particular service usage report from Limont (or Wright's) mobile devices indicates unusual service usage (either by applications, or too much usage, or too slow), the proposed combination might attempt to "repair" the mobile device by performing a wipe operation which would allow the device to reset itself. Such an action would

be obvious to a POSA in light of the ability to measure service usage and actions that result in quarantine or suspension such as wiping, repairing, and denying service.

521. [This paragraph left intentionally blank].

g) Claim 10: *[10.0] The method of claim 6, further comprising obtaining secondary information associated with the wireless end-user device, and wherein the action is to verify the service usage measure using the secondary information.*

522. Limont discloses this system.

523. As discussed for Claim 6, Limont discloses obtaining a service usage measure in the form of download connection speed. Further, Limont discloses obtaining information regarding the correct plug-ins on a mobile device, and information regarding whether sufficient resources have been allocated to a mobile device (*obtaining secondary information associated with the wireless end-user device)*, in order to determine if sufficient resources have allocated at a mobile device or if a mobile device includes correct plug-ins for viewing content (*action is*

verify the service usage measure using secondary information). EX-1004, [0077], [0086].

524. Such service usage measurements can be verified by, for example, the settings reflecting the "sufficient resources" which may include sufficient memory and allocated bandwidth (and the correct operation of, for example, plug-ins). A POSA would have found such verification to be obvious because it beneficially allows the system to possibly determine whether the network service usage report actually reflects the operation of the device including a correct configuration or whether such usage reflects, for example, conditions that are unrelated to, and cannot be fixed by, the configuration such as network congestion on one or more of the links in the communications path.

525. As detailed for claims 6, 8, and 11, Wright's diagnostic module requests, and receives diagnostic information (including network usage information) from the mobile client ("secondary information") and performs processing on those logs. A POSA would understand this to render obvious the claimed verification for the reasons stated in claim 8.

526. [This paragraph left intentionally blank].

h) Claim 11: *[11.0] The method of claim 1, further comprising receiving, from the wireless end-user device, an integrity report configured to assist a network element in identifying an access control integrity violation.*

527. Limont in combination with Wright discloses this limitation.

528. As discussed in the Motivation to Combine section above, Limont discloses that the policy settings should be "locked down" and protected on the wireless device, but does not expressly disclose an integrity report to assist a network element in identifying an access control integrity violation.

529. Moreover, Limont discloses the ability to remotely "wipe" data on the mobile device (including wipe's controlled by Limont's server [*network element*]) to "limit the ability of malicious user to access data." EX-1004, [0047-0049], [0071]. A POSA would have recognized the value of receiving integrity information that would allow the server to determine if the mobile's data needs to be "wiped." For example, if the integrity information (such as the checksum) indicated that the critical passages of memory (such as policy information as discussed herein) had been altered, modified or corrupted, the administrator can

take repair action to wipe the device to ensure that the information cannot be used by "malicious users" or 'hackers" to access corporate data.

530. Wright discloses a client diagnostics module 246 on the wireless mobile that performs audits of all files to verify no corruption (e.g. checksum) (*integrity report*) and for security violations and registry errors.

> [0068] The policy setting module 212 communicates the current security policy to the policy enforcement control module 214 via a communication interface implemented in the same manner described in any one of the examples discussed above with respect to the location detection module 208 or in any manner known to those of ordinary skill in the art. The policy enforcement module 214 comprises one or more enforcement mechanism modules as specified by the policy. For example, in a communication session between the mobile device and another computer in which data is being transferred over a wireless connection, based on this connection type, in one example, the enforcement module 214 may prevent certain files from being transferred over the wireless connection as opposed to the cases in which the data is being transferred over a wired connection, or the case in which 802.11i cryptography is being used over the wireless connection. Again, in an alternate embodiment the policy enforcement control module 244 may operate as part of a separate computer system that transfers commands over a network to the mobile device. In the illustrated embodiment of FIG. 2B, a remote diagnostics module 246

> processes events and performs audits relating to processing performed by one or more of the modules. The remote diagnostics module 246 transmits over a network 204 diagnostic information to the remote diagnostic module 224 on the server computer system. Examples of tasks that the diagnostics module 246 performs in order to obtain diagnostics information are as follows:
>
> [0069] Verify that correct files are in correct locations.
>
> [0070] Verify (e.g. checksum) all files to verify no corruption.
>
> [0071] Verify time/date stamps for correct versions.
>
> [0072] Check for outdated installation (INF, PNF) files.
>
> [0073] Verify that all registry entries are correct and correct any errors found. For example, it is verified whether the indications of the installation of the network interface cards (NICs) is accurate.

531. EX-1005, [0068-0073].

532. Notably, the '042 Patent specifically identifies "checksums" as one form of integrity check. EX-1001, 17:6-23.

533. Checksums allow for determination if, for example, memory has been changed / modified or corrupted. Checksum essentially performs certain mathematical operations on blocks of data (such as in memory) to calculate a "checksum" value. If the memory has been changed, then the "checksum" for that block of data will change (reflecting that the memory has been changed / modified / corrupted).

534. In Wright, a remote diagnostics module 224 (*network element*) receives the audit logs from a client device and analyzes the audit information (including the checksum information).

> The remote diagnostics module 224 is illustrated in the context of a server computer system embodiment 200 in FIG. 2A concerned with security or protection of data accessible by mobile client devices. However, the remote diagnostics module 224 may also function to provide diagnostic support for computer problems generally encountered by mobile client devices independently of security related software. In this embodiment, the remote diagnostics module 224 provides diagnostic assistance and/or corrective instructions with respect to problems not only associated with security…

535. EX-1005, [0053]. The information transmitted to the server includes "current version of the security policy software components on the client device" which would allow the server to potentially determine if the secure information has been altered or corrupted. EX-1005, [0057]. The versions of such software can indicate if the device has old (or improperly installed) software that reflect an access control integrity violation because it reflects that some user (perhaps a malicious user) has installed files or software that are not the correct ones or not the authorized ones or not the most current version.

536. The remote diagnostic module may provide a repair to a problem in the client device, determine that a trend is occurring for the device, or determine that preventive maintenance is to be scheduled for the client device (*receiving, from the wireless end-user device, an integrity report configured to assist a network element in identifying an access control integrity violation)*. EX-1005, [0046], [0052-0054], [0057-0059] ("diagnostics information [] is sent to the remote diagnostics module 224 of the server…"), [0068-0077], [0220]; Fig. 11. In Wright's system "support information may be in the form of instructions or code to the client device to repair a problem or perform maintenance" which "provides an advantage of taking corrective or preventive actions without requiring user intervention or action." EX-1005, [0055]. Wright's client "may also run tests with respect to the security policies" such as security violations with the output of such tests transmitted to the server. EX-1005, [0076]. These reflect the claimed reports receive from the wireless end-user devices.

537. A POSA would have been motivated to modify the Limont's teachings to include a diagnostic module to audit the policy settings as taught by Wright in order to protect and lockdown the policy settings on the wireless device. Moreover, such an integrity report can provide information to Limont's

administrator that secure data (such as encryption keys, user-id, passwords, and PINs) have been compromised thus allowing the administrator to take corrective or repair action such as the "remote wipe" action discussed above. EX-1004, [0047-0049]. Thus, Limont's security is beneficial enhanced by Wright's integrity reports and corresponding actions.

538. Wright's disclosure of using an audit as an integrity report is consistent with the disclosure of the '042 Patent an access integrity function includes audit scans of memory and files on the wireless device to detect unauthorized data. The audits are reported to controller to identify access control integrity violations. EX-1001, 10:3-20. The audit scan can use checksums or other information that may be indicative of tampering, corruption, and/or a compromise of any of the data.

539. [This paragraph left intentionally blank].

i) Claim 12: *[12.0] The method of claim 1, wherein the configuration information comprises at least a portion of the service profile.*

540. Limont discloses this element.

541. As noted in [1.6], the claimed "*configuration information*" is sent from the server to the mobile device to modify at least one of the "*service policy settings*."

542. As discussed for element [1.4], Limont's "*service profile*" is a "group of one or more configuration settings" identified by Limont's "configuration [policy] version." EX-1004, [0075]. For example, Limont identifies an exemplary "group of one or more configuration settings" ("service profile") with a configuration / policy "version." EX-1004, [0073], [0075]; Fig. 3.

543. Limont's Fig. 3 shows Limont's "configuration settings" (e.g., settings 191B, K, N, R) that correspond to a "service profile" identified by Limont's "version 192C" transmitted to the mobile device in the **purple arrow**.

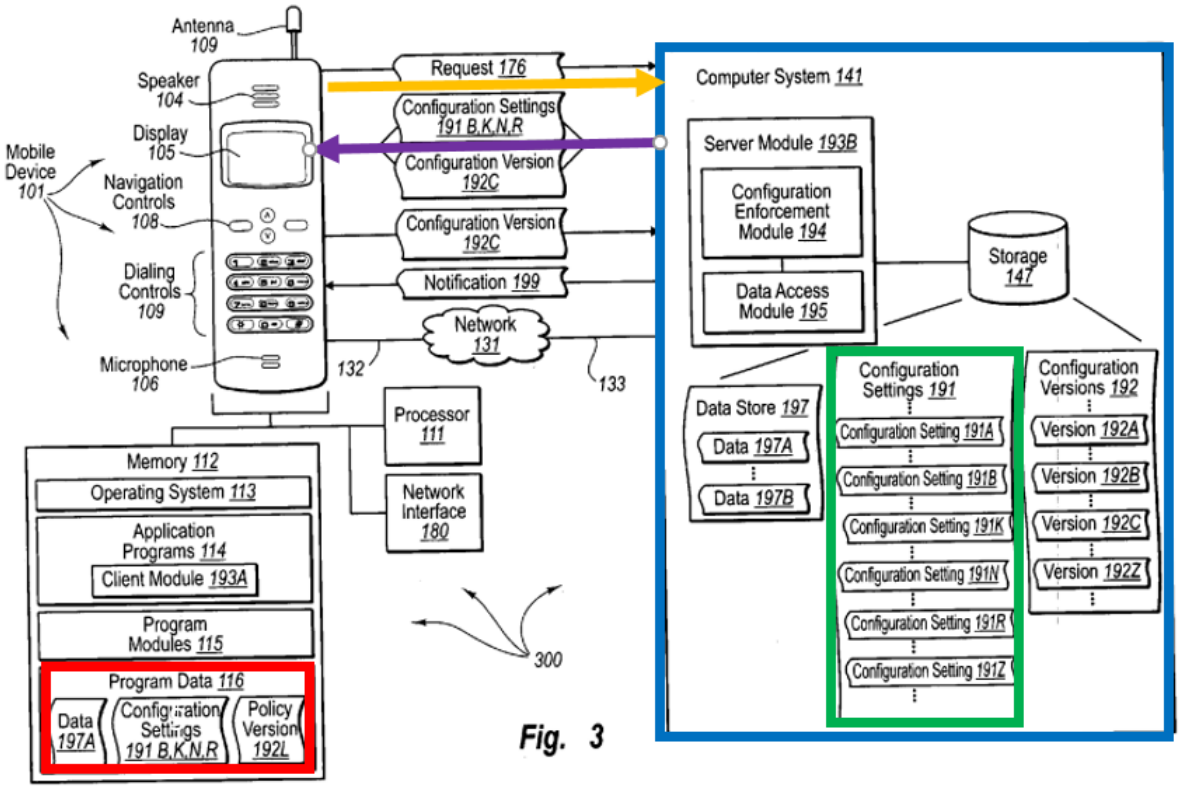


Fig. 3

544. EX-1004, Fig. 3.

545. Because the "service profile" identified by "version 192C" includes all four of "settings 191B, K, N, R," each transmitted "configuration setting" is "*a portion*" out *"of the service profile*" (the group of these four settings identified by the "version") as is the "version 192C."

546. This analysis applies to the Fig. 1 components (settings 117, version 192). The "service profile" is the group of settings 117A, B, F H along with, and identified by, the "version 118D." Thus, the transmission of all of these settings

(and the version) shows the claimed configuration information (transmitted settings) is at least a portion of the service profile (the collection of all of these settings).

547. [This paragraph left intentionally blank].

j) Claim 13: *[13.0] The method of claim 1, wherein the service control link is secured by an encryption protocol.*

548. Limont discloses this limitation.

549. Element 1.1 discusses communication links 132, 133 (*service control link*). Limont further discloses computer systems receiving a policy update to use "a specified version of encryption algorithm." EX-1004, [0009]. While this is in the context of a "wired" system, a POSA would understand this to be a teaching to use encryption techniques on the links between the server and the client devices to prevent "hackers or malicious users" from accessing the data. EX-1004, [0012-0013].

550. Moreover, Limont also identifies the problem users that "access data wirelessly" are at "increased risk of a malicious user" accessing the confidential information. EX-1004, [0013].

551. Given these teachings, a POSA would have found it obvious that well-known encryption algorithms and protocols would be used to secure the communications links between Limont's wireless mobile devices and the servers on which the corporate data was stored. Such encryption would beneficially enhance the data protections for Limont's traveling users accessing data wirelessly.

552. Furthermore, Limont teaches that "wireless protocols" such as "GPRS [and] GSM" are used for the communications link. A POSA would understand that such wireless protocols use encryption protocols to protect the data transmitted wirelessly (or else every device could intercept such data) or, at a minimum, that it would be obvious to use such encryption protocols for wireless transmissions at least on the wireless links.

553. Moreover, given that Limont contemplates that the "Internet" may form part of the communication links (EX-1004, [0034]), a POSA would have recognized that well-known techniques existed as of 2009 to protect confidential data in Internet transmissions. Such well-known techniques included end-to-end encryption such as by use of the well-known HTTPS transmissions and techniques such as VPN that used encryption and were widely deployed for corporate users as of that time.

554. Moreover, Wright further discloses types of network services according to a policy can include service protocols for transferring data over a network (*service control link*). The service protocols can include Virtual Private Network (VPN) and HTTPS which encrypt the data across the communication link. EX-1005, [0009], [0223], [0279], FIG. 8 (element 820). As noted above, such techniques were widely known and pervasively used by 2009. It would have been an obvious modification to Limont's transmissions to use these techniques with the known benefits of protecting the transmitted data.

