IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	Gregory G. Raleigh	
U.S. Patent No.:	8,406,733	Attorney Docket No.: 39843-0164IP1
Issue Date:	March 26, 2017	
Appl. Serial No.:	13/461,141	
Filing Date:	May 1, 2012	
Title:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION	

DECLARATION OF DR. PATRICK G. TRAYNOR

SAMSUNG 1003

Table of Contents

I. QUALIFICATIONS AND BACKGROUND 4

II. LEGAL PRINCIPLES 11

A. Anticipation 11

B. Obviousness 12

III. OVERVIEW OF CONCLUSIONS FORMED 13

IV. BACKGROUND KNOWLEDGE ONE OF SKILL IN THE ART WOULD HAVE HAD PRIOR TO THE PRIORITY DATE OF THE '733 PATENT 14

V. INTERPRETATIONS OF THE '733 PATENT CLAIMS AT ISSUE 15

VI. TECHNOLOGY BACKGROUND 15

VII. OVERVIEW OF THE '733 PATENT 21

VIII. PROSECUTION HISTORY OF THE '733 PATENT 24

IX. THE CHALLENGED CLAIMS ARE UNPATENTABLE 25

A. Ground 1: Claims 1-17, 19, 21-27, 29, and 30 Are Obvious Over TS-23.140 and Ogawa… 25

1. TS-23.140 (EX-1004) 25

2. Ogawa (EX-1005) 28

3. MMS-Ogawa Combination 32

4. Claim Analysis 55

B. Ground 2: Claims 1, 2, 5, 7-10, 13-15, 19-22, and 26-30 Are Obvious Over Houghton and Ogawa 137

1. Houghton (EX-1006) 137

2. Houghton-Ogawa Combination 141

3. Claim Analysis 156

C. Ground 3: Claims 3, 4, 6, 11, 12, 16-18, 23, 24 Are Obvious Over Houghton-Ogawa, And Hwang 233

1. Hwang (EX-1007) 233

2. Houghton-Ogawa and Hwang Combination 235

3. Claim Analysis 239

X. ADDITIONAL REMARKS 248

I, Patrick Gerard Traynor, of Gainesville, Florida, declare that:

I. QUALIFICATIONS AND BACKGROUND

1. My name is Patrick Gerard Traynor and I have been retained as an expert witness by Samsung and Google in petitions for *inter partes review* challenging claims of U.S. Patent No. 8,406,733. My qualifications for forming these conclusions are summarized below.

2. I earned a B.S. in Computer Science from the University of Richmond in 2002 and an M.S. and Ph.D. in Computer Science and Engineering from the Pennsylvania State University in 2004 and 2008, respectively. My dissertation, entitled "Characterizing the Impact of Rigidity on the Security of Cellular Telecommunications Networks," focused on security problems that arise in cellular infrastructure when gateways to the broader Internet were created.

3. I am currently a Professor in the Department of Computer and Information Science and Engineering (CISE) at the University of Florida. I was hired under the "Rise to Preeminence" Hiring Campaign and serve as the Associate Chair for Research in my Department. I also hold the endowed position of the John and Mary Lou Dasburg Preeminent Chair in Engineering.

4. Prior to joining the University of Florida, I was an Associate Professor from March to August 2014 and an Assistant Professor of Computer Science from

2008 to March 2014 at the Georgia Institute of Technology. I have supervised many Ph.D., M.S., and undergraduate students during the course of my career.

5. My area of expertise is security, especially as it applies to mobile systems and networks, including cellular networks and messaging. As such, I regularly teach students taking my courses and participating in my research group to program and evaluate software and architectures for mobile and cellular systems. I have taught courses on the topics of network and systems security, cellular networks, and mobile systems at both Georgia Tech and the University of Florida. I also advised and instructed the Information Assurance Officer Training Program for the United States Army Signal Corps in the Spring of 2010. My PhD dissertation concentrated on security issues in messaging for cellular systems.

6. I have received numerous awards for research and teaching, including being named a Kavli Fellow (2017), a Fellow of the Center for Financial Inclusion (2016), and a Research Fellow of the Alfred P. Sloan Foundation (2014). I also won the Lockheed Inspirational Young Faculty Award (2012), was awarded a National Science Foundation (NSF) CAREER Award (2010), and received the Center for Enhancement of Teaching and Learning at Georgia Tech's "Thanks for Being a Great Teacher" Award (2009, 2012, 2013).

7. I have published over 100 articles in top conferences and journals in the areas of information security, mobile systems, and networking. Many of my results

are highly cited, and I have received multiple "Best Paper" Awards. I have also written a book entitled "Security for Telecommunications Networks", which is used in wireless and cellular security courses at a number of top universities.

8. I am a Senior Member of the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE). I am also a member of the USENIX Advanced Computing Systems Association.

9. I serve as an Associate Editor for IEEE Security and Privacy Magazine, have been the Program Chair for eight conferences and workshops, and have served as a member of the Program Committee for over 50 different conferences and workshops. I am also currently the Security Subcommittee Chair for the ACM US Technology Policy Committee (USACM).

10. I was a co-Founder and Research Fellow for a private start-up, Pindrop Security, from 2012 to 2014. Pindrop provides anti-fraud and authentication solutions for Caller-ID spoofing attacks in enterprise call centers by creating and matching acoustic fingerprints. Pindrop Security currently employs over 200 people, and their technology is based off of my research (US Patent 9,037,113 B2).

11. I was a co-Founder and Chief Executive of a private start-up, CryptoDrop. CryptoDrop developed a ransomware detection and recovery tool to provide state of the art protection to home, small business, and enterprise users. This technology was also based off of my research (US Patent 10,685,114 B2).

12. I was also a co-Founder and Chief Executive of a private start-up, Skim Reaper. Skim Reaper developed tools to detect credit card skimming devices, and worked with a range of banks, international law enforcement, regulators, and retailers. This technology was also based off of my research (US Patent 10,496,914 B2).

13. I am a named inventor on ten US patents. These patents detail methods for determining the origin and path taken by phone calls as they traverse various networks, cryptographically authenticating phone calls, providing a secure means of indoor localization using mobile/wireless devices, detecting credit card skimmers, identifying cloned credit cards, and blocking ransomware from encrypting data.

14. My curriculum vitae, included with this declaration, includes a list of publications on which I am a named author. It contains further details regarding my experience, education, publications, and other qualifications to render an expert opinion in connection with this proceeding.

15. In writing this Declaration, I have considered the following: my own knowledge and experience, including my work experience in mobile systems and networks; my experience in teaching those subjects; and my experience in working with others involved in those fields. In addition, I have analyzed the following publications and materials, in addition to other materials I cite in my declaration:

- U.S. Patent No. 8,406,733 (EX-1001), and its accompanying prosecution history (EX -1002)
- 3GPP TS 23.140 v6.9.0 (2005-03); 3rd Generation Partnership Project; Technical Specification Group Terminals; Multimedia Messaging Service (MMS); Functional Description; Stage 2 ("TS-23.140") (EX -1004)
- U.S. Patent No. 8,195,961B2 to Ogawa ("Ogawa") (EX-1005)
- WO 2006/077283 Al to Houghton et al ("Houghton") (EX -1006)
- EP Patent Application Publication No. 1,909,463 A1 to Hwang et al ("Hwang") (EX-1007)
- WO 2008/048075 A1 to Lee et al. ("Lee") (EX-1008)
- U.S. Patent No. 7,975,147 B1 to Qumei ("Qumei") (EX-1009)
- U.S. Patent No. 9,032,192 B2 to Frank ("Frank") (EX-1010)
- Open Mobile Alliance; OMA-ERELD-MMS-v1_2-20030923-C, Enabler Release Definition for MMS Version 1.2," available at *https://www.openmobilealliance.org/release/MMS/V1_2-20030923-C/OMA-ERELD-MMS-V1_2-20030923-C.pdf* (EX-1011)
- Open Mobile Alliance; Multimedia Messaging Service Architecture Overview (MMSARCH) specification, *available at*

https://www.openmobilealliance.org/release/MMS/V1_2-20030923-C/OMA-MMS-ARCH-V1_2-20030920-C.pdf (EX-1012)

- The Secure Sockets Layer ("SSL") Protocol, V. 3.0, available at *https://web.archive.org/web/19970614041044/http://home.netscape.com/eng/ssl3/ssl-toc.html* and *https://web.archive.org/web/19970617034012/http://home.netscape.com/eng/ssl3/3-SPEC.HTM#1* (EX-1013)
- The Transport Layer Security ("TLS") Protocol, V. 1.1, available at *https://www.ietf.org/rfc/rfc4346.txt* (EX-1014)
- U.S. Patent Application Publication No. 2003/0096625 to Mi-Su Lee (EX-1015)
- U.S. Patent No. 7,844,915 to Platzer (EX-1016)
- U.S. Patent No. 8,370,818 to Osminer (EX-1017)
- European Telecommunications Standards Institute AT-F Rapporteur, 4-6 February 2003, Gothenburg, *SP-030167_TD18 -- Liaison from AT-F to 3GPP -- MMS for PSTN-ISDN.doc* (EX-1018)
- Plaintiff Headwater Research LLC's Disclosure of Asserted Claims And Infringement Contentions, *Headwater Research LLC*

v. Samsung Electronics Co., 6:23-cv-00103-JRG-RSP (WDTX) (EX-1021)

- U.S. Patent No. 7,509,487 to Lu et al. ("Lu") (EX-1026)
- U.S. Patent Pub. No. 2005/0207379 to Shen et al. ("Shen") (EX-1027)
- *Transporting data between wireless applications using a messaging system—MMS*, Miraj E Mostafa, Wireless Communications and Mobile Computing (2007) ("Mostafa") (EX-1028)
- Dictionary of Computer Science, Engineering, and Technology, CRC Press LLC, 2001 (EX-1029)
- U.S. Patent No. 8,010,669 to Sathish (EX-1031)
- U.S. Patent No. 7.689,252 to Nishida (EX-1032)
- U.S. Patent No. 6,101,485 to Fortenberry (EX-1033)
- U.S. Patent Pub. No. 2009/0037270 to Patro (EX-1034)
- RDF Primer, W3C Recommendation 10 February, 2004 available at *https://www.w3.org/TR/rdf-primer/* (EX-1035)
- Yahoo's RSS Reader goes LIVE on My Yahoo, available at *https://www.searchenginejournal.com/yahoos-rss-reader-goes-live-on-my-yahoo/212/* (EX-1036)

- Nokia E71 review: Nokia E71, available at *https://www.cnet.com/reviews/nokia-e71-review/* (EX-1037)
- Plaintiff Headwater Research LLC's Amended Infringement Contentions, *Headwater Research LLC v. Samsung Electronics Co.*, 6:23-cv-00103-JRG-RSP (WDTX) (EX-1038)
- U.S. Patent No. 8,620,988 to Sohm et al. ("Sohm") (EX-1039)
- U.S. Patent No. 5,581,704 to Barbara et al. ("Barbara") (EX-1040)

II. LEGAL PRINCIPLES

A. Anticipation

16. I have been informed that a patent claim is invalid as anticipated under 35 U.S.C. § 102 if each and every element of a claim, as properly construed, is found either explicitly or inherently in a single prior art reference. Under the principles of inherency, if the prior art necessarily functions in accordance with, or includes the claimed limitations, it anticipates.

17. I have been informed that a claim is invalid under 35 U.S.C. § 102(a) if the claimed invention was known or used by others in the U.S., or was patented or published anywhere, before the applicant's invention. I further have been informed that a claim is invalid under 35 U.S.C. § 102(b) if the invention was patented or published anywhere, or was in public use, on sale, or offered for sale in this country,

more than one year prior to the filing date of the patent application (critical date). And a claim is invalid, as I have been informed, under 35 U.S.C. § 102(e), if an invention described by that claim was described in a U.S. patent granted on an application for a patent by another that was filed in the U.S. before the date of invention for such a claim.

B. Obviousness

18. I have been informed that a patent claim is invalid as "obvious" under 35 U.S.C. § 103 in light of one or more prior art references if it would have been obvious to a POSITA, taking into account (1) the scope and content of the prior art, (2) the differences between the prior art and the claims, (3) the level of ordinary skill in the art, and (4) any so called "secondary considerations" of non-obviousness, which include: (i) "long felt need" for the claimed invention, (ii) commercial success attributable to the claimed invention, (iii) unexpected results of the claimed invention, and (iv) "copying" of the claimed invention by others. For purposes of my analysis above and because I know of no indication from the patent owner or others to the contrary, I have applied a date of January 28, 2009, as the date of invention in my obviousness analyses, although in many cases the same analysis would hold true even at an earlier time than January 28, 2009.

19. I have been informed that a claim can be obvious in light of a single prior art reference or multiple prior art references. To be obvious in light of a single

prior art reference or multiple prior art references, there must be a reason to modify the single prior art reference, or combine two or more references, in order to achieve the claimed invention. This reason may come from a teaching, suggestion, or motivation to combine, or may come from the reference or references themselves, the knowledge or "common sense" of one skilled in the art, or from the nature of the problem to be solved, and may be explicit or implicit from the prior art as a whole. I have been informed that the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. I also understand it is improper to rely on hindsight in making the obviousness determination.

III. OVERVIEW OF CONCLUSIONS FORMED

20. This expert Declaration explains the conclusions that I have formed based on my analysis. To summarize those conclusions:

- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claims 1-17, 19, 21-27, 29, and 30 of the '733 Patent are obvious over TS-23.140 in view of Ogawa.
- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claims 1, 2, 5, 7-

10, 13-15, 19-22, and 26-30 of the ’733 patent are obvious over Houghton in view of Ogawa.

- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claims 3, 4, 6, 11, 12, 16-18, 23, and 24 of the ’733 Patent are obvious over Houghton in view of Ogawa and Hwang.

IV. BACKGROUND KNOWLEDGE ONE OF SKILL IN THE ART WOULD HAVE HAD PRIOR TO THE PRIORITY DATE OF THE ’733 PATENT

21. Based on the foregoing and upon my experience in this area, a person of ordinary skill in the art (“POSITA”) relating to the subject matter of the ’733 Patent as of January 28, 2009 (“Critical Date”) would have had (1) at least a bachelor’s degree in computer science, electrical engineering, or a related field, and (2) three to five years of experience in services and application implementation in communication networks. Additional graduate education could substitute for professional experience, and *vice versa*.

22. Based on my experiences, I have a good understanding of the capabilities of a POSITA as I possessed and exceeded qualifications of a POSITA at the time of the Critical Date. Moreover, I have taught, participated in

organizations with, and worked closely with many such persons over the course of my career.

V. INTERPRETATIONS OF THE '733 PATENT CLAIMS AT ISSUE

23. I have been informed by Counsel and understand that the best indicator of claim meaning is its usage in the context of the patent specification as understood by one of ordinary skill. I further understand that the words of the claims should be given their plain meaning unless that meaning is inconsistent with the patent specification or the patent's history of examination before the Patent Office. Counsel has also informed me, and I understand that, the words of the claims should be interpreted as they would have been interpreted by one of ordinary skill at the time of the invention was made (not today). I have been informed by Counsel that I should use January 28, 2009 as the point in time for claim interpretation purposes.

VI. TECHNOLOGY BACKGROUND

24. The original and still most common configuration for networked computing is the client/server architecture. As an early example, users of mainframe computers in the 1960s relied on simple "thin clients" with little to no processing power of their own to outsource their computing tasks to mainframes.

25. The benefits of the client/server architecture have long outlived the mainframe era. Client devices, generally with fewer resources (e.g., storage, bandwidth, processing capabilities, power, uptime), still often rely on servers to centralize services and for content distribution. As an example, an email or instant messaging server would not only be better provisioned than a mobile phone communicating with it, but also far more likely to be continuously powered and available on the network.

26. Because servers are better provisioned than their corresponding clients, their communication patterns are generally many-to-one. That is, because of their significant resources (and the expense in provisioning them), a small number of servers are expected to interact with a large number of clients.

27. Networking between the devices is facilitated by networking stacks in both the client and the server. The stacks implement what is known as the "Internet Model," which creates five layers of abstraction for network function: Physical Layer, Data Link Layer, Network Layer, Transport Layer, and Application Layer. The advantage to this approach is that it abstracts away most of the complexity of networking, allowing applications developers to take advantage of communications services without having to know all of the details required to provide said communications.

28. Communication over a network often requires additional security precautions. For instance, an adversary may attempt to read or modify the communications between two parties (in both public and private networks). Before the Critical Date, the security community had created a wide array of mechanisms (specifically, protocols using encryption) allowing for secure communications.

29. These protocols are neither new or uncommon. For instance, Needham and Schroeder developed the first network-based encryption key establishment protocol in 1978 (R. Needham and M. Schroeder, "Using encryption for authentication in large networks of computers." Communications of the ACM. 21 (12): 993–999, 1978). This protocol formed the basis of security protocols (e.g., Kerberos) included in many popular operating systems from the late 1980s and beyond.

30. The need to provide security mechanisms that could be used easily across all communications quickly became widespread. Instead of requiring individual applications or processes to develop their own secure communications protocols, efforts to build secure communications layers into network stacks began in the early 1990s.

31. For instance, the Internet Engineering Task Force (IETF) formed the IP Security (IPsec) Protocol working group in 1992 (IP Security Protocol (ipsec), https://datatracker.ietf.org/wg/ipsec/history/). The IPsec protocol, which is

implemented in nearly all modern operating systems, can provide cryptographic guarantees for confidentiality and integrity for all communications data above the Network Layer.

32. Another important effort to provide security services directly in the network stack was the Secure Sockets Layer (SSL) standardization process, which began in 1994 (The SSL Protocol, https://wwwarchive.mozilla.org/projects/security/pki/nss/ssl/draft02.html, 1994). This standard eventually evolved into the Transport Layer Security (TLS) protocol.

33. TLS is implemented above the Transport Layer and provides security for applications. Possibly the most visible of all security protocols, TLS is used widely to secure applications ranging from the Web (e.g., "https" in browsers) and email to teleconferencing and secure messaging. TLS connections now represent over 80% of all requests on the web (Google Transparency Project - HTTPS encryption on the web, https://transparencyreport.google.com/https/overview?hl=en, 2023).

34. Security mechanisms within individual systems have also long been known to the state of the art. Separation between process (e.g., different applications, users, operating system-level processes) has long been implemented in modern operating systems. For example, classical time-sharing systems from the 1960s separated user processes into isolated time slots not only to allow for seemingly

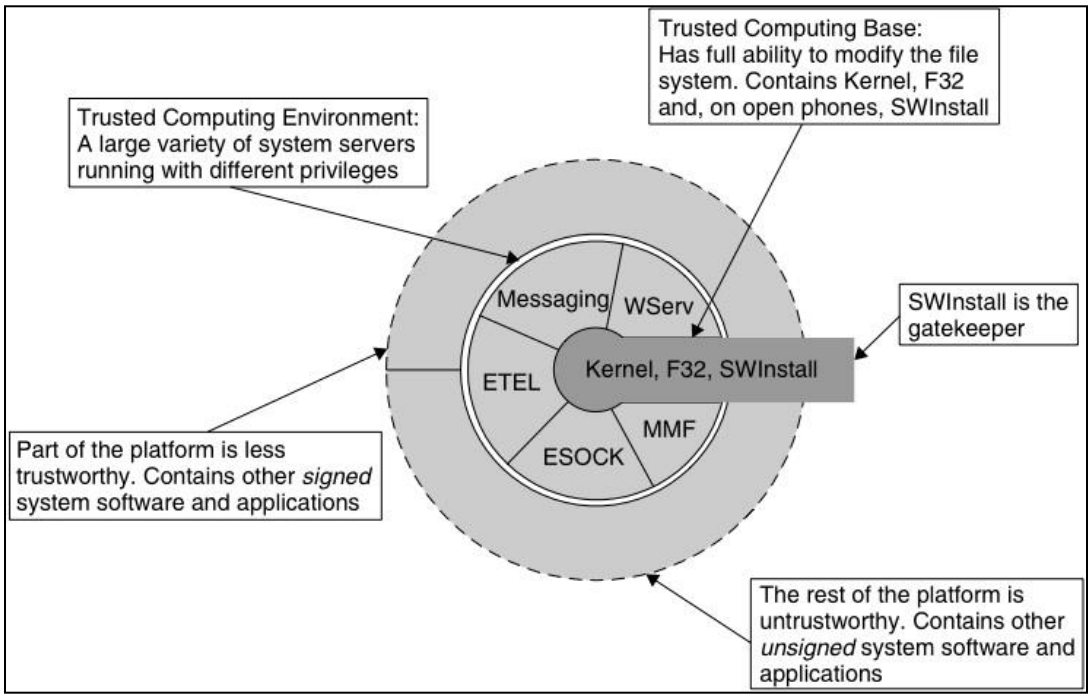
concurrent execution, but also to limit how those processes interacted with each other.

35. Many different techniques were considered in isolation; however, strong protection from and isolation supported by both hardware and software were codified in the MULTICS system in 1969 (M. Schroeder and J. Saltzer, A Hardware Architecture for Implementing Protection Rings, Communications of the ACM, 15 (3). March 1972). Using "Protection Rings", operating systems could now allow not only for the separation of different processes depending on their security needs, but also allow for communication across such security boundaries through highly-controlled mechanisms. Further innovations in the community lead to increasingly secure enclaves, or operating environments, for individual processes.

36. Due to expense, not all operating systems that followed implemented the entire combined hardware and software controls developed for MULTICS; however, the ideas of process separation and controlled communication between such processes continued to be crucial to systems security (J. Saltzer and M. Schroeder, The Protection of Information in Computer Systems, Proceedings of the ACM Symposium on Operating Systems Principles (SOSP), 1974).

37. Advances in hardware made it possible for modern systems, including mobile systems, to implement more secure systems. For example, in the early 2000s, the Symbian mobile operating system (B. Li, E. Reshetova, T. Aura, "Symbian OS

platform security model", LOGIN: Magazine, August 2010; Craig Heath, Symbian OS Platform Security: Software Development Using the Symbian OS Security Architecture (Wiley, 2006)) separated processes into three "Trust Tiers": The Trusted Computing Base (TCB), The Trusted Computing Environment (TCE), and Applications, as illustrated below:



38. The first two layers/tiers shown were primarily dedicated to components of the Operating System with relatively higher operating privileged, followed by the Applications tier with applications having relatively lower privileges.

39. The first two tiers included the Trusted Computing Base and the Trusted Computing Environment. As shown, the Trusted Computing Environment includes, among other services, a Messaging service.

40. The Application Tier could be further subdivided into Signed and Unsigned applications. Signed applications could interact with the TCE and have this layer execute higher privileged requests, whereas Unsigned applications could not access that same functionality.

41. Through these mechanisms and others like them on more recent mobile platforms, it has long been possible for processes to operate in secure enclaves on mobile platforms, and with platform-supported encrypted communications across networks.

VII. OVERVIEW OF THE '733 PATENT

42. The '733 Patent is directed to "devices" "receiving control-plane communications from a network element over a secure service control link." EX-1001, Abstract. Control-plane communications include communications sent over a network "involving supervision" and "control" of "service[s]" being delivered to a device. EX-1001, 37:34-46, 68:19-28.

43. FIG. 16 (below) shows ***service control link 1653*** between service controller 122's ***service control server link 1638*** and device 100's ***service control device link 1691***. In FIG. 16, service control link 1653 is a "control plane communication link [that] provides for a secure (e.g., encrypted) communications link for providing secure, bidirectional communications between the [device's]

service processor 115 and the service controller 122." EX-1001, 68:28-37. FIG. 16's service controller 122 comprises multiple servers (e.g., 1650, 1652, 1654, 1656, 1662). *Id.*, 75:20-77:46.

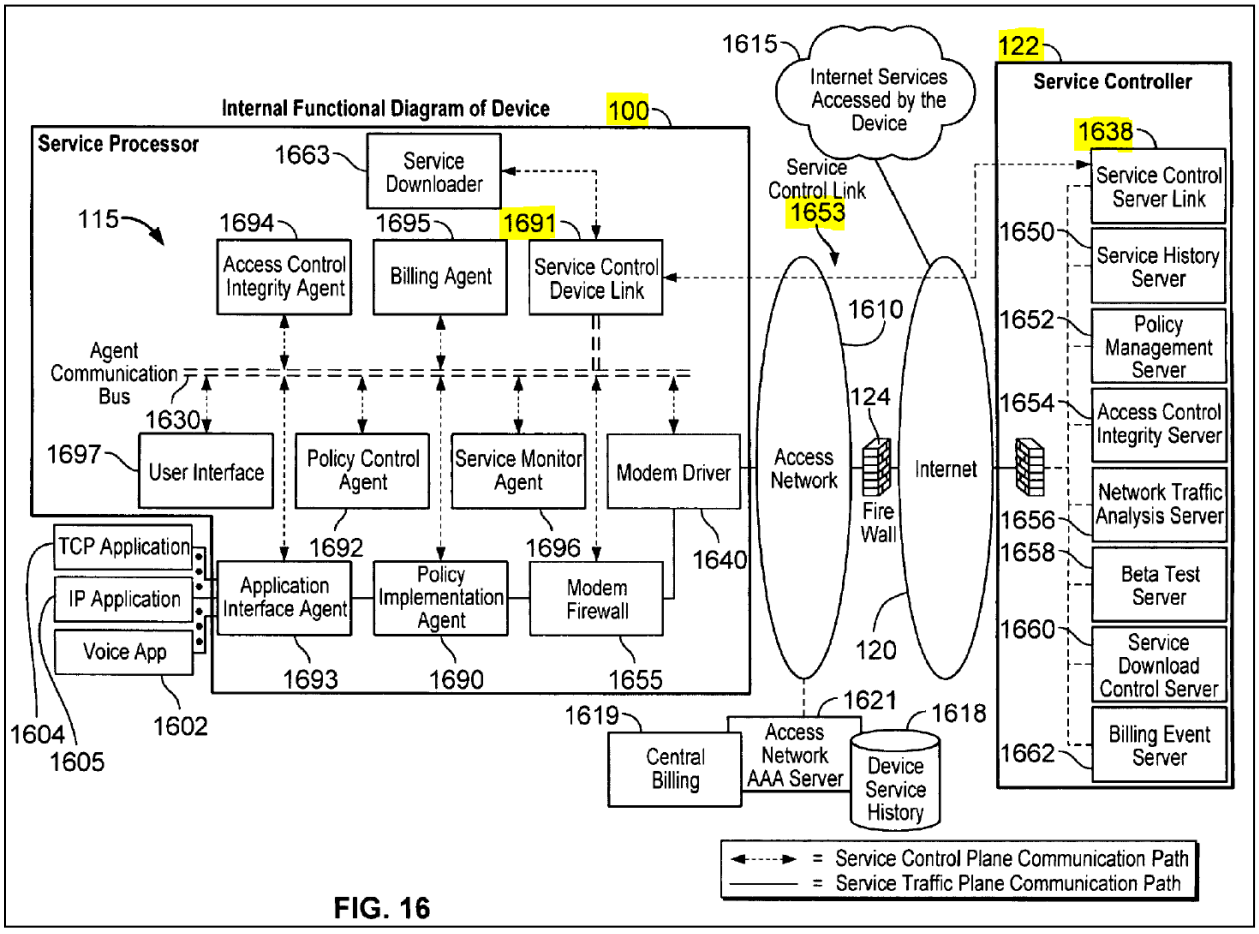


FIG. 16

EX-1001, FIG. 16 (annotated)

44. The specification describes "two or three layers of encryption in the service control link," with one layer "implemented in the transport services stack." EX-1001, 87:58-63. For "secure control plane communication[s]" received by a device from a service controller 122 over link 1653, service control device link 1691 "decode[s]" (*e.g.*, "decrypts"), unpacks, and routes the communication "to the

appropriate agent" on the device using "agent route 2416." *Id.*, 87:49-58, 89:21-33, 90:19-53.

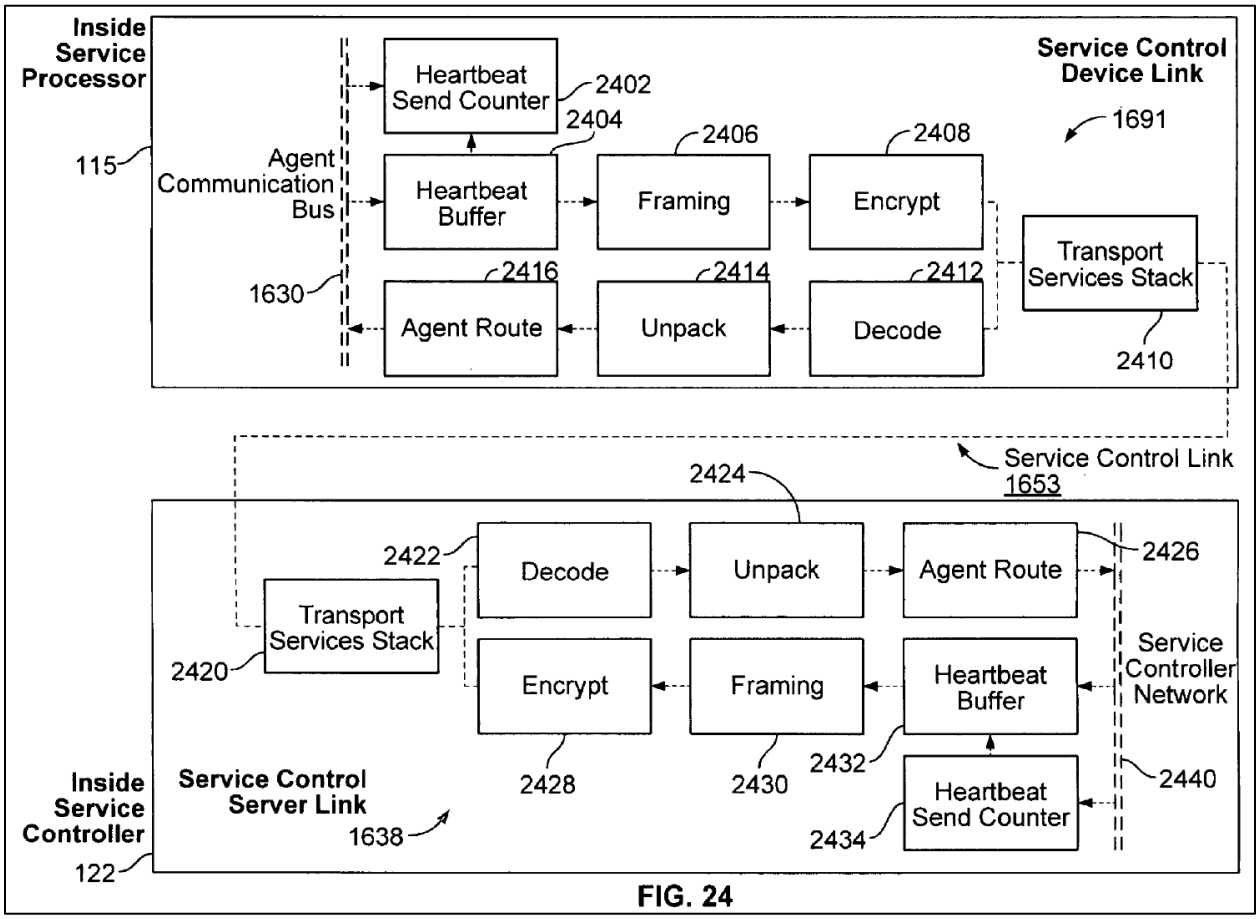
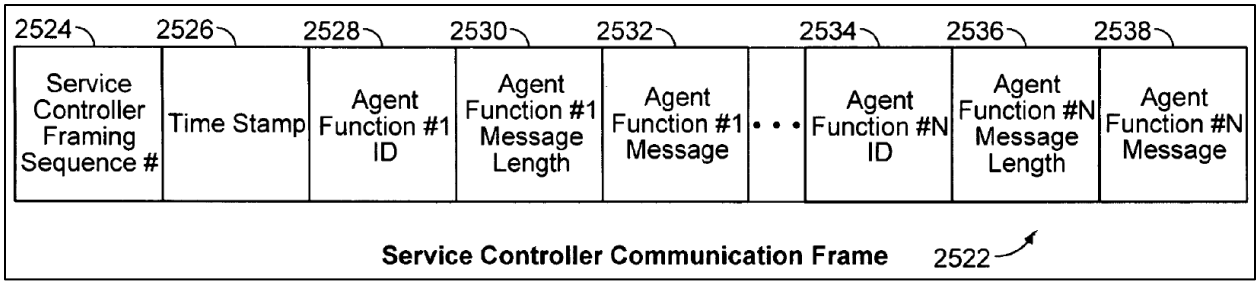


FIG. 24

EX-1001, FIG. 24

45. A communication received from service control server link 1638 "can include one or more messages as shown in FIG. 25." *Id.*, 90:19-53. A message included in a communication received from server link 1638 can include a function ID (e.g., 2528), and an agent function message length (e.g., 2530). *Id.* After decrypting the communication, service control device link 1691 routes the content of the message "to the appropriate agent" on device 100. EX-1001, 89:21-33.



EX-1001, FIG. 25 (annotated)

VIII. PROSECUTION HISTORY OF THE '733 PATENT

46. The application ('141 application) that led to the '733 patent was filed on August 23, 2012, claiming priority to multiple provisional applications. EX-1001, p. 1. The earliest of those provisional applications was filed on January 28, 2009 ("Critical Date").

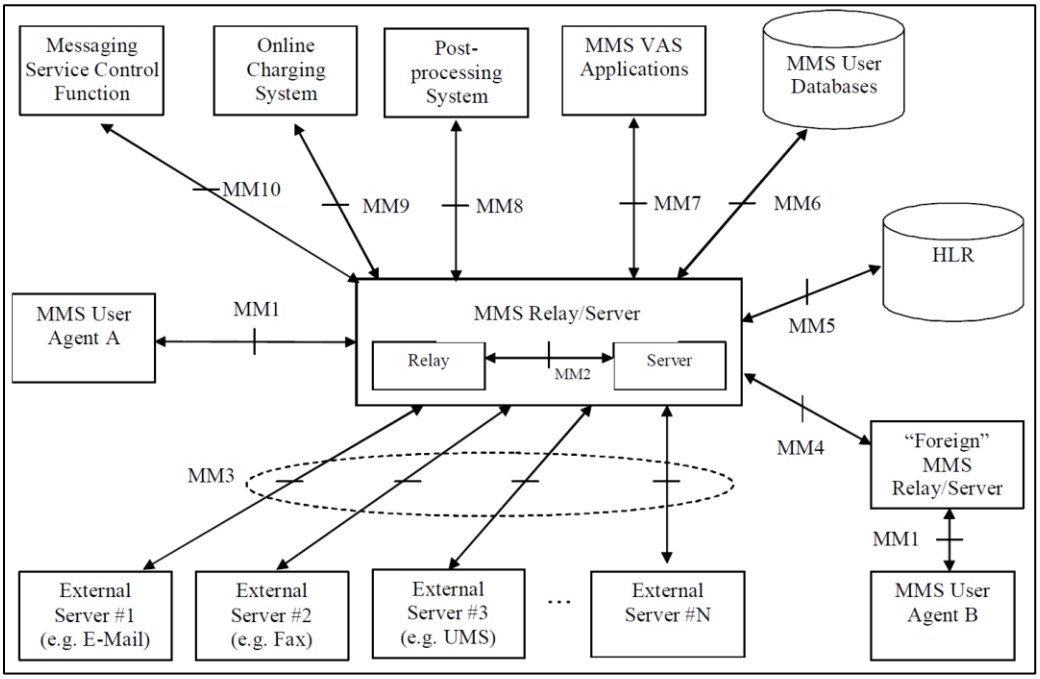
47. The '141 application was allowed after one Office Action that included 35 U.S.C. §112 rejections for multiple phrases recited in independent claims 1 and 30. EX-1002, pp. 99-100. In response, Patent Owner cited to particular portions of the application's specification to provide support, and in the next action, the claims were allowed. *Id*., pp. 36 and 76-78. During prosecution, the Examiner did not consider any of the TS-23.140 (EX-1004), Ogawa (EX-1005), Houghton (EX-1006), and Hwang (EX-1007) references used in this document that in the presented combinations render the Challenged Claims obvious.

IX. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Ground 1: Claims 1-17, 19, 21-27, 29, and 30 Are Obvious Over TS-23.140 and Ogawa

1. TS-23.140 (EX-1004)

48. TS-23.140 is a standard describing a "non-realtime Multimedia Messaging Service, MMS." EX-1004, 10. One MMS implementation environment is shown below:



EX-1004, 24, Figure 3

49. In the figure shown above, "MMS User Agent A" is an "application residing on a UE… or… external device" that "performs MMS-specific operations on a user's behalf and/or on another application's behalf." *Id.*, 14, 18-19. "UE" is used in the field as an abbreviation for "user equipment."

50. The MMS Relay/Server relays messages from the network to the MMS User Agent using interface MM1. EX-1004, 17-18, 21, 23-25. The messages may include "MMS VAS [Value Added Services]" content, "provided… by third-party Value Added Service Providers (VASP)" via interface MM7 (*id.*, 14, 18, 23), and relayed to the MMS User Agent to "provid[e] Value Added Services (e.g. news service or weather forecasts) to MMS users." *Id.*, 14, 41. The MMS Relay/Server can relay messages from "***several*** MMS VAS [Value Added Services] Applications"[1] in the MMS network environment. *Id.*, 18.

51. "MMS may be used to transport data specific to applications" "other than the MMS User Agent." *Id.*, 14, 54-56; *see also* EX-1028, pp. 732-733, section 2.2 (describing multiple applications residing on a user device terminal implemented to use MMS for messaging). The MMS User Agent and the destination applications "reside on [the] MMS User Agent [device]," which a POSITA would have understood to be the same as the UE in the context of this sentence because "MMS User Agent" was a term that was used also to refer to a client device. *See*., *e.g.*, EX-1028, p. 731 ("An MMS user agent (UA), also known as an ***MMS client***, provides means for composing, sending, retrieving, viewing, and other controlling functions to users.").

[1] Emphasis is added throughout unless otherwise indicated.

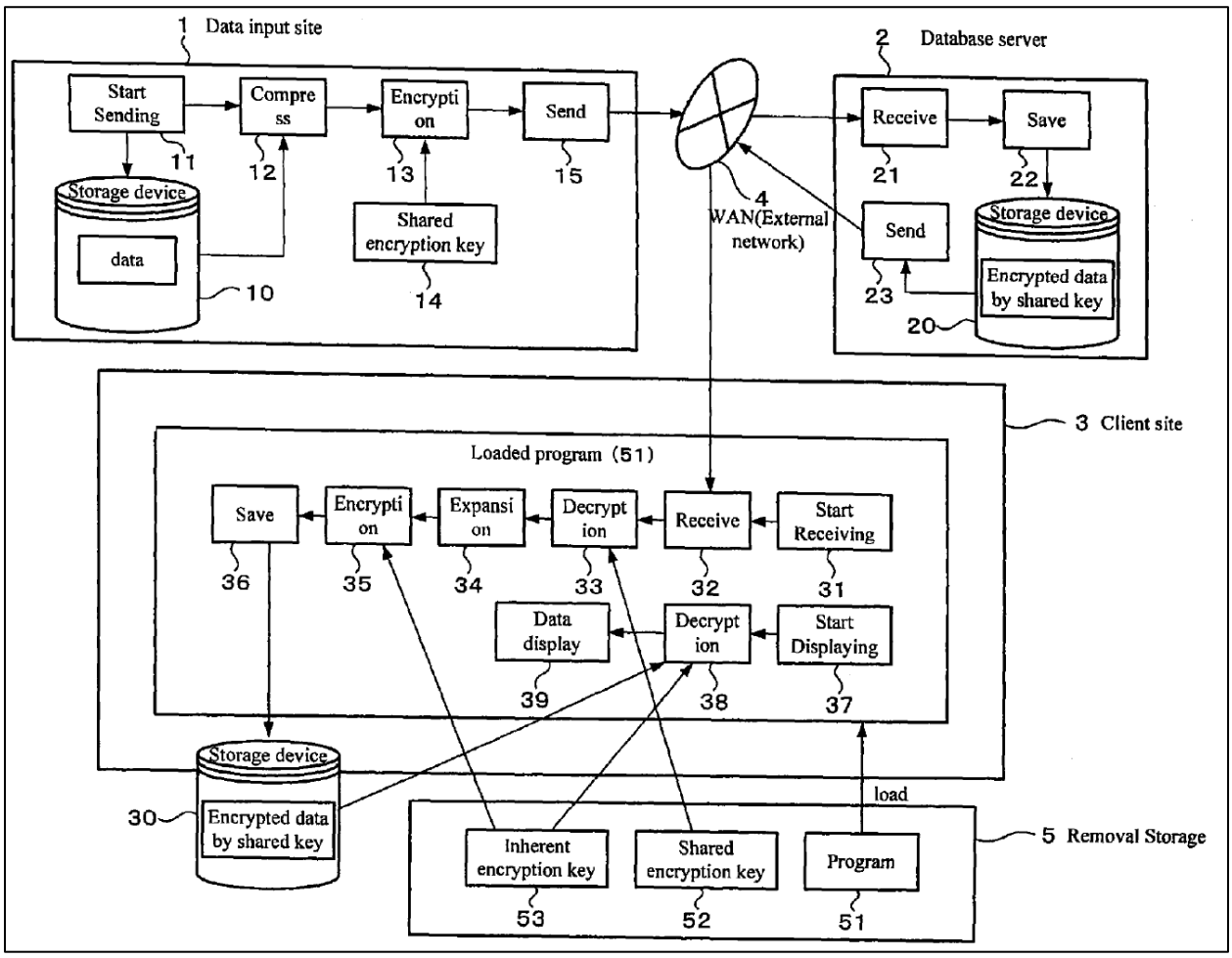
52. For "application data" received as part of a message, "the MMS User Agent… route[s] the received MMS information on to the destination application" using a "destination application identifier" included with the received message. EX-1004, 14, 54-56. More specifically, an application-specific message includes an "application identifier of the destination application" residing on the recipient user device. *Id*. "Upon reception of an abstract message containing a destination application identifier[,] the receiving MMS User Agent…shall first check if the destination application resides on [the UE device]." *Id*. "If the destination application resides on a receiving MMS User Agent, the MMS User Agent shall immediately route the received MMS information on to the destination application that is referred to from the destination application identifier." *Id*.

53. TS-23.140 discloses both "encryption… on an end-user to end-user basis," and using security protocols such as Transport Layer Security (TLS) and "authentication mechanisms based on public/private key cryptography" for securing communications. EX-1004, 19, 41. For example, TS-23.140 notes that "[d]etails for implementation of the MM1 transfer protocol are described in Annex B." EX-1004, §6.3, pp. 25, 162. Annex B refers to EX-1011, which in turn refers to EX-1012 for implementation details of MM1. EX-1004, p. 162; EX-2011, p. 11. EX-1012 explains that "[t]he TLS [WP-TLS] transport layer security protocol provides for secure data transmission between the MMS Client and the MMS Proxy-Relay in

architectural configurations that employ HTTP based protocol stacks for MMSM implementation." EX-1012, p. 21.

2. Ogawa (EX-1005)

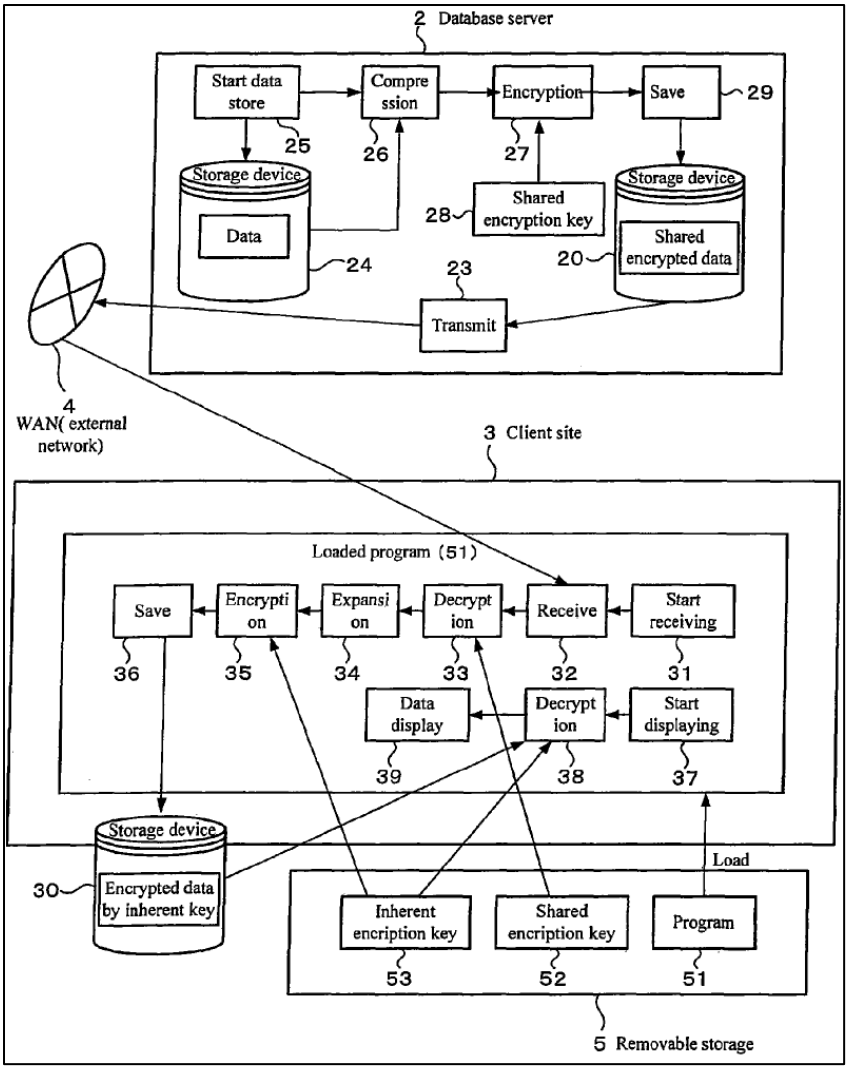
54. Ogawa discloses a "data encryption system," an example of which is shown below:



EX-1005, FIG. 1, 3:18-21

55. As shown, this system facilitates communications between multiple entities, including: (i) data input site 1, (ii) database server 2, and (iii) client site 3. These entities are "operably linked via an external wide area telecommunication network 4," for example, "the Internet" supported by "hyper text transfer protocol (HTTP)." *Id.*; EX-1005, 3:44-54.

56. Ogawa discloses several configurations for its system. FIG. 7, for example, illustrates a client-server system that performs functions described for FIG. 1. In the system shown in FIG. 7, "the database server 2 is integrated with the function of a data input site 1" and "the database server 2 and the client site 3 are connected through the external network 4." EX-1005, 9:16-34.



EX-1005, FIG. 7

57. Ogawa uses security protocols for data transmission between network entities, e.g., between a client computer and a server. "For example, in network communications utilizing a conventional TCP/IP (Transmission Control Protocol/Internet Protocol) or UDP (User Datagram Protocol), ***encryption communication, such as*** IPsec (Internet Protocol Security) or SSL (Secure Socket Layer), is utilized to prevent some security risks presented during the exchange of

data between network terminals." EX-1005, 3:61-4:4. SSL is known as a predecessor of TLS, and thus, TS-23.140 and Ogawa contemplated similar secure data transport within their networks. *See, e.g.*, EX-1010, 1:38-42 ("the Secure Socket layer (SSL) protocol and its successor Transport Layer Security (TLS) provides a mechanism for securely sending data between a server and a client.").

58. Ogawa teaches ***further*** encrypting data using a "shared encryption key" distributed to (and used by) both the client and server. In Ogawa, as shown in FIG 1, data input site 1 includes an encryption unit 13 that encrypts data using a "shared encryption key 14" and transmission unit 15 that transmits the encrypted data over network 4 to data server 2. EX-1005, 4:48-57. Data server 2 stores this data "on a storage device 20 in an encrypted state" (*id.*, 4:58-61) and subsequently transmits it to the client site 3 via network 4. *Id.*, 5:18-23.

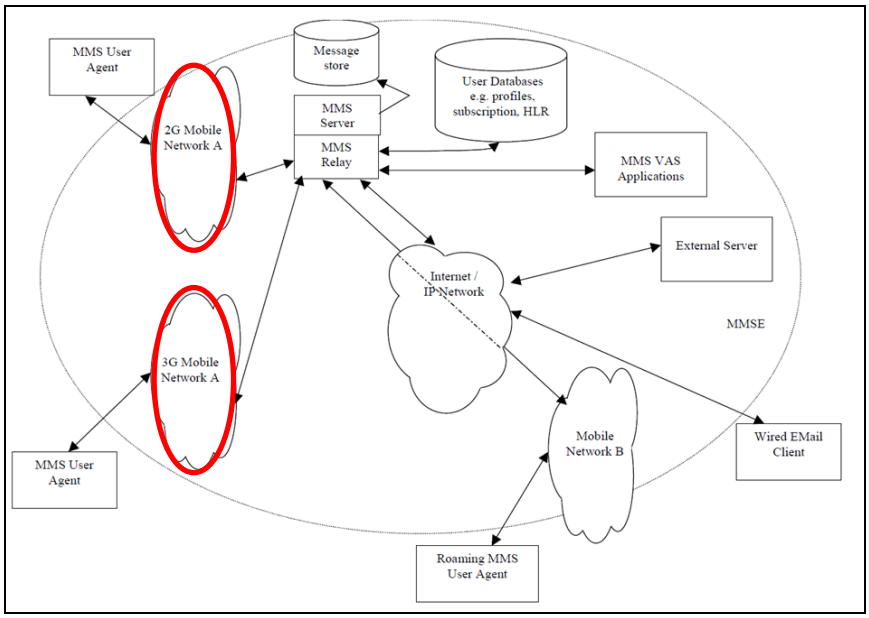
59. The key is used to (1) encrypt data that is transmitted as encrypted data to the client (as discussed above), and (2) decrypt received encrypted data at the client. EX-1005, 9:21-34, 5:60-65. At the client site 3, the encrypted data is received by the receive unit 32 and this encrypted data is decrypted by decryption unit 33 using a shared encryption key 52. *Id.*, 5:59-6:9, 7:11-21. The shared encryption key is stored in storage (e.g., a removable storage 5) and is provided to decryption unit 33 to perform the decryption. *Id*.

60. The shared encryption key is distributed to both data input site 1 and client site 3. EX-1005, 6:42-45. Once client site 3 has the key, "the client site 3 will send the encryption key to the removable storage 5," which is "is operably linked to the client site 3 (physically or wirelessly)." *Id*., 6:46-47, 7:16-21. "When the removable storage 5 receives the encryption key from the client site 3[,] it stores the encryption key into the memory device in the removable storage." *Id*.

3. MMS-Ogawa Combination

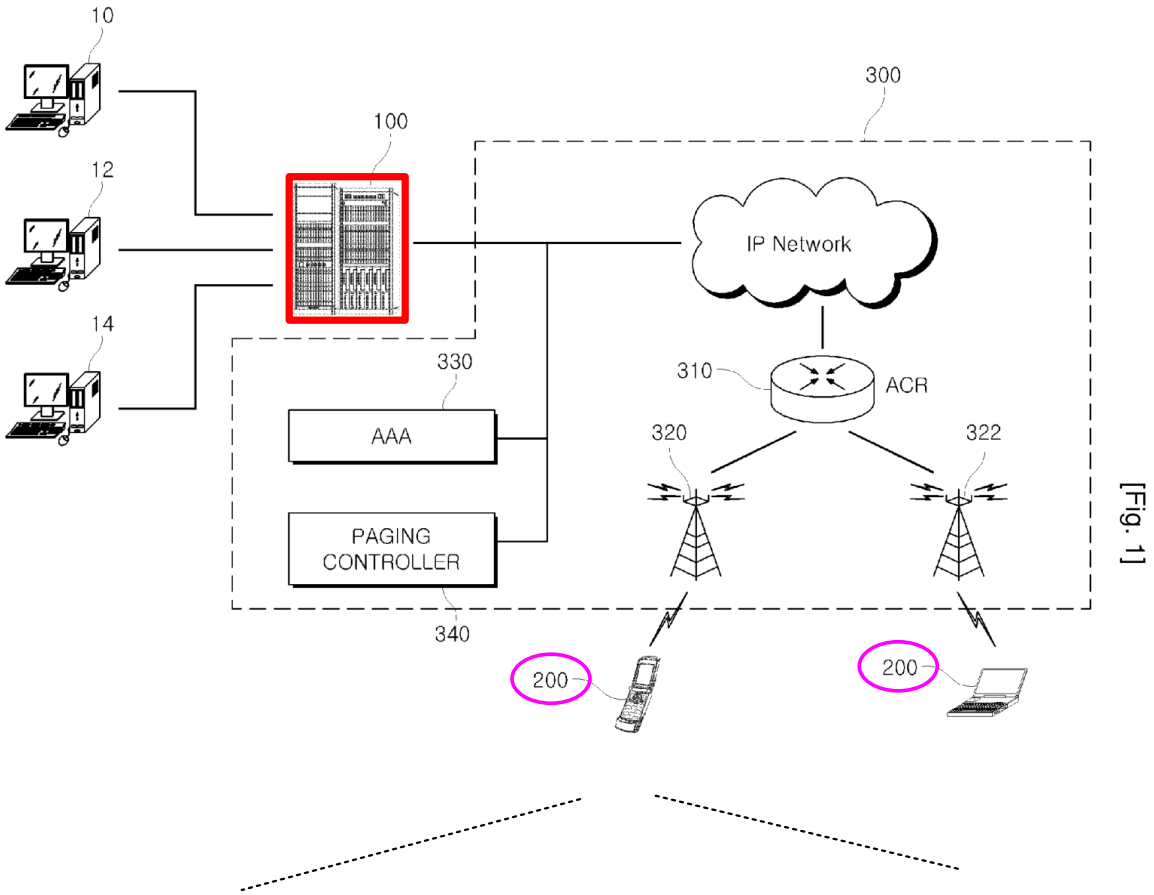
a) Implementing TS-23.140's User Device with a Modem for Network Communications

61. "MMS User Agent" in TS-23.140 "resid[es] on a UE [user equipment]… or… external device." EX-1004, 14, 18-19. TS-23.140 says the User Agent communicates with the MMS Relay/Server using, for example, "2G and 3G wireless networks," but does not disclose details regarding how the device on which the User Agent resides facilitates communications over such networks. *E.g.*, EX-1004, 17, 23-24.