555. In addition, Wright discloses TLS and SSL service protocols which are known to encrypt data/communications over the network including for VPNs. EX-1005, [0265-0267], [0279]. A POSA would be motivated to modify Limont's teaching that: (1) wireless devices are less secure (and therefore would benefit by securing the links with encryption) and (2) by encrypting the communication links to allow secure communication between the wireless device and computer as taught by Wright for the reasons discussed in the Motivation to Combine section. Such techniques are particularly obvious in light of Limont's stated concerns of protecting data being accessed from remote locations across untrusted networks such as wireless networks.

556. A POSA would have had a reasonable expectation of success because adding such known techniques from Wright that were widely used to protect data across transmission links reflected merely the use of known techniques for their known purposes to achieve the known and expected result of data protections.

557. Furthermore, Xu describes using encryption techniques (such as in Wright) and provides a further motivation to combine such encryption into Limont's communications links.

558. [This paragraph is left intentionally blank].

k) Claim 14: ***[14.0] The method of claim 1, wherein the device service state comprises a service profile setting, a service usage policy setting, or a device-assisted services (DAS) setting.***

559. Limont discloses this element.

560. Limont discloses several examples of this limitation as also detailed in element 1.1. For example, Limont configuration / policy version (*service profile setting*) is a reduced set of data that represents one or more configuration settings as also detailed in claim 12. EX-1004, [0075].

561. Limont's mobile device's policy settings include the mobile device connection speed (*service usage policy setting*) sufficient to download a Web page in a reasonable period of time as detailed in claim 6. EX-1004, [0077].

562. As detailed in element 1.1, these different settings may be transmitted from the device to the network as part of the device service state although this claim does not require such transmission.

563. For example, such settings may include "operating system settings, application program settings, hardware settings, allocated resource settings, network interface settings, wireless protocol settings, etc." EX-1004, [0073]. They also include "a Personal Identification Number ("PIN") lock activation setting, a minimum PIN length setting, a PIN format setting (e.g., alphanumeric or numeric), a number of PIN failures permitted before performing a local wipe setting, a number of PIN failures after which an override "passcode" must be entered setting, a force wipe on next connection to server setting, a client application version setting, a protocol version setting, a protocol commands allowed setting, a custom application permitted setting, a time interval for enforcing compliance setting, a remote wipe enabled setting, and a require policy check setting." EX-1004, [0047].

564. The service usage policy setting is rendered obvious by various wipe settings because such settings can control whether service usage is permitted or not by wiping the ability to access services.

565. Moreover, "service profile settings" are rendered obvious (at least) by network interface settings, wireless protocol settings, and protocol version settings because such settings provide the information to provide service such as service plan information and identification of the parameters for such service.

566. [This paragraph is left intentionally blank]

l) Claim 15: [*15.0] The method of claim 1, wherein the device service state provides information about a user preference.*

567. Limont and Wright disclose this limitation.

568. Limont discloses that policy settings reflecting the device service state can include Personal Identification Number ("PIN") lock activation settings, which *provide information about a user preference* because the user's selection of a "PIN" discloses, or renders obvious, a user preference.

569.

[0047] Policy settings can include: a Personal Identification Number ("PIN") lock activation setting, a minimum PIN length setting, a PIN format setting (e.g., alphanumeric or numeric), a number of PIN failures permitted before performing a local wipe setting, a number of PIN failures after which an override "passcode" must be entered setting, a force wipe on next connection to server setting, a client application version setting, a protocol version setting, a protocol commands allowed setting, a custom application permitted setting, a time interval for enforcing compliance setting, a remote wipe enabled setting, and a require policy check setting.

[0048] Generally, if a PIN lock setting is activate (or TRUE), a user of a mobile device must enter a PIN through an input interface (e.g., dialing controls) to unlock the mobile device. If a specified number of incorrect PIN entries are detected, the mobile device can initiate a local wipe of memory contents.

[0049] Remote (or server initiated) wipe settings can include: a user agent string setting providing a human readable indication the involved mobile deice (e.g., Trey-T5600/1.2), a DeviceID setting uniquely identifying a mobile device and resolve ambiguity between devices using the same user agent string, a pending remote wipe setting indicating if a mobile device has been designated for a storage wipe, remote wipe timestamp setting indicating a wipe action and when the wipe action occurred.

570. EX-1004, [0047-0049]. For example, the claim merely requires "information about" a user preference. Given that the user's secret PIN is a user preference, the settings about the PIN are "information about" the PIN such as "information about" the length, format, and incorrect entries for the PIN meet, or render obvious this claim element.

571. Moreover, Limont's request 176, request 164, and command 161 (*information about device service state* as per element 1.1) indicate the user's selection (preference) as to the specific data (including types such email, web content or other data) the user wants to access. EX-1004, [0044], [0054-0055]; [0067-0069], [0080]. The "user preference" is the type and content of the requested data maintained on the server. The "information about" such a user preference is reflected in the device's service state that allows for entry, storage, request, receipt and display of the user-requested data. All of this information would be stored on the mobile device (e.g., in the application or operating system data) and reflects the device's current service state (the state of requesting/receiving/displaying the desired service data).

572. Wright's teachings include that there is a "settings application" on the mobile device giving a user the "[a]bility to modify" or "override" settings such as

"visual settings" and "location." EX-1005, [0078-0103]. Wright's "user interface module 218" allows users specify "supplemental policy definitions or customization of policy definitions based upon user input" and other "aspect of a policy." EX-1005, [0061], [0065], [0173], [0178]. Such "settings" and user-customizable policy aspects are part of the *device service state* and are *information about a user preference*. For example, the override settings allow the user to prefer certain aspects of the device's service state including the visual settings (e.g., such as the brightness of the screen and/or the arrangement of different applications' information on the screen). The override on location allows the user to specify the current location which is used in the policy assessments as discussed above. Thus, each of these would render obvious the claimed device service state providing information about user preferences.

573. Furthermore, a POSA would understand that a mobile device would store "*information about a user preference*" as part of its programming to provide services to a user. For example, as noted in Wright and Limont, the mobile devices provide user interfaces that allow users to enter and customize features of their mobile device. Common user preferences that would be stored in the device service state would include usability features such as volume or brightness of a

screen, connection features such as the specific networks to which a user prefers to connect for communications, identification of the applications that the user preferred to install, the user's username, and addresses for connecting to frequently used sources of data. Each of these would render obvious to a POSA that the device service state provides (including stores) information about user preferences and each of these was prevalent on mobile devices such as phones prior to the 2009 priority date of the '042 Patent.

574. This claim does not require the "user preference" to be transmitted to the server – merely that the "device service state" present on the device "provides information about a user preference."

575. [This paragraph is left intentionally blank].

m) Claim 16: *[16.0] The method of claim 1, wherein the device service state comprises information associated with an encryption key.*

576. Limont and Wright disclose this limitation.

577. Limont's "[p]olicy updates" may force using a "specified version of encryption algorithm [and] a specified key length." EX-1004, [0009]. This information is "*information associated with an encryption key*" that is part of the

device's service state because such encryption key is stored by the device and used by the device as part of its provision and access to services such as email and Web browser functionality described in Limont above.

578. As noted in element 1.1, the "device service state" is broadly defined in the '042 Patent. It encompasses "information reported from the device and received or derived outside the device that is required to adequately define the actions needed from the service controller to maintain proper [] system operation." EX-1001, 17:46-18:11. Limont's "specified version of encryption algorithm [and] a specified key length" (EX-1004, [0009]) is required to define the actions needed from Limont's servers to properly be able to access information (at a minimum, over any wired connection).

579. The claimed "information" is not required to be transmitted. Thus, Limont's disclosure of such "wired" information (above) teaches, including rendering obvious, that the "device service state" would include the claimed information about encryption keys to allow for communication across wired and wireless links because a POSA would recognize that such encryption is beneficial to both forms of communication (wired and wireless) and also that many mobile devices include the ability for wired and wireless communication as referenced in

Limont (such as laptops with Ethernet connectors for LAN access or mobile phones with wired connectors to access networks through wired networks). See claim 12.

580. Moreover, Limont in view of Wright discloses this limitation. As detailed in element 1.3, Wright's mobile device stores and uses "cryptographic information" which is a "key for user with a cryptographic authentication protocol" that is stored in configuration information such as policies sent to the mobile device. EX-1005, [0078-0103]. Thus, when Limont transmits its stored "policy settings" (*see* element 1.1), those settings would include the encryption keys (or, at a minimum, information associated with an encryption key) associated with the policies. Such storage and usage meets the broad definition of device service state provided in the '042 Patent.

581. Wright's keys allow the mobile device to authenticate updated policies. EX-1005, [0130-0131]. Moreover, Wright's communication between the mobile device and the server (to send / receive, for example, Limont's policy settings) uses a secure protocol that involves the transmissions of "information associated with an encryption key" to establish the session. EX-1005, [0133-0159].

582. A POSA understood that using an encryption key to limit access to stored data "reduce[s] the likelihood of a compromised device or a device with noncompliant policy setting being able to access data" and would be confident of its success, as discussed in the Motivation to Combine section. EX-1004, [0071].

583. [This paragraph is left intentionally blank].

n) Claim 17: *[17.0] The method of claim 1, wherein the device service state comprises an agent report, a service usage record, a transaction record, or an integrity report.*

584. Limont and Wright discloses this limitation.

585. As detailed above in element 1.1 and claims 12, 15-16, the "device service state" is broadly defined and would encompass the disclosures of information stored by Limont and Wright.

586. Limont and Wright discloses the *device service state* as discussed with reference to claim element 1.1.

587. They also discloses a *service usage* measure (*record*) (e.g., measurement of connection speed and evaluation thereof in Limont and the

"usage" logs in Wright) as discussed in Claim 6, and further disclose an *integrity report* as discussed in claim 11.

588. Wright further discloses a "transaction record" in the "status, usage and error logs" and the "status, configuration, error logs, audit logs, and debug information" that Wright's client stores and transmits to the server as detailed in claim 11. EX-1005, [0220], [0269]. Wright also stores and reports "diagnostic information such as events, or audit logs" such as "system event logs, crash dumps and diagnostic outputs…" EX-1005, [0054], [0074], [0079]. Each of these forms of logs records "transactions." For example, an "event" may include the transaction of an application logging its location:

> Alternatively, in the embodiment of FIG. 2B, any one of the modules (e.g. 206, 208, 210, 212, 214, 218, 245) may have an event logging module and/or an auditing module which sends diagnostic information to the remote diagnostics module 224. In one example, each of the event logging module or the auditing module may record events pertinent to its respective module (e.g. location detection module 208). In another example, either or both of the event logging module or the auditing module may process events and perform audits relating to the processing performed by more than one of the modules.

589. EX-1005, [0077]. It also helps track the parameters, such as the IP address for specific transactions.

> An event logging module may be helpful in tracking which parameters match successfully on a consistent basis. In the above example, the client user or an administrator may view the event log and see that there has never been a match for DNS3 since the "work" location was defined. This may indicate that a check of the IP address for DNS3 may be in order to verify it was entered correctly. In another example, this trend may be noted by the monitoring module 226 on the server side or the client diagnostics module 246 on the device. If it is not the current location, it is determined 626 if it is another defined location. If so, then the policy setting module is notified 628 that the location has changed to this other defined location, and the next set of N parameters is processed 604.

590. EX-1005, [0197]. See also [0225], [0251]. "Events" are illustrated in Figs. 10A and 10B and described in [0278-0285]

591. To the extent that this claim requires that information recited in the claim be transmitted to the server (it does not recite such transmission), a POSA understood that the s*ervice usage* measure or *integrity report* could be provided to the server in the device service state information so it can be "determin[ed] if a requesting mobile device's policy setting are appropriate for accessing data." EX-1004, [0077]. Such reports (as noted in Wright) are beneficially used by the server to adjust the policies and to diagnose and address any issues (e.g., unauthorized

access / unusual access or need for repair or additional diagnosis or wiping as noted in Wright and Limont)

592. [This paragraph is left intentionally blank].

o) Claim 18: ***[18.0] The method of claim 1, wherein the device service state comprises user status information, device status information, application status information, a device location, or a device quality-of-service (QOS) state.***

593. Limont and Wright disclose this limitation.

594. As discussed for claim limitation 1.1, Limont teaches that the configuration settings (*device service state*) maintained on the mobile device (and potentially transmitted between the server and device) can include "application program settings" (*application status information*). EX-1004, [0073], [0085].

595. Limont's settings can also include "current configuration of one or more of an operating system, an application program, hardware, allocated resources, a network interface, and wireless protocol settings, at the mobile device." EX-1004, [0087]. The claimed "*device status information*" encompasses

each of these forms of settings because they each provide information about the current status of the mobile device.

596. Thus, Limont discloses this claim.

597. Furthermore, Limont's server module determines whether sufficient resources (*device status information*) have been allocated at the mobile device in response to the mobile device request, which can include determining if correct plug-ins for viewing content are included at the mobile device (*application status information*) or if the mobile device connection speed to download a webpage can be accomplished in a reasonable amount of time (*device QOS/device status information*). EX-1004, [0077].

598. Wright discloses that its device service state stores and uses the device's location. EX-1005, FIGs. 2B ("Location Detection Module"); 3A (element 302); 3D-3E (both "detecting a location…" for the device); [0174-0212] (all using the device's location).

599. [This paragraph is left intentionally blank].

B. Ground 2: The Challenged Claims Are Obvious Over Limont in combination with Wright and optionally Xu in further view of Polson.

600. Challenged Claims 3-5 recite an "intermediate networking device" that "forwards" data or "assists" other devices in communicating.

601. Polson describes a portable client device that receives policy updates from the network, enforces those policies and allows for forwarding of data between the WWAN and WLAN to assist end-user devices in accessing the various network

602. Polson's gateway is the type of device that Limont uses in its network to update and control policies. Polson's client device acts as a gateway between the WWAN and WLAN to forward data between the two networks pursuant to policies programmed by the network.

603. [This paragraph is left intentionally blank]

1. Motivation To Include Polson In The Combination.

604. A POSA would have been motivated to consider, and include, Polson's disclosure of its client device with Limont and the other two references in the Proposed Combination.

605. Polson provides a further exemplary client device of the type used in Limont with complementary and overlapping functionality.

606. Limont is directed to a managing, enforcing, and updating configuration settings (policies) on client devices such as mobile devices.