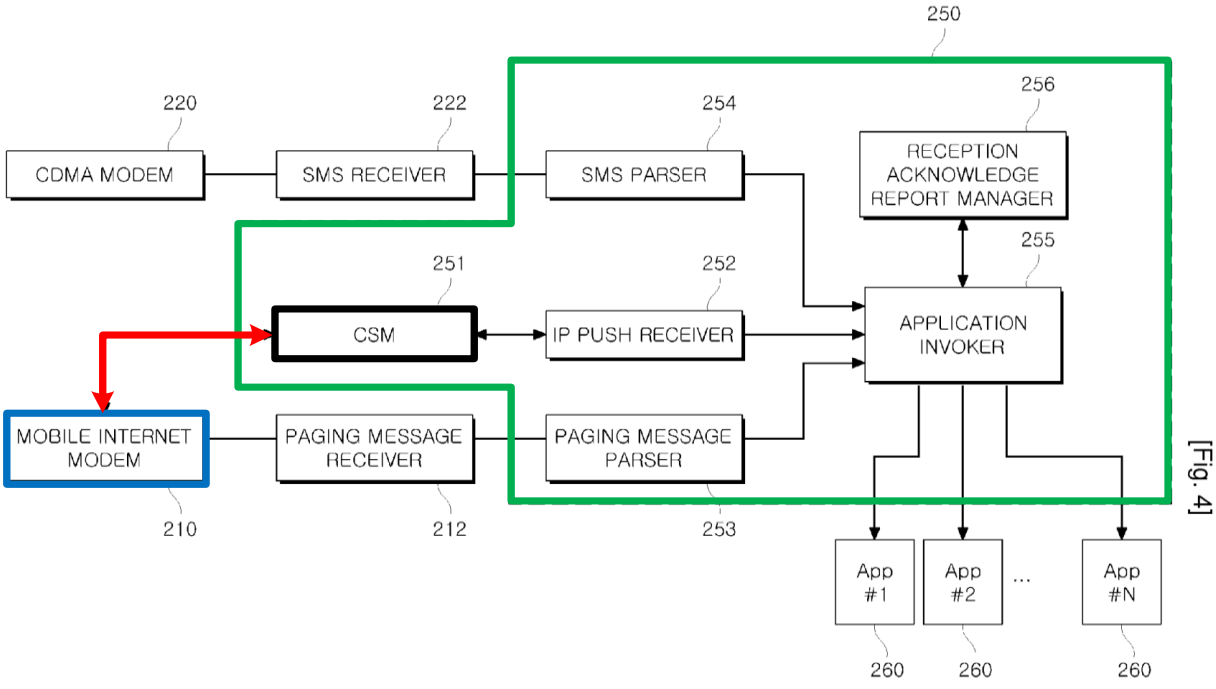


EX-1004, Figure 2 (annotated)

62. Before the Critical Date, it was well-known to use a modem to enable communications over the networks described in TS-23.140. Lee, for example, is a corroborating reference in the general technical field of push communications between network entities and applications executing of a user device. EX-1008, Abstract, ¶¶[1], [8], [44]. Like the MMS User Agent on UE/user device in TS-23.140 that receives messages from MMS relay/server, in Lee, a service agent 250 (green in the figure below) on mobile terminal 200 (pink) receives messages from a service server 100 (red), and the mobile terminal 200 receives the messages through a mobile internet modem 210 (blue). *Id.*, ¶¶[22-23], [27-28].



[Fig. 1]



[Fig. 4]

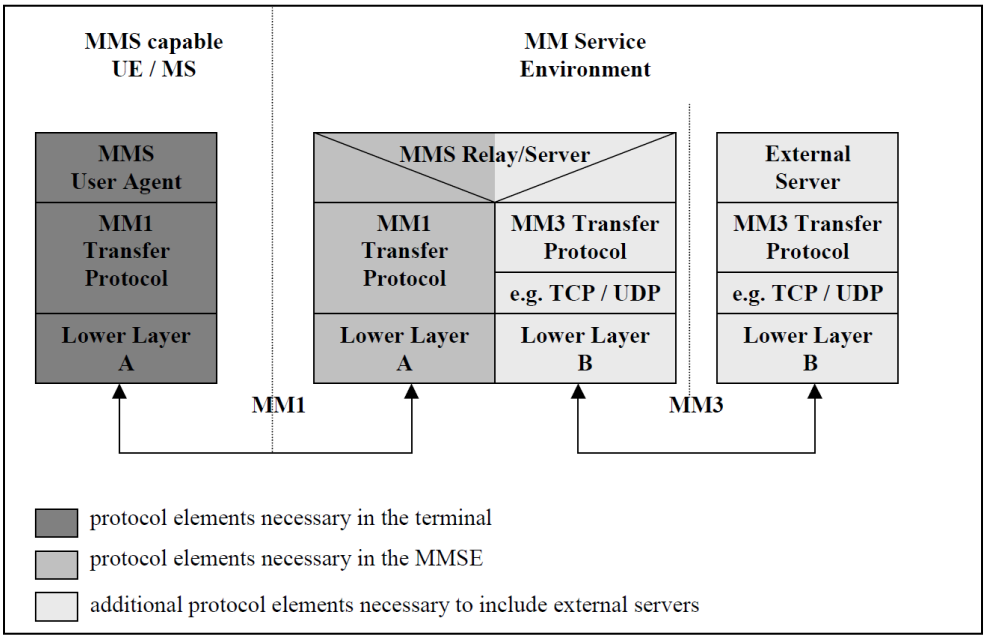
EX-1008, FIG. 1 (top, annotated), and FIG. 4 (bottom, annotated)

63. Indeed, a POSITA would have found it obvious for a computing device to use known networking components, such as a modem, to achieve the predictable result of facilitating network communications, as already contemplated by TS-23.140. Using a modem to enable a user device to communicate over the wireless networks in TS-23.140 would have been a conventional and obvious way to implement what TS-23.140 describes, and is nothing more than utilizing familiar, known components to achieve a predictable result of facilitating TS-23.140's communications. Thus, in view of TS-23.140's teachings of network communication between user devices and networked servers, and knowledge of a POSITA before the Critical Date (as evidenced by Lee's disclosures of the user device using a modem to facilitate such network communications), a POSITA would have found it obvious to implement TS-23.140's system to include a ***modem*** to facilitate the above-described network communications. A POSITA would have reasonably expected success in implementing TS-23.140's device with a modem because this was a well-known, conventional way of achieving the wireless network communications that TS-23.140 describes.

b) Securing Interface MM1 Using SSL/TLS

64. TS-23.140 explains that network communications between the MMS User Agent and the MMS Relay/Server use the MM1 Transfer Protocol. For example, TS-23.140 discloses that MMS shall "make use of the protocol framework

outlined in figure 4" pursuant to which the MMS User Agent communicates with MMS Relay/Server. EX-1004, 24, FIG. 4 (below).



EX-1004, 24, FIG. 4 (annotated)

65. As shown, TS-23.140 discloses that the MM1 Transfer Protocol is implemented both at the MMS Relay/Server and the MMS UE. *See id.* A POSITA would have understood that the MM1 Transfer Protocol facilitates transmission/transport of network communications between the MMS User Agent and MMS Relay/Server (and with other network elements such as MMS VAS Applications, which additionally leverage the MM7 transport interface). *See*, e.g., EX-1018.

66. A POSITA would have had multiple reasons to secure interface MM1 with a TLS/SSL security protocol.

67. ***First,*** it was conventional and well-known before the Critical Date for client-server communications to use SSL/TLS to achieve secure communications between a client and server. *See*, *e.g.*, EX-1012, 21 (disclosing "encrypt[ing] the communication channel between the client and the backend MMS server with some security protocols, e.g., WTLS (Wireless Transport Layer Security")); EX-1010, 1:38-42 ("A variety of ***cryptographic techniques*** are known for securing transactions in data networks. ***For example, the Secure Socket layer (SSL) protocol and its successor Transport Layer Security (TLS) provides a mechanism for securely sending data between a server and a client***."); EX-1013, p. 3 ("Cryptographic security[:] SSL should be used to establish a secure connection between two parties.").

68. ***Second,*** TS-23.140 contemplates implementations which use "transport layer security mechanisms" (*e.g.*, SSL/TLS) to secure its system's communication links, including MM1 between the user device (with the MMS User Agent) and MMS Relay/Server. For example, TS-23.140 contemplates "WAP/OMA implementation" for the "MM1 Transfer Protocol." EX-1004, 56. *See e.g.*, EX-1004, 55, 24-25 (citing to EX-1011, 11, which was incorporated-by-reference into EX-1004, at 13, 162); EX-1012, 21, which was incorporated-by-reference into EX-1011, at 4, 5, 10 ("[t]he ***TLS*** [WP-TLS] transport layer security protocol ***provides for secure data transmission between the MMS Client and the***

MMS Proxy-Relay in architectural configurations that employ HTTP based protocol stacks for MMSM implementation.").

69. ***Third***, such an implementation is nothing more than utilizing familiar, known protocols to achieve a predictable result of facilitating TS-23.140's user agent and other applications to securely interface with one another. For example, in view of TS-23.140, the WAP/OMA implementation contemplated in EX-1012, and the well-known use of TLS/SSL to secure client-server communications before the Critical Date, a POSITA would have found it obvious for the communication link between the MMS User Agent and MMS Relay/Server to use an encryption protocol, such as TLS/SSL to secure the communications sent/received over this link. *See also* EX-1013, p. 3 ("Cryptographic security[:] SSL should be used to establish a secure connection between two parties.").

70. Moreover, a POSITA would have reasonably expected success implementing MM1 to use a TLS/SSL security protocol, given how common their use was before the Critical Date, and given TS-23.140's disclosures.

c) Applying Ogawa's Symmetric Encryption Techniques

71. In addition to "transport layer security mechanisms," TS-23.140 says "authentication mechanisms based on public/private key cryptography may ***also*** be used." EX-1004, 41. TS-23.140 discloses "encryption of an MM [Multimedia Message] on an end-user to end-user basis." EX-1004, 19. A POSITA understood

that "an end-user" can be an MMS User Agent, or an MMS Relay/Server. *See e.g.*, EX-1004, 62 ("Reference point MM1 defines the transactions between the MMS User Agent and the MMS Relay/Server. …Figure 6 illustrates some of these transactions and their relationships, in an ***end-to-end*** manner."). Alternatively, it would have been obvious to a POSITA to ensure a message (being sent between end-users via the MMS Relay/Server) is encrypted when it is stored on the MMS Relay/Server and sent from the MMS Relay/Server to the receiving MMS User Agent. *See* EX-1004, 17 ("The MMS Relay/Server is responsible for storage and handling of incoming and outgoing messages and for the transfer of messages between different messaging systems."). A POSITA would have been motivated to do so, for example, to make sure a message received at the MMS Relay/Server would be secure from, *e.g.*, theft, access, or manipulation while stored there and when sent to the MMS User Agent. *See e.g.*, EX-1005, 8:16-19 (disclosing encryption of a message before storing it and forwarding it to an application for use.)

72. TS-23.140 does not provide details regarding how to implement the additional end-user-to-end-user encryption. However, before the Critical Date, it was well-known to implement encryption for messages transmitted by a push server (*e.g.*, TS-23.140's MMS Relay/Server) to an end-user device using symmetric encryption, with a key that is shared between the server and the end-user device and stored in the respective memories. Multiple references before the Critical Date

disclose encryption solutions where the data in the push messages (MMS messages) is encrypted using a shared key stored by the client and server, and using this shared key for encrypting/decrypting messages between the client and the server. For example, Shen discloses data encryption over push messages (MMS messages) using a shared key established by the client and server and distributed to users, and using this shared key for encrypting/decrypting messages between user devices. EX-1027, [0054]-[0060]; *see also,* EX-1009, 3:25-27 ("an enciphering algorithm and an enciphering key may be stored in the electronic devices"), 8:1-5 ("symmetric cyphering/enciphering may use one or multiple keys for both encryption and decryption").

73. Ogawa discloses details regarding how to implement symmetric encryption on messages in a client-server environment like the one described in TS-23.140, where "SSL… is utilized to prevent some security risks presented during the exchange of data between network terminals." EX-1005, 3:61-4:4, 9:16-34; 3:44-53. A POSITA would have had multiple reasons to Implement Ogawa's symmetric data encryption techniques with TS-23.140's MMS system ("MMS-Ogawa Message Encryption").

74. ***First***, implementing the data encryption taught in Ogawa to TS-23.140's MMS system would have achieved a system "having improved security" and providing "an end-user to end-user" security solution for MMS applications, as

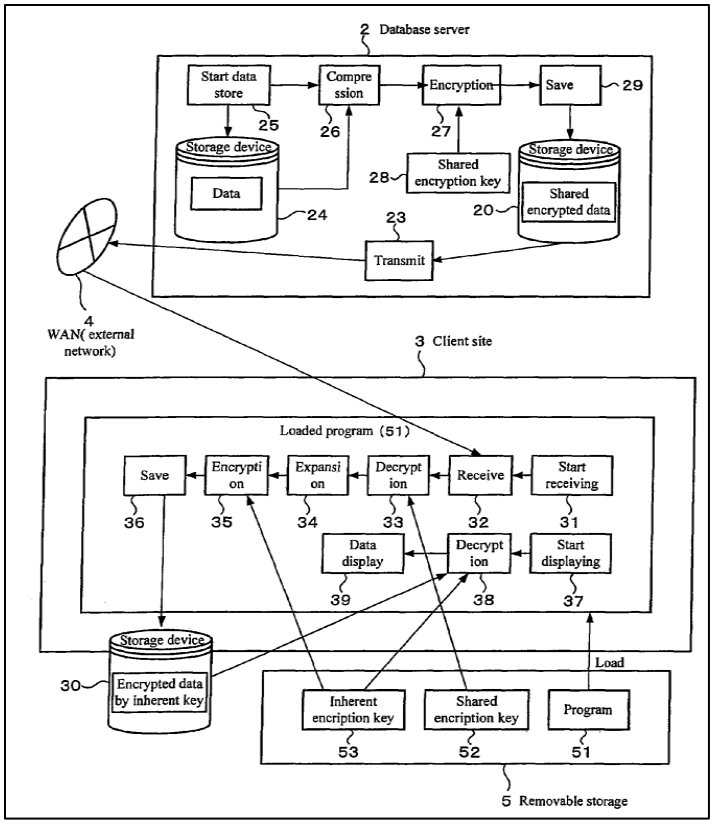
contemplated by TS-23.140. EX-1004, 19; *see also id*., 24-25 (incorporating EX-1011, which incorporates EX-1012); EX-1012, 21 ("[t]he ***TLS*** [WP-TLS] transport layer security protocol ***provides for secure data transmission between the MMS Client and the MMS Proxy-Relay*** in architectural configurations that employ HTTP based protocol stacks for MMSM implementation.").

75. ***Second***, encrypting MMS communications using an additional layer of security beyond SSL/TLS as taught in Ogawa would have provided an MMS system "having improved security," including "providing an end-to-end security solution for MMS applications," which is particularly beneficial for "enterprise applications"—a type of value-added service application that a POSITA would have been motivated to ensure its MMS system could handle. EX-1027, [0017], [0021-0022]; EX-1004, 54.

76. ***Third***, implementing Ogawa's data encryption into TS-23.140's MMS system would have been nothing more than implementing known methods/techniques (symmetric encryption using a shared key as taught in Ogawa) to known systems/devices (the MMS Relay/Server and MMS User Agent device taught in TS-23.140) to achieve predictable results (end-to-end encrypted data, as contemplated by TS-23.140).

77. A POSITA would have had a reasonable expectation of success in implementing Ogawa's encryption techniques to the TS-23.140 system given (1) the

similar client-server communication architectures taught by both references (with connections between network elements protected by, *e.g.*, SSL/TLS) and (2) TS-23.140 contemplates end-user-to-end-user encryption, and Ogawa (and corroborating references) provided an exemplary, predictable implementation of such encryption using a symmetric, shared encryption key. Specifically, in the same field of client-server communications, Ogawa explains how symmetric encryption can be implemented for securing communications in similar networked environments. Similar to TS-23.140, Ogawa uses the SSL protocol (which is a predecessor of the TLS protocol) to facilitate secure network communications between a server and a user device. EX-1005, 3:60-4:4. As illustrated in FIG. 7 of Ogawa (reproduced below), database server 2 transmits an encrypted message to client site 3 through network 4 using this secure, SSL-enabled communication link and in doing so, Ogawa seeks "to prevent some security risks presented during the exchange of data between network terminals." EX-1005, 3:44-53; 9:16-34 (network 4 uses HTTP protocol for message transmission).



EX-1005, FIG. 7

78. Additionally, Ogawa discloses applying data encryption to messages transmitted between devices, and for such data to be encrypted, using a symmetric/shared key between the client and server. EX-1005, 4:53-54, 7:10-12. Ogawa provides an example of how such symmetric encryption works—i.e., by storing a shared key in each respective device's memory that would be used for both encrypting and decrypting a transmitted or received message. EX-1005, 4:48-57, 5:59-65, 6:64-7:21. This is further corroborated by Qumei. *See e.g.*, EX-1009, 3:25-27 ("an enciphering algorithm and an enciphering key may be stored in the

electronic devices"), 8:1-5 ("symmetric cyphering/enciphering may use one or multiple keys for both encryption and decryption").

79. Given TS-23.140's teaching of end-to-end encryption and the well-known use of symmetric encryption implemented at the MMS Relay/Server to facilitate such end-to-end data encryption, a POSITA would have been motivated and would have had a reasonable expectation of success to implement Ogawa's encryption teachings of using a shared encryption key to encrypt such server-client communications. Such a combination would have amounted to implementing known methods/techniques (symmetric encryption) to known systems/devices (MMS Relay/Server, devices/terminals with MMS User Agents) to achieve predictable results (end-user-to-end-user encrypted data, as contemplated by TS-23.140). Such a combination would have also been predictable and straightforward to implement (and a POSITA would have had a reasonable expectation of success in doing so) given the similar MMS/client-server architectures taught by both references and given that TS-23.140 contemplates end-to-end encryption and Ogawa (and the above-described corroboration references) provides one example and predictable implementation of such encryption using a symmetric/shared encryption key.

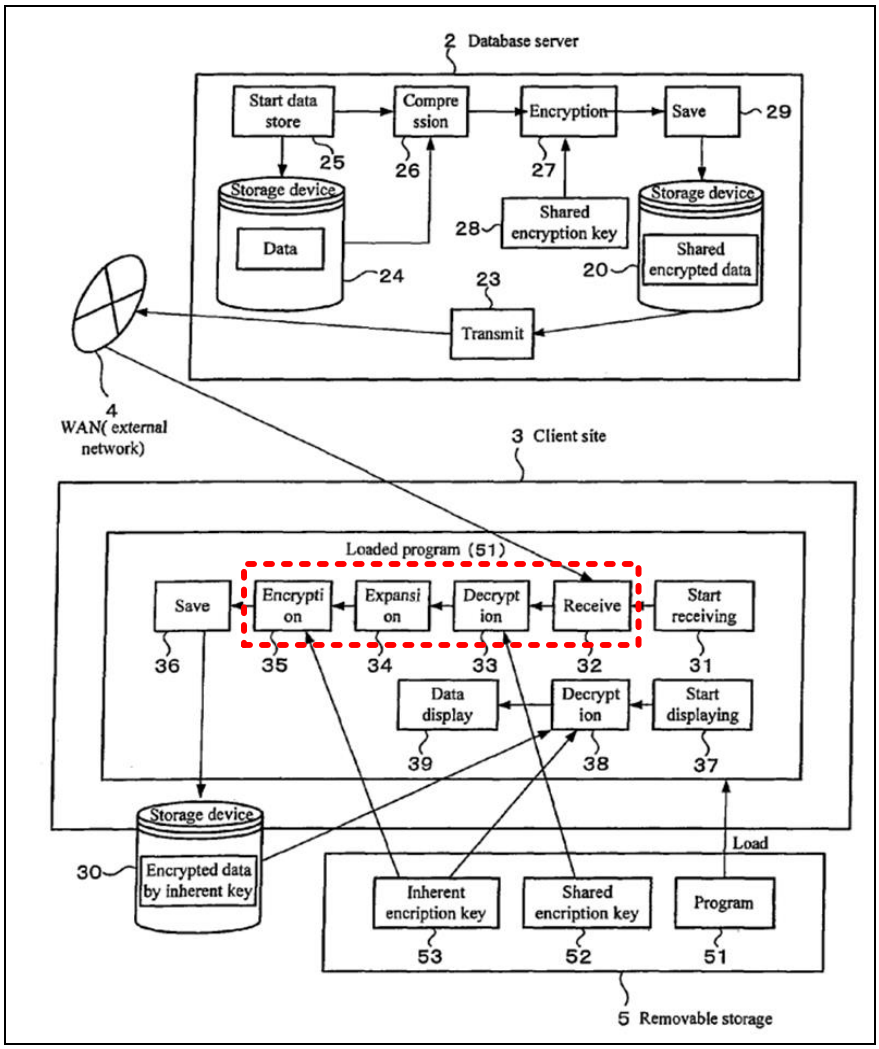
d) Ogawa's Decryption and Encryption Units

80. Ogawa teaches a "decryption unit" for decrypting received encrypted data as part of its symmetric encryption system. EX-1005, 5:59-6:9 ("[R]eceived shared key encrypted data will be decrypted using the shared encryption key 52 which was supplied to the decryption unit 33 and beforehand stored…"). A POSITA would have had reason to implement the decryption unit as part of the MMS User Agent in TS-23.140, because (1) the MMS User Agent is responsible for receiving data from TS-23.140's MMS Relay/Server and distributing the data to the correct applications on the user device, and (2) TS-23.140 expressly identifies the MMS User Agent as "provid[ing]… functionalities such as … ***decryption***." EX-1004, 14, 54-56. Such an implementation would have, for example, beneficially allowed the MMS User Agent to decrypt an encrypted message from the MMS Relay/Server and any information identifying the destination application to which the message should be routed.

81. Further, a POSITA would have sought to implement the decryption unit as part of MMS User Agent because the MMS User Agent is responsible for receiving messages from the push server and subsequently distributing them to the correct agents/applications on the mobile terminal. A POSITA would have recognized that the MMS User Agent in such an implementation would have beneficially been able to decrypt the encrypted message to identify the destination

application included in the message—particularly in the case where the entire message is encrypted (including the identifying information specifying where to route the received message).

82. Ogawa also teaches an encryption unit for encrypting (or "re-encrypt[ing]") data before transmitting it to another part of the device, *e.g.*, storage. EX-1005, 5:59-6:9. As with the decryption unit, a POSITA would have had reason to implement the encryption unit as part of the MMS User Agent in TS-23.140, because (1) being able to securely store data on a user device was a desirable feature that would have helped prevent, *e.g.*, theft, (2) the MMS User Agent is responsible for "all aspects of ***storing***" messages on TS-23.140's user device, and (3) TS-23.140 expressly identifies the MMS User Agent as "provid[ing]… functionalities such as … ***encryption***." EX-1004, 14. Further, a POSITA would have found it obvious to incorporate into MMS User Agent any unit that perform intermediary tasks coming between the data receiving function and the data distribution function, to prepare the data for use by the mobile terminal. Examples of such units are decryption unit 33 and encryption unit 35 in Ogawa. Decryption unit 33 decrypts the data received from server 2, and encryption unit 35 re-encrypts the decrypted data before transmitting it to another part of the device, e.g., storing on the storage device 30. EX-1005, 5:59-6:9.



EX-1005, FIG. 7 (annotated)

83. A POSITA would have reasonably expected success in an implementation with Ogawa's encrypt and decrypt units incorporated into TS-23.140's MMS User Agent, because the prior art components would continue to perform functions they performed prior to the combination—MMS User Agents and the MMS Relay/Server would continue to exchange data using secure communication links, and Ogawa's decrypt and encrypt units (as implemented as part of the MMS User Agent) would use encryption keys to decrypt/encrypt data

received from the MMS Relay/Server. Such a combination would have been well within a POSITA's capability to implement.

e) Storing Ogawa's Shared Encryption Key

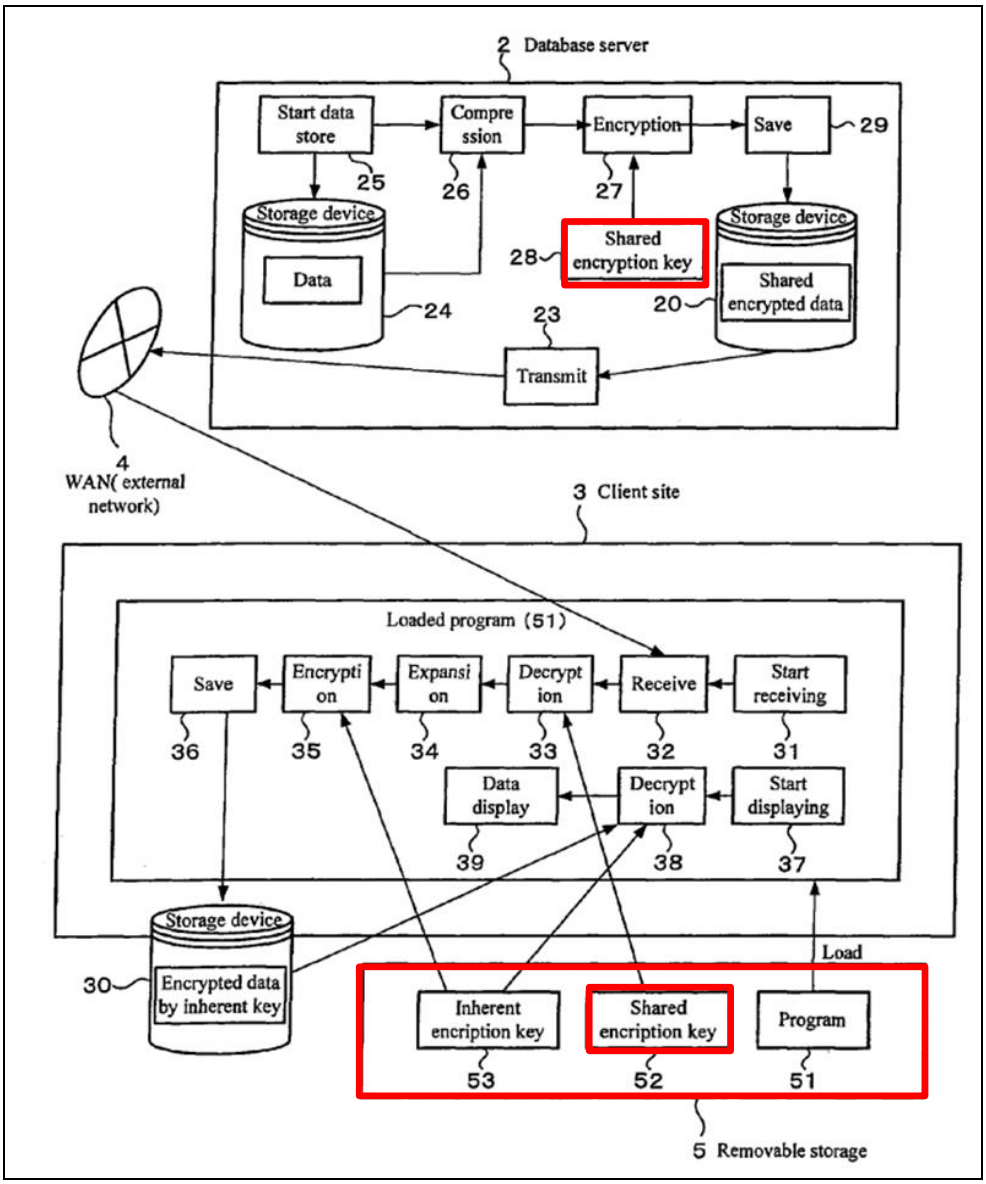
84. TS-23.140's user device has "memory." EX-1004, 19-20. Ogawa teaches the well-known technique of ensuring that each device/entity in a network environment that encrypts or decrypts communications using symmetric encryption ***stores*** the encryption key in memory connected to it. EX-1005, 3:18-34, 4:48-57, 5:59-65, 6:64-7:21, FIGS. 1, 7. Specifically, multiple references before the Critical Date, including Ogawa, contemplated each device/entity—involved in encrypted communication using symmetric encryption—stores the encryption key in memory connected to the respective device. *See, e.g.*, EX-1005, 3:18-34, FIGS. 1, 7; EX-1009, 8:1-5, 3:25-27; EX-1006, 29, claim 3 (contemplating "exchanging security keys" between the server and the client).

85. For symmetric encryption, there were a limited number of ways to ensure the same key was used by encrypting/decrypting devices, including: (1) storage of the same key at each encrypting/decrypting device in persistent memory, and (2) generation of the same key at each encrypting/decrypting device prior to performing the encrypting/decrypting operation, and storage of that key temporarily during the operation. In the first scenario, the shared key would be stored in persistent memory of one or both devices, and in the second scenario, the generated

key would be generated at runtime but would be stored temporarily during the encryption/decryption process. In both ways, the key was stored during the encryption/decryption.

86. A POSITA would have had multiple reasons to store Ogawa's encryption key in the TS-23.140 user device's memory to facilitate decryption of encrypted messages received from the MMS Relay/Server.

87. ***First***, an implementation in which the encryption key was stored in TS-23.140 user device's memory would have been a way to implement the symmetric encryption teachings of Ogawa, which discloses storing the shared encryption key in removable storage 5 that is connected to client site 3 and functions as a memory for the client site 3, so that the key can be retrieved and used when needed to decrypt a message. EX-1005, 3:61-4:7, 5:41-47, 5:60-65, 9:21-34, FIG. 7.



EX-1005, FIG. 7 (annotated)

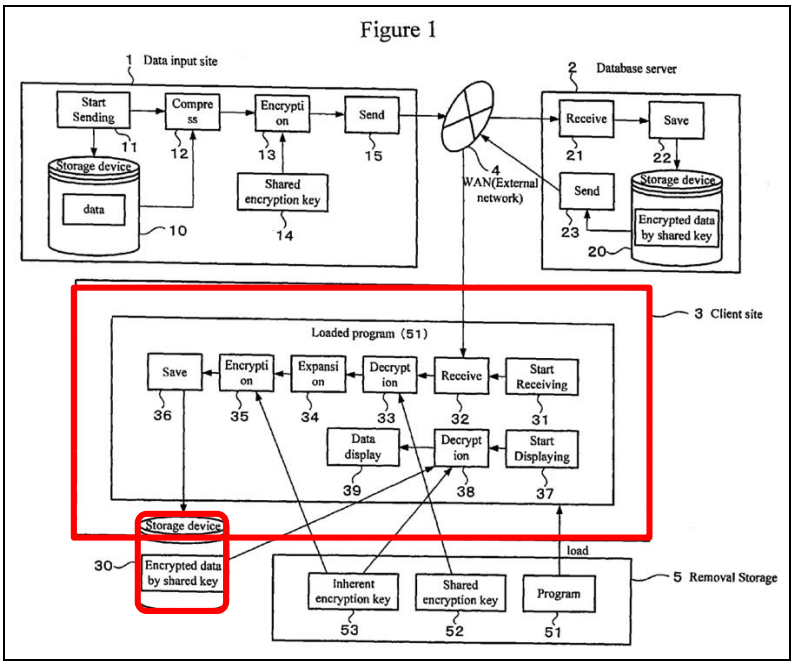
88. Storing Ogawa's encryption key in memory of the TS-23.140 user device (i.e., the client site, in Ogawa's terminology) would have beneficially enabled the MMS User Agent (modified to include Ogawa's decryption and encryption units, as discussed above) to access the key and perform the decryption/encryption described in Ogawa.

89. ***Second,*** such an *implementation* would have been nothing more than implementing a known method (storage of a symmetric/shared key in memory as taught by Ogawa and background references) to known systems (TS-23.140's user device with memory) to achieve a predictable result of enabling Ogawa's symmetric encryption/decryption of communications between TS-23.140's MMS User Agent and MMS Relay/Server.

90. ***Third***, storing the shared key on memory within TS-23.140's user device would have been an obvious, readily-implementable design choice that a POSITA would have known would facilitate storing of Ogawa's shared encryption key in a location accessible to the user device, as was necessary for symmetric encryption. That this design was well-known to POSITAs is corroborated by references like Qumei, which describes storing an "enciphering key" in an end-user device (e.g., a mobile handset). EX-1009, 3:25-27.

91. Ogawa's removable storage 5 is part of the end-user device because it is connected to the client site 3 and functions as a memory for the client site 3 to store the shared key, and to retrieve it when needed to decrypt a message. EX-1005, 5:41-47. Ogawa further discloses that "the shared key encrypted data will be received by the [client site 3] from the database server 2 via network 4." EX-1005, 5:60-65. "This received shared key encrypted data will be decrypted using the shared encryption key 52 which was supplied to decryption unit 33 and beforehand

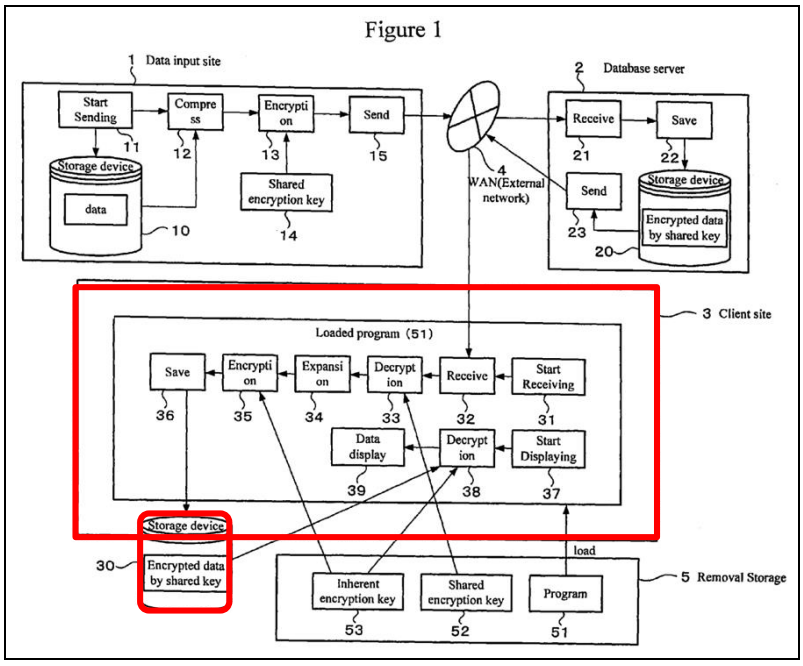
stored on the removable storage 5." *Id.*; *see also id.*, 6:64-7:21 ("When the removable storage 5 receives the encryption key from the client site 3 in step S15, it stores the encryption key into the memory device in the removable storage in step S16.").



EX-1005, FIG. 7 (annotated)

92. However, even if Ogawa's removable storage 5 were not considered part of the end-user device, having such memory resident on the end user device would have been obvious in view of Ogawa's teachings as well as the well-known use of storing encryption keys in memory resident in end-user device in the relevant timeframe. For example, Ogawa uses the removable memory 5 for mobility or group settings. EX-1005, 5:49-58. Removable memory 5 enhances mobility because it can be implemented "as a USB memory device, flash drive, Zip disk, floppy disk,

compact disc, miniSD, or even DVD RAM," attachable to the client 3 by being "physically coupled to the client site 3." EX-1005, 5:42-51. "A plurality of removable storage 5 devices may also be used, wherein each removable storage 5 contains the same program (or encryption key)…for encrypted data to be shared by members of a common group." *Id.*, 5:54-58. If such independent mobility or group settings are not required or needed for the intended environment, a POSITA would have found it obvious to simply store the shared key on a memory fixed to the client site 3, for example, on storage device 30.



EX-1005, FIG. 7 (annotated)

93. Alternatively, or additionally, storing the shared key on a memory installed/resident within the end user device would have been an obvious design choice that would be readily implemented to facilitate data storage, including storage

of the above-described shared encryption key. Qumei, for example, corroborates storing the "enciphering key" in the end-user device (e.g., a mobile handset), thus confirming that it would have been obvious to implement storage of the shared key within memory resident within the end-user devices. EX-1009, 3:25-27.

94. Therefore, in the MMS-Ogawa combination, a POSITA would have found obvious to store the encryption key in the device's memory—as contemplated by Ogawa and further corroborated by other references such as Qumei—to facilitate the (symmetric) encryption/decryption of the communications between MMS Relay/Server and MMS User Agent over the communication link. Also, in the MMS-Ogawa combination, the key would then be retrieved from memory to facilitate decryption of an encrypted message, as further contemplated by Ogawa. EX-1005, 3:61-4:7; 9:21-34.

95. Storing the encryption key in TS-23.140's device's memory and enabling it to be retrieved from memory when needed would have been well within a POSITA's skill to implement, and a POSITA would reasonably have expected success in doing so, because this would have involved using components to perform the functions they performed prior to the combination.

f) MMS-Ogawa

96. "MMS-Ogawa" refers to the above-discussed encrypted MMS system that a POSITA would have been led to form based on TS-23.140 and Ogawa. MMS-

Ogawa implements TS-23.140's user device (which is configured to use the MMS service as described in TS-23.140) with a modem for wireless network communications. *Supra* § IX.A.3(a).

97. MMS-Ogawa also implements TS-23.140's MMS Relay/Server and user device so that messages transmitted across the interface between TS-23.140's user device and the MMS Relay/Server are secured with both SSL/TLS and encrypted using symmetric MMS-Ogawa Message Encryption. *Supra* §§ IX.A.3(b)-IX.A.3(c).

98. In MMS-Ogawa, Ogawa's encrypt and decrypt units are implemented as part of the MMS User Agent in TS-23.140's user device (*supra* § IX.A.3(d)), and a common key is distributed to (and stored in the respective memories of) TS-23.140's user device and MMS Relay/Server (*supra* § IX.A.3(e)).

4. Claim Analysis

a) Claims 1 and 30

[1pre]: An end-user device comprising:
[30pre]: A method performed by an end-user device, the method comprising:

99. The '733 specification does not define any requirements for an "end-user device" (*see* EX-1001, 8:3-15, 8:60-9:15), but uses the term to include "networked" devices that have "services delivered" to them. EX-1001, 5:65-6:28, 6:49-56. A POSITA understood that the "devices" described in columns 5-6 were

the "end user devices" described in columns 8-9. To the extent the preambles are limiting, a POSITA understood MMS-Ogawa's "UE [***user*** equipment]"/"external ***device***"—with a MMS User Agent that "performs… operations on a ***user's*** behalf," and through which "Value Added Services" are "provided" (delivered) to "***users***"—is an "end-user device." EX-1004, 14. As explained below, MMS-Ogawa's end-user device performs the method of claim 30.

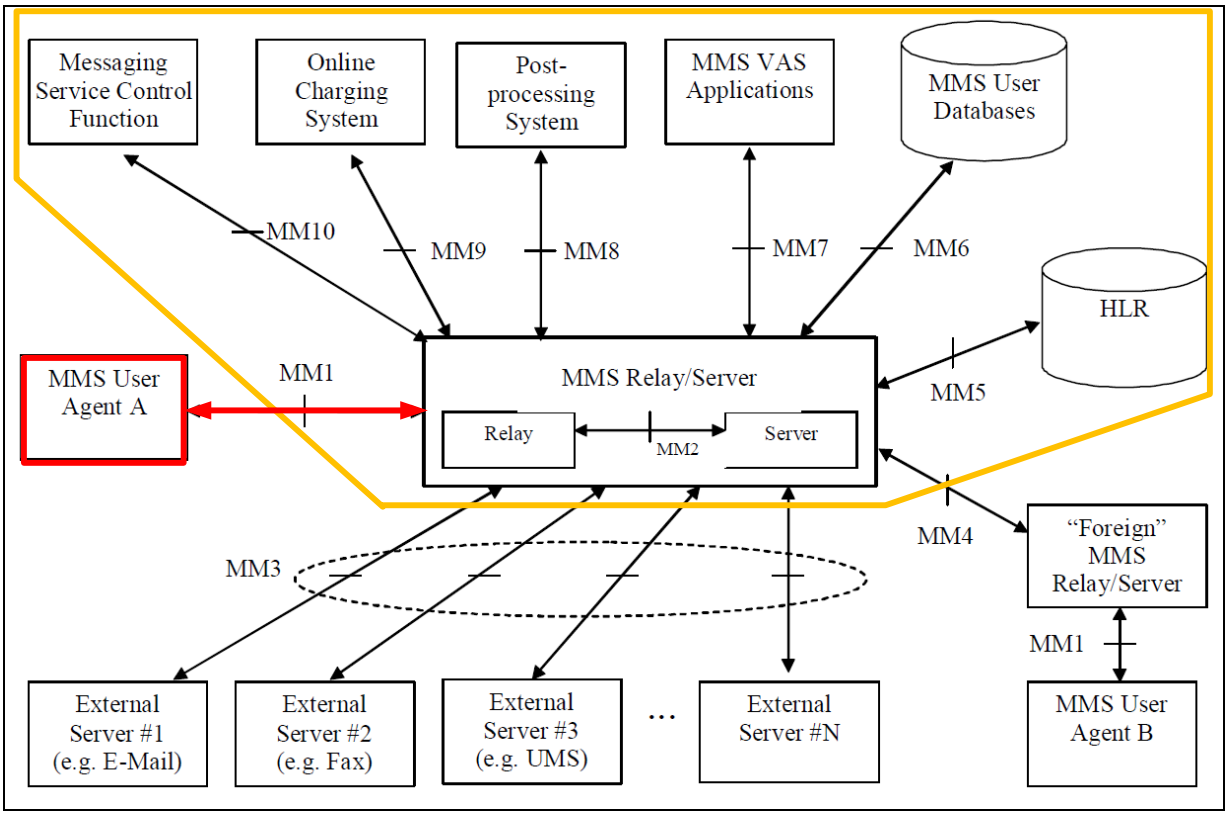
[1a] a modem for enabling communication with a network system over a service control link provided by the network system over a wireless access network,

100. Element [1a] requires "a ***modem*** for enabling communication" that takes place "over a wireless access network." The '733 specification uses "modem" broadly to include those that enable communication over "2G" and "3G" "wireless access networks." EX-1001, 12:61-13:32, 25:29-45, 27:38-44, 29:52-53, 33:59-65, 34:24-27. MMS-Ogawa's modem for 2G and 3G wireless networks (*supra* § IX.A.3(a)) is thus a "modem for enabling communication" taking place "over a wireless access network" as claimed.

101. Element [1a] also requires that the modem enable communication "with a ***network system*** over a service control link." The '733 specification never describes a "***network system***" in the context of a "service control link." Although the term "network systems" is used in column 135 (lines 29-53) of the '733 Patent, it was in a different context where it does not appear to be describing "communication" "over a service control link." According to the specification, a "service control link"

is a "communication link" "between a device and ***the network***"—which, in the specification's embodiments, is represented by "service controller 122." EX-1001, 17:8-11, 68:20-37, FIGs. 16-20 (showing that service control link 1653 is always shown to link the device to service controller 122). The specification says service controller 122 may "include[] one or more server functions," and may be "implemented on multiple servers… or…. on a single server." EX-1001, 16:13-26. A POSITA thus understood that one or more servers performing one or more server functions would meet the claimed "network system."

102. The modem in MMS-Ogawa's end-user device enables a MMS User Agent to communicate with various network elements (orange below) through interface MM1—including MMS-Ogawa's Relay/Server and multiple VAS applications (via the Relay/Server). EX-1004, 14, 18, 23.

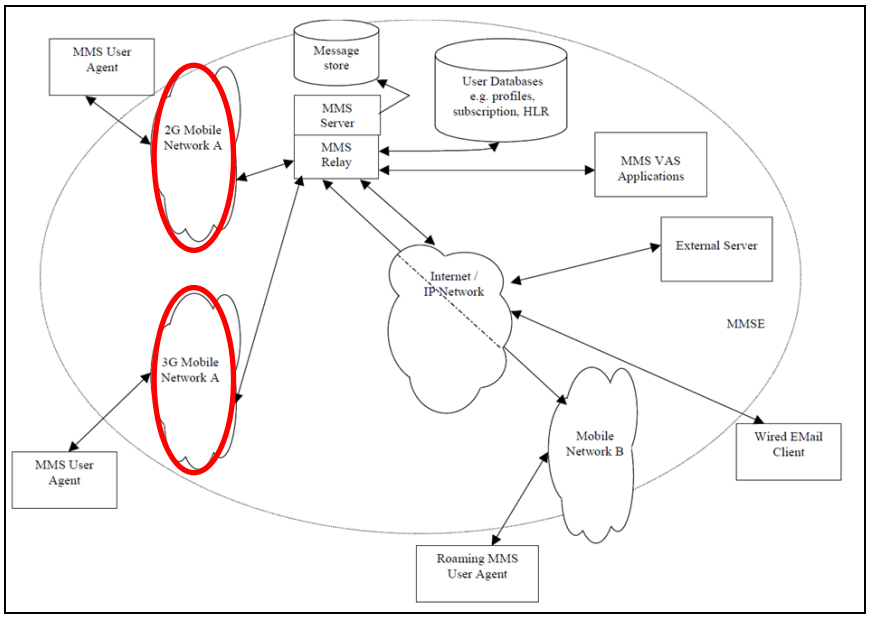


EX-1004, Figure 3 (annotated)

103. A POSITA understood that the outlined network elements above are a "network system" as claimed, because (1) the specification only ever describes a "service control link" as connecting a device to a "network" that comprises one or more servers performing one or more server functions and thus the claimed "network system" encompasses at least that, and (2) the Relay/Server and multiple VAS Applications in TS-23.140's MMS environment (MMSE) comprise servers that perform server functions. EX-1001, 16:13-26, FIGs. 16-20; *see* discussion *infra* regarding [1e].

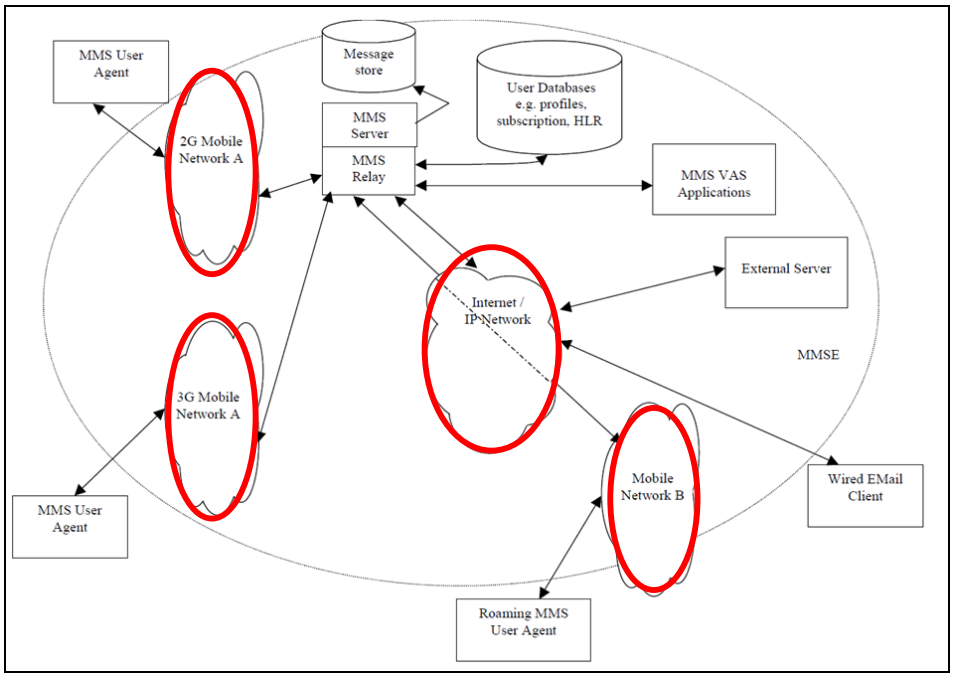
104. The network system includes multiple MMS entities that are in communication with MMS Relay/Server within the MMS environment (MMSE) of the MMS Relay/Server. EX-1004, p. 14 ("MMSE [is] collection of MMS-specific ***network elements*** under the control of a single administration."). The network elements include, e.g., MMS VAS Applications, which communicate with the MMS Relay/Server. EX-1004, §6.9, p. 25.

105. The MMS User Agent is an "application residing on a UE, an MS or an external device that performs MMS-specific operations on a user's behalf and/or on another application's behalf," and that communicates with the multiple entities of the network system via the MMS Relay/Server. EX-1004, 14, 25. Communications between the MMS User Agent (on the end-user device) and MMS Relay/Server (as part of the network system) happen over wireless networks, as shown in Figure 2 below. EX-1004, p. 17. Specifically, and as shown below, TS-23.140 discloses that communications between the MMS User Agent and MMS Relay/Server are facilitated through "2G and 3G ***wireless networks***" as well as over Internet/IP network. EX-1004, p. 17.



EX-1004, Figure 2 (annotated)

106. TS-23.140 also discloses that communication with the network system that is facilitated via interface MM1 occurs ***over a wireless access network***.

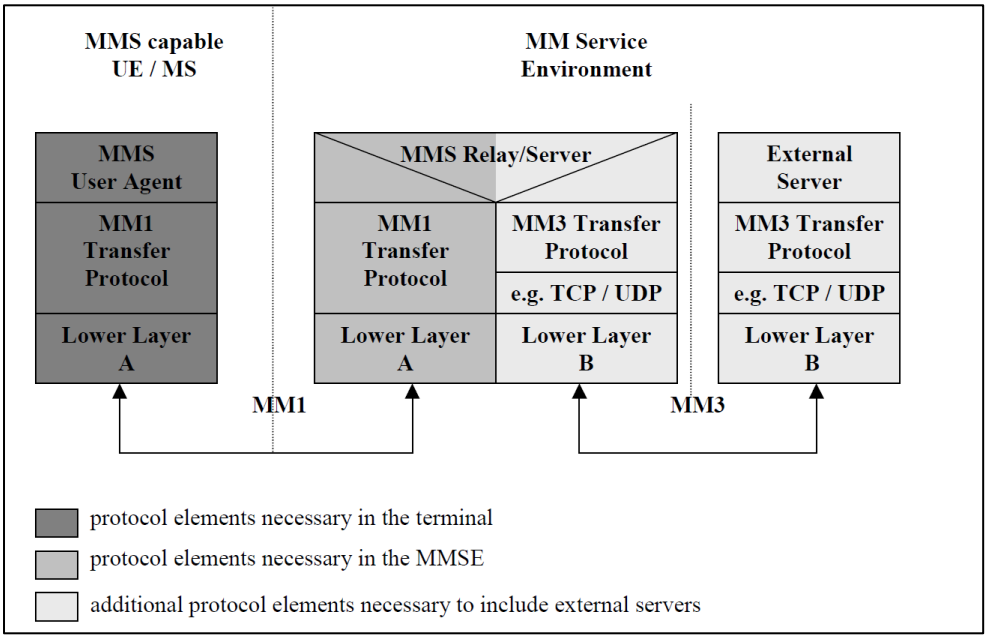


EX-1004, Figure 2 (annotated)

107. Regarding "service control link," the '733 specification does not set forth any requirements but says it "can provide an efficient and flexible control plane communication link" used for "***controlling***" some aspect of a "service." (*e.g.*, "data traffic, application usage, communication with certain network end points"). EX-1001, 7:23-33, 19:67-20:4, 25:46-53, 37:36-61, 68:19-58. MMS-Ogawa's interface MM1 is a "service control link" because it facilitates transmission of, *e.g.*, multimedia message service "associated ***control*** information" and "application/implementation specific ***control*** information" between MMS-Ogawa's network system (which includes the MMS Relay/Server) and the end-user device. EX-1004, 14, 55-56.

108. Element [1a] also requires that the "service control link" be "provided by the network system." The '733 specification never describes how a "network system" "***provide[s]***" a "service control link." During prosecution, the examiner rejected this limitation under §112 as indefinite. *See* EX-1002, 99-100. In response, Applicant argued this limitation "is supported at least by FIG. 16[,] illustrating service control link 1653 communicatively coupling service processor 115 and service controller 122," and the disclosures that "service processor 115…provides for device side of [the] communications with network elements" and "service controller 122…provides for network side of [the] communications with device 100." EX-1002, 76.

109. Based on the Applicant's argument, a POSITA would have understood that the "service control link is provided by the network system" in MMS-Ogawa because (1) the MMS Relay/Server and MMS User Agent device are implemented to "communicate[] with" each other through (and thus are communicatively coupled by) the MM1 interface, and (2) both entities are implemented to provide for communications with one another. As shown in FIG. 4 of TS-23.140, the MM1 Transfer Protocol is implemented both at the MMS Relay/Server and the MMS User Agent. EX-1004, 24. A POSITA would have understood that the MM1 Transfer Protocol facilitates transmission/transport of network communications between the MMS User Agent and MMS Relay/Server (and with other network elements such as MMS VAS Applications, which additionally leverage the MM7 transport interface). *See*, e.g., EX-1018.



EX-1004, FIG. 4

110. MMS-Ogawa's modem is thus "a modem for enabling communication with a network system over a service control link provided by the network system over a wireless access network," as claimed.

[1a1] the service control link secured by an encryption protocol
[30a1] the service control link secured by an encryption protocol,

111. Regarding communication links, the '733 specification says "traffic… can be provided… with ***secure transport protocols running over Transmission Control Protocol (TCP)***," and that "approaches for implementing a secure control channel over the Internet including… ***running TCP Transport Layer Security (TLS)***." EX-1001, 17:2-26; *see also id.*, 87:62-88:7 (communications between end-user and server devices can be "implemented with standard secure or open Internet networking protocols, such as TLS or TCP."). The specification uses "TLS" and Secure Socket Layer (SSL) interchangeably. *See*, *e.g.*, EX-1001, 98:42-44; 99:26-29; 101:65-67 (providing "basic TCP setup, TLS/SSL" as example protocols used in "socket assignment and session management" layer in FIGs. 31-37).

112. In MMS-Ogawa, SSL/TLS is used to secure interface MM1, between the user device (with the MMS User Agent) and the MMS Relay/Server. *Supra* § IX.A.3(b); *see also* EX-1004, §6.2, §6.3, pp. 24-25; EX-1012, 21 ("[t]he ***TLS*** [WP-TLS] transport layer security protocol ***provides for secure data transmission between the MMS Client and the MMS Proxy-Relay*** in architectural configurations

that employ HTTP based protocol stacks for MMSM implementation"). MMS-Ogawa's MM1 (***service control link***) that facilitates communication between a user device and a MMS Relay/Server, is thus "secured by an encryption protocol" such as TLS or SSL.

[1a2] [the service control link] configured to support control-plane communications between the network system and a service control device link agent on the end-user device;

[30a2] the service control link supporting control-plane communications between a service control device link agent on the end-user device and the network element;

113. The same "network element" recited in [30a2] is recited in [30c] and [30d1]. The '733 Patent broadly uses "network element" to mean any element that is part of a network, e.g., a server. EX-1001, 23:46-54, FIGs. 1-8. A POSITA would have understood that MMS-Ogawa's MMS Relay/Server 401/801—which is a server in claim 1's "network system" (as discussed above for [1a])—is also a "network element" as that term is used in the '733 Patent.

114. As discussed for [1a], MMS-Ogawa's interface MM1 (the claimed "***service control link***") is how the MMS Relay/Server (which is part of the claimed "***network system***" in [1a2] and is the "***network element***" in [30a2]) communicates with the MMS User Agent on MMS-Ogawa's "***end-user device***."

115. A POSITA would have understood that MMS-Ogawa's interface MM1 (the service control link) is "configured to support control-plane communications"

as claimed. Although the '733 specification does not use the phrase "control plane communications," it uses a similar phrase "control plane communication link." The "control plane communication link," as recited in the specification, manages "various aspects of device based network service policy implementation." EX-1001, 9:23-24. The '733 patent explains that "aspects of the service policy [include] a set of policies/policy settings for the device for network services, typically referring to lower level settings, such as access control settings, traffic control settings, billing system settings, user notification settings, user privacy settings, user preference settings, authentication settings and admission control settings." *Id.*, 8:60-9:15. The '733 Patent specifies that "an efficient and flexible control plane communication link between the device agents and the network elements" provides for "communicating with, controlling, monitoring, or verifying service policy." *Id.*, 37:36-43, 68:20-28.