> The present invention extends to methods, systems, and computer program products for enforcing device settings for mobile devices. Generally, a computer system enforces appropriate mobile device settings (e.g., policy and/or configuration settings) prior to permitting a mobile device to access maintained data. The computer system receives a request from a mobile device. The computer system determines that current mobile device settings are not appropriate for accessing the maintained data. The computer system sends device settings, representing a new mobile device configuration that is appropriate accessing the maintained data, to the mobile device. The computer system receives an indication that the mobile device is configured in accordance with the device settings. The computer system permits the mobile device to access the maintained data in response to receiving the indication that the mobile device is configured in accordance with the device settings.

607. EX-1004, Abstract.

> [0016] The foregoing problems with the prior state of the art are overcome by the principles of the present invention, which are directed towards methods, systems, and computer program products for enforcing device settings for mobile devices. Generally, a computer system (e.g., an electronic mail server) enforces an

appropriate mobile device configuration prior to permitting a mobile device to access maintained data. The computer system receives a request from a mobile device. The request requests that the mobile device be permitted to access data maintained by the computer system, the request indicating a current mobile device configuration of the mobile device.

[0017] The computer system determines that current mobile device configuration is not appropriate for accessing the maintained data. The computer system sends device configuration settings to the mobile device. The device configuration settings representing a new mobile device configuration that is appropriate accessing the maintained data. The computer system receives an indication that the mobile device is configured in accordance with the device configuration settings. The computer system permits the mobile device to access the maintained data in response to receiving the indication that the mobile device is configured in accordance with the device configuration settings.

[0018] In some embodiments, a computer system enforces mobile device access policies prior to permitting mobile device access to maintained data. The computer system receives a data command from a mobile device. The data command indicates a policy version representing the current policy settings at the mobile device. The computer system determines that the current policy settings at the mobile device are not appropriate for accessing data maintained by the computer system

608. EX-1004, [0016-0018].

609. Limont identifies "mobile devices" as a broad category that encompasses the ability for humans to transport.

> A "mobile device' is defined as a subset of computer systems that primarily (or solely) access networked data using wireless mechanisms and are easily transportable by a human….

610. EX-1004, [0036]. Limont also notes that its invention can be practices with "many types of computer system configurations."

> [0037] Those skilled in the art will appreciate that the invention may be practiced in network computing environments with many types of computer system configurations, including, personal computers, laptop computers, hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, mobile telephones, PDAs, pagers, and the like. The invention may also be practiced in distributed system environments where local and remote computer systems, which are linked (either by hardwired data links, wireless data links, or by a combination of hardwired and wireless data links) through a network, both perform tasks. In a distributed system environment, program modules may be located in both local and remote memory storage devices.

611. EX-1004, [0037].

612. Polson's WLAN / WWAN gateway device includes embodiments that are "easily transportable by a human."

> [0027] [G]ateway 108 may be adapted to be powered through … an internal or external battery. Inclusion of the [battery] power supplies enables the gateway 108 to be used in portable settings. For example, teams of users may carry the gateway 108 in a briefcase or bag.

613. EX-1008, [0027-0028]. Polson's "gateways" are not limited to any form factor but are "any computing device" capable of forwarding data between the WWAN and WLAN networks.

> [0026] Further, as is used herein, the term "gateway" refers to **any computing device capable** of facilitating transmission of data from one or more LANs to one or more WWANs, and transmission of data from the one or more WWANs to the one or more LANs. The interfaces, sockets, subscriber determination logic, routing engine, other processes, and storage comprising the gateway 108 may, in some embodiments comprise a single enclosure. Additionally, gateway 108 may be provided with LED lights and display screens on the gateway 108 or on an attached peripheral device to indicate the status of the gateway 108 as well as the status of the LAN and/or WWAN connections.

614. EX-1008, [0026].

615. Thus, Polson's gateway falls readily into the category of devices identified by Limont as benefiting from Limont's policy management system. The various devices ("personal computers, laptop computers, hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, mobile telephones, PDAs, pagers, and the like") all provide the computing functionality to forward data and enforce policies as is described for Polson's gateway. Limont describes it devices as having various "network interface settings, wireless protocol settings" (EX-1004, [0073] which teaches, or renders obvious, that Limont's devices include network interface cards to implement WLAN and WWAN wireless protocol settings. "For example, a sales person executive may use a mobile device to connect to a corporate LAN through an external GPRS service provider (e.g., a mobile phone company) to access e-mail." EX-1004, [0011] (a teaching of a WWAN network interface).

616. Polson assists Limont in addressing the problem of traveling corporate users.

617. Limont describes extensively that one of the problems to be solved is to allow corporate administrators to ensure that policies can be updated for devices used by employees outside the normal "wired" offices. EX-1004, [0005-0015].

> Computer system users typically desire available and flexible access to their data regardless of location and/or the type of computer system that will be used to access the data. For example, sales personnel and executives may frequently be out of the office on business travel and while traveling may need access to corporate data….

618. EX-1004, [0010]. Thus, corporate administrators needed solutions (as provided in part by Wright) for enforcing policies for traveling users.

619. A POSA would have recognized that Polson's mobile / portable gateway provides an ideal device to effectuate Limont's policy enforcement for traveling users. Polson's portable gateway allows for an additional layer of enforcement for Limont's access policies for traveling users. For example, Polson's ability to forward data between devices would allow teams of traveling corporate users to share a single WWAN connection which, in 2009, would be beneficial.

620. Furthermore, a POSA would recognize that the ability for Limont's traveling users to include a device (such as Polson's) with the ability to provide a

WLAN connection for use of a WWAN network would benefit the traveling users. For example, a user may not have WWAN connectivity on his / her laptop device. Polson's portable WWAN / WLAN gateway would allow the user to still use the laptop as connected to the WWAN / WLAN gateway (perhaps implemented in a mobile phone or other portable device) and provide beneficial additional functionality and ability to use the corporate resources while traveling.

621. A POSA would have recognized that Polson's layer of policy enforcement at the WWAN/WLAN gateway can be used to supplement (or even replace) Limont's policy enforcement of other end-user devices (such as mobile phones or laptops). For example, Limont's policies related bandwidth and connection speed would have particular application to a shared WWAN connection such as provided in Limont. Moreover, the centralized point of control for the WWAN connection would allow the administrator the ability to control the WWAN access (and thus the entire pipeline) with less effort and impact because it is a centralized point of control for access. Rather than distributing the WWAN access policies to all devices, it could be distributed to the WWAN / WLAN gateway and then multiple devices can access the WWAN through the WLAN.

622. Polson provides a similar solution. Polson's gateway allows for downloading customized policies specific to subscriber agreements and such "customization may be implemented by a wireless service provider for a certain customer, for example for a large corporate customer of the wireless service provider." EX-1008, [0037]. Thus, Polson's gateway would add the benefit to Limont of applying customized corporate policies across all corporate users of the WLAN provided by Polson's gateway and allowing sharing of that gateway among users.

623. Furthermore, as noted in element 1.1, Limont allows the policies on the managed mobile devices to be changed to reflect additional needs of the mobile users. Polson almost exactly matches this ability in allowing for its mobile users to change their subscription as needed and update the related policies to match the new capabilities of the subscription.

> [T]he subscriber determination logic of gateway 108 may facilitate a subscriber in altering their existing WWAN 112 access ability on attempting WWAN 112 access via gateway 108. In some such embodiments, the subscriber may be able to change their service agreement to one that allows for WWAN 112 access via gateway 108, or to purchase WWAN 112 access on another basis, e.g., a certain period of time, a certain quantity of bytes downloaded, etc. An

> example of a service agreement that does not permit use of gateway 108 may be a service agreement that envisions the subscriber only being able to use a single computer at a time to access the carrier's WWAN 112. Another example of a service agreement that doesn't permit a gateway 108 is one that's designed specifically for a phone. In a subset of such an example, the service agreement may permit use of gateway 108, but only in connection with a single computer at a time.

EX-1004, [0031].

624. Polson's "gateway may also facilitate a subscriber in altering the features of his/her service agreement" and change features such as "a quality of service, a throughput limitation, and a data transfer rate limitation" that are provided in "policies" transmitted to the gateway by a "server."

625.

> [0078] In various embodiments, the gateway may then determine whether its WWAN interface is associated with a service agreement with a wireless service provider, block 806, the service agreement having one or more features outlining gateway usage benefits and restrictions. The gateway may determine the existence of the service agreement and one or more features of any such agreement in a number of ways. The gateway may inquire of a server, such as a server associated with the gateway or with a wireless service provider,

> as to the existence and features of a service agreement associated with one of a number of inputs, such as an IP address associated with a WWAN interface, an APN, a SIM, a MIN, a SSID, or a LAN user authentication. Exemplary features include a limitation on a number of simultaneous WiFi or Ethernet LAN connections of the gateway, a restriction associated with data ports, a quality of service, a throughput limitation, and a data transfer rate limitation. In addition to providing the features of a service agreement, the server may also return one or more policies of the wireless service provider. In one embodiment, the gateway may also facilitate a subscriber in altering the features of his/her service agreement, block 808.
>
> [0079] If the gateway determines the existence of a service agreement, the gateway may provide WWAN access in accordance with either or both the one or more service agreement features and the one or more wireless service provider policies, block 810. On the other hand, if the gateway determines that the WWAN interface is not associated with a service agreement, the gateway may deny access to all WWAN traffic, block 812. In one embodiment, if the gateway determines that service plans are associated with multiple WWAN interfaces, the gateway may coordinate access to the WWAN through the multiple interfaces, block 814. Further, if the WWAN interface provides access to a plurality of WWANs, the gateway may facilitate a user in choosing one of multiple WWANs, block 816.

626. EX-1008, [0078-0079]. This is depicted in Polson's Fig. 8.

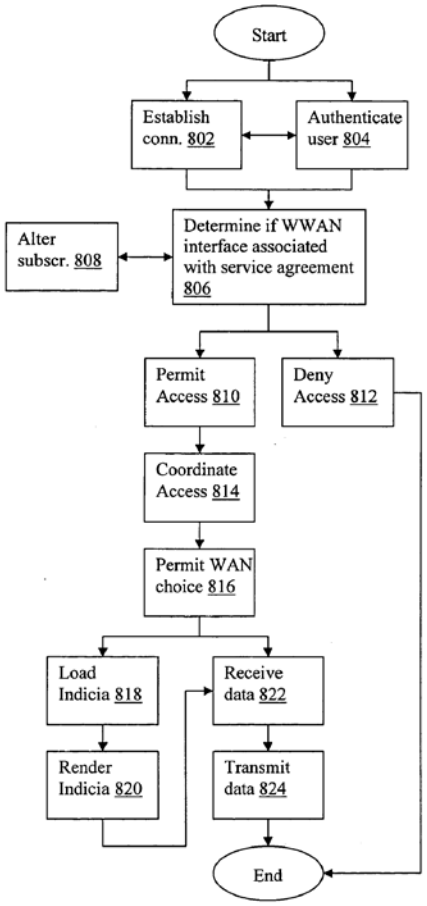


FIG. 8

627. EX-1008, Fig. 8.

628. Limont similarly describes that a "server" sends the policy updates to the clients to modify the service (policies) as detailed for claim 1. EX-1004, [0077].

629. A POSA evaluating Limont would recognize that Limont's advantage of updating policies using a server to a client is replicated by Polson's client gateway which provides additional devices (and device types) for Limont's

corporate administrators to effectuate the desire to control data usage and policy enforcement for traveling users. As I have detailed above, the corporate administrator can update and enforce at least some of the relevant policies at a centralized point (the WWAN interface in the WWAN / WLAN gateway) and have those policies the apply to all users of the gateway device.

630. Based on their complementary capabilities in managing, enforcing and updating policies for traveling users (including corporate users), a POSA would have recognized the benefits of including Polson's portable WWAN gateway as one of the managed mobile devices managed by Limont's network servers. Limont is focused on updating and enforcing policies wirelessly, including for traveling users. Polson provides the type of client device identified in Limont as useful for its invention which has the added benefit of providing the traveling users with enhanced functionality such as the ability to use a WLAN connection to communication over a WWAN network (thus providing additional flexibility in locations of usage).

631. Moreover, a POSA would have had a reasonable expectation of success in the combination. As noted above, Polson and Limont describe their managed client devices with overlapping categories of computing devices.

632. Limont's managed devices need the capabilities to: (1) communicate with network servers; (2) receive updated policies; and (3) enforce those policies. Polson's gateway already performs all three functions using the same basic components (processor, memory, WLAN/WWAN interfaces) that implement Limont's managed client devices.

633. Operating Polson's gateway as one of Limont's mobile devices is merely operating a known and predictable product (a computing device with wireless transmission capabilities) in its known and intended usages (to transmit data across wireless connections) for its known and intended functionality (to allow users access to network data such as through the Internet using known WLAN and WWAN interface card) with the result being the known, intended and predictable result (users have access to the corporate data servers and other information available on the accessed networks).

634. The presence of Wright (and optionally Xu) does not impact the combination with Polson. Polson itself uses encryption on its various interfaces. For example, although it is difficult to read, Polson's Figure 13 describes the well-known usage of encryption on WLAN interfaces using the well-known WEP and WPA options for encryption on an 802.11 WLAN network.