116. In view of the plain claim language and the above-described disclosures in the '733 Patent, a POSITA would have understood control-plane communications to encompass communications "across a network" that involv[e] supervision" and "device-based" "control" of "service[s]" delivered to a device, for example by "communicating…, controlling, monitoring, or verifying service policy." *Id.*, 37:36-43, 68:19-28.

117. As discussed for [1a], MMS-Ogawa's interface MM1 facilitates transmission of, *e.g.*, MMS-"associated ***control*** information" and "application/implementation specific ***control*** information." EX-1004, 14, 55-56. TS-23.140 also expressly discusses interface MM1 being used to communicate information that affects how a service is delivered based on a user device's "capabilities." EX-1004, 19, 21, 30 ("MMS User Agent… and MMS Relay/Server shall support Terminal Capability Negotiation," and "the specific mechanism for terminal capability negotiation shall be defined by the MM1 implementation"). The MMS Relay/Server "use[s] the information about the capabilities of the recipient MMS User Agent in preparation of MMs to be delivered to the recipient MMS User Agent" and "adjust[s] an MM to be delivered" based on those capabilities. EX-1004, 30-31; *see also id.*, 35-36 ("MMS Relay/Server decides whether to use ***streaming based on*** the media type and the media format of the subjected MM contents, capability negotiation ***and/or user settings/preferences***."). These are the same types of control-plane communications—which affect the service being delivered—disclosed in the '733 Patent. EX-1001, 8:60-9:15. Thus, a POSITA understood MM1 is "configured to support control-plane communications" as claimed.

118. A POSITA would likewise have understood these communications are "between" MMS-Ogawa's Relay/Server (which is part of the claimed "network

system" ([1a]) and is the "network element" ([30a2])) and "***a service control device link agent*** on the end-user device," as claimed. While the '733 specification does not describe any "service control device link agent"[2], the specification describes a "service control device ***link*** 1691," saying it is a "device side" component that may "provide an efficient and secure solution for transmitting and receiving service policy implementation, control, monitoring and verification information with other network elements." EX-1001, 37:43-62. And it uses the term "agent" to refer to any component—that may be "implemented entirely in software"—that performs some function (e.g., transmitting information for, *e.g.*, "control plane communication"). *Id.*, 15:58-16:2, 42:51-52, claim 26. The specification ***does not*** set forth any required function. EX-1001, 16:2-12 ("It will be apparent to those of ordinary skill in the art that the division in functionality between one device agent and another is a design choice."). Moreover, by the Critical Date, it was well-known that an agent performed function(s) on behalf of an entity (e.g., a user, client, server, etc.). EX-1029, 12. This use of "agent" is consistent with Patent Owner's

[2] The '733 Patent notes on 37:62-64 that "the service control device link 1691 agent ***messages*** are transmitted asynchronously as they are generated by one or more of the service agents," which refers to the messages, and provides no specific definition for the "service control device link agent" recited in claim 1.

interpretation in litigation. For example, in its Exhibit 4 of Infringement Contention (EX-1021), Patent Owner mapped the "agents" in recited in claim 1 to "client app[s]" on an alleged device. EX-1021, Exhibit 4, 13-23 and 62; EX-1038, 17.

119. MMS-Ogawa's "MMS User Agent" is a device-side "application" (i.e., implemented in software) that communicates with the MMS Relay/Server and "perform[s] [service]-specific operations on a user's behalf and/or on another application's behalf" (*supra* § III.A.1) and, as discussed above, enables the transmission and receipt of communications that affect and control the services the device receives via (and on behalf of) the MMS Relay/Server. EX-1004, 14, 19, 23-24, 30-31, 35-36. MMS-Ogawa's User Agent is thus a "service control device link agent," as claimed.

[1b] [the end-user device comprising:] a plurality of device agents communicatively coupled to the service control device link agent through an agent communication bus, each of the plurality of device agents identifiable by an associated device agent identifier[3]; and

[30b] each of the plurality of device agents identifiable by an associated device agent identifier and communicatively coupled to the service control device link agent through an agent communication bus,

120. As discussed for [1a2], the '733 Patent uses the term "agent" to include "component" implemented "entirely in software" that performs some function (e.g., transmitting information) on behalf of a client or server. EX-1001, 15:58-16:2, 42:51-52; EX-1029, 12; EX-1021, 13-23 and 62; EX-1038, 17. A "***device*** agent" is an agent on a device.

121. In MMS-Ogawa, MMS is "used to transport data specific to applications" residing on the end-user device that are not the MMS User Agent. *Supra* § IX.A.3(a), IX.A.3(f); EX-1004, 54-55; *see also* EX-1028, 732-733, section 2.2 (contemplating that multiple destination applications reside on the user device). TS-23.140 discloses transporting data that include the "application identifier of the

[3] The '733 Patent does not provide support for the term "device agent identifier." FIG. 25 presents IDs associated with agents, but those IDs are "function" IDs, and the Patent does not make a connection between those and the "device agent identifier" recited in claim 1.

destination application" and "application/implementation specific control information." EX-1004, 54-55. This "received MMS information" is "immediately routed" by the MMS User Agent "on to the destination application that is referred to from the destination application identifier (based on the negotiated details upon application registration process) without presentation to the user." EX-1004, 56.

122. A POSITA understood that this information is used by the destination application to perform functions on behalf of, e.g., a server (e.g., a VASP) for a VAS application or an application on another terminal. *See e.g.*, EX-1028, 732-733, section 2.2 (noting that "multiple applications" can reside on a mobile terminal.). Because the destination applications are implemented "in software" on the user device and receive information specific to their associated services to perform functions on behalf of another entity, a POSITA would have understood these applications to be "a plurality of device agents," as claimed.

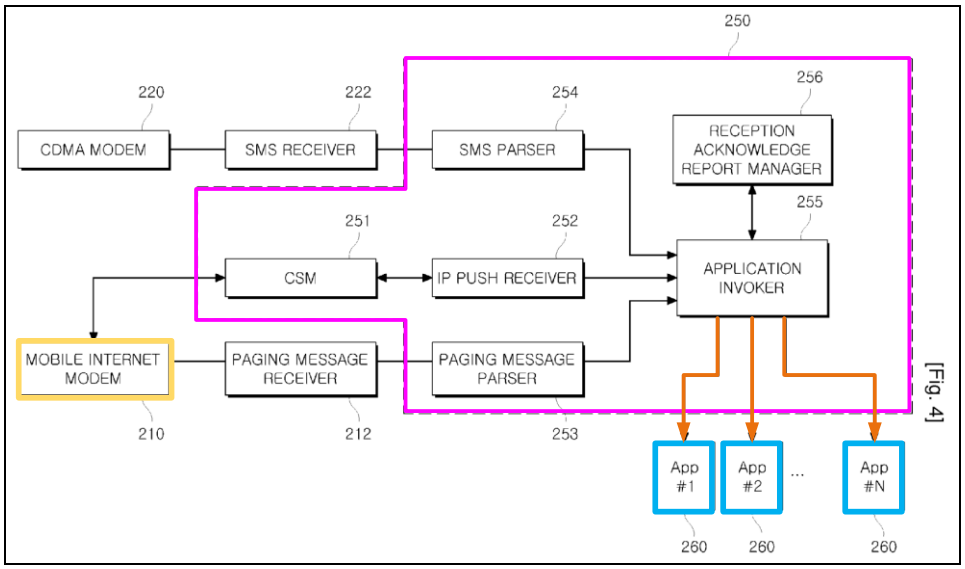
123. A POSITA would likewise have understood that in MMS-Ogawa, the MMS User Agent is communicatively coupled to the device's other applications "through an agent communication bus," as claimed.

124. TS-23.140 discloses that its multiple additional "[a]pplications that… transport application specific data using MMS" on the user device, but does not describe "[d]etails of these applications or how an MMS User Agent… would interface with them[.]" EX-1004, 54. A POSITA would have understood that the

MMS User Agent and other applications would interface "through an agent communication bus" as that term is used in the '733 patent. Per the '733 Patent, the "agent communication bus" can be a communication link that facilitates communications with the device agents. EX-1001, 42:48-61; *see also* EX-1038, 24 (Patent Owner's statement in infringement contentions submitted in litigation indicating that "an agent communication bus" is "e.g., communication path for various agents and functions to communicate over"). Consistent with the Patent's disclosure, and as commonly used in the field, busses facilitate inter-process communications between two pieces of software, such as two software applications. Similarly, a POSITA would have understood that there is a communication bus/link between user agent and the applications in TS-23.140 to facilitate communications of the application-specific messages between MMS User Agent and the destination applications.

125. Alternatively, a POSITA would have reason to implement communications between the MMS User Agent and the device's other applications to occur over a bus. Before the Critical Date, it was well-known to use a communications bus (*e.g.*, a "D-bus") for inter-process communications that enable applications to interface with one another, as TS-23.140 describes. *See, e.g.*, EX-1031, 10:56-62 ("Bus may be an example of a device inter-process communication channel used to send information between applications. As such, method calls made

over the D-Bus may be serialized as a message addressed to a particular application. The particular application may then listen and perform the service requested and place an output back on the D-Bus addressed to the browser application."); EX-1008, ¶28, FIG. 4. Using such a bus on the TS-23.140 device would have been a conventional, obvious way to implement what TS-23.140 describes. Lee, for example, corroborates that there would be a communication channel in the end-user device between a push service agent 250 that receives messages intended for applications resident on a device from external sources, and a target application 260 to which the service agent 250 sends the message. EX-1008, ¶28. As shown in Lee's FIG. 4 below, the push service agent 250 (***service control device link agent***) is ***communicatively coupled*** to the multiple applications 260 (***the plurality of device agents***) ***through a communication bus*** including respective communication channels (depicted in orange in figure below). *See also* EX-1028, 732-733 section 2.2, FIG. 4 (contemplating communication interface between the MMS User Agent and an Application).



EX-1008, FIG. 4 (annotated)

126. Thus, using a communications bus for inter-process communications that enable applications to interface with one another on the TS-23.140 device is nothing more than utilizing familiar, known components to achieve a predictable result of facilitating TS-23.140's user agent and other applications to interface with one another. A POSITA would have reasonably expected success doing so. The end-user device in MMS-Ogawa thus has "a plurality of device agents communicatively coupled to the service control device link agent through an agent communication bus," as claimed.

127. In MMS-Ogawa, "each of the plurality of device agents" are also "identifiable by an associated device agent identifier," as claimed. The '733 specification does not describe any requirements for the claimed "associated device agent identifier." TS-23.140 says that applications need to register with MMS User

Agent after been loaded on the end-user device. EX-1004, 54-55. In MMS-Ogawa, the MMS User Agent delivers application-specific messages to the correct destination application based on a "destination application identifier" included in the message that is associated with the destination application. EX-1004, 55-56. A POSITA would have understood that use of a "destination application identifier" for accurately routing messages to specific destination applications, as TS-23.140 teaches, meant that each of MMS-Ogawa "device agents" was "identifiable by" an "associated device agent identifier," as claimed.

[1c] [the end-user device comprising:] memory configured to store an encryption key,

128. Per the '733 Patent, the "encryption key" recited in features [1c], [1c1], and [1d2] is used for encryption/decode functions that are applied in addition to the "encryption protocol" applied on the link, as recited in feature [1a1]. For example, the '733 Patent specifies that "[v]arious embodiments include ***two or three layers of encryption*** in the service control link, ***with one embodiment or layer*** being implemented in the ***encrypt functions (2408, 2428) and decode functions (2412, 2422), and another embodiment or layer implemented in the transport services stack (2410, 2420)***." EX-1001, 87:57-63. "For example, various known security encryption techniques can be implemented in ***the encrypt functions (2408, 2428), with*** public/private or ***completely private keys*** and/or signatures so that very strong levels of security for service processor control plane traffic can be achieved even

through the basic transport services (2410, 2420) implemented with standard secure or open Internet networking protocols, such as TLS or TCP." *Id*., 87:67-88:7.

129. Consistent with this disclosure, MMS-Ogawa's end-user device includes memory that stores Ogawa's shared encryption key (*supra* § Ie)), which as discussed *supra* § IX.A.3(f) is used to secure MMS-Ogawa's communication interface MM1 with MMS-Ogawa Message Encryption. MMS-Ogawa's end-user device thus includes "a memory configured to store an encryption key," as claimed.

130. Additionally, under Patent Owner's claim interpretation, the "encryption key" limitations recited in [1c], [1c1]/[30c], and [1d2]/[30d2] may be ***part of*** the "encryption protocol" that secures limitation [1a1]'s service control link. EX-1021, pp. 3-13 and 24-34 (using the same features of the "security protocols" used in the targeted product(s) to allege infringement of "encryption protocol" in [1a1] and "encryption key" in [1c]); EX-1038, 8, 29. In other words, Patent Owner asserts these "encryption key" limitations are satisfied by systems where encryption is performed using SSL (or similar) "encryption protocol" without an additional layer of encryption. Even if the claims were interpreted in this manner, MMS-Ogawa separately meets the claims under this interpretation.

131. To the extent the limitations recited in [1c], [1c1]/[30c], and [1d2]/[30d2] are interpreted to encompass encryption performed ***as part of*** a SSL/TLS-enabled encryption protocol that also meets limitation [1a1] (*i.e.*, single-

layer encryption), MMS-Ogawa's memory meets [1c], because MMS-Ogawa's MM1 interface is secured using SSL. *Supra* §§ IX.A.3(b); IX.A.3(f).

132. While TS-23.140 does not describe the details of how SSL/TLS is implemented, such details were well-known to a POSITA before the Critical Date. *See e.g.*, EX-1013, p. 3; EX-1014, p. 3; EX-1026, 29:31-30:24 (corroborating that in TLS/SSL, the client and server generate and exchange keys that are used to encrypt/decrypt communications transmitted over a network channel.). For example, it was well-known that SSL/TLS use ***symmetric*** encryption that involves using the ***same*** key at the source and destination of a message for encryption and decryption. *See id.; see also* EX-1009, 3:25-27; EX-1005, 5:41-47. A POSITA likewise understood that such keys were conventionally stored (at least temporarily) in the respective memories of the encrypting and decrypting entities. Thus, under Patent Owner's claim interpretation—which reads the claims onto systems that ***only*** secure client-server communication channels based on the symmetric encryption used in SSL/TLS—MMS-Ogawa, which uses SSL/TLS (*supra* §§ IX.A.3(b); IX.A.3(f)), includes "memory configured to store an encryption key," as required by limitation [1c] (under Patent Owner's interpretation).

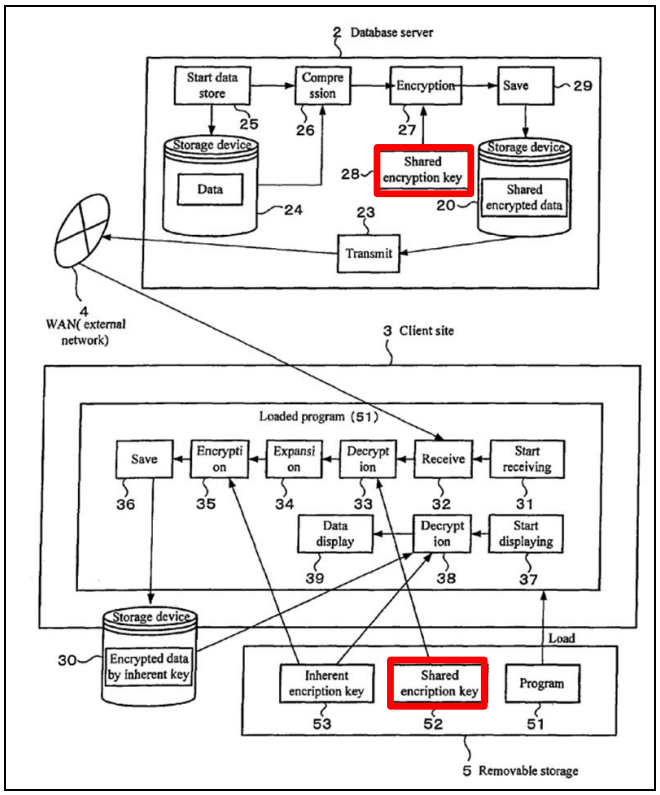
[1c1] the encryption key shared between the service control device link agent and a service control server link element of the network system; [30c] …an encryption key shared between the service control device link agent and the network element…

133. While the '733 specification never describes element [1c1]'s "service control server link ***element*** of the network system," it refers to a "service control server link 1638," and says it is a "network side" component that may "provide[] an efficient and secure mechanism for transmitting and receiving service policy implementation, control, monitoring and verification information between the device agents (e.g., service processor agents/components) and other network elements (e.g., service controller agents/components)." EX-1001, 68:19-40.

134. As discussed above for [1a], MMS Relay/Server is part of MMS-Ogawa's "network system." A POSITA would have understood that MMS-Ogawa's MMS Relay/Server "provides a mechanism for transmitting and receiving" "service policy… information" to and from "device agents" and the "network elements," because (1) TS-23.140 discloses various communication interfaces between the MMS Relay/Server and other elements in TS-23.140's MMS environment (*e.g.*, MM1, MM7), and (2) TS-23.140 specifically discloses an interface (MM1) which facilitates, as discussed above for [1a2], control-plane communications (affecting a service being delivered) between a MMS User Agent and the MMS Relay/Server. EX-1004, 23-24, FIG. 4. A POSITA would thus have understood that the MMS

Relay/Server—which can communicate with the MMS User Agent over interface MM1—was a "service control server link element of the network system," as claimed. EX-1001, 68:19-40.

135. In MMS-Ogawa, Ogawa's encryption key is stored on the end-user device to enable the MMS User Agent to decrypt data received from the MMS Relay/Server, on which the same encryption key is also stored. *Supra* § IX.A.3(e). As discussed *supra* § IX.A.3(e), before the Critical Date, this was well-known for symmetric encryption. EX-1004, §7.1.13.3, p. 42; EX-1009, 8:3-5 ("Symmetric ciphering/enciphering may use one or multiple keys for both encryption and decryption"). Similarly, Ogawa teaches encrypting the message at server 2 and decrypting it at client site 3 using a "shared encryption key" that is shared by the client site and the server. EX-1005, 5:59-65, 6:64-7:12, 9:24-34; *see also id*., 6:64-7:21; 9:16-20 (describing communications between the data input site 1 and client site 3 that leads to generating the shared key and storing the key on the data unit site 1 (or server 2 in configuration of FIG. 7) as well as and on a memory—removable memory 5—attached to the client site 3).



EX-1005, FIG. 7 (annotated)

136. First, a POSITA would have understood that the same, "shared" Ogawa key stored at both MMS-Ogawa's end user device and MMS Relay/Server for MMS-Ogawa Message Encryption—which is used by both the MMS User Agent (the claimed "service control device link agent, as discussed for [1a2]) and the MMS Relay/Server ([1c1]'s "***service control server link element of the network system***" and [30c]'s "***network element***") for encryption/decryption—i.e., was "***shared between***" those claimed components, as required.

137. Additionally and alternatively, a POSITA would have understood that under Patent Owner's claim interpretation—which covers systems that only secure

client-server communications using the single layer of symmetric encryption used in SSL/TLS—the key for MMS-Ogawa's symmetric SSL/TLS encryption (*supra* §§ IX.A.3(b), IX.A.3(f)), is being stored temporarily at both the end-user device (with the MMS User Agent) and the MMS Relay/Server, was likewise "***shared between***" the components as claimed (under Patent Owner's interpretation). *See e.g.*, EX-1013, p. 3 (noting that in SSL, symmetric "[e]ncryption is used after an initial handshake to define ***a*** secret key.")

[1d1] wherein the service control device link agent is configured to: receive, over the service control link, an encrypted agent message from the service control server link element,

[30d1] receiving, over a service control link, an encrypted agent message from a network element,

138. In MMS-Ogawa, the MMS User Agent (the claimed "***service control device link agent***," as discussed for [1a2]) receives, over interface MM1 (the claimed "***service control link***," as discussed for [1a]), encrypted data from the MMS Relay/Server (the claimed "***service control server link element***," as discussed for [1c1], and "***network element***" in claim 30, as discussed for [30a2]). The data the MMS User Agent receives includes messages from various "MMS VAS applications" provided by third-party VASPs to "provid[e] Value Added Services (e.g. news service or weather forecasts) to MMS users." EX-1004, 14, 18; *see supra* § IX.A.1. Communication link "MM7 is used to transfer MMs from MMS

Relay/Server to MMS VAS applications and to transfer MMs from MMS VAS applications to MMS Relay/Server." EX-1004, §6.9, p. 25. The received MMs are then "targeted to the recipient" MMS User Agent by the MMS Relay/Server and through MM1. *Id*., §7.1.13, p. 41.

139. The '733 specification never uses the term "encrypted agent message." Based on the plain language of the claims, a POSITA would have understood the term to encompass an encrypted message sent to an agent. In MMS-Ogawa, messages are encrypted both using MMS-Ogawa Message Encryption and an SSL/TLS encryption protocol before they are transmitted to the MMS User Agent. *Supra* §§ IX.A.3(b), IX.A.3(f).

140. First, because the messages are encrypted using MMS-Ogawa Message Encryption, a POSITA would have understood that, in MMS-Ogawa, the service control device link agent is thus "configured to" "receive, over the service control link, an encrypted agent message from the service control server link element," as claimed in claim 1 and that the message is received "from a network element," as claimed in claim 30.

141. Additionally and alternatively, under Patent Owner's claim interpretation—which covers systems with only the single layer of symmetric encryption used in SSL/TLS—MMS-Ogawa's symmetric SSL/TLS encryption (*supra* §§ IX.A.3(b), IX.A.3(f)) alone also meets limitations [1d1] and [30d1],

because SSL/TLS is a protocol for encrypting messages sent over the data connection to MMS-Ogawa's MMS User Agent. *See e.g.*, EX-1013, p. 3 ("Cryptographic security[] SSL should be used to establish a secure connection between two parties."); EX-1014, p. 3.

[1d2] [wherein the service control device link agent is configured to:] using the encryption key, obtain a decrypted agent message, [30d2] using [the] encryption key shared between the service control device link agent and the network element, obtaining a decrypted agent message

142. The claims require the service control device link agent to (or be configured to) "us[e]" the "encryption key" to "obtain[]" a "decrypted agent message." The '733 specification never uses the term "decrypted agent message." Based on the plain language of the claims, a POSITA would have understood the term to encompass a message sent to an agent that has been decrypted.

143. In MMS-Ogawa, encrypted messages (*e.g.*, received from VASPs via the MMS Relay/Server) are decrypted at the MMS User Agent, which is implemented to use Ogawa's decrypt unit and a shared encryption key to decrypt messages that were encrypted using MMS-Ogawa Message Encryption. *Supra*, §§ IX.A.3(c), IX.A.3(e); EX-1004, 19. Because decryption would be performed by the MMS User Agent (as contemplated by both TS-23.140 and Ogawa), a POSITA would have understood that, in MMS-Ogawa, the service control device link agent

is thus configured to "us[e] the encryption key" to "obtain a decrypted agent message," as claimed.

144. Additionally and alternatively, under Patent Owner's claim interpretation—which covers systems with only a single layer of symmetric encryption used in SSL/TLS—MMS-Ogawa's symmetric SSL/TLS encryption (*supra* §§ IX.A.3(b), IX.A.3(f)) alone also meets limitations [1d2] and [30d2], because messages encrypted using SSL/TLS must be decrypted using the same encryption key used to encrypt the message, and the result is a message for the agent that has been decrypted, i.e., "a decrypted agent message" (under Patent Owner's interpretation). *See e.g.*, EX-1009, 6:59-7:17, 7:34-40, 8:1-5).

[1d3] the decrypted agent message comprising a particular agent identifier and message content for delivery to a particular device agent of the plurality of device agents, the particular agent identifier identifying the particular device agent,

[30d3] the decrypted agent message comprising a particular agent identifier and message content for delivery to a particular device agent of a plurality of device agents on the end-user device, … [30d4] the particular agent identifier identifying the particular device agent,

145. In MMS-Ogawa, the MMS User Agent (the claimed "***service control device link agent***," discussed in the context of [1a2]) receives encrypted ***messages*** from various value-added service applications provided by third-party VASPs (as discussed in the context of [1d1]).

146. As discussed in the context of [1d2], the MMS User Agent decrypts those messages to obtain "decrypted agent messages," as claimed. The MMS User Agent then transports such application-specific data to other applications on the user device (the claimed "***plurality of device agents***," as discussed in the context of [1b]). EX-1004, 54-55 ("MMS may also be used to transport data specific to ***applications***."); *see supra* § IX.A.1.

147. TS-23.140 teaches that a message delivered to MMS User Agent includes application specific information as well as an identifier of the destination application. Specifically, TS-23.140 discloses that "MMS may also be used to transport data specific to applications." EX-1004, §7.1.8, p. 54-55. "Applications that want to transport data specific to applications other than MMS will initially need to register with the appropriate MMS User Agent or MMS VAS Application." *Id*. "During this registration process the application provisions an MMS User Agent or an MMS VAS Application with ***its application identification value*** and may negotiate with the MMS User Agent or MMS VAS Application ***the details (amount and format) of information to be exchanged*** between the two entities." *Id*. "***Abstract messages*** that are sent by … an MMS VAS Application … ***shall contain a destination application identifier***." *Id*., p. 5. "They may, in addition,… contain ***additional application/implementation specific control information***." *Id*. Thus, the messages containing such application-specific data are a form of what TS-23.140

calls "[a]bstract messages": "information which is transferred between two MMS entities used to convey an MM and/or associated control information between these two entities." EX-1004, 14. These messages comprise "a destination application identifier" and "additional application/implementation specific control information." EX-1004, 54-55. MM1-retrieve.RES is an exemplary abstract message with a destination application identifier as well as "MMS control information and the MM content." *Id*., 56, 69 (indicating that MMS Relay/Server sends MM1-retrieve.RES to user agent in response to MMS User Agent's request to retrieve information).

148. "Upon reception of an abstract message containing a destination application identifier ([e.g.,] MM1_retrieve.RES…)," the MMS User Agent "route[s] the received MMS information on to the destination application that is referred to from the destination application identifier (based on the negotiated details upon application registration process)." EX-1004, 56.

149. Based on these disclosures, a POSITA would have understood that MMS-Ogawa's "destination application identifier" (which is the "***associated device agent identifier***" discussed in the context of [1b]) is a "particular agent identifier" in MMS-Ogawa's "decrypted message" that "identifies the particular device agent" to which the message should be delivered. *See also* EX-1008, ¶22, (corroborating that an application-specific message from a server to the user device includes

application-specific data as well as an app_ID of the target application that resides on the user device). The inclusion of the destination application identifier in the abstract message specifies which application from among multiple applications (identifying the particular device agent from among a plurality of device agents) on the end-user device is the destination for the abstract message. *See e.g.*, EX-1009, FIG. 4 (illustrating multiple applications 260); *id.*, ¶22 ("The plurality of push application servers 10, 12 and 14 generate the push data push_data such as *a real time news data for a news application, a chatting message for a peer-to-peer messenger application and an e-mail message for an e-mail application*. A push information push_info including a receiving mobile terminal information specifying the mobile terminal that receives the push data, and *an associated application ID app_ID specifying the application for invoking the push data* along with the push data is also generated.").

150. Additionally, while the '733 specification never uses the term "message content," a POSITA would have understood that the above-described application-specific "MMS control information and the MM content" in a message is "message content" that will likewise be delivered.

151. Thus, a POSITA would have understood that MMS-Ogawa's "decrypted agent message" includes "a particular agent identifier and message content for delivery to a particular device agent of the plurality of device agents,"

where "the particular agent identifier identifies the particular device agent," as claimed.

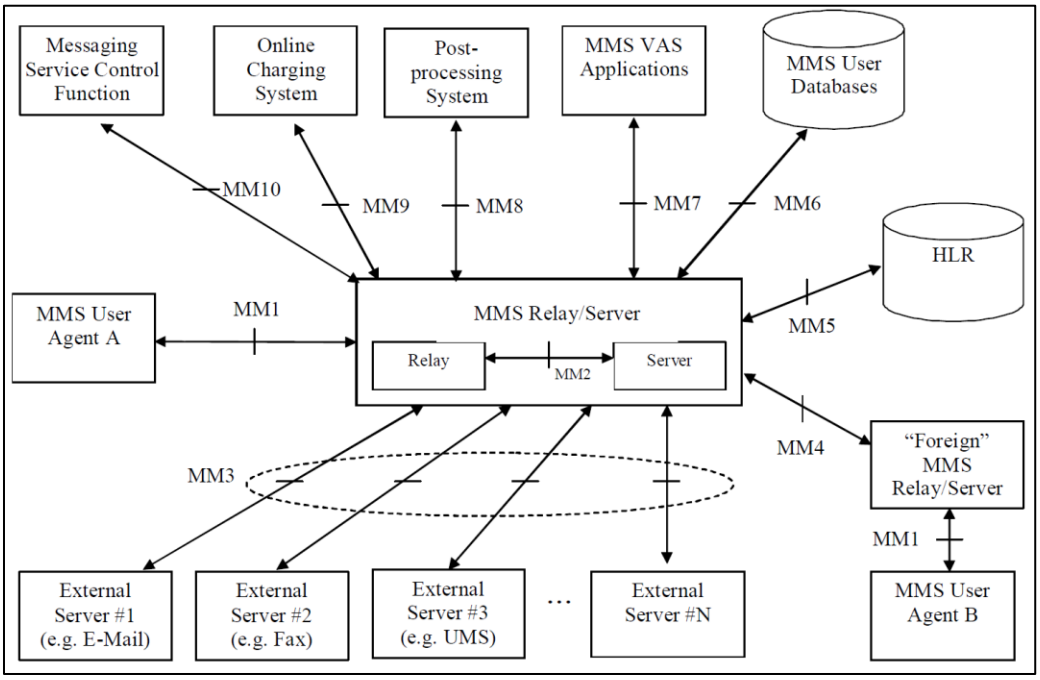
[1e] the message content [being] from a particular server of a plurality of servers communicatively coupled to the service control server link element, and [30e] the message content [being] from a particular server of a plurality of servers communicatively coupled to the network element; and

152. MMS-Ogawa's MMS Relay/Server is the claimed "service control server link element" in claim 1 (as discussed for [1c1]), and the claimed "network element" in claim 30 (as discussed for [30a2]).

153. MMS-Ogawa's application-specific data from VAS Applications provided by third-party VASPs (discussed in the context of [1d1]) is "message content," as discussed in the context of [1d3].

154. TS-23.140 discloses "several MMS VAS Applications… connected to an MMSE." EX-1004, 18. A POSITA understood that each VAS Application resides on a server associated with a Value-Added Service Provider (VASP) that communicates with MMS-Ogawa's MMS Relay/Server through interface MM7. EX-1004, 25-26, 41, 112 ("a VASP… provide[s] the service by sending a multimedia message to one or more subscribers or to a distribution list"). TS-23.140 also shows numerous other "servers" that can communicate with MMS Relay/Server through various interfaces, including, *e.g.*, "External Server #1" and

"External Server #N" (which use interface MM3), and "'Foreign' MMS Relay/Server (which uses interface MM4). EX-1004, 23-24, FIG. 3.

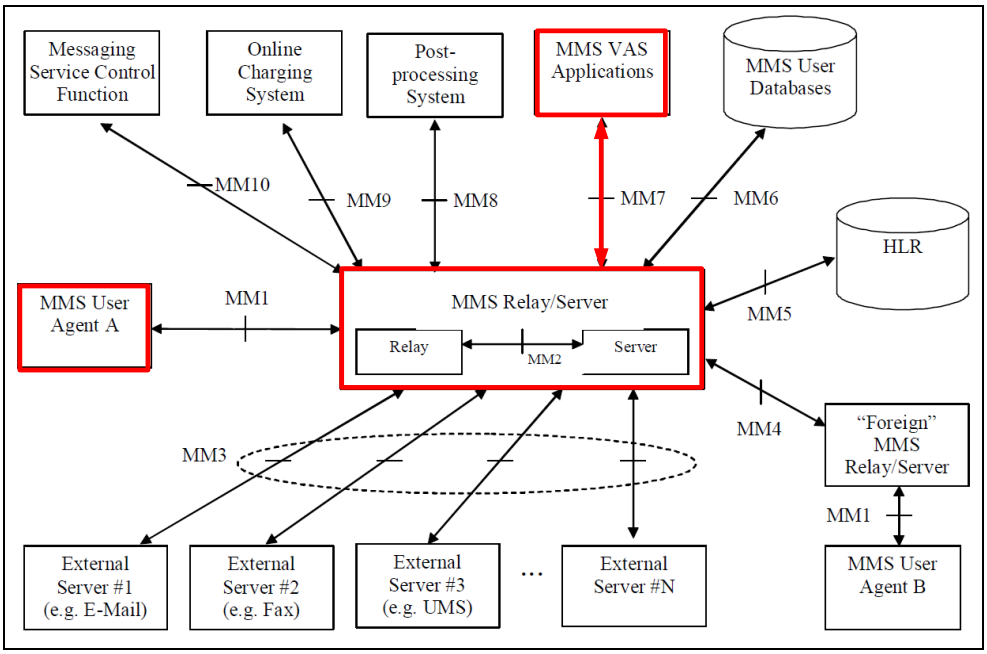


EX-1004, 24, Figure 3

155. Given the large number of servers that the MMS Relay/Server in MMS-Ogawa interfaces with, a POSITA would have understood that MMS-Ogawa's "message content" from a VAS Application provided by third-party VASPs (as discussed above in the context of [1e]) was from "a particular server," and that "a plurality of servers" were "communicatively coupled to" MMS-Ogawa's MMS Relay/Server ("the service control server link element," as discussed above in the context of [1c1]), as claimed.

156. Alternatively, it would be obvious to include multiple servers as Value Added Service Providers (VASP) in the network to provide a variety of services. As

discussed with respect to [1d2]-[1d3], an abstract message includes application-specific data (***message content***). "Applications that intend to transport application specific data using MMS may either reside on an MMS User Agent or on an MMS VAS Application." EX-1004, §7.1.18, p. 55. A VAS Application resides on a server associated with a Value-Added Service Provider (VASP) that communicates with MMS Relay/Server through communication link MM7. EX-1004, §6.9, p. 26, §7.1.13, p. 42; §8.7.1, p. 113 ("a VASP [provides] the service by sending a multimedia message to one or more subscribers or to a distribution list").



EX-1004, FIG. 3 (annotated).

157. As shown above, MMS Relay/Server communicates with multiple VAS Applications. The multiple VAS applications may be associated with the same VASP, or with multiple VASPs. *See, e.g.*, EX-1004, p. 38 ("Support for reply-

charging in MMS is restricted to MMS User Agents and ***VASPs*** belonging to the same MMSE"). A POSITA would have understood that each VASP may have its own server housing one or more VAS applications, and multiple VASP-associated servers (***a plurality of servers***) can provide value added services via their respective VAS applications. Since there are different types of Value Added Services (e.g., news, weather forecast, etc.), a POSITA would find it obvious to use different service providers for each type, and thus, separate servers for different services. Further, a POSITA would be motivated to use multiple servers for providing the Value Added Services because by doing so, a vulnerability or population of one server would not affect other or all value added services. As such, each VASP and its associated VAS applications communicates over a network with MMS User Agents via MMS Relay/Server and its associated link elements. In case of the multiple VAS applications residing on multiple VASP-associated servers (***a plurality of servers***), the VAS application that triggered/sent the abstract message resides on one of those multiple servers, and thus, the message is from a particular server.

[1f] [wherein the service control device link agent is configured to:] based on the particular agent identifier, deliver the message content to the particular device agent over the agent communication bus.
[30f] delivering the message content to the particular device agent over the agent communication bus based on the particular agent identifier.

158. MMS-Ogawa's MMS User Agent is a "service control device link agent" (as discussed in the context of [1a2]). It delivers application-specific data to a destination application on the end-user device using the destination application identifier that was included in the message received from the MMS Server/Relay (as discussed in the context of [1b] and [1d3]). A POSITA understood that such communication would occur "through the agent communication bus" (discussed in the context of [1b]). MMS-Ogawa thus meets this element.

b) Claim 2:

[2] The end-user device recited in claim 1, wherein the particular server comprises a service usage history server, a policy management server, an access control integrity server, a network traffic analysis server, a beta test server, a service download control server, a billing event server, an activation server, a transaction server, an authentication server, or a content management server.

159. Claim 2 recites a list of alternative servers ("or") that claim 1's "particular server" may comprise, including "a billing event server," and "a content management server." The '733 specification calls a server that "collects billing events," "and/or provides trusted third[-]party function for certain ecommerce billing transactions" a "billing event server." EX-1001, 77:39-46. The '733

specification does not describe a "content management server," but describes "content billing" as a type of "content management." *Id.*, 16:53-54.

160. In MMS-Ogawa, as discussed above in connection with [1e], MMS is used by servers to provide "value added services" content such as news or weather to users. EX-1004, 14, 25-26 (§6.9). A VASP server "provide[s] the service by sending a multimedia message to one or more subscribers or to a distribution list." EX-1004, 112. A POSITA understood that the VASP server manages various aspects of content provision, including determining which MM content is intended for distribution, cancelling MMs that have already been sent to a user agent, determining which subscribers receive MM content, "classif[ying] content of the MM based on e.g. media types/formats, size, presentation formats," "indicat[ing] a condition which needs to be met to allow delivery," etc. EX-1004, 87, 112-114.

161. TS-23.140 also discloses MMS VAS applications generating Charging Data Records (CDR) "when submitting MMs to the MMS Relay/Server" "for the purpose of billing and traceability." EX-1004, 18, 23, 163; *see also id.*, 112-114 (VASP can perform billing services such as "indicat[ing] which party is expected to be charged for an MM submitted by the VASP," and "mark[ing] the content of the message with a service code that may be transferred by the MMS Relay/Server."). A POSITA would have understood that a VASP server that manages content delivery and billing for that content, as taught in TS-23.140, is both a "content

management server" because it manages billing for content delivery and a "billing event server" because it creates CDRs for the purpose of billing—thus meeting claim 2.

c) Claims 3-4

[3] The end-user device recited in claim 1, wherein the message content comprises information associated with a service usage.

[4] The end-user device recited in claim 3, wherein the information associated with the service usage comprises information about one or more of a service usage value, a projected service usage value, a service usage plan limit, a projected service usage overage, a projected service cost overage, a service plan period time duration, a service plan time remaining before end of period, and a service overage.

162. Claim 3 requires claim 1's "message content" to "comprise[] information associated with a service usage." Claim 4 requires claim 3's "information" to comprise "information about one or more" of several alternatives, including "a service usage value," "a projected service usage value," "a service plan time remaining before end of period," and "a service usage plan limit."

163. In MMS-Ogawa, the "VASP may mark the content of the message with a service code that may be transferred by the MMS Relay/Server in the form of charging information for use by the billing system to properly bill the user for the service being supplied." EX-1004, 113. A POSITA would have understood that because TS-23.140's service code includes information that allows a billing system

to properly bill for a service, the information indicates the value of the service being used by/supplied to the user and thus constitutes a "***service usage value***."

164. Additionally, or alternatively, TS-23.140 discloses that the abstract message includes information about a ***projected service usage*** given its disclosures of message reply-charge indicator. A VASP can mark an abstract message (intended for a destination application on the user device) to indicate that the VASP will "take over the charge for the sending of a reply-MM to their submitted MM from the recipient(s)" and associated "reply-charging limitations." EX-1004, 37-38 (§7.1.10). "Within submission of an MM," the VASP indicates "willingness to pay the charge for one reply-MM," and "may define a reply-charging limitation request (e.g. may specify the latest time of submission of the reply-MMs or a maximum size of reply-MMs)." *Id*., 38. Upon receiving the VASP's MM, the MMS Relay/Server "pass[es] the indication" of the reply-charging and associated "limitations" "when routing" the MM to the user. *Id*.; *see also id.*, 70 ("In case of reply-charging the MMS Relay/Server should indicate in the MM1_retrieve.RES that a reply to this particular original MM is free of charge and the reply-charging limitations.").

165. A POSITA would have understood that information indicating that the VASP will cover the charge of a reply-MM is information about an anticipated service usage—*i.e.*, "a projected service usage value," as claimed. Additionally, a POSITA understood that information regarding time limitations imposed on the

offered reply-MM service constitutes "***a service plan period time duration***," "***a service plan time remaining before end of period***," and a "***service usage plan limit***," as claimed, because the information TS-23.140 provides to the user device is regarding time-based limits on the reply-charging service usage. EX-1004, 38 (noting the reply-charging limitations "may specify the latest time of submission of the reply-MMs."). A POSITA also understood the above-identified information is "associated with a service usage," as required by claim 3.

d) Claim 5

[5] The end-user device recited in claim 1, wherein the message content is based, at least in part, on a user preference.

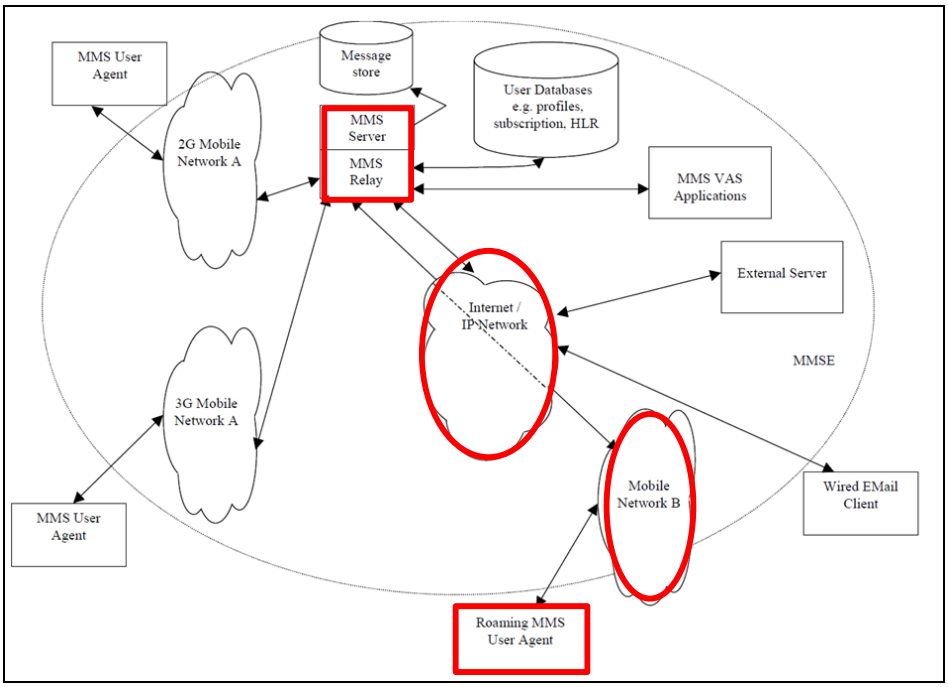
166. Claim 5 requires claim 1's "message content" to be "based, at least in part, on a user preference." In MMS-Ogawa, the MMS Relay/Server can adjust the characteristics of a message and its content, including its presentation format, based on the user preferences before delivering the message to the user's device. For example, MMS Relay/Server converts the media type/format to make it streamable or non-streamable on the user's device based on the user's settings/preferences. EX-1004, 35-36. In particular, "MM contents may be either delivered as non-streaming MM elements, or made available for streaming retrieval." *Id*. "The recipient ***MMS Relay/Server decides whether to use streaming based on*** the media type and the media format of the subjected MM contents, capability negotiation and/or ***user***

settings/preferences." *Id.* "***The recipient MMS Relay/Server may convert media types and/or formats of MM contents*** to make it available for streaming retrieval" by the MMS User Agent. *See id.* MMS-Ogawa thus meets claim 5.

e) Claim 6

[6] The end-user device recited in claim 1, wherein the message content comprises information associated with a roaming service usage or a roaming service cost.

167. The MMS-Ogawa user device is configured to use the MMS service as described in TS-23.140. *Supra* § IX.A.3(f). TS-23.140 discloses its "MMS User Agent" communicating with the MMS Relay/Server while "[r]oaming." EX-1004, 17, FIG. 2, 19-20.



EX-1004, Figure 2 (annotated)

168. Part of the MMS service described in TS-23.140 (and implemented in MMS-Ogawa) involves notification about incoming MMs sent to an MMS User Agent. TS-23.140 discloses the MMS Relay/Server sending the MM1_notification.REQ abstract message to an MMS User Agent that includes an "indication about ***charging related information*** if recipient has to pay for the retrieval [of the incoming MM] or ***roaming condition***." EX-1004, 55-56, 67-68; *see also id.*, pp. 46, 57 (suggesting informing a user about the charges associated with a service before the user uses that service). Thus, the message content includes information associated with a roaming service usage and roaming service cost (whether to retrieve message and thereby use roaming charges to facilitate delivery from a roaming service and user).

169. A POSITA understood that the above-described message content included in MM1_notification.REQ constitutes information "associated with a ***roaming service usage***," as claimed, because information on whether receipt of a message will incur roaming charges is information associated with usage of a roaming service. *Id*. A POSITA also understood that receiving roaming services from a visited network would generally and conventionally cost the user a ***roaming service cost*** because operators of visited network servers conventionally sought compensation for providing such services. Indeed, prior to using a roaming service and incurring associated roaming charges, it was well known (before the Critical

Date) for users to be informed about their rights, service conditions and restrictions, and the costs associated with such roaming services. *See e.g.*, EX-1007, ¶¶[110-112] (disclosing that the user is being informed about the roaming costs before the roaming service begins). Thus, in MMS-Ogawa, the "message content" in MM1_notification.REQ while the end-user device is roaming as disclosed in TS-23.140—which would have been sent over MM1 from the MMS Relay/Server in MMS-Ogawa and would have satisfied claim 1—comprises "information associated with a roaming service usage or a roaming service cost," as claimed.

f) Claim 7

[7] The end-user device recited in claim 1, wherein the message content comprises a service offer, an advertisement, or a transaction offer.

170. TS-23.140 discloses messages sent by a third-party VASP to the MMS Relay/Server for sending to an MMS User Agent—*see* [1d1]-[1d3] *supra*—can include a classification indicating the message is an advertisement. EX-1004, 112 ("This section [8.7.1] addresses the operations necessary for a VASP to ***provide the service*** by sending a multimedia message ***to one or more subscribers***…"), Figure 8 (showing "data flow of MM7 message distribution"), 115 (listing information elements in an MM7 to a MMS Relay/Server, including "[m]essage class" indicating the "[c]lass of MM (***advertisement***, information service, accounting)."), 63 ("Figure 6 illustrates some of [MM1] transactions," including "notifications of new MMs,

retrieval of MMs…"), 69, 73 (listing information elements in an MM1 message, including "[m]essage class" of "advertisement, information service"). Thus, in MMS-Ogawa, "message content" includes "a service offer" or "an advertisement."

171. Further, TS-23.140 teaches that the abstract message includes a "transaction offer," with its disclosures of message reply-charge indicator. As discussed above for claim 4, a VASP can mark an abstract message (intended for a destination application on the user device) to indicate that the VASP will "take over the charge for the sending of a reply-MM to their submitted MM from the recipient(s)" and associated "reply-charging limitations." EX-1004, 37-38 (§7.1.10). "Within submission of an MM," the VASP indicates "willingness to pay the charge for one reply-MM." *Id.*, 38. Upon receiving the VASP's MM, the MMS Relay/Server "pass[es] the indication" of the reply-charging "when routing" the MM to the user. *Id.*; *see also id.*, 70 ("In case of reply-charging the MMS Relay/Server should indicate in the MM1_retrieve.RES that a reply to this particular original MM is free of charge and the reply-charging limitations."). A POSITA understood that the reply-charging indicator is a "transaction offer" because it is an offer to the user for taking over the charge of a reply-MM.

g) Claim 8

[8] The end-user device recited in claim 1, wherein the message content comprises information from a third party configured to provide control of a service or a billing for a service.

172. Neither claim 8's language nor the specification of the '733 Patent clarifies whether the "third party" is the same as or a different entity (e.g., a different server) from the "particular server" recited in claim 1. For example, FIG. 16 of the '733 shows two billing servers: billing event server 1662, and central billing server 1619. Within a plain view of the figure, billing event server 1662 is communicatively coupled to service control server link element 1638, and thus represents a "particular server" within the scope of claim 1, while central billing server 1619 communicates with link element 1638 indirectly (through multiple networks), and thus, can be viewed as a "third party" billing server in communication with server 1662 or link element 1638. However, the specification states that billing event server 1662 can also perform "third party functions for certain billing transactions." The patent explains "***the billing event server 1662*** collects billing events,… serves as interface between device and central billing server 1619, and/or ***provides trusted third party function for certain ecommerce billing transactions***." EX-1001, 77:39-46.

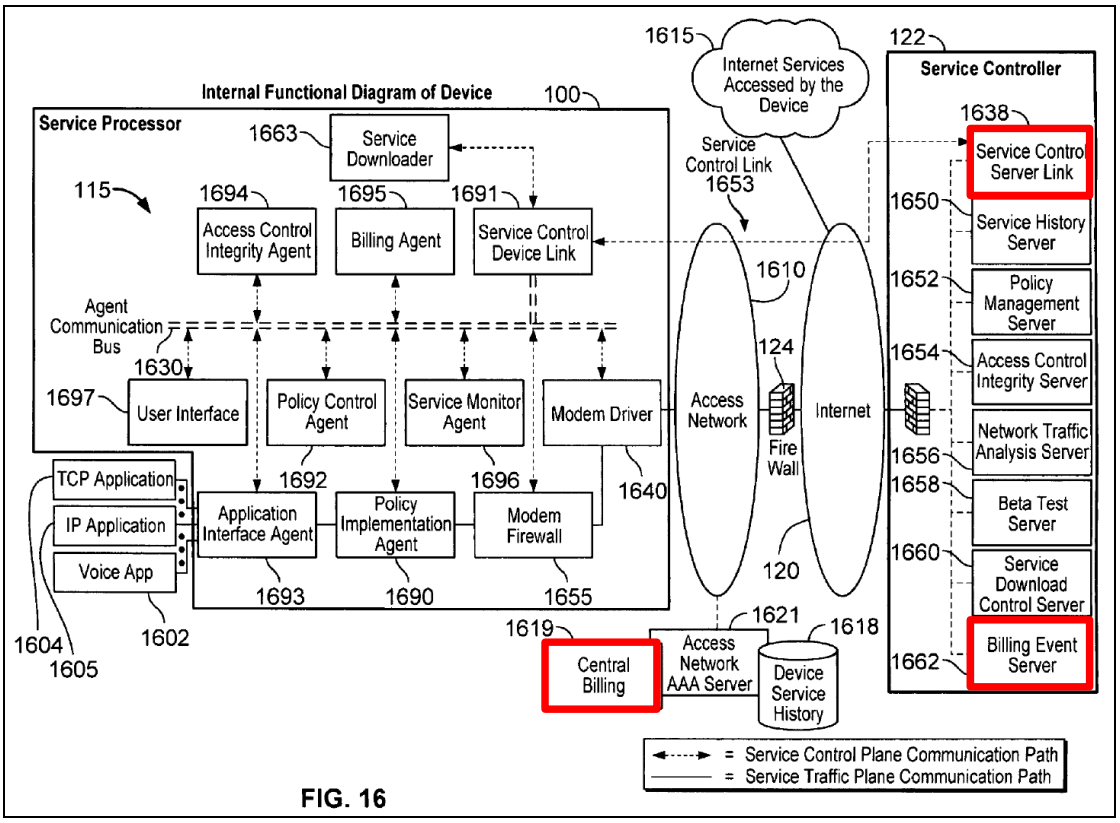


FIG. 16

EX-1001, FIG. 16 (annotated)

173. MMS-Ogawa renders obvious both scenarios—i.e., the first scenario where the third party is the same as the particular server, as well as the second scenario where the third party is different from and in communication with the particular server.

174. In more detail, TS-23.140 discloses that the message content includes information from a third party (e.g., VASP) configured to provide control of a service (e.g., control of a value added service, or a reply-charging service) or a billing for a service (e.g., CDR). TS-23.140 discloses a third-party value-added service provider (VASP) that controls a service and associated VAS Application(s)

in the MMS environment and delivers ***services*** (e.g., news, weather services), via abstract messages, to the MMS User Agent. EX-1004, 14, 34, 112.

175. As described for claim 2, the VASP controls the content included in the abstract messages intended for MMS User Agents, and is therefore configured to control the service. As discussed for claims 3-4, the VASP is configured to control a reply-charging service by activating this service and setting limitations for it. The VASP is also configured to provide billing for the above services by generating and providing a CDR (described for claim 2). Thus, in MMS-Ogawa, the content in VASP abstract messages "comprise information from a third party configured to provide control of a service or billing for a service," as claimed.

176. Alternatively, to the extent this claim is read to require the "third party" be an entity that is ***not*** claim 1's "particular server," using the VASP server to provide User Agents (via the Relay/Server) information controlled by some other source would have been obvious. A POSITA understood that a VASP server could be implemented to act as an intermediary server that receives VAS messages from other entities (third-party servers)—for example, third-party news applications/sources (*e.g.*, blogs, news servers, weather stations)—from which third-party data for the value-added services are retrieved and then transmitted by the VASP to the MMS Relay/Server for delivery to user devices. *See e.g.*, EX-1035 (noting the use of an MMS environment for implementing a distributed Resource

Description Framework (RDF) that benefits from aggregating information from multiple third-party resources); EX-1036 (noting that Yahoo® used news aggregation by 2004). Such an implementation would have desirably allowed a single value-added service provider to offer users a wide variety of content from many sources. In such an implementation, the VASP would be implemented to create messages with content originating from third-party sources, and then transmit them to MMS User Agent(s). Because each third-party source would originate content (*e.g.*, news, weather), such third-parties would control messages and content sent to the VASP—and thus would be "configured to ***provide control of***… [the] service" that originates at the third-party server.

h) Claim 9

[9] The end-user device recited in claim 1, wherein the message content comprises an agent instruction, a setting value, an agent configuration, or a software update.

177. Claim 9 requires claim 1's "message content" to "comprise[]" one of several alternatives, including "an agent instruction," "or an agent configuration."

178. TS-23.140 discloses that "[t]he application identifier of the destination application [and] some additional application/implementation specific control information" are "present in an abstract message." EX-1004, 55. The "additional application/implementation specific control information" allows the abstract message to be delivered to the correct destination. EX-1004, 55. For example, such

information includes data "distinguishing between multiple instances of the same application" so that a particular instance of the receiving application can be distinguished and targeted. *Id*. As another example, such information includes data "specifying a particular logical channel" that is used in addressing a particular part of the application, e.g., a discussion thread. *Id*.

179. A POSITA understood that the "additional application/implementation specific control information" recited in TS-23.140 provides instructions regarding application, and thus, constitutes "***an agent configuration***" as claimed, because it has details on structure/configuration of the destination application. By using this data, the abstract message can be delivered to a particular instance of the target application and to the correct location/instance of that application. For example, such information includes data "distinguishing between multiple instances of the same application" so that a particular instance of the receiving application can be distinguished and targeted. As another example, such information includes data "specifying a particular logical channel" that is used in addressing a particular part of the application, e.g., a discussion thread. The data also constitutes as "***an agent instruction***," as claimed, because it instructs the destination application to use a "particular logical channel" for addressing.