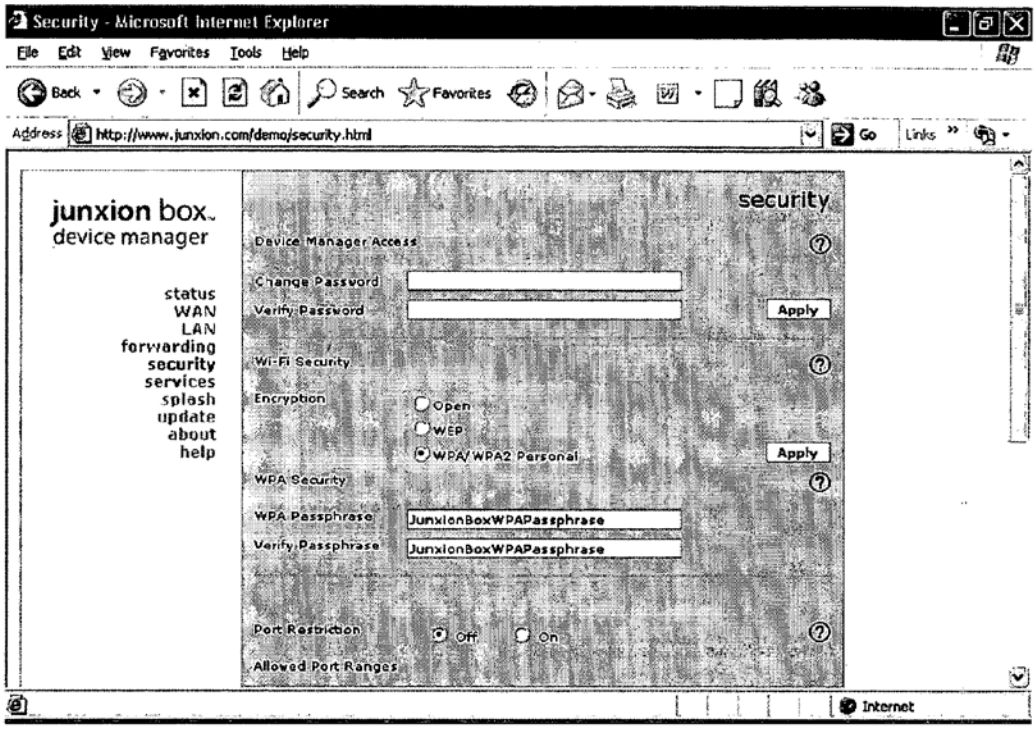


FIG. 13

635. EX-1008, Fig. 13 (encryption on WiFi interface).

636. Polson and Wright (and Xu) describe compatible computing devices with similar computing and storage capabilities that would facilitate storage of any network access information and policies in encrypted and/or secure memory as detailed in Wright and Xu.

637. As noted above, it was well-known to incorporate protected partitions of memory in a variety of devices to protect policies, encryption-related information and programs, and other confidential data and programs. This is

detailed in Xu but was known since at least Arm's TrustZone patents filed in 2003. The usage of such protected partitions was an implementation option provided by commercial processors from Arm and Intel (and others) prior to the 2009 priority date.

638. A POSA would have understood the benefits of protecting confidential data through encryption and hardware protections to protect malicious users or hackers (see Limont) from making unauthorized access to data on mobile devices, including the access of encryption and connection information that could be used to hack into corporate services. This is a known problem with maintaining confidential data on devices that might be "lost or stolen" (as described in Limont, but a problem for which Arm and others (including the Wright and Xu references) had fully addressed many years prior to the '042 Patent priority date in 2009.

639. Indeed, as I have noted above, the '042 Patent does not add any functionality or novel aspect of the protected partition, but merely relies upon the already-known and used technologies for providing such protections (either through encryption or hardware-enforced mechanisms as in Xu).

640. [This paragraph is left intentionally blank].

2. This Combination Renders Obvious Challenged Claims 3-5.

641. Polson provides a client device as managed in Limont's network that functions as the "intermediate networking device" recited in Challenged Claims 3-5.

642. [This paragraph left intentionally blank].

p) Claim 3: *[3.0] The method of claim 1, wherein the wireless end-user device is an intermediate networking device for forwarding traffic between a wireless wide-area network (WWAN) and a wireless local-area network (WLAN).*

643. Polson teaches a WWAN to WLAN gateway that meets this claim and is a *is an intermediate networking device for forwarding traffic between a wireless wide-area network (WWAN) and a wireless local-area network (WLAN)*.

644. The '042 Patent identifies "gateways" such as Polson's as the claimed "intermediate network device."

> FIG. 1 illustrates a secure execution environment 100 (e.g., for a communications device) for device assisted services in accordance with some embodiments. As shown in FIG. 1, the device execution environments include program/functional elements for a

> communications (e.g., a communications device can be an intermediate networking device, such as 3G/4G WWAN to WLAN bridges/routers/gateways, femto cells, DOCSIS modems, DSL modems, remote access/backup routers, and other intermediate network devices, or a mobile communications device, such as a mobile phone, a PDA, an eBook reader, a music device, an entertainment/gaming device, a computer, laptop, a netbook, a tablet, a home networking system, and/or any other mobile communications device) device that utilizes the modem subsystems #1 (125) through #N (127) to connect to one or more of the access networks #1 (136) through #N (138). In some embodiments, a communications device includes multiple program execution partitions.

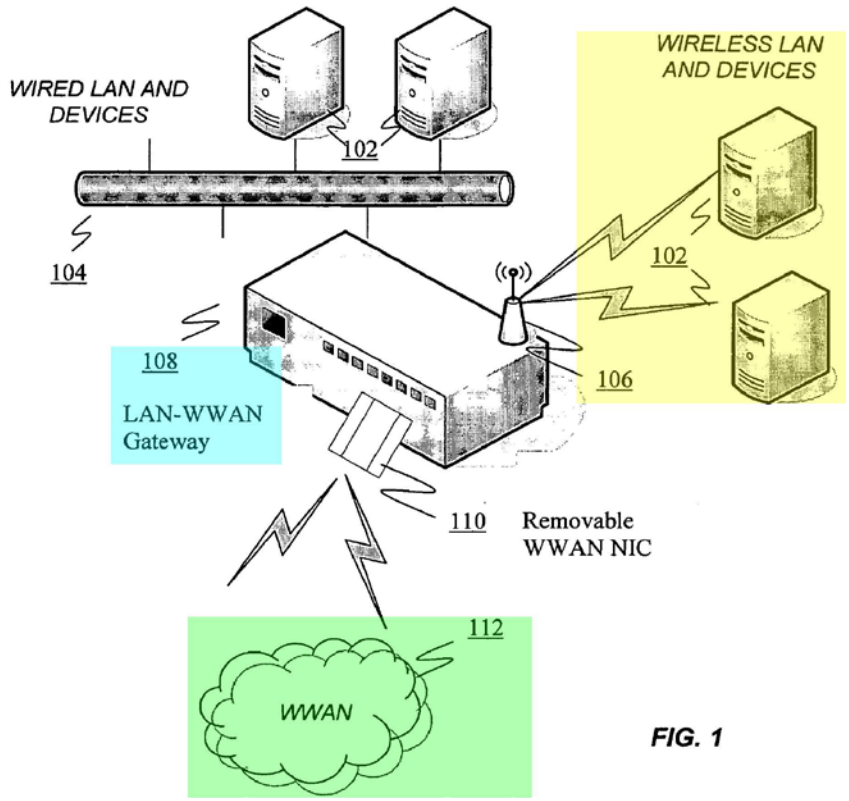
645. EX-1001, 5:37-52.

646. As noted above, Polson's gateway is:

> [0026] Further, as is used herein, the term "gateway" refers to any computing device capable of facilitating transmission of data from one or more LANs to one or more WWANs, and transmission of data from the one or more WWANs to the one or more LANs….

647. EX-1008, [0026]. For example, Polson's gateway forwards data between a WWAN and a user connected on one of the WLAN (WiFi) connections. By itself, paragraph 0026 describes that Polson's gateway has the functionality required in this claim of forwarding data between the networks.

648. Polson depicts the gateway in Figure 1:



649. EX-1008, Fig. 1 (annotated). As depicted above, the gateway connects to "wired" and "wireless" LANs as well as WWAN.

> [G]ateway 108 has one or more local networking interfaces, such as wireless LAN interface 106, adapted to receive data from, and transmit data to one or more devices 102 of one or more LANs, such as the wireless LAN shown as connected to gateway 108 through local networking interface 106. Gateway 108 further comprises a socket adapted to removably receive a selected one of a first and a second WWAN interface ….

650. EX-1008, [0020].

651. Polson's gateway *forward[s]* (routes) data between the WWAN and WLAN based on the user's subscription (as implemented by policies):

> [T]he routing engine of gateway 108 may facilitate two-way transmission of data to and from the one or more LANs and to and from one or more WWANs. As mentioned above, capabilities of the routing engine may be affected by the results of the subscriber determination logic. That is, receipt from and transmission to a WWAN may be based on a service agreement between a user and a wireless service provider.

652. EX-1008, [0039].

653. For example, data received from the WWAN can be forwarded to the recipient device on the LAN (either wired or wireless) as shown in Fig. 6.

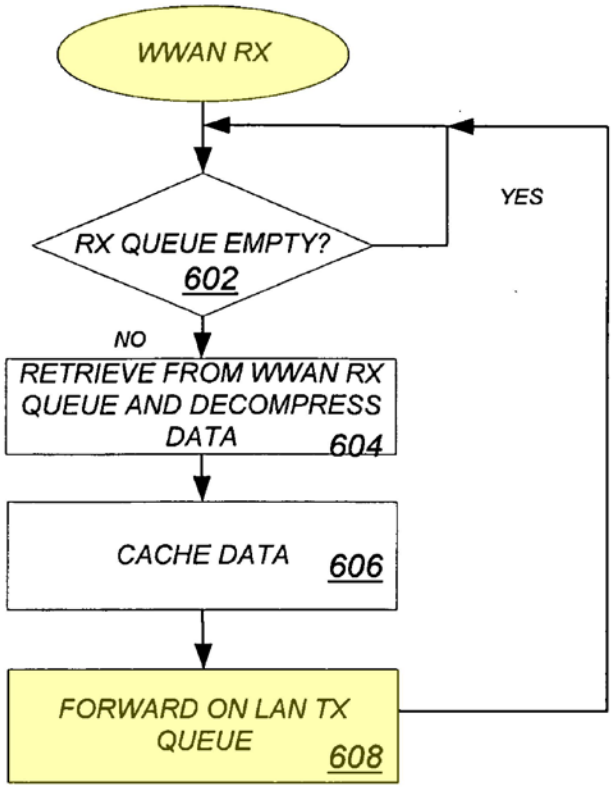


FIG. 6

654. EX-1008, Fig. 6.

655. Such forwarding is described in detail in Polson's description:

> [0070] FIG. 6 illustrates the operational flow of selected aspects of a WWAN Receive process at the gateway 108 for handling receipt processing of WWAN data. As is illustrated, the routing engine implementing the WWAN Receive process may first determine if a WWAN Receive Queue of gateway 108 is empty, block 602. The queue may be implemented as any sort of data structure known in the art capable of organizing and storing data. Data received from a

WWAN may, in some embodiments, first be placed in this receive queue. If empty, the routing engine may check the queue periodically, on some basis, until it is not found to be empty. In other embodiments, received WWAN data is processed as it is received, and is not placed in a receive queue.

[0071] In various embodiments, the WWAN Receive process implemented by the routing engine may next retrieve data from the WWAN receive queue and decompress the received data, block 604, if the data is compressed. As mentioned above, compression of data may result in higher transmission speeds across a WWAN 112, and may also be used to lower the connectivity cost to a user or reduce the load for a carrier. The routing engine may employ any compression algorithm known in the art to achieve decompression of the data, such algorithms including Huffman, Lempel-Ziv, Venturi, or any combination of such algorithms.

[0072] Upon decompressing the data, the WWAN Receive process of the routing engine may, in some embodiments, next determine if the data is content received from a device of a WWAN 112. If the data is determined to comprise some sort of content, such as a web page, a PDF, or any other sort of content known in the art, the routing engine may then determine if the content is cached in persistent storage 208 of gateway 108. If the received content is not cached, the routing engine, in various embodiments, may cache the content received from the WWAN 112, block 606, in a data structure of some type known in

> the art, and store the cached content in the persistent storage 208 of gateway 108. Other caching may be proactive, storing new data at non-peak hours when the WWAN 112 is underutilized.
>
> [0073] After caching the data, the WWAN Receive Process may, in some embodiments, place the data in a LAN Transmit Queue of gateway 108, block 608, to await transmission to its destination device 102 of LAN 104. In alternate embodiments, the routing engine may, immediately following caching, transmit the data across the LAN 104 to its destination device 102.

656. EX-1008, [0070-0073]. Thus, this describes the gateway receiving data on the WWAN interface, evaluating the destination of that data, and forwarding that data to the WLAN interface for transmission to another end-user device.

657. Figure 4 depicts the analogous operation when the gateway receives data from the LAN (LAN RX), determines to which network the data is addresses and forwards the LAN RX data to the WWAN TX queue.

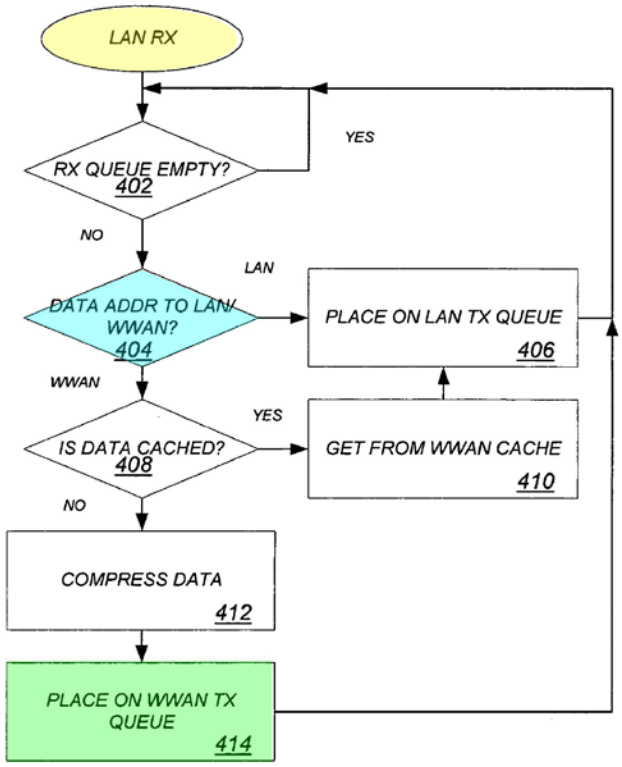


FIG. 4

658. EX-1008, Fig. 4.

659. The WLAN->WWAN forwarding is described in Polson:

> [0063] FIG. 4 illustrates the operational flow of selected aspects of a LAN Receive process at the gateway 108 for handling receipt processing of LAN data. As is illustrated, the routing engine implementing the LAN Receive process may first determine if a LAN Receive Queue of gateway 108 is empty, block 402. The queue may be implemented as any sort of data structure known in the art capable of organizing and storing data. Data received from a LAN may, in some embodiments, first be placed in this receive queue. If empty, the routing engine may check the queue periodically, on some basis, until

it is not found to be empty. In other embodiments, received LAN data is processed as it is received, and is not placed in a receive queue. In yet other embodiments, the receive queue may contain buffered LAN data that has been placed in the queue to await transmission while a connection to a WWAN 112 is unavailable.

[0064] Upon determining that the receive queue is not empty, the routing engine implementing the LAN Receive process may next determine whether the received LAN data is destined for another device 102 of the same LAN 104 or of a second LAN, or whether the received data is destined for a device accessible over a WWAN 112, block 404. If destined for a device 102 of a LAN 104 or a second LAN, the data may be placed in a LAN Transmit Queue of gateway 108, block 406. The queue may be implemented as any sort of data structure known in the art capable of organizing and storing data. In other embodiments, the data may be transmitted immediately to the destination device 102 without being placed in such a queue.

[0065] As is shown, if on the other hand, the data is destined for a device accessible over a WWAN 112, the LAN Receive process of the routing engine may then determine whether the data is cached, block 408. Such a determination may be appropriate where the data received from a device 102 of a LAN 104 is a request for content from a device of a WWAN 112, and the content may be cached in the persistent storage 208 of gateway 108. If the content is cached, the routing engine may simply retrieve the requested content from the storage of

gateway 108, block 410, and transmit the content to the device 102 of LAN 104 requesting the content. In alternate embodiments, rather than immediately transmitting the cached content, the LAN Receive process of the routing engine may place the cached content on a LAN Transmit Queue of gateway 108, block 406, such as the one described above. In such embodiments, no current connection to the WWAN 112 is required.

[0066] If on the other hand the content is not cached, or the data received from device 102 of LAN 104 is not a request for content, the LAN Receive process implemented by the routing engine may, in various embodiments, compress the received data prior to transmitting it, block 412. By compressing the data, the routing engine may facilitate transmission of the data at a higher speed than might otherwise be achieved, especially given the typically low speeds at which data is transmitted across a WWAN, and may also lower the connectivity cost to a user or reduce the load for a carrier. Such compression may be achieved through recourse to any compression algorithm known in the art, such as Huffman, Lempel-Ziv, or Venturi, or any combination of such algorithms.

[0067] After compressing the data, the LAN Receive Process may, in some embodiments, place the data in a WWAN Transmission Queue of gateway 108, block 414, to await transmission across WWAN 112. In alternate embodiments, the routing engine may, immediately following compressing, determine if a WWAN 112 connection exists,

> as is further illustrated and described above, and if such a connection exists, transmit the data across the WWAN 112 to its destination.

660. EX-1008, [0063-0067].

661. This process describes the gateway receiving information (including requests such as web page requests for content) from another device using the WLAN interface, then evaluating the receiving information, and, as appropriate transmitting / forwarding the information across the WWAN interface to its intended destination.

662. Moreover, Limont specifically identifies that "intermediate network devices" can exist in the communications path between an end-user device and the servers.

> [0043] Communication link 132 logically represents that mobile device 101 is connected to network 131. Communication link 132 abstracts the actually physical representation of the connection from mobile device 101 to network 131. The actual physical representation can include communication through one or more intermediate network devices and can include communication in one or more different protocols. At least a portion of the actual physical representation can include wireless communication using wireless protocols (e.g., GPRS, GSM, etc. to a mobile telephone server provider).

663. EX-1004, [0043].

664. Thus, for example, in the claimed combination, Polson's "intermediate networking device" gateway would be place on link 132 between "network 131" and "the mobile device 101"

> [0056] Communication link 133 logically represents that computer system 141 is connected to network 131. Communication link 133 abstracts the actually physical representation of the connection from computer system 141 to network 131. The actual physical representation can include communication through one or more intermediate network devices and can include communication in one or more different protocols. At least a portion of the actual physical representation can include wireless communication using wireless protocols.

665. EX-1004, [0056].

666. Polson's "gateway" devices correspond to Limont's intermediate network devices and provide additional security by allowing Limont's server to control the policies on those intermediate network devices (Polson's gateways) and the devices attached to those gateways using the WLAN interfaces. As I have detailed below, many of Polson's policies fit correspond to the policies specified in Limont for providing access and defining the parameters, permissions and contours of that access. Thus, in one proposed combination, Polson's gateway would be placed on link 132 and allow mobile device 101 to use the WLAN interface and

forward data to the WWAN interface toward the server. Similarly, Limont's policy settings include Polson's policies. The overlap in policies and the type of policies is discussed below for claim 5. Polson's policies relate heavily to those in Limont and Wright – particularly for controlling access to various networks and/or functionalities as discussed herein such as Limont's policies related to network interface and wireless protocols for access to particular networks and data in the corporate networks as well as the policies that seek to manage and control performance and capabilities of the handsets such as resource allocation.

667. Moreover, as I have described above, by 2009, it was well-known to a POSA that such WLAN gateways for forwarding traffic between WLAN and WWAN could be implemented in the form / size factor of a mobile phone or laptop and would meet the description in Polson of "any computing device" that may implement the "gateway" functionality.

668. [This paragraph is left intentionally blank].

q) Claim 4: ***[4.0] The method of claim 1, wherein the wireless end-user device is an intermediate networking device comprising a cellular device, the intermediate***

networking device for forwarding traffic between the wireless access network and a second network.

669. Polson's "gateway" is an "*intermediate networking device comprising a cellular device, the intermediate networking device for forwarding traffic between the wireless access network and a second network*."

670. As detailed above for claim 3, Polson's device forwards data between the WWAN network and LAN networks either wired or wireless. Thus, Polson's gateway is a "*intermediate networking device for forwarding traffic between the wireless access network and a second network*."

671. Polson's WWAN interface may also be cellular. EX-1008, [0051] ("The WWAN interface 110 may be of any sort known in the art, such as cellular, PCS, and WiMax WWAN interfaces."); [0054-0056], [0005] (each reciting that the WWAN may be "cellular").

672. Unlike Polson, the '042 specification does not use the term "cellular" (much less "cellular device"). Moreover, the '042 specification specifically distinguishes "mobile communications devices" as being different from "intermediate networking devices."

> a communications device can be an intermediate networking device, such as 3G/4G WWAN to WLAN bridges/routers/gateways, …, and other intermediate network devices, **or** a mobile communications device, such as a mobile phone, a PDA, an eBook reader, a music device, an entertainment/gaming device, a computer, laptop, a netbook, a tablet, a home networking system, and/or any other mobile communications device)

673. EX-1001, 5:41-50. The "or" clearly delineates between an "intermediate networking device" (as recited in this claim) and "mobile communication device[s]."

674. Thus, the teachings of the '042 Patent support that the claimed "cellular device" need not be a mobile phone (which would actually be contrary to the disclosure above).

675. Thus, if PO attempts to restrict the term "cellular device" to any specific type of device (such as a "mobile phone"), such a construction conflicts with the '042 specification.

676. Moreover, as I have noted above, by 2009, it was well-known to a POSA that such WLAN gateways for forwarding traffic between WLAN and WWAN could be implemented in the form / size factor of a mobile phone or laptop.

677. [This paragraph is left intentionally blank].

r) Claim 5: [5.0] The method of claim 1, wherein the wireless end-user device is an intermediate networking device, and the particular service policy setting assists one or more other end-user devices in communicating over the wireless access network via the intermediate networking device.

678. As I have explained above in Polson's description and for claim 3, Polson's gateway is an intermediate networking device.

679. Polson teaches several policy settings that assist other end-user devices in communicating over the wireless access networks (both WLAN and WWAN) and thus is a*n intermediate networking device, and the particular service policy setting assists one or more other end-user devices in communicating over the wireless access network via the intermediate networking device*.

680. As I have noted above for claim 3, Polson's gateway forwards data between the WLAN and WWAN network and thus "*assists one or more other end-user devices in communicating over the wireless access network via the intermediate networking device*."

681. Polson's WWAN gateway includes "subscriber determination logic" that is applied to the gateway as well as the devices and networks to which the gateway connects. This is described in detail in Polson at [0029-0040] and shown in Figures 3-7 and 8-12.

682. For example, one "particular service policy setting" that "assists" as claimed is disclosed by the policies related to the "service agreement" and that the forwarding of data for end-users depends on the "service agreement" as implemented by the policies in the gateway.

> In various embodiments, the routing engine of gateway 108 may facilitate two-way transmission of data to and from the one or more LANs and to and from one or more WWANs. As mentioned above, capabilities of the routing engine may be affected by the results of the subscriber determination logic. That is, receipt from and transmission to a WWAN may be based on a service agreement between a user and a wireless service provider. Also, transmission of data from one device 102 of a LAN 104 to another device 102 of a second LAN is described in greater detail above.

683. EX-1008, [0039].

684. Such a policy fits squarely with Limont's description of its configuration / policy settings specifying "network interface settings [and] wireless protocol settings" (EX-1004, [0073], [0085], [0087]) because control over the

WWAN would be effectuated in Polson's device by control over the "WWAN interface 110" which may be "may be of any sort known in the art, such as cellular, PCS, and WiMax WWAN interfaces. The interface may come in the form of a PC Card or Modem, the PC Card or Modem capable of plugging into the socket of gateway 108." EX-1008, [0051-0053].

685. As Polson notes (and consistent with Limont's disclosure of control over these "network interface settings [and] wireless protocol settings" because such settings define the type and specific network to which the client device may connect (in both Limont and Polson):

> In various embodiments, each WWAN interface may be adapted for a specific wireless service provider, as described above, and may be associated with a service agreement with that service provider. Thus, gateway 108 facilitates the switching of WWAN interfaces in areas where another provider having a different WWAN interface is stronger, or where the provider associated with the current WWAN interface 110 does not provide service. Accordingly, the use of multiple WWAN interfaces 110 with the socket of gateway 108 facilitates the mobility of the gateway 108, as described above.

686. EX-1008, [0052].

687. Polson's ability to switch between different WWAN networks (for a better connection) mirrors Limont's described functionality of evaluating the

"connection speed" and potentially updating the policies (such as the "network interface settings [and] wireless protocol settings") to use a new network that would provide the required connection speed to access the requested data.

688. Another specific example of such an "assist" policy is that the "LAN 104 users may be authenticated onto the gateway … for WWAN 112 access…." EX-1008, [0035]. By "authenticating" the LAN users to allow for "WWAN access," the policy settings "assists" other end-user devices (the LAN users) in communicating over the WWAN as claimed. Such authentication is described in Limont as a prerequisite to data access:

> If other access requirements are satisfied (e.g., authentication, authorization, and policy enforcement), mobile device 101 can subsequently access data 197A

689. EX-1004, [0090].

> Policy enforcement module 143 can interoperate with authentication and/or authorization modules of server module 142B (not shown) to reduce the likelihood of inappropriate data access. When policy settings are appropriate (and, for example, a user is authenticated and authorized), data access module 144 accesses requested data and transfers requested data to the requesting mobile device. On the other hand, when policy settings are inappropriate (and even if a user is authenticated and authorized), policy enforcement module 143 can

access appropriate policy settings and transfer the appropriate policy settings to the requesting mobile device.

690. EX-1004, [0055]. See also EX-1004, [0070], [0078].

691. By including authentication policies in the WLAN / WWAN gateway, the gateway provides an extra level of protection for the corporate data. These policies "assists one or more other end-user devices in communicating…" by allowing the communication when appropriate (e.g., when authorized).

692. Polson's specifically identifies additional policies that assist other end-user devices in accessing the WWAN including:

- the gateway will "allow" (or restrict) use of the WWAN "according to the features of the [subscriber's] service agreement and/or the policies of the wireless service provider" which may include "quality of service (e.g., of a suitable level to support Voice-over-IP), the throughput provided, the cumulative bits per hour, day or month, port-forwarding, on-board VPN…." EX-1008, [0029-0030]. Such a policy is consistent with Limont's enforced policies related to, for example, "connection speed."

- specifying access for "certain period of time, a certain quantity of bytes downloaded, etc." or a particular number or type of device or a particular IP address. EX-1008, [0031-0032];
- Policies that allow for specific access (*e.g.*, "unrestricted and restricted" access) to different aspects ("Access Point Name") on a cellular network such as "GSM." EX-1008, [0033]. Such a policy fits squarely with Limont's policies related to "network interface settings [and] wireless protocol settings" discussed above and "assists" in the communication by providing the specific networks (and associated protocols and interfaces) for the communication.
- Policies allowing access based on the SIM, MIN or ESSID. EX-1008, [0034];
- Policies that "coordinate the wired and wireless access" for various subscribers where "such coordination of wired and wireless access may be a feature of the service agreement, such as, for example, simultaneous wired and wireless access to maximize throughput for a premium service agreement" or the ability to have a "wireless preference" for access. EX-1008, [0036]. Such policies allow for

Limont's corporate users to transition between the described "wired" and "wireless" connections. Such a policy fits squarely with Limont's policies related to "network interface settings [and] wireless protocol settings" discussed above and "assists" in the communication by providing the specific networks (and associated protocols and interfaces) for the communication.

- "Customizable" policies to better the "overall user experience" including specific "customization may be implemented by a wireless service provider for a certain customer, for example for a large corporate customer of the wireless service provider." EX-1008, [0037].
- Policies that allow end-users to switch between different WWAN providers (networks) based on user preferences for access. EX-1008, [0038].

693. Each of these policies as programmed into, and implemented by, Polson's gateway assists other users (for example, the LAN users) in communicating over the WWAN by, for example, allowing for access and specifying the contours of such access.

694. Moreover, by 2009, it was well-known to a POSA that such WLAN gateways for forwarding traffic between WLAN and WWAN could be implemented in the form / size factor of a mobile phone or laptop as I have detailed above.

695. Limont also specifically identifies such policies (such as for access and the specific contours of the user's access) to be programmed into the client devices, such as Polson's gateway, as detailed in Ground 1 above.

696. [This paragraph is left intentionally blank].

XI. SECONDARY CONSIDERATIONS DO NOT REBUT THE PRIMA FACIE CASE OF OBVIOUSNESS

697. In my opinion, secondary considerations do not rebut the prima facie case of obviousness for at least two reasons. *First*, I have not seen any evidence of any secondary consideration to date.

698. Patent Owner never proffered such evidence during prosecution of the '042 patent.

699. *Second*, I do not believe that Patent Owner will be able to establish a nexus between any secondary consideration and the Challenged Claims. I have

been advised that a nexus does not exist where the alleged secondary consideration results from something other than what is both claimed and novel in the claims.