180. Further, as discussed above for claim 5, TS-23.140 teaches that message content is adjusted based on the settings of the end-user device, e.g.,

whether the application can or cannot stream the message content. EX-1004, 35-36. A POSITA would have understood such adjusted message content to include a configuration of the destination application, i.e., an "agent configuration" as claimed.

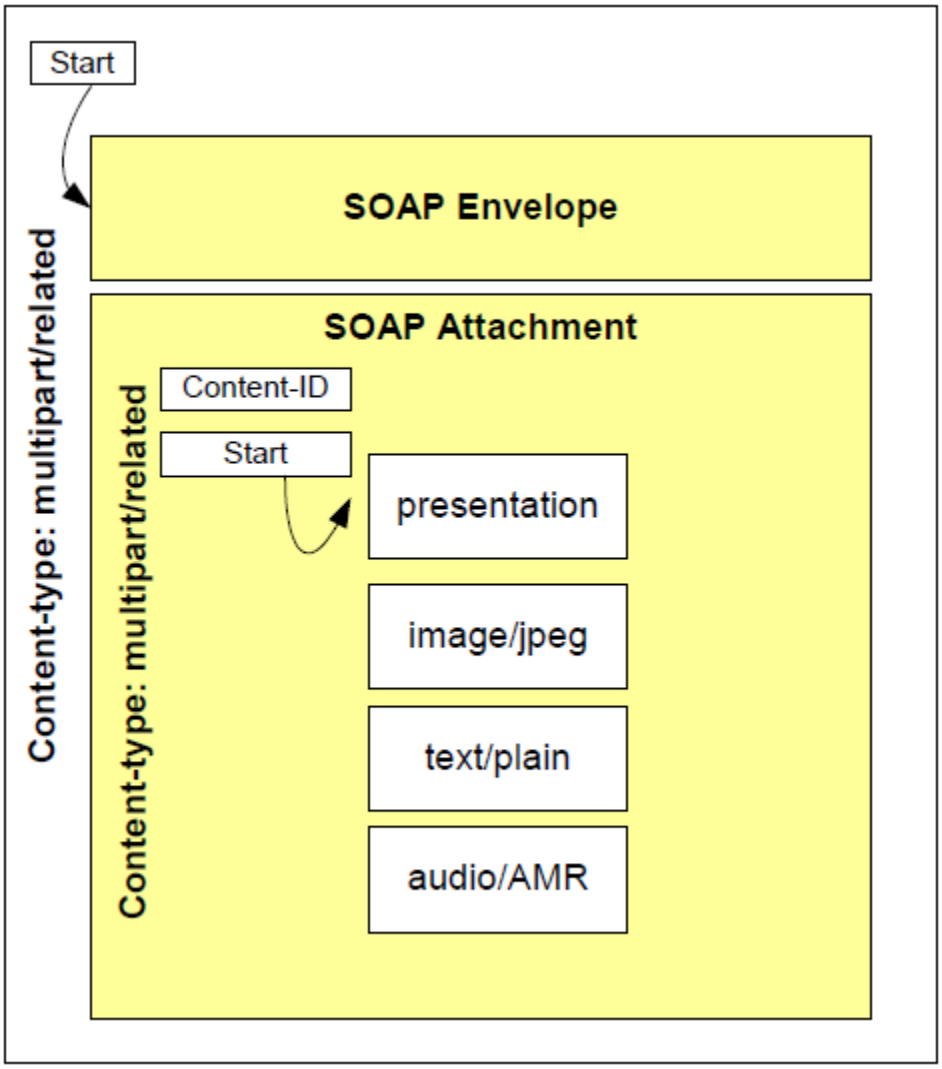
i) Claim 10

[10] The end-user device recited in claim 1, wherein the message content comprises software or a media file.

181. TS-23.140 discloses that a VASP "provide[s] the service by ***sending a multimedia message*** to one or more subscribers or to a distribution list." EX-1004, 112. TS-23.140 further discloses that MM7 messages from a VASP can "carry a SOAP attachment," which includes "[m]ultimedia content, e.g. audio, image, text, presentation or a combination of different media types and/or formats." *Id.*, 15, 133; *see also id.*, 113 (explaining that an "originator" (VASP) provides to the MMS Relay/Server "information about the nature of the content in the message" such as "***media types/formats***"). Before delivering the message to MMS User Agent, MMS Relay/Server adjusts the multimedia message (MM) based on the presentation capabilities of MMS User Agent. *Id*., p. 31. The adjustment can include deletion or adaptation of unsupported media types and media formats. *Id*.

182. A POSITA would have understood that such multimedia content would be delivered in a file container and would therefore constitute a ***media file***. TS-

23.140 discloses structure of the SOAP attachment file that carries the multimedia content:



EX-1004, 133

183. Thus in MMS-Ogawa, the "message content" comprises a "media file," as claimed, because a multimedia message including media such as image and audio would include a media ***file*** including such media.

j) Claim 11

[11] The end-user device recited in claim 1, wherein the message content comprises information associated with a service policy.

184. The ’733 Patent does not explain what constitutes “information associated with a service policy.” Nor does the Patent provide a clear definition for “service policy.” However, the Patent notes that several “aspects of the service policy [include] a set of policies/policy ***settings for the device for network services***, typically referring to lower level settings, such as ***access control settings***, traffic control settings, ***billing system settings***, user notification settings, user privacy settings, user preference settings, authentication settings and admission control settings.” EX-1001, 8:62-9:3. This disclosure conveys that the type and size of content that the user device can receive from a network (“access control settings”), for example, based on their payment policy such as a prepaid plan (“billing system settings”) are examples of service policy.

185. TS-23.140 discloses that, for “prepaid customer[s],” prior to sending a message to an MMS User Agent, the MMS Relay/Server performs a credit check based on “several criteria” that depend on information included ***in*** the message (e.g., size, content type) to see if the customer can send or retrieve such a message. EX-1004, §7.1.8, 36. Depending on the credit check result and the message content, the Relay/Server rejects or accepts delivering the message to the prepaid customer. *Id*. A POSITA understood that an MMS service for prepaid customers that predicates

delivery of messages to a user based on criteria like size and type of the content in the message is a "service policy," as claimed. A POSITA likewise understood that the criteria TS-23.140 discloses to determine whether a service will be delivered are "information associated" with that service policy. Thus, messages that are successfully delivered to the MMS User Agent of a prepaid customer, as disclosed in TS-23.140, "comprise[] information" that satisfies the service policy of a prepaid service and is thus "associated with a service policy," as claimed.

k) Claim 12

[12] The end-user device recited in claim 1, wherein the message content comprises service usage accounting information.

186. As discussed earlier regarding [1f], messages sent from a VASP to the MMS User Agent are transmitted through the MMS Relay/Server.

187. TS-23.140 also discloses VASP messages (e.g., MM7_submit.REQ) that are classified as "accounting" messages, and that the Relay/Server can forward VASP messages to MMS User Agent. EX-1004, 115, 112, 68, 72-73, 30. Further, VASP generates billing information such as charging data record (CDR) or other billing information related to a VASP message sent to the MMS Relay/Server for delivery to a MMS User Agent. EX-1004, 17, 18, 23, 154; *see also* discussion above for claim 2. The VASP sends to MMS Relay/Server the billing information for a

service it provides, for example, for a message to be delivered to MMS User Agent. EX-1004, p. 41.

188. Per TS-23.140, a user is alerted of charges associated with a service so that the user can decide whether to use that service. *See, e.g., id.*, p. 45 ("An MMS User Agent should ask for end-user confirmation before following a hyperlink which triggers a terminal action…. End user confirmation is recommended as accessing a resource on the network might result in additional charges."); p. 56 ("An MMS User Agent may ask for end user confirmation before any submission or retrieval of an MM triggered by an application ***due to charging***, privacy or security reasons."). Given TS-23.140's disclosure that there may be charges associated with using a service provided by a VASP (and messages received therefrom), and that users may be alerted of charges associated with such service, a POSITA would have had reason to implement (and would have reasonably expected success implementing) MMS-Ogawa to provide messages with this information to the MMS User Agent. This would have allowed the user to be aware of service charges being incurred as a result of receiving messages associated with the VASP service. EX-1004, §8.1.4, pp. 66-67 (indicating that MM1_notification.REQ, as an example abstract message, includes charging (i.e., accounting) information regarding a message retrieval (i.e., service usage)); pp. 38, 67 (discussing that a message that includes the reply-charging feature includes information indicating that the originator of the message

covers the reply-MM cost and the expiry time of the reply-charging feature). Such content would constitute "service usage accounting information," as claimed.

l) Claim 13

[13] The end-user device recited in claim 1, wherein the service control device link agent is further configured to send a device message to the service control server link element over the service control link.

189. As described with reference to claim 1, the MMS User Agent (the "service control device link agent," as discussed for [1a2]) communicates with the MMS Relay/Server (the "service control server link element," as discussed for [1c1]) over MM1 interface (the "service control link," as discussed for [1a]). TS-23.140 discloses that MMS is used to transport data between two MMS User Agents or between an MMS User Agent and a MMS VAS Application. EX-1004, 54-56. Because all communications between the MMS User Agent and MMS VAS Applications occurs through the MMS Relay/Server, such communications use the TLS-enabled MM1 interface. *See* EX-1004, p. 24 ("Reference point MM1 is used to submit Multimedia Messages from MMS User Agent to MMS Relay/Server."); p. 25 ("Reference point MM7 is used to transfer MMs from MMS Relay/Server to MMS VAS applications").

190. Moreover, as described with reference to claim 3, TS-23.140 supports a reply-charging capability whereby the message sender (e.g., the VASP) indicates

that it will cover a charge for a recipient's (e.g., the MMS User Agent's) reply message. In response, the MMS User Agent submits the reply message to the MMS Relay/Server and marks the message as a "reply-MM," indicating that the MMS User Agent is using the reply charging service offered by the sender. EX-1004, 37-39.

191. The '733 specification does not describe a "device message." Based on the claim's plain language, a POSITA understood that because the MMS User Agent's reply message is from MMS-Ogawa's end-user device, it is a "device message," as claimed. Moreover, because communications between the MMS User Agent and MMS Relay/Server happen over the TLS-enabled MM1 interface between these entities, the reply-MM message is sent "over the service control link," as claimed. Thus, MMS-Ogawa's "service control device link agent" (MMS User Agent) "is further configured to send a device message" (reply-MM) "to the service control server link element" (MMS Relay/Server) "over the service control link" (MM1), as claimed.

m) Claim 14

[14] The end-user device recited in claim 13, wherein the device message comprises a service usage report or an integrity report.

192. As discussed with respect to claim 13, TS-23.140 discloses that a VASP sending an MM can use a reply-charging functionality whereby the VASP offers to

pay for a reply message by the recipient (an MMS User Agent). A POSITA would have understood that reply charging is an offered service, and therefore the recipient's (MMS User Agent) reply to the message (the reply-MM) constitutes a usage of the service. The reply-MM in MMS-Ogawa combination includes information regarding ("***a report of***") this service usage by "mark[ing] the MM as a reply-MM," and "includ[ing] the message ID of the original MM which it replies to." EX-1004, pp. 37-39. This is consistent with the disclosure of the '733 Patent. The '733 Patent does not provide a definition for a "service usage report." But as an example, it notes that "provid[ing] a service usage report, include[es] monitored service usage for the device 101." EX-1001, 57:37-46. In light of this disclosure, an indication of a service usage (such as the ***information*** in the reply-MM noted above) would constitute a service usage report.

n) Claim 15

[15] The end-user device recited in claim 13, wherein the device message comprises a user response.

193. A POSITA understood MMS-Ogawa's reply-MM (described for claim 13) "comprises a user response" because it responds to a message received from an originator (a VASP) and is sent when a "user intends to send" this message. EX-1004, pp. 37-39.

o) Claim 16

[16] The end-user device recited in claim 15, wherein the user response comprises an acknowledgment of a roaming cost or a roaming usage.

194. As discussed for claim 6, TS-23.140 discloses that the "MMS User Agent" may communicate with the MMS Relay/Server while "[r]oaming." EX-1004, 17, FIG. 2, 19-20. Further, MMS Relay/Server can recommend to the User Agent a particular retrieval mode to retrieve a particular message. EX-1004, 19-20. The recommendation is "based on different factors," including "roaming conditions." *Id*. The recommendation can include an "indication about ***charging*** related information if recipient has to pay for the retrieval or ***roaming condition***," explaining why the particular retrieval mode is recommended for the particular MM. *Id.*, 67.

195. Upon being made aware of this notification, the end user "make[s] a decision whether to download the MM." *Id.*, 19. The MMS User Agent "ask[s] for end user confirmation before any… retrieval of an MM triggered by an application due to charging…" *Id.*, 56. Upon user confirmation, the MMS User Agent requests retrieval of the received MM message from the MMS Relay/Server. *Id.*, 19-20, 56.

196. Because the user is made aware of cost of the service while roaming and subsequently can decide to retrieve the message, a POSITA would have understood or found obvious that such a user response (carried out by the MMS User Agent) requesting delivery of the message despite being made aware of roaming cost

or usage, is an acknowledgement of the roaming cost and/or usage of the MM services while the device is roaming.

p) Claim 17

[17] The end-user device recited in claim 15, wherein the user response comprises an acknowledgment of a service usage, a service cost, or a service overage.

197. A POSITA understood the user response (described for claim 15) "comprises an acknowledgement of… a service usage" because when the user sends a reply message marked as a reply-MM that provides the message ID of the original message to which it replies, the user acknowledges that the offered reply-charging service was accepted and used. EX-1004, 37-39.

q) Claim 19

[19] The end-user device recited in claim 1, further comprising a user interface, and wherein the particular device agent is configured to assist in presenting a notification through the user interface, the notification based on the message content.

198. MMS-Ogawa's User Agent is on an end-user device (as discussed for [1pre]), which includes destination applications that are "particular device agent[s]" (as discussed for [1d3]).

199. TS-23.140 discloses the "MM presentation" and "presentation of notifications to the user." EX-1004, 19; *id.* ("[T]he MM may be ***displayed*** to the

end user with or without any pre-notice."), 16 (Figure 1, showing end-user devices including displays), 155 (Figure A.1, similar). Given these disclosures, and the well-known use of user interfaces on devices to facilitate content presentation to a user, a POSITA understood TS-23.140's user device to include a "user interface," as claimed. Alternatively, such an implementation would have been a conventional and obvious way to implement what TS-23.140 describes, and is nothing more than utilizing familiar, known components (a user interface on, e.g., a display) to achieve a predictable result of facilitating content-presentation to a user.

200. TS-23.140 also discloses that, in a manual message retrieval mode, a "pre-notice" notification about a multimedia message (MM) is presented to the user so that the user can decide whether to request retrieving and viewing the MM. EX-1004, 19-20. In particular, the MMS Relay/Server sends a "MM1_notification.REQ" message to the MMS User Agent to notify it of content included in an upcoming MM, *e.g.*, details about the MM's class and size. EX-1004, 61, 67-68. Based on these disclosures, a POSITA understood that the pre-notice notification is based on message content in MM1_notification.REQ received from the MMS Relay/Server. As discussed above, in MMS-Ogawa, notifications (including pre-notice notifications) are displayed/presented using a ***user interface*** of the end-user device.

201. A POSITA would also have understood that MMS-Ogawa's destination application "assists" in presenting this notification, as claimed. MM1_notification.REQ is an abstract message and the MMS User Agent "***immediately*** route[s]" content of such messages to the destination application specified in the message (*see* discussion above regarding [1f]) "without present[ing the content] to the user." EX-1004, 57, 67-68. Given that the MMS User Agent routes information that is intended to be presented to a user (e.g., an option to accept/retrieve an MM), to a ***destination application***, and given that the User Agent itself does not present such information to the user, a POSITA would have understood TS-23.140 to teach its destination applications "assist[ing]" with presentation of such notifications, either because the destination application itself presents the notification to the user, or because it sends pertinent information to another component responsible for displaying such notifications (*see* discussion *infra* regarding claim 27), thereby causing the notification to be displayed.

202. Further, TS-23.140 teaches a received MM (intended for a destination application) containing visual content. EX-1004, 15, 20, 30 (indicating that an MM can include image or video). A POSITA would have understood that a destination application that receives an MM would be configured to assist in presenting the notification of any visual content contained in the received MM. Alternatively, a POSITA would have had reason to implement the destination application to assist in

providing such presentations to the user visually, because it was conventional and obvious for messages containing visual content to be presented visually to users. *See e.g.*, EX-1004, 35-36 (discussing a presentation of a notification regarding streamable content of an MM). A POSITA would have reasonably expected success with such an implementation, and it would have been well within the skill of a POSITA.

203. A POSITA thus understood the device agents in MMS-Ogawa to be "configured to assist in presenting a notification through the user interface, the notification being based on the message content," as claimed.

r) Claim 21

[21] The end-user device recited in claim 1, wherein the service control link supports asynchronous transmissions by the service control server link element.

204. The '733 Patent uses the term "asynchronous" to encompass transmissions from a server that occur in response to the server receiving (and after the server receives) a user request for the transmission, or as a result of polling. *See e.g.*, EX-1001, 38:19-32, 69:23-24. A POSITA thus understood that the term "asynchronous transmissions" encompasses transmissions by a server sent to a client in response to a request from the client.

205. TS-23.140 discloses that MM1 (the claimed ***service control server link element*** in MMS-Ogawa) can be used to transmit messages from the MMS

Relay/Server in response to receiving a trigger event from the MMS User Agent device. EX-1004, §7.1.2 ("Upon reception of an MM the recipient ***MMS Relay/Server… shall generate a notification to the recipient MMS User Agent***"), §7.1.2.1 (MMS User Agent requests retrieval of the message upon receipt of the notification), §8.1.5.1 ("MMS User Agent… issue[s] an MM1_retrieve.REQ to the… MMS Relay/Server to initiate the retrieval process"), §5.1.1.1.

206. In other words, using MM1, the MMS User Agent may request delivery of a message stored by the recipient MMS Relay/Server (based on a user action) and in response, the MMS Relay/Server may provide the message. A POSITA thus understood that MM1 (the claimed ***service control link***) in MMS-Ogawa supports asynchronous transmissions, consistent with how this term is used in the '733 specification.

207. In addition, TS-23.140 discloses that the MMS User Agent can request delivery of the message received and stored by the recipient MMS Relay/Server, and that such requested delivery can be manual—i.e., based on user request. See, e.g., EX-1004, §7.1.2.1, pp. 29-30 ("the MMS User Agent shall be able to … retrieve the MM, either immediately or at a later time …, ***either manually or automatically*** …."); §8.1.5.1, p. 70 ("The recipient MMS User Agent shall issue an MM1_retrieve.REQ to the recipient MMS Relay/Server to initiate the retrieval process. The MMS Relay/Server shall respond with an MM1_retrieve.RES, which

contains MMs control information and the MM content."); §5.1.1.1, p. 20 (in "manual mode," the "user is made aware of the MM notification and ***is allowed to make a decision whether to download the MM or not***"). This further confirms that MM1 supports asynchronous transmissions, consistent with how this term is used in the '733 Patent.

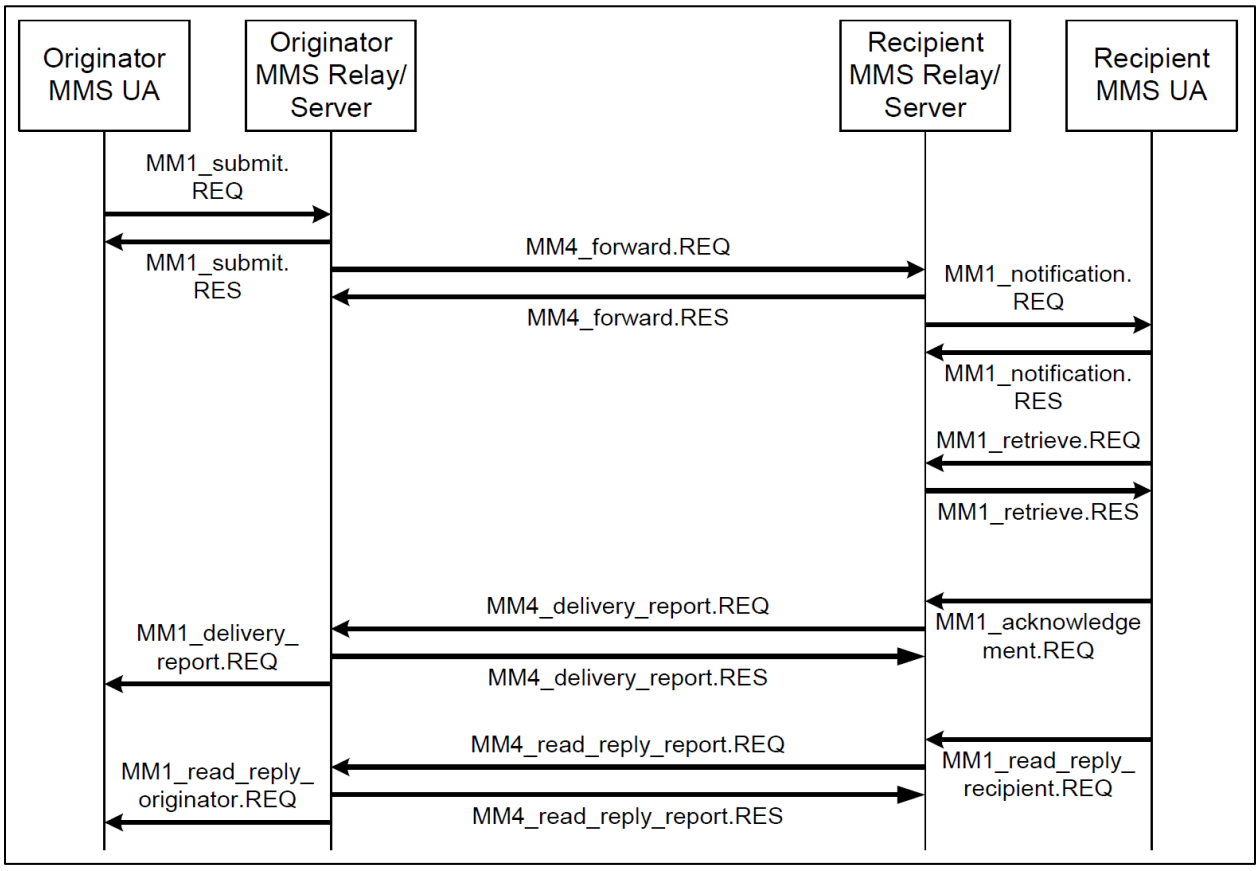
s) Claim 22

[22] The end-user device recited in claim 1, wherein the service control link supports periodic transmissions by the service control server link element.

208. TS-23.140 discloses that, "[f]or discovery of incoming messages from external messaging systems different mechanisms may be utilized, e.g. [by] ***periodic polling*** for messages on External Server, ***followed by retrieval by the MMS User Agent via the MMS Relay/Server***." EX-1004, 90-91, 59-61.

209. An obvious way to implement in TS-23.140's "periodic polling" was by implementing the MMS Relay/Server to aggregate messages between periodic requests from the MMS User Agent, and send the aggregated messages upon receipt of a periodic polling message. As with all transmissions between the MMS Relay/Server and the MMS User Agent, a POSITA understood that such "periodic" retrieval of message(s) from External Server(s) via the MMS Relay/Server (or pre-notifications associated with such messages) occurred over MM1. A POSITA also understood that the MMS Relay/Server's transmissions over MM1 responding to

periodic polling from the MMS User Agent would likewise be periodic whenever network conditions permitted—thus meeting claim 22. In more detail, in its Figure 6, TS-23.140 shows the sequence of events for "a typical transaction for an MMS User Agent submitting an MM addressed to an MMS User Agent serviced by another MMS Relay/Server." EX-1004, pp. 59-60.



EX-1004, Figure 6

210. As shown, a MM4_forward.REQ message from an Originator Relay/Server to a Recipient Relay/Server is followed by a pre-notification MM1_notification.REQ sent from Recipient Relay/Server the Recipient MMS UA, and a retrieval request MM1_retrieve.REQ sent from the Recipient MMS UA to the

Recipient Relay/Server. Consequently, the Recipient Relay/Server sends to the Recipient UA a MM1_retreive.RES message corresponding to the MM4_forward.REQ that the Recipient Relay/Server received from the Originator Relay/Server.

211. Since the periodic polling disclosed in TS-23.140 is "for discovery of incoming messages," a POSITA would have recognized that a MM4_forward.REQ message follows a polling (not shown in FIG. 6). A POSITA also would have recognized that as a result of this, at least in the case of frequent transmission of new messages between the Originator and the Recipient MMS Relay/Servers, MM4_forward.REQ would be transmitted periodically to the Recipient MMS Relay/Server when network conditions permitted (i.e., a message is sent in response to each polling, causing the responses to the periodic polling to be transmitted periodically). Since the receipt of the MM4_forward.REQ message follows by the Recipient Relay/Server sending out a corresponding pre-notification MM1_notification.REQ to the Recipient MMS UA, the POSITA would have recognized that the Recipient Relay/Server sends out the pre-notification periodically when network conditions permitted due to the periodic nature of receiving the MM4_forward.REQ message. Also, since the delivery of MM1.retrieve.RES message (associated with the polled MM4_forward.REQ) follows receiving a confirmation of the pre-notification MM1_notification.RES, a

POSITA would have recognized that the delivery of such messages also would be periodic at least in a frequent messaging transmission between the Originator and the Recipient MMS Relay/Servers when network conditions permitted.

212. A POSITA also had reason to ensure that MM1 "***support[ed]*** periodic transmissions" by the MMS Relay/Server to the MMS User Agent, since this would have beneficially allowed the MMS Relay/Server to (1) immediately respond to periodic requests for content (*e.g.*, at the frequency that a MMS User Agent indicated using TS-23.140's "periodic polling") whenever network conditions permitted, and (2) facilitate other periodic communications from external servers (*e.g.*, periodic news/weather updates). A POSITA would reasonably have expected success doing so, since periodic server-client communications were commonplace before the Critical Date. *See, e.g.*, EX-1039, 12:53-60 ("The news aggregation service is configured to ***push an updated document to its subscribers every X minutes*** (where X may be defined by, for example, the administrator or by the user). When this occurs the mobile syndication document is checked to verify if it has been updated since the time of the last push to a subscriber. ***If there has been an update the news aggregation service pushes the mobile syndication document to the subscriber's mobile device***."); EX-1040, 2:59-64 ("***The server processor periodically broadcasts invalidation reports to the client processor.*** Each respective invalidation report includes information ***identifying which, if any, of the plurality of data values have***

been updated within a predetermined period of time before the server processor broadcasts the respective invalidation report.").

t) Claims 23-24

[23] The end-user device recited in claim 1, wherein the service control device link agent is further configured to send a device credential to the network system or receive the device credential from the network system during a service authorization sequence.

[24] The end-user device recited in claim 23, wherein the device credential comprises one or more of a phone number, an identification number, a security signature, a security credential, a subscriber identity module (SIM) identifier, a mobile equipment identifier (MEID), and a device identifier.

213. Claim 23 requires claim 1's "service control device link agent" (the MMS User Agent, as discussed in the context of [1a2]) to be "configured to send" or "receive" a "device credential" to "the network system" (of which the MMS Relay/Server is a part, as discussed in the context of [1a]) "during a service authorization sequence." Claim 24 requires that the "device credential," comprise one of several alternatives, *e.g.*, a "phone number," "identification number," or "device identifier."