700. As I explained above, there is nothing novel in the claims. Indeed, all claim elements are disclosed in the prior art. Thus, I do not see a basis for Patent Owner to assert that there is a nexus between any secondary consideration and the claims.

XII. CONCLUSION

701. I may utilize the documents cited and/or listed herein, or portions of those documents, as exhibits at any hearing or trial in this proceeding. I may further prepare and use exhibits that summarize portions of my testimony or key terms or concepts presented therein, or other demonstrative exhibits, at any hearing or trial in this proceeding.

702. I reserve the right to supplement my testimony and this report in response to any judicial determinations, in response to the opinions expressed by the Patent Owner's experts in this proceeding, and/or in light of additional evidence or testimony brought forth at trial or otherwise brought to my attention after the date of my signature below.

703. I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct, and that all statements made of my own knowledge are true and that all statements made on information and belief are believed to be true. I understand that willful false statements are punishable by fine or imprisonment or both. *See* 18 U.S.C. § 1004.

Date: April 18, 2024

Henry H. Houh.

Henry Houh

Henry H. Houh

15 Ballard Ter.
Lexington, MA 02420
henry.houh@gmail.com
cell: 781-325-8273

Education

Massachusetts Institute of Technology, Cambridge, MA

- PhD in Electrical Engineering and Computer Science, February 1998. "Designing Networks for Tomorrow's Traffic," thesis supervised by Professor David Tennenhouse and Professor John Guttag. GPA 4.7/5.0
- Master of Science in Electrical Engineering and Computer Science, February 1991. "Demonstration of a laser repetition rate multiplier," thesis. GPA 4.5/5.0
- Bachelor of Science in Electrical Engineering and Computer Science, June 1989. "Boundary element analysis of arbitrarily shaped dielectric structures," thesis. GPA 4.7/5.0
- Bachelor of Science in Physics, February 1990. GPA 4.7/5.0

MITx, Cambridge, MA

- September 2020 – present: Enrolled in Statistics and Data Science MicroMasters program, a sequence of five MIT-offered graduate-level courses in statistics and machine learning, culminating in a MicroMasters certificate. Have completed four of five required courses.

Experience

Houh Consulting Inc. / Independent Consultant

- 2009 - present: Technical consultant specializing in Social Networking, Web 2.0, Web Site Development, Data Networking, Optical Networking, Telecommunications, Media Streaming and Voice Over IP. Clients include: Akin Gump Strauss Hauer & Feld LLP, Arnold & Porter Kaye Scholer LLP, BBN, Baker Botts LLP, Barnes & Thornburg LLP, BBN Technologies, Beus Gilbert McGroder PLLC, Bracewell LLP, Christensen O'Connor Johnson Kindness PLLC, Cooley LLP, Covington & Burling LLP, Cozen O'Connor P.C., DLA Piper, Davis Polk & Wardwell LLP, Desmarais LLP, Duane Morris LLP, Erise IP, P.A., Faegre Baker Daniels LLP, Finnegan, Henderson, Farabow, Garrett & Dunner, LLP, Fish & Richardson P.C., Goldman Ismail Tomaselli Brennan & Baum

LLP, Haynes and Boone, LLP, Kaye Scholer, Kellogg Huber Hanson Todd Evans & Figel PLLC, Kirkland & Ellis LLP, Klarquist Sparkman, LLP, McCarthy Tetrault LLP, McGuireWoods LLP, Morgan, Lewis & Bockius LLP, Munger Tolles & Olson LLP, Orrick, Herrington & Sutfliffe LLP, O'Melveny & Myers LLP, Orrick, Herrington & Sutcliffe LLP, Paul Hastings LLP, Paul, Weiss, Rifkind, Wharton & Garrison LLP, Perkins Coie LLP, Quinn Emanuel Urquhart & Sullivan, LLP, Sidley Austin LLP, Smith Baluch LLP, Sterne, Kessler, Goldstein & Fox PLLC, Troutman Sanders LLP, Venable LLP, Weil, Gotshal & Manges LLP, Wiley Rein LLP, Wilmer Cutler Pickering Hale and Dorr LLP, and Winston & Strawn LLP.

BlocksCAD Inc. (H3XL spin-out)

- 2014 - present: Founder and member of Board of Directors. BlocksCAD is a visual Computer-Aided Design (CAD) program, designed to teach children mathematics and geometric visualization. BlocksCAD is being used in U.S. schools and worldwide in maker spaces, with 350,000+ users. BlocksCAD was selected to be part of the LearnLaunch 2017 Boost Accelerator, the MIT Play Labs 2018 Summer Accelerator, and the MassChallenge 2018 Boston Cohort. Recipient of DARPA DSO grant in 2014, and SBIR grant from the USDA in 2019.

H3XL Inc. d/b/a Einstein's Workshop (formerly Lexington Robotics)

- 2009 - 2022: Founder and President. Started a science, technology, engineering and math enrichment program and creative/maker space, in 7,000 square feet of space. Serve 2,000+ kids and families annually. As of end of 2022, have delivered an estimated 250,000 student-instruction-hours of STEM courses. Principle Investigator for 2-year DARPA grant to improve 3D Computer Aided Design tool developed in-house for the purposes of teaching 8 year olds and up 3D CAD.

Eons

- 2008 - 2009: Chief Technology Officer. Created product that Eons acquired from BBN Technologies. Integrated BBN product with Eons social networking platform and significantly increased the Eons group creation rate. Helped evaluate advertisement platform offerings and rolled out the "Boom Network" advertising network. Eons raised $32 million from General Catalyst Partners, Charles River Ventures, Sequoia Capital, and Intel Capital.

BBN Technologies

- 2007 - 2008: Delta Division, Vice President of Technology. Grew "Boomerang" counter-sniper project engineering team and significantly de-risked $10 million worth of product deliveries. Identified sales team leading to $10 million dollars of new sales within 6

months and $100+ million in additional orders in the following two years. Boomerang was a significant asset leading to the acquisition of BBN by Raytheon in 2009. Created new business plan and grew team; launched new fully-featured social networking web site in 5 months. Served as lead expert witness in patent infringement lawsuit, resulting in $58 million jury award to client; verdict for patents I testified on were upheld on appeal which resulted in a $120 million settlement.

- 2004 - 2007: Delta Division, Director of Technology, responsible for commercializing IP and creating new businesses. Hired and grew division's initial engineering team. Wrote three business plans, two of which were funded. For call center business plan, acted as general manager, hiring and managing engineering team, inside sales team, and identifying and recruiting a new general manager. Identified and recruited other key employees to Delta Division, including senior members of team leading to successful internal sales growth and spin-outs of projects. Contracted by BBN to BBN spin-out PodZinger as VP of Operations and Technology. Additional areas studied include mesh networking, network security, satellite communications, and semantic web.

PodZinger Inc. (BBN spin-out, also known as EveryZing and now RAMP)

- 2006: Vice President of Operations and Technology. Significantly upgraded capability of consumer-facing search site and redeployed web site from company to co-location facility. Identified key portions of infrastructure for upgrading and cost reduction. Helped write business plan, evaluating advertisement models of revenue. Hired in operations replacement and phased back to BBN.

Commonwealth Capital

- 2004: Entrepreneur-in-residence (informally), performed technical due diligence on business plans, brainstormed ideas for new businesses with venture partner. With venture partner, left for portfolio company BBN to form core of commercialization team.

Empirix, Inc./Teradyne, Inc.

- 2001 - 2004: Chief Technologist, Engineering Manager, Web Application Test Group. Researched potential new product areas; developed product plan and prototype. Responsible for three new and existing products. Managed off-shore development team. Chief architect for all web testing products. Re-architected core testing product, helped write javascript interpreter. Provided technical vision for core product.
- 2000 - 2001: Chief Technologist, Communication Infrastructure Test Group. Responsible for incorporating new technology internally, tracking new technologies, technical evaluation of partnerships and potential acquisitions. Helped develop division strategy. Developed plans which formed core capabilities for successful new products introduced in 2004-5.

- 2000 - 2001: Engineering Manager, Communications Infrastructure Test Group. Execution of new product plan developed in prior role. Grew team from four existing engineers to team of over 30 on immediate team and over 40 on project. Delivered new platform in one year. Platform and derivatives accounted for large portion of booked products for the division within 2 years and is currently (2008) a key portion of new product offerings.
- 2000: Empirix was formed as a spin-out of Teradyne in January 2000. Reported to CEO in carve-out of Empirix from Teradyne.
- 1999: (Teradyne) Director of Business Development, Software Test Units. Reported directly to Chairman of the Board/Founder and then to general manager of software test unit (6 divisions of Teradyne). Evaluated and researched acquisition and partnership candidates. Internally assessed technology position in market and gaps in product lines. Worked with senior division staff to develop new product strategies. Attended internal Teradyne divisional board meetings. Chairman served as my mentor.

3Com Corporation/NBX Corporation

- 1999: Software Engineer 5. Continued work after 3Com acquisition of NBX. Built cross-division relationships for new products and research directions. NBX was acquired by 3Com in March 1999.
- 1997 - 1999: (NBX) Senior Scientist and Engineer. Work in IP Telephony. Architected next-generation product. Protocol design and validation for core protocol now used tens of millions of times daily. Led team in integration of IP protocols into current product. Designed audio reconstruction algorithms. Developed applications for bug analysis and diagnosis of system problems. Implementation of network simulator. Work on collaborative projects with external partners. Worked to identify gaps in product. Representative at numerous trade shows. Innovated novel methods of using product.

MIT Department of Electrical Engineering and Computer Science, Cambridge, MA

- 1991 - 1998: Research assistant, Telemedia Network Systems Group. Design, development, and implementation of Gigabit ATM network for distributed multimedia system. Studied host interface design issues. ATM network simulation.
- Spring 1989, Fall 1990, Spring 1995: Teaching assistant, Computation Structures digital systems course. (Spring 1995 Head TA)
- 1988 - 1989: Head laboratory teaching assistant for Computation Structures. Responsibilities included writing and revising lab assignments, and maintaining the lab.
- 1987: Laboratory teaching assistant for Computation Structures.
- 1987: Design, construction, and programming of 16-bit computer.

Agora Technology Group, Incorporated

- 1994 - 1996: Founder and CEO. Conceived and oversaw development of targeted advertising-supported Web sites. Responsible for company's vision and direction. Attended the first two WWW Conferences, presenting a workshop and paper at the first, and appearing on the "Commercialization and Economics of the Web" panel and chairing the "Where Commercial Services and the Web Are Headed" panel at the second. Sold company intact; is currently an operating stand-alone company.

AT&T Bell Laboratories, Holmdel, NJ

- 1989 - 1990: Implementation of cascadable all-optical fiber logic gate. Modelocking of all-fiber erbium laser. Construction of modelocked laser repetition rate booster. Strong optics laboratory and fiber optic experience.
- Summer 1988, 1987: Research in integrated optics. Analysis of rectangular waveguides using microwave modeling. Fabrication of integrated optical components.

Honors

- MIT Alumni Association Great Dome Award, 2010, Baker 60th Anniversary Reunion Co-Chair (highest group award given by MIT Alumni Association)
- MIT Alumni Association Presidential Citation Award (now known as Great Dome), 2008, Member of MIT Chairman's Salon committee
- MIT Alumni Association Bronze Beaver Award, 2007 (highest individual award given by MIT Alumni Association)
- MIT Alumni Association Volunteer Honor Roll, February 2004
- MIT Alumni Association Lobdell Award, 1999
- Boston Museum of Science Gold Pin for 1000 hours of Volunteer Service, April 1999
- MIT Alumni Association Presidential Citation Award (now known as Great Dome), 1997, Member of Alumni Online Communications Committee

Patents and Patent Publications

- U.S. Patent #9,697,231, H. Houh, J. Stern, R. Spina, M. Meteer, "Methods and apparatus for providing virtual media channels based on media search," July 4, 2017.
- U.S. Patent #9,697,230, H. Houh, J. Stern, "Methods and apparatus for dynamic presentation of advertising, factual, and informational content using enhanced metadata in search-driven media applications," July 4, 2017. See also WO2007056485.
- U.S. Patent #7,975,296, L. Apfelbaum, H. Houh, T. Mayberry and G. Friedman, "Automated security threat testing of web pages," July 5, 2011. See also US20030159063, WO2003067405.

- U.S. Patent #7,877,736, H. Houh and J. N. Stern, "Computer language interpretation and optimization for server testing," January 25, 2011. See also US20050138104, WO2005043300.
- U.S. Patent #7,801,910, H. Houh and J. N. Stern, "Method and apparatus for timed tagging of media content," September 21, 2010. See also US20070112837, US20090222442, WO2007056535.
- U.S. Patent #7,590,542, D. C. Williams, W. C. Hand, H. Houh, A. R. Seeley, "Method of Generating Test Scripts Using a Voice-Capable Markup Language," September 15, 2009. See also EP1530869, US20030212561, WO2003096663.
- U.S. Patent #6,967,963, H. H. Houh, P. Anderson, C. Gadda, "Telecommunication method for ensuring on-time delivery of packets containing time-sensitive data," November 22, 2005. See also EP1060400, WO2000033092, CA2318774.
- U.S. Patent #5,144,375, M. C. Gabriel, H. H. Houh, N. A. Whitaker, "Sagnac Optical Logic Gate," September 1, 1992. Also issued as European Patent # EP0456422, July 23, 1997, German Patent #DE69126913, August 28, 1997
- U.S. Patent Application Publication No. 20020015387, "Voice Traffic Packet Capture and Analysis Tool for a Data Network" (Abandoned in 2007)
- U.S. Patent Application Publication No. 20020016708, "Method and Apparatus for Utilizing a Network Processor as Part of a Test System" (Abandoned in 2007)
- U.S. Patent Application Publication No. 20020016937, "Method and Apparatus for Utilizing a Network Processor as Part of a Test System." (Abandoned in 2007) See also WO2002011413.
- U.S. Patent Application Publication No. 20070106646, "User-directed navigation of multimedia search results" (Abandoned in 2009)
- U.S. Patent Application Publication No. 20070106660, "Method and apparatus for using confidence scores of enhanced metadata in search-driven media applications" (Abandoned in 2009)
- U.S. Patent Application Publication No. 20070106685, "Method and apparatus for updating speech recognition databases and reindexing audio and video content using the same" (Abandoned in 2015)
- U.S. Patent Application Publication No. 20070118873, "Methods and apparatus for merging media content" (Abandoned in 2015)
- U.S. Patent Application Publication No. 20090222442, "User-directed navigation of multimedia search results" (Abandoned in 2016)
- U.S. Patent Application 11/395,732, "Search snippet creation for audio and video data" (Abandoned in 2009)
- U.S. Patent Application 11/774,931, "Methods and apparatus for managing a social networking web site"
- U.S. Patent Application 11/774,947, "Methods and apparatus for organizing media files"
- U.S. Patent Application 11/774,956, "Methods and apparatus for managing an online event"
- U.S. Provisional Patent Application 61/086,909, "Measuring and ranking relationship activity"

- U.S. Provisional Patent Application 61/086,914, "Detecting media object commonality"
- U.S. Provisional Patent Application 61/086,904, "Message categorization based on message characteristics"
- U.S. Provisional Patent Application 61/086,905, "Photo tagging to request action"

Trials, Testimony and Depositions

- Case No. 1:06CV682 (CMH/BRP), Verizon vs. Vonage, U.S. District Court for the Eastern District of Virginia, filed expert report, was deposed and testified at trial.
- Case No. 1:08CV157 (CMH/TRJ), Verizon vs. Cox, U.S. District Court for the Eastern District of Virginia, was deposed and testified at trial.
- Case No. 5:09-cv-476, Two-Way Media vs. AT&T, U.S. District Court for the Western District of Texas, filed expert report, testified at trial.
- Case No. 2:10-cv-248 (RAJ/FBS), ActiveVideo Networks vs. Verizon, U.S. District Court for the Eastern District of Virginia, filed expert report and was deposed as an expert witness.
- Case No. 1:11-cv-00880-TSE-JFA, Bear Creek Technologies, Inc. vs. Verizon Services Corp., et al, U.S. District Court for the Easter District of Virginia, was deposed as an expert witness.
- Case No. 3:10-CV-298-BBC, AlmondNet, Inc. vs. Microsoft Corp., U.S. District Court for the Western District of Wisconsin, filed expert report.
- Case No. 6:10-cv-00597, Guardian Media Technologies, Ltd. Vs. AT&T Operations, Inc. et al., U.S. District Court for the Eastern District of Texas, Tyler Division, filed expert report.
- Case No. ESCV2010-02282C, The Octopus Solution LLC v. Gary Brown et al., Essex, MA Superior Court, testified at trial.
- Investigation No. 337-TA-882, In the matter of Certain digital media devices, including televisions, Blu-ray disc players, home theater systems, tablets and mobile phones, components thereof and associated software, U.S. International Trade Commission, filed expert reports, was deposed and testified at hearing.
- Investigation No. 337-TA-995, In the matter of Certain communications or computing devices, and components thereof, U.S. International Trade Commission, filed expert reports, and was deposed.
- Case No. 8:12-cv-122-LES-TDT, Prism Technologies LLC v. AT&T Mobility LLC, U.S. District Court for the District of Nebraska, filed expert report, was deposed and testified at trial.
- Case No. 11-2684 (JWL), Sprint Communications Co., L.P., v. Comcast Cable Communications, LLC, et al., U.S. District Court for the District of Kansas, filed expert report and was deposed.
- Case No. 11-2686 (JWL), Sprint Communications Co., L.P., v. Time Warner Cable, Inc., et al., LLC, et al., U.S. District Court for the District of Kansas, filed expert report, was deposed, and testified at trial.

- Case No. 12-487 (SLR), Cox Communications, Inc., et al., v. Sprint Communications Company L.P., et al., U.S. District Court for the District of Delaware, filed expert report and was deposed.
- Case IPR 2014-00039, Microsoft Corporation v. B.E. Technology LLC, U.S. Patent No. 6,628,314. Submitted declaration and cross-examined in deposition.
- Case IPR 2014-00086, Apple, Inc. v. Evolutionary Intelligence, LLC, U.S. Patent No. 7,010,536. Submitted declaration and cross-examined in deposition.
- Case No. 6:11-CV-421, Stragent, LLC v. Intel Corporation, U.S. District Court for the Eastern District of Texas, Tyler Division, deposed and testified at trial as a fact witness.
- IPR2014-01366, IPR2014-01367, IPR2014-01368, Samsung et al. v. Straight Path, submitted IPR declarations and was deposed.
- IPR2015-1006, IPR2015-1007, Cisco v. Straight Path, submitted IPR declarations.
- IPR2014-01457, IPR2014-01459, Microsoft v. Biscotti, submitted IPR declaration and was deposed.
- IPR2016-00302, Apple v. Nonend, submitted IPR declaration.
- IPR2014-00812, Yelp and Twitter v. Evolutionary Intelligence, submitted IPR declaration.
- IPR2015-00307, Cisco v. AIP, submitted IPR declaration.
- Microsoft v. Acacia, submitted IPR declaration.
- IPR2015-00342, AT&T Mobility LLC and Cellco Partnership d/b/a Verizon Wireless v. Solocron, submitted IPR declaration.
- Mediatube v. Bell Canada, Canadian Federal Court, submitted expert report and testified at trial.
- CBM2016-00036, Google v. At Home Bondholder's Liquidating Trust, submitted CBM declaration.
- IPR2016-01198, IPR2016-01201, Apple, Inc. v. VoIP-Pal.com, Inc., submitted IPR declaration and was deposed.
- Case No. 3:14-cv-2824-VC, Trend Micro Incorporated v. Rpost Holdings, Inc., et al, submitted expert report and was deposed
- Akamai v. Limelight Networks, IPR2016-01631, IPR2016-01711, IPR2017-00249, IPR2017-00349, submitted IPR declarations and was deposed
- Hyperlync Technologies v. Verizon Sourcing, No. 650151/2015 New York Supreme Court, submitted declaration and was deposed
- Cascades Streaming Technologies v. Big Ten Networks, submitted expert reports and was deposed
- Klaustech, Inc. v. Google LLC., Case No. 4:10-CV-05899-JSW (N.D. Cal.), submitted expert report and was deposed
- Cisco v. Uniloc, IPR2017-00198, IPR2017-00058, submitted IPR declarations and was deposed.
- Cisco v. Uniloc, IPR2017-00597, submitted IPR declaration and was deposed
- Twitter v. Youtoo Technologies, LLC, IPR2017-01133, IPR2017-01131, submitted IPR declarations and was deposed

- Taser International Inc. (now Axon Enterprise, Inc.) v. Digital Ally Inc., IPR2017-00375, submitted IPR declaration and was deposed
- Taser International Inc. (now Axon Enterprise, Inc.) v. Digital Ally Inc., IPR2017-00376, IPR2017-00515, IPR2017-00775, submitted IPR declarations
- HTC Corporation v. IPA Technologies, IPR2018-00306, IPR2018-00307, submitted IPR declaration
- Hulu v. Soundview, IPR2018-00864, IPR2018-01023, submitted IPR declarations and was deposed
- XpertUniverse v. Cisco, 3:17-cv-3848, U.S. District Court for Northern District of California, submitted declaration in support of claim construction and was deposed
- Improved Search v. Microsoft, C.A. No. 16-cv-650-JFB-SRF (Del.), submitted declaration in support of claim construction
- Apple v. Uniloc, IPR2018-00361, IPR2018-00394, IPR2018-00395, IPR2019-00700, IPR2019-00701, IPR2019-01667, submitted IPR declarations
- LG Electronics v. Uniloc, submitted IPR declaration
- SRC Labs and Saint Regis Mohawk Tribe v. Microsoft, 2:18-cv-00321-JLR, U.S. District Court for Western District of Washington at Seattle, submitted declaration in support of claim construction and was deposed
- Verizon Wireless v. Barkan Wireless IP Holdings LP, submitted IPR declarations
- Verizon Wireless and Samsung Electronics America Inc. v. Barkan Wireless IP Holdings LP, IPR2019-199, IPR2019-200, IPR2019-234, IPR2019-631, IPR2019-632, submitted IPR declarations
- Samsung Electronics America Inc. v. Barkan Wireless IP Holdings LP, IPR2019-100, submitted IPR declaration
- Cisco Systems Inc. v. Meetrix IP LLC, IPR2019-539, IPR2019-540, IPR2019-541, IPR2019-542, IPR2019-543, IPR2019-544, submitted IPR declarations
- GMG Products LLC v. Traeger Pellet Grills LLC, PGR2019-24, PGR2019-34, PGR2019-35, PGR2019-36, submitted PGR declaration and was deposed
- Uniloc 2017 LLC v. Google LLC, 2:18-cv-00502-JRG-RSP, U.S. District Court for the Eastern District of Texas, Marshall Division, submitted declaration in support of claim construction
- Microsoft Corporation v. Uniloc 2017 LLC, IPR2020-00102, IPR2020-00103, submitted IPR declarations
- Microsoft Corporation and HP Inc. v. Synkloud Technologies, LLC, IPR2020-00316, IPR2020-01031, IPR2020-01032, IPR2020-01269, IPR2020-01270, IPR2020-01271, submitted IPR declarations
- Seven Networks, LLC v. Apple Inc, 2:19-cv-115-JRG, U.S. District Court for the Eastern District of Texas, Marshall Division, submitted declaration in support of claim construction
- Unified Patents Inc. v. Ortiz & Associates Consulting, LLC, IPR2019-00743, submitted IPR declaration

- Uniloc 2017 LLC v. Apple Inc., 3:19-cv-01905-JD, U.S. District Court for the Northern District of California, San Francisco Division, submitted declaration in support of claim construction and was deposed
- ClearPlay Inc. v. Dish Network LLC et al.; 2:14-cv-00191, U.S. District Court for the District of Utah, Central Division, submitted expert report and re-examination declarations, was deposed, and testified at trial
- AMC Networks, Inc. et al v. Sound View Innovations, LLC, IPR2020-00482, submitted IPR declaration
- Case No. 1:17-cv-01734-RGA, Sprint Communications Co., L.P., v. Charter Communications, Inc., et al., U.S. District Court for the District of Delaware, filed expert report and was deposed.
- CommScope Technologies LLC et al. v. Barkan Wireless IP Holdings LP et al., IPR2020-00827, IPR2020-00829, IPR2020-00831, IPR2020-00833, IPR2020-00835, IPR2020-00838, submitted IPR declarations
- Cisco Systems Inc. v. Monarch Networking Solutions LLC, IPR2020-01226, submitted IPR declaration
- CoolTV Network.com v. Blackboard, Inc., Facebook, Inc., International Business Machines Corporation, Kaltura, Inc., Limelight Networks, Inc., Microsoft Corporation, Ooyala, Inc., Snap, Inc., and Trapelo Corp., submitted declaration in support of claim construction and was deposed
- Facebook, Inc. v. Onstream Media Corporation, IPR2020-01507, IPR2020-01508, IPR2020-01525, IPR2020-01527, IPR2020-01528, submitted IPR declarations
- Hisense Co LTD. v. Maxell, LTD, IPR2020-01598, IPR2020-01600, submitted IPR declarations
- Microsoft Corp. v. O'Brien, IPR2021-00015, submitted IPR declaration and was deposed
- Sable Networks Inc. v. Cisco Systems, Inc., WA:20-CV-00288-ADA, U.S. District Court for the Western District of Texas, Waco Division, submitted declaration in support of claim construction
- Peloton Interactive, Inc. v. Icon Health and Fitness Inc et al., IPR2021-00342, submitted IPR declaration
- Hulu, LLC v. SITO Mobile R&D IP, LLC et al., CBM2020-00028, IPR2020-00158, IPR2020-00206 , IPR2020-00219 , IPR2020-00265 , IPR2020-00298 , IPR2020-00304 , IPR2020-00308 , submitted CMB and IPR declarations and was deposed
- Twitter, Inc. and Google LLC v. B.E. Technology, LLC, IPR2021-00482, IPR2021-00483, IPR2021-00484, IPR2021-00485, submitted IPR declarations
- MG Freesites LTD v. ScorpCast, LLC, IPR2021-00511, submitted IPR declaration
- Avionte, LLC v. Sandeep Acharya, Samar Basnet, and Aqore LLC, Arbitration, Hon. Jeffrey Keyes (Ret.)
- Microsoft Corporation v. WSOU Investments, LLC d/b/a Brazos Licensing and Development, IPR2021-00751, submitted IPR declaration
- SAP America, Inc. v. Express Mobile, Inc., IPR2021-01144, IPR2021-01145, IPR2021-01146, submitted IPR declarations

- StratosAudio Inc. v. Hyundai Motor America, 6:20-cv-01125-ADA, U.S. District Court for the Western District of Texas, Waco Division, submitted claim construction declaration and was deposedPeloton Interactive, Inc. v. Ifit Health and Fitness Inc, IPR2022-00029, IPR2022-00030, submitted IPR declarations and was deposed
- Investigation No. 337-TA-1263, In the matter of Certain televisions, remote controls, and components thereof, U.S. International Trade Commission, filed expert reports, was deposed, and testified at hearing
- Alexander Stross v. Netease, Inc., et al., U.S. District Court (Central District of California), Case 2:20-cv-00861-AB(JC), filed expert reports, and was deposed
- Ralph Ledergerber v. Netease, Inc., et al., U.S. District Court (Central District of California), Case 2:20-cv-00862-AB(JC), filed expert reports and was deposed
- John Walmsley v. Netease, Inc., et al., U.S. District Court (Central District of California), Case 2:20-cv-00863-AB(JC), filed expert reports and was deposed
- Bernhard Kuhmstedt v. Netease, Inc., et al., U.S. District Court (Central District of California), Case 2:20-cv-02044-AB(JC), filed expert reports and was deposed
- Netflix, Inc. v. CA, Inc., IPR2021-01319, submitted IPR declaration and was deposed
- F45 Training Pty Ltd. v. Body Fit Training USA Inc., C.A. No. 20-1194 (LPS) (D. Del.), filed expert report
- Apple v. Fintiv, IPR2022-00976, IPR2022-01149, IPR2022-01150, IPR2023-00399, submitted IPR declarations and was deposed
- Estech Systems, Inc. v. Howard Midstream Energy Partners d/b/a Howard Energy Partners, C.A. No. 6:20-cv-777-ADA (Western District of Texas, Waco Division), filed expert reports and was deposed
- Echelon Fitness Multimedia, LLC. v. Peloton Interactive, Inc., IPR2020-01187, submitted IPR declaration and was deposed
- VIZIO. V. Maxell Ltd., IPR2022-01458, submitted IPR declaration
- Maxell, Ltd. et el. v. VIZIO, Inc., Case No. 2-21-cv-06758 (C.D. Cal.). filed declaration and was deposed
- Microsoft Corporation v. SurfCast, Inc., submitted IPR declarations
- The Walt Disney Company et al. v. WAG Acquisition LLC, IPR2022-01227, IPR2022-01228, IPR2022-01346, submitted IPR declarations and was deposed
- Rakuten Rewards et al. v. IBM, submitted IPR declarations and was deposed
- Fubotv Media Inc. v. Sito Mobile R&D IP, LLC et al., submitted IPR declarations
- Unified Patents, LLC v. Noblewood IP LLC, IPR2022-01111, submitted IPR declaration
- Unified Patents, LLC. v. Pedersen, Peter Henrik, IPR2023-00029, submitted IPR declaration
- Ericsson Inc v. Dali Wireless Inc., submitted IPR declarations
- Universal Electronics, Inc. et al. v. Roku, Inc., IPR2022-00818, submitted declarations and was deposed
- Google LLC. v. Wildseed Mobile LLC et al., IPR2023-00244, IPR2023-00245, IPR2023-00246, IPR2023-00247, IPR2023-00248, submitted declarations
- Lululemon Athletica Canada Inc. et al. v. Nike, Inc., IPR2023-00180, IPR2023-00424, submitted declarations

- Zoho Corporation, et al. v. Meetrix IP, LLC, IPR2023-00371, IPR2023-00377, IPR2023-00379, IPR2023-00380, IPR2023-00382, submitted declarations
- WSOU Investments, LLC d/b/a/ Brazos Licensing and Development v. Google LLC, 6:20-cv-572, U.S. District Court for the Western District of Texas, Waco Division, submitted reports and was deposed
- Google LLC v. Safecast Limited LLC, IPR2023-00652, submitted declaration
- Investigation No. 337-TA-1338, In the matter of Certain smart televisions, U.S. International Trade Commission, filed reports and was deposed
- Cisco Systems, Inc. v. Orckit IP LLC, IPR2023-00714, submitted declaration
- SupplyPro, Inc. v. Sandvik Machining Solutions AB, et al., AAA Case No. 01-22-000-7897. submitted declaration
- TrackThings LLC v. NETGEAR, Inc., Case No. 22-00981-RGA-JLH, U.S. District Court for the District of Delaware, submitted declaration
- Walt Disney Parks & Resorts US Inc. v. Agile Journeys LLC; IPR2024-00029, submitted declaration
- Aylo Freesites Ltd v. Dish Technologies LLC; IPR2024-00043, IPR2024-00044, IPR2024-00045, IPR2024-00046, IPR2024-00047, IPR2024-00048, IPR2024-00146, IPR2024-00147; submitted declarations
- Arm Inc. et al. v. Icpillar LLC; IPR2024-00476, IPR2024-00566; Retained by Arm; submitted declarations
- Microsoft Corp et al. v. Litl LLC, IPR2024-00454, IPR2024-00455, IPR2024-00456, IPR2024-00457, IPR2024-00458; submitted declarations
- Cisco Systems Inc et al. v. InfoExpress Inc, IPR2024-00539, IPR2024-00540, IPR2024-00677, IPR2024-00678; submitted declarations
- Vizio Inc v. Multimedia Technologies Pte Ltd; IPR2024-00722, IPR2024-00723; Retained by Vizio; submitted declarations
- Sap America Inc v. Isix IP LLC; IPR2024-00615; Retained by SAP; submitted declarations
- Cisco Systems Inc et al. v. Portsmouth Network Corp; IPR2024-00505, IPR2024-00506; submitted declarations

Publications

- "IP switching: server driven flow classification," H. H. Houh, *Proceedings of the Washington University Workshop on Integration of IP and ATM* , November 1996.
- "Aurora at MIT," D. D. Clark, H. H. Houh, and D. L. Tennenhouse, Editors, *MIT Laboratory for Computer Science Technical Report 673*, December 1995.
- "ViewStation Applications: Implications for Network Traffic," C. J. Lindblad, D. Wetherall, W. Stasior, J. F. Adam, H. H. Houh, M. Ismert, D. Bacher, B. Phillips, and D. L. Tennenhouse, *IEEE Journal of Selected Areas in Communications*, 1995.

- "The VuNet Desk Area Network: Architecture, Implementation, and Experience," H. H. Houh, J. F. Adam, M. Ismert, C. J. Lindblad, and D. L. Tennenhouse, *IEEE Journal of Selected Areas in Communications*, 13 (4), May, 1995.
- "Reducing the Complexity of ATM Host Interfaces," H. H. Houh and D. L. Tennenhouse, Hot Interconnects II Symposium Proceedings, Stanford, August 11-12, 1994.
- "Media-intensive data communications in a `desk-area' network," J. F. Adam, H. H. Houh, M. Ismert, and D. L. Tennenhouse, IEEE Communications, August 1994.
- "ViewStation Applications: Intelligent Video Processing Over A Broadband Local Area Network," C. J. Lindblad, D. J. Wetherall, W. Stasior, B. Phillips, D. Bacher, J. Adam, H. Houh, M. Ismert, and D. L. Tennenhouse, Proceedings of the 1994 USENIX Symposium on High-Speed Networking, Oakland, CA, August 1994.
- "The Media Gateway: Live Video on the World Wide Web," H. H. Houh, C. J. Lindblad, J. Soo, D. L. Tennenhouse, and D. J. Wetherall, Workshop at the 1994 World Wide Web Conference, Geneva, Switzerland, May 1994.
- "Active Pages: Intelligent Nodes on the World Wide Web ," H. H. Houh, C. J. Lindblad, and D. J. Wetherall, Proceedings of the 1994 World Wide Web Conference, Geneva, Switzerland, May 1994.
- "Wavelength Division vs. Code Division Access Methods for Optical Networks," H. H. Houh, Area Exam Paper, May 1993.
- "Experience with the VuNet: A Network Architecture for a Distributed Multimedia System," J. F. Adam, H. H. Houh, D. L. Tennenhouse, Proceedings of the 18th Conference on Local Computer Networks, pp. 70-76, September 1993
- "The VudBoard: A Simple DMA Interface," H. H. Houh, Proceedings of the 4th Gigabit Minijam, January 1994.
- "A Software-Oriented Approach to the Design of Media Processing Environments," D. L. Tennenhouse, J. Adam, D. Carver, H. Houh, M. Ismert, C. Lindblad, W. Stasior, D. Weatherall, D. Bacher, and T. Chang., submitted to the International Conference on Multimedia Computing and Systems, May 1994.
- "A Network Architecture for Distributed Multimedia Systems," J. F. Adam, H. H. Houh, M. Ismert, and D. L. Tennenhouse, submitted to the International Conference on Multimedia Computing and Systems, May 1994.
- "The Viewstation Collected Papers," D. L. Tennenhouse, J. Adam, C. Compton, A. Duda, D. Gifford, H. Houh, M. Ismert, C. Lindblad, W. Stasior, R. Weiss, D. Wetherall, D. Bacher, D. Carver, and T. Chang, MIT Laboratory for Computer Science Technical Report, MIT/LCS/TR-590, November 1993.
- "The Viewstation Collected Papers II," W. F. Stasior, D. L. Tennenhouse, J. F. Adam, D. R. Bacher, H. H. Houh, M. Ismert, C. J. Lindblad, B. M. Phillips, D. J. Wetherall, MIT Laboratory for Computer Science Technical Report, MIT/LCS/TR-696, April 1996.
- "A System's Perspective of the Sagnac Fiber Logic Gates and Their Possible Applications," A. Huang, N. Whitaker, C. Gabriel, H. Avramopoulos, P. M. W. French, H. H. Houh, and I. Chuang, Applied Optics, September 10, 1994

- "Complete Switching in a Three-Terminal Sagnac Switch," H. Avramopoulos, P. M. W. French, M. C. Gabriel, H. H. Houh, N. A. Whitaker, T. Morse, IEEE Phot. Tech. Lett. **3** (3), 235
- "Complete Switching in a Three-Terminal Sagnac Switch," H. Avramopoulos, P. M. W. French, M. C. Gabriel, H. H. Houh, N. A. Whitaker, IEEE/LEOS Annual Meeting, Paper PDP-13, November 1990
- "All-optical phase-locked oscillator," N. A.Whitaker, Jr., H. H. Houh, H. Avramopoulos, T. F. Morse, IEEE/LEOS Annual Meeting, Paper ELT2.4/MOO3, November 1990
- "Passive modelocking of an all-fiber erbium laser," H. Avramopoulos, H. H. Houh, N. A. Whitaker, M. C. Gabriel, T. F. Morse, IEEE/LEOS Conference on Optical Amplifiers and their Applications, Paper PDP-8, August 1990
- "Transverse modes, waveguide dispersion, and 30ps recovery in submicron GaAs/AlAs microresonators," J. L. Jewell, S. L. McCall, A. Scherer, H. H. Houh, N. A. Whitaker, A. C. Gossard, and J. H. English, Appl. Phys. Lett. **55** (1), July 3, 1989

Leadership, Activities and Interests

- Leadership
  - Reading Symphony Orchestra
    - Board of Directors (Treasurer), 2022 - present
  - Discovery Museums (Acton, MA)
    - Board of Directors, 2023 – present
    - Board of Directors, Development Committee, 2023 – present
    - Science and Technology Advisory Council, 2012 - present
  - Tau Beta Pi National Engineering Honor Society
    - Executive Councilor, 2024-2026
    - Advisor, MA B Chapter at MIT, 2003 - present
    - District Director (National Officer), Tau Beta Pi, New England Area, 1991 - 2003
    - President, MA B Chapter at MIT, Fall 1988 - Spring 1989
    - Laureate award, 1989
  - MIT Alumni Association Board of Directors
    - MIT Annual Giving Board, 3 year term, 2024 – 2027
    - National Selection Committee, 3 year term, 2020 – 2023
    - K-12 STEM Initiatives Co-chair, 2013 – 2017
    - Awards Committee Chair, 2012 – 2014
    - Awards Committee, 3 year term, 2011 – 2014
    - Vice President, 2 year term, 2004 – 2006

- Alumni Ad-Hoc Committee, Chair, 2005-2006
- Board Member, 2 year term, 1997 – 1999

- MIT Club of Boston
  - Board of Directors, 2006 - 2011
  - K-12 Initiatives Chair, 2009 - 2012
  - VP of Communications, MIT Club of Boston, 2003 - 2006
  - Past-President, MIT Club of Boston, 2002 - 2003
  - President, MIT Club of Boston, 2001 - 2002
  - President-Elect, MIT Club of Boston, 2000 - 2001
  - VP of Programs, MIT Club of Boston, 1999 - 2000
  - Activities Super-Chair, MIT Club of Boston, 1998 - 1999
- MIT Enterprise Forum of Cambridge, Inc.
  - Past Chair, 2009 – 2011
  - In-NOW-vation Co-chair, 2010
  - Chair, 2007 - 2009
  - Vice Chair, 2005 - 2007
  - Executive Board Member, 2002 - 2011
  - Winter Workshop Co-Chair, February 2007 - conceived idea for conference, which sold-out and produced largest attendance numbers in recent memory
  - Spring Workshop Co-Chair, Spring 2004
  - Membership Committee Chair, Fall 2003 - 2006
  - 25th Anniversary Dinner Chair, Fall 2003
  - As Membership Chair and Board Member, started Special Interest Groups in 2004; a SIG won the MIT Presidential Citation award, the MIT Alumni Association's highest award for organizations, in 2006
- Estabrook Elementary School PTA
  - Advisory committee to the superintendent on PCB issue, 2010-2011
  - 4th Grade after-school science program co-organizer, 2010-2012
  - 4th and 5th Grade before-school Math Olympiad co-organizer, 2009-2013
  - 5th Grade BBQ and Yearbook Committee, 2011, 2013
  - Family Math Night volunteer, 2008-2012
- MIT Class of 1989
  - Secretary, five consecutive 5 year terms, 1989 - 2014
  - 30-year Reunion Committee, 2019
  - 25-year Reunion Committee, 2014
  - 20-year Reunion Committee and Gift Committee, 2009
  - 15-year Reunion Committee and Gift Committee, 2004
  - 10-year Reunion Committee and Gift Committee, 1999
  - 5-year Reunion Committee, 1994
  - Interim Treasurer, 1993 - 1994
  - Instituted annual senior class career fair, now raising over $100,000 annually for senior class activities, Fall 1988

    - Strong, consistent record of leadership dating to high school
- Acting
    - '21' (Sony Pictures), credited as "Chinatown Dealer," 2007, Kevin Spacey's movie about the MIT Blackjack Team inspired by "Bringing Down the House" by Ben Mezrich, opened nationwide on March 28, 2008. 21 was the number one movie in US for two weeks and number one globally for one week. 21 also topped the DVD sales, Blu-ray sales and DVD rental charts.
    - Spring Lake Theater Company, first New York-area off-broadway production of "A Chorus Line," played role of Mark, Summer 1990
- Former member of the MIT Blackjack team
- Producer for 10,000 Maniacs' 2013 album "Music from the Motion Picture"
- Executive Producer for 10,000 Maniacs' 2015 album "Twice Told Tales"
- Violist, violist, harpist, guitarist, singer, actor: played in many amateur/semi-professional groups including Firebird Pops Orchestra, Reading Symphony Orchestra, MIT Summer Philharmonic Orchestra, Carlisle Chamber Orchestra, Rivers Symphony Orchestra, Opera51 Orchestra, Freisinger Chamber Orchestra, Merrimack Valley Philharmonic, Longwood Symphony, MIT Symphony, and Somerville Community Chorus
- Violist, "Coming Home" album by Karen Phillips, 2014
- Google Scholar citations: 2079, h-index: 21, i10-index: 26 (since 2017: 662/12/14)
- Erdos-Bacon number of 7
- Erdos-Bacon-Sabbath number of 11