214. When submitting an MM message, an originating MMS User Agent provides an address of the recipient in a recipient address field that is transmitted to the MMS Relay/Server. EX-1004, 57-58. The recipient's address can be "an E.164 (MSIDN) or RFC2822 address." *Id.* The address can be a "PLMN address" such as

"an E.164 address, a local telephone number, or a numeric short code". *Id*. The message also includes the "address of the originator" (the originating MMS User Agent and its associated device), which has the same address format. *See id.* Such addresses each constitute a device credential because they identify the originating or receiving entity. *Id*. Thus, when an MMS User Agent sends a MM message, the MMS User Agent sends a "device credential" to the MMS Relay/Server.

215. Moreover, TS-23.140 discloses that an "originator MMS User Agent may support a request for the sender's address to be hidden from the recipient(s)." EX-1004, 36-37. "If the originator's MMS Relay/Server does not allow address hiding (anonymous messages) (e.g. legislation does not permit anonymous messages) a message containing a request for address hiding shall be rejected." *Id*. MMS Relay/Server may thus reject or authorize the address hiding request and either authorize use of this service as part of the message sending sequence or reject the use of this service during the message sending sequence. For example, if "MMS Relay/Server does not allow address hiding… MMS Relay/Server shall return an error information to the originator MMS User Agent." EX-1004, 36. A POSITA understood this sequence of communications for requesting an address hiding service to constitute a "service authorization sequence," as claimed.

216. Thus, a POSITA understood that the MMS User Agent (the "service control device link agent," per the discussion regarding [1a2]) is "configured to send

a device credential" (TS-23.140's originator and recipient addresses) to "the network system" (because it is sent to the MMS Relay/Server, per the discussion regarding [1a]) during a "service authorization request"—the sequence of communications between MMS User Agent and MMS Relay/Server regarding authorization for an address hiding service, discussed above, as part of the message transmission. A POSITA likewise understood the originator and recipient addresses constituted "a phone number," "identification number," or "device identifier," as required by claim 24. EX-1004, 57-58.

u) Claim 25

[25] The end-user device recited in claim 1, wherein a transmission over the service control link is within an ambient service.

217. The '733 Patent specification never uses the term "within an ambient service," or explain what it means. The '733 patent appears to use the term "ambient" service to encompass a service that the user may pay for (e.g., pay as you go sessions, news service, etc.) beyond a "basic" calling plan/service for the user's user device. *See* EX-1001, 67:37-53 ("a device 100 starts with ***ambient services that include free transaction services*** wherein the user ***pays for transactions or events rather than the basic service*** (e.g., a ***news service***, eReader, PND service, ***pay as you go*** session Internet).").

218. The MMS-Ogawa combination renders obvious applicability of ambient services within an MMS environment because it conveys that MMS User Agent is charged for the MMs it receives. TS-23.140 discloses that the "VASP may mark the content of the message with a service code that may be transferred by the MMS Relay/Server in the form of charging information for use by the billing system to properly bill the user for the service being supplied." EX-1004, 113. Further, TS-23.140 teaches alerting a user of charges associated with a service so that the user can decide whether to use that service. *See, e.g.*, *id*., p. 45 ("An MMS User Agent should ask for end-user confirmation before following a hyperlink which triggers a terminal action…. End user confirmation is recommended as accessing a resource on the network might result in additional charges."); p. 56 ("An MMS User Agent may ask for end user confirmation before any submission or retrieval of an MM triggered by an application ***due to charging***, privacy or security reasons."). Because each such message is being coded with charging information for that message (or for the services offered by that message), a POSITA would have understood that the user would be billed (and would have to pay for) the service used, that this service is beyond the "basic" messaging service described in TS-23.140, and thus that the service was an ***ambient service***, as claimed.

219. Additionally, the VASP in TS-23.140 transmits services that are similar to those identified as "ambient services" in the '733 Patent. The '733 Patent lists "a

news service, eReader, PND service, ***pay as you go*** session Internet" as example ambient services provided to the user device. EX-1001, 67:37-53. Similarly, the VASP provides, via messages sent by a respective VAS application, "news services or weather forecasts" to the MMS users. EX-1004, 14.

220. Given these disclosures, a POSITA would have understood or found obvious that the VASP can provide in messages transmitted to the MMS User Agent information associated with certain services (e.g., news, weather, etc.) and that such services would be paid for services for which billing information/service usage information would be coded into the message. As a result, a POSITA would have understood or found obvious that the transmitted messages including information associated with such paid-for services would be a transmission over the service control link that is within an ambient service, consistent with how this limitation would be understood in the context of the '733 Patent. Since VASP sends its transmissions to MMS User Agents through the MM1 interface (the "service control link," as discussed for [1a]), a POSITA understood that transmissions of messages related to these services are "within an ambient service," as claimed.

221. It should be noted that the '733 Patent does not appear to use the term "ambient service" in its ordinary sense. The term "ambient service" was used in the art to convey services that a device receives when placed within a communication coverage area of a network provided by a service provider. *See e.g.*, EX-1032, 8:60-

67 ("To receive the service in the service providing system 21 of FIG. 4, the mobile terminal carried by the user needs to be present… within ***a predetermined area (i.e., the communication coverage area*** 41AB) [to] receive ***ambient service*** in the service providing system 21.), 17:18-27 ("the service providing system 201 provides different services depending on the area where the mobile terminal 32 carried by the user is present. The user can thus enjoy the service responsive to the position of the user by simply carrying the mobile terminal 32 and moving to ***a predetermined area***. The service providing system 201 thus provides the user with ***ambient services***."). Instead, as noted above, the '733 Patent used the term "ambient services" differently, and in connection to a service that the user pays for beyond a basic service.

222. Had the Patent used the term "ambient service" in its ordinary sense as used in the field (i.e., a service that the mobile device receives when placed within a communication coverage area of a network), the MMS-Ogawa combination would still render the claim obvious. A POSITA understood that an MMS Relay/Server provides services (i.e., "ambient services") to a user device when the user device is within a network coverage supported by MMS. TS-23.140 discloses that a "terminal" (i.e. a device) benefiting from a Multimedia Messaging Service Environment (MMSE), has to be within a network coverage (e.g., a 2G or a 3G network) that the MMSE supports. EX-1004, 16-17. When a message (MM) is received at the MMS Relay/Server of an MMSE for delivery to a particular user

device, the recipient MMS Relay/Server delivers the message to the MMS User Agent of the user device, or "store[s the] message[] in the network until the recipient MMS User Agent becomes reachable (e.g. ***user moves back into coverage***)." *Id*., 29. Thus, a POSITA understood that the MMS User Agent benefits from the message receiving services ("ambient services") when placed within the communication coverage of the network supported by the MMS Relay/Server.

223. Since the MMS Relay/Server transmits messages to the MMS User Agents through the MM1 interface (the "service control link," as discussed for [1a]), a POSITA understood that transmissions of messages related to these services are "within an ambient service," as claimed.

v) Claim 26

[26] The end-user device recited in claim 1, wherein the particular device agent comprises software.

224. MMS-Ogawa's destination applications (the "device agents," as discussed in the context of [1b]) "comprise software," as claimed. For example, TS-23.140 describes registration for application data transport using MMS, where the registering entity is a "downloadable application" on a "mobile phone". EX-1004, §7.1.18, p. 54. By virtue of being downloadable, and particularly being downloadable on a mobile device, a POSITA understood that the application is a software application that is downloadable (or downloaded) on a mobile device.

w) Claim 27

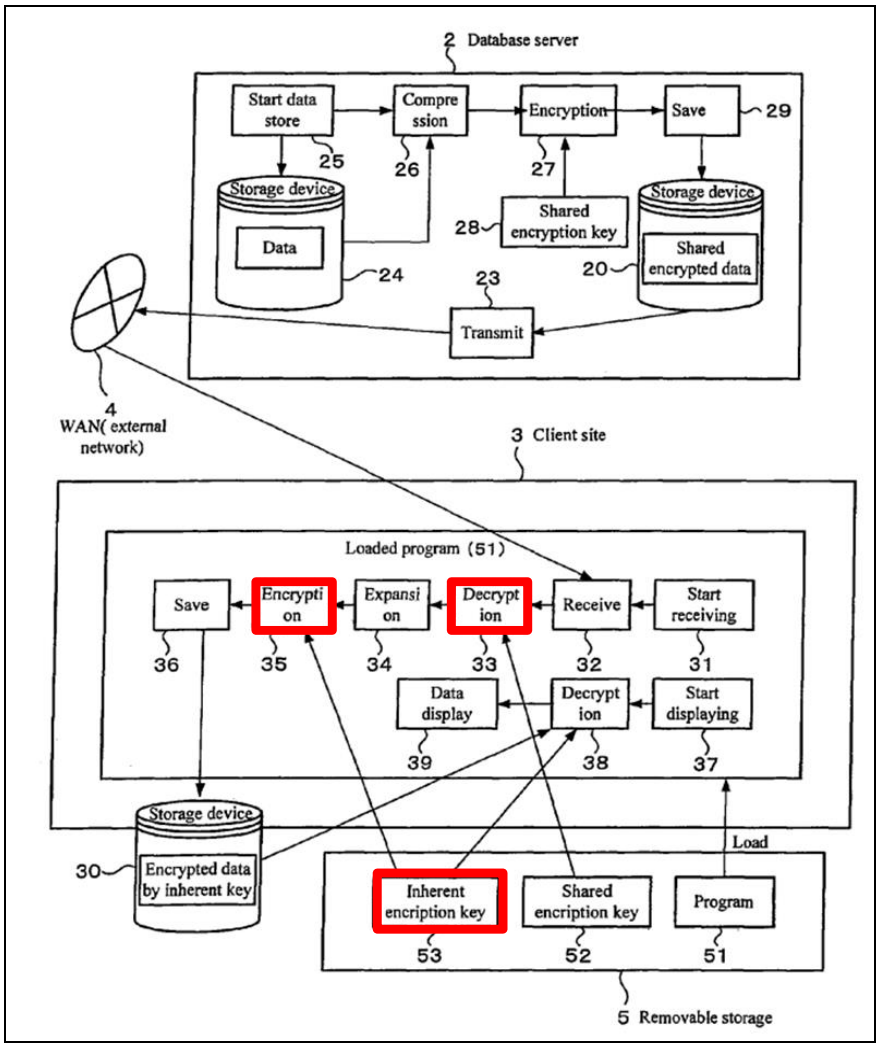
[27] The end-user device recited in claim 1, wherein the encryption key is a first encryption key, and the service control device link agent is further configured to encrypt the message content using a second encryption key before delivering the message content to the particular agent, the second encryption key shared by the service control device link agent and the particular agent.

225. Claim 27 calls the encryption key (recited in claim 1) "a first encryption key," requires claim 1's "service control device link agent" to be "configured to encrypt the message content using a second encryption key before delivering the message content to the particular agent."

226. TS-23.140 teaches that MMS User Agent (the ***service control device link agent***, as discussed for [1a2]/[30a2]) is responsible for receiving a message from TS-23.140's MMS Relay/Server, decrypting the message using a first encryption key, and sending message content to a destination application (the ***particular device agent***, as discussed for [1d3]/[30d3]-[30d4]).

227. As discussed *supra* §IX.A.3(d), Ogawa discloses an encryption unit for re-encrypting data for, e.g., transmission within the user device. EX-1005, 5:59-6:9. In Ogawa, a message received and decrypted at the client (using receive unit 32 and encryption unit 33) is converted back to its original format (using decompression/expansion unit 34), and encrypted again—before being transmitted within the client device, e.g., for storage—by encryption unit 35, using an "inherent encryption key 53." EX-1005, 5:59-6:26, 5:24-25. Ogawa's inherent encryption

key 53 is a second encryption key that is different from the first encryption key used to encrypt/decrypt data transmitted between the server and client.



EX-1005, FIG.7 (annotated)

228. As discussed *supra* §IX.A.3(d), a POSITA had reason to include the encryption functionality as part of MMS-Ogawa's User Agent—*e.g.*, to secure decrypted received data before transmitting it to any other component on the user device—and would have reasonably expected success with such an implementation.

229. A POSITA would have been motivated to implement MMS-Ogawa's user device to secure/encrypt message content (received from, e.g., the MMS Relay/Server) using a different encryption key than the one used to decrypt the received data (e.g., Ogawa's disclosed inherent key) prior to delivery to device storage or a destination application, as taught by Ogawa. EX-1005, 6:1-26; *see also* EX-1037 (corroborating that that encrypting the received data within a device before storing it there was a well-known technique). Such internal encryption within the device using an inherent key was expressly taught by Ogawa and would have improved security of data in MMS-Ogawa's user device when stored on the device or when transmitted within the device, and would have helped, *e.g.*, prevent unauthorized viewing or use of the data by rogue/unauthorized software on the device.

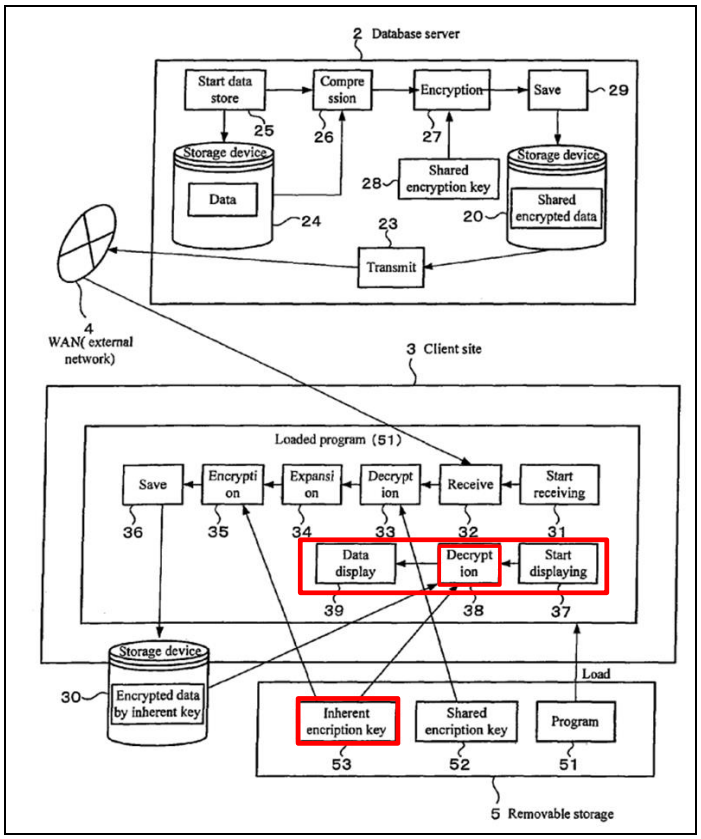
230. A POSITA would also have had reason to implement MMS-Ogawa's User Agent such that it performed any intermediary functions/steps between decryption (e.g., by Ogawa's unit 33) and re-encryption (e.g., by Ogawa's unit 35) that were required to ensure that the destination (on the user device) received data with correct format and content. For example, the expansion unit 34 in Ogawa decompresses the decrypted data "to convert the data back to [its] original format" before re-encrypting that data at unit 35. EX-1005, 5:65-6:3. A POSITA would have reasonably expected success implementing MMS-Ogawa's User Agent to

perform the intermediary functions described in Ogawa, as discussed above—*e.g.*, by incorporating Ogawa's expansion unit 34—because the prior art components would continue to perform functions they performed prior to the combination. For example, the MMS User Agent would continue to receive, decrypt, and send data within the user device, and Ogawa's expansion and encryption units (implemented as part of the MMS User Agent) would continue to convert decrypted data into its original format before encrypting it for use within the user device.

231. Claim 27 also requires "the second encryption key" to be "shared by the service control link agent and the particular agent."

232. As noted for claim 19, MMS-Ogawa's user device is capable of displaying messages to a user. EX-1004, 16 (Figure 1), 19, 155 (Figure A.1). As discussed below, POSITA had reason to implement the display functionality in the MMS-Ogawa user device such that it could display data that was encrypted using Ogawa's inherent key 53 (pursuant to Ogawa's teachings discussed above) and subsequently decrypted for the display.

233. Ogawa teaches using "display units 37-39" to "provide the necessary functionality for rendering decoded data to a display of" the client. In order to "render" and display data stored on the client, Ogawa teaches decrypting the data using the same inherent key 53 that encryption unit 35 used to encrypt the data for storage within the device. EX-1005, 5:24-30, 6:10-18.



EX-1005, FIG. 7 (annotated)

234. Based on Ogawa's teachings, a POSITA had reason to implement MMS-Ogawa's user device to incorporate Ogawa's display units 37-39 to be able to decrypt and display data encrypted using Ogawa's inherent key 53. A POSITA would have reasonably expected success implementing MMS-Ogawa's user device to use Ogawa's display units 37-39 to perform the decryption and display functions described in Ogawa, because the prior art components would continue to perform functions they performed prior to the combination. In such an implementation, for data received by the MMS User Agent from the MMS Relay/Server that was intended for immediate display to the user by the MMS User Agent device (instead

of, e.g., data intended for a specific application associated with a VASP, as discussed for previous claims), a POSITA understood that MMS-Ogawa's display units 37-39 themselves collectively constituted a destination application in the user device that performed display functions on behalf of an entity (e.g., client, server, another application), and thus constituted one of the "***plurality of device agents***" (identifiable by a "associated device agent identifier" in order to allow accurate routing of data intended for immediate display) for [1b], and "***a particular device agent***" for [1d3], in claim 1.

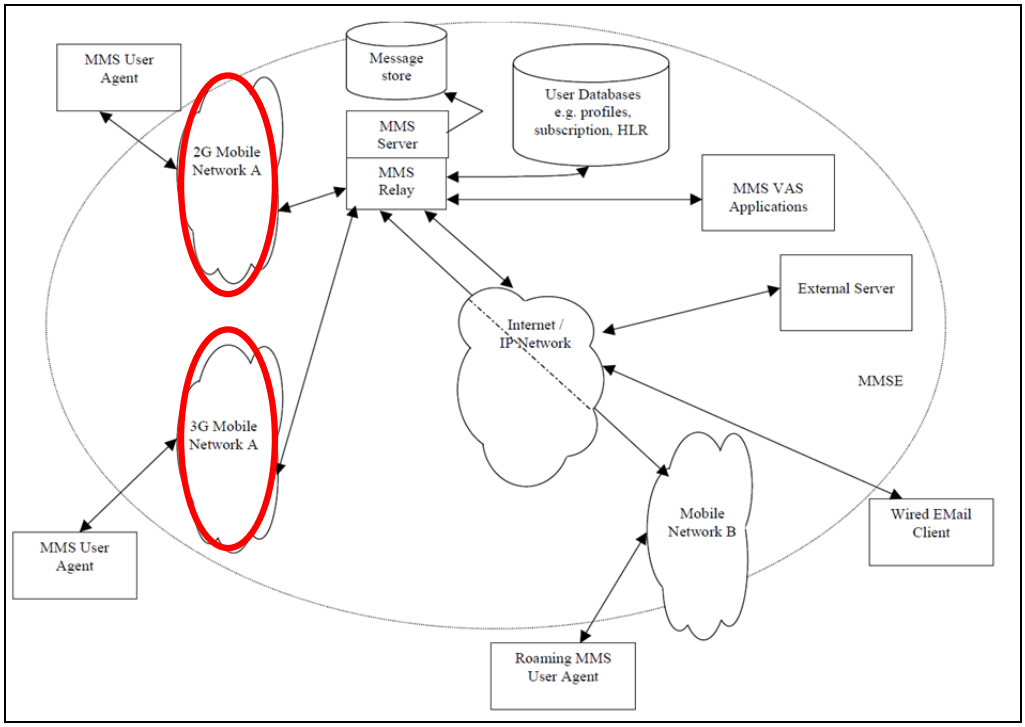
235. Because both the MMS User Agent and MMS-Ogawa's display units 37-39 use the same key for encryption and decryption, a POSITA would have understood that the inherent key (the claimed ***second encryption key***) is ***shared*** by encryption unit 35 in the MMS User Agent (***the service control device link agent,*** as claimed) and the destination display units 37-39 (***the particular agent***, as claimed).

x) Claim 29

[29] The end-user device recited in claim 1, wherein the service control link is configured to support control-plane communications using an Internet protocol.

236. As described with reference to [1a], [1a1], and [1a2], MM1 in MMS-Ogawa (the claimed "service control link") supports control-plane communications. Moreover, communications between the MMS User Agent and the MMS

Relay/Server occur over wireless networks that use an Internet protocol. In FIG. 2 reproduced below, a 2G mobile network and a 3G mobile network each facilitate communications between a MMS User Agent and the MMS Relay/Server.



EX-1004, Figure 2 (annotated)

237. TS-23.140 explains that the "basis of connectivity between these different networks shall be provided by the ***Internet Protocol*** and its associated set of messaging protocols." EX-1004, 17. "This approach enables messaging in 2G and 3G wireless networks to be compatible with messaging systems found on the Internet." *Id*. Given these disclosures in TS-23.140, a POSITA would have understood that each of the 2G and 3G networks use an Internet protocol. Alternatively, this would have been a conventional, obvious way to implement what

TS-23.140 describes, and is nothing more than utilizing familiar, known components to achieve a predictable, desirable result of enabling TS-23.140's user agent to send and receive data over the Internet.

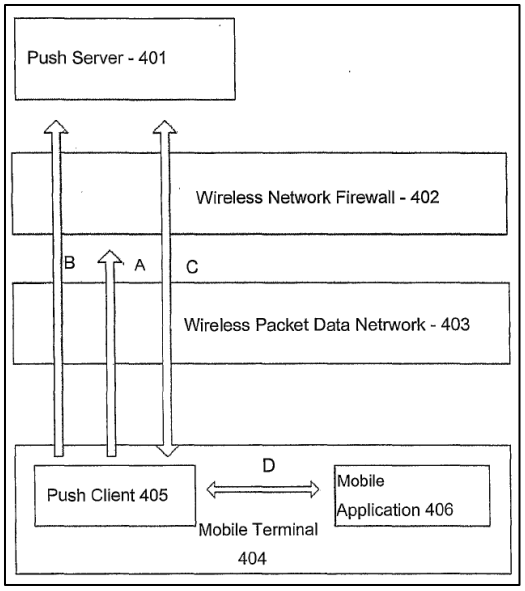
238. Thus, because communications in MMS-Ogawa occur over MM1, including control plane communications, MMS-Ogawa meets the requirement that the "service control link" (MM1, as described with reference to [1a2]) "is configured to support control-plane communications using an Internet Protocol," as claimed.

B. Ground 2: Claims 1, 2, 5, 7-10, 13-15, 19-22, and 26-30 Are Obvious Over Houghton and Ogawa

1. Houghton (EX-1006)

239. Houghton discloses pushing commands from a server to a mobile terminal (which Houghton also calls a "client device") to "initiate control of… applications on [the] terminal." EX-1006, 10-11[4], 14-15. Through the pushed commands, the server can "deliver through that mobile application real time information, interactivity and rich media content, regardless of which mobile operator is being used and where the mobile user happens to be at that moment." *Id*. An exemplary embodiment is shown in Houghton FIG. 4:

[4] References to Houghton (EX-1006) are to page numbers printed on the document rather than to page numbers stamped on the exhibit.

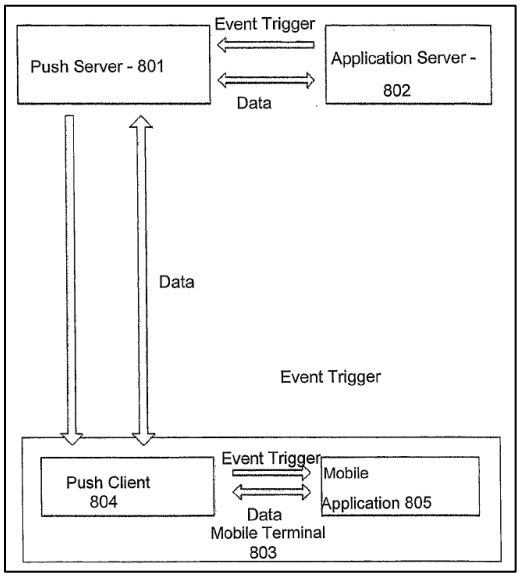


EX-1006, Figure 4

240. As shown, ***push client 405*** on ***mobile terminal 404*** and ***push server 401*** send and receive messages through ***data connection C***. *Id*., 20. Push messages (from a push server) include "application-specific" information "specifying which mobile application 406" ("of a plurality of mobile applications 406") on mobile terminal 404 is the target of the push message. *Id*., 21. Upon receiving this message, "appropriate automated actions and user interface media capabilities of the mobile terminal as specified in the command C from the server 401 are executed by the push client 405." *Id*. "The most common case is playing a sound, asking the user if the mobile application should be launched, and if affirmative passing the command details (arrow D) to the specified mobile application." *Id*.

241. Houghton's "persistent[,] managed, tested and configured" data connection C shown above (Figure 4) may be used to "establish[]" "a data

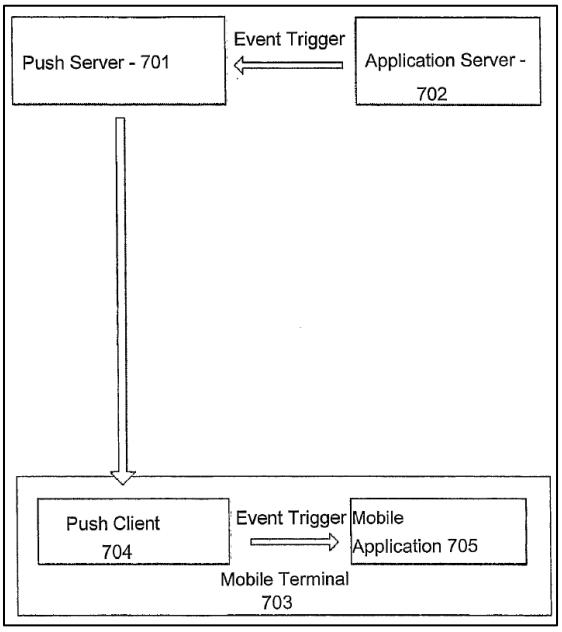
connection between [a separate] application server 802" and the mobile application on the mobile terminal, as shown in Figure 8 (below). *Id.*, 23.



EX-1006, Figure 8

242. In Houghton, a "'COMMAND PUSH' procedure" is used, "wherein the push server… is triggered by a trigger event… from an application server… to push an application command message to the push client… and thereby initiate a mobile terminal client trigger event in a mobile application… from a plurality of such applications, program modules, and user interface features on the terminal…" EX-1006, 23. "Figure 7 illustrates an example of an "COMMAND PUSH" procedure wherein the push server 701 is triggered by a trigger event as for example from an application server 702 to push an application command message to the push client 704 and thereby initiate a mobile terminal client trigger event in a mobile

application 705 from a plurality of such applications, program modules and user interface features on the terminal 705." *Id.*, 21-22.



EX-1006, FIG. 7

243. FIG. 8 (shown above) depicts an "embodiment [that] all aspects of "COMMAND PUSH" [shown in FIG. 7] with the additional step that a data connection between application server 802 and mobile application 805 is established with the aid of the persistent managed, tested and configured data connection in Figure 4, arrow C between push server 401/801 and push client 405/804." *Id.*, 23. In this declaration document, components of Houghton's system in which the mobile terminal uses data connection C to exchange messages with an application server through a push server are sometimes referred to using reference numbers from both Figures 4 and 8 (*e.g.*, mobile terminal 404/803, push client 405/804).

244. Houghton discloses using a "connection-oriented protocol such as TCP/IP, SSL [Secure Socket Layer], HTTP or HTTPS" to facilitate a secure communication link between the push server and mobile terminal. EX-1006, 20. Houghton also discloses "exchanging security keys" between server and client. EX-1006, 29 (claim 3). As explained below, before the Critical Date, both Houghton's example protocols and exchanging security keys were well-known techniques in securing data transmission between entities.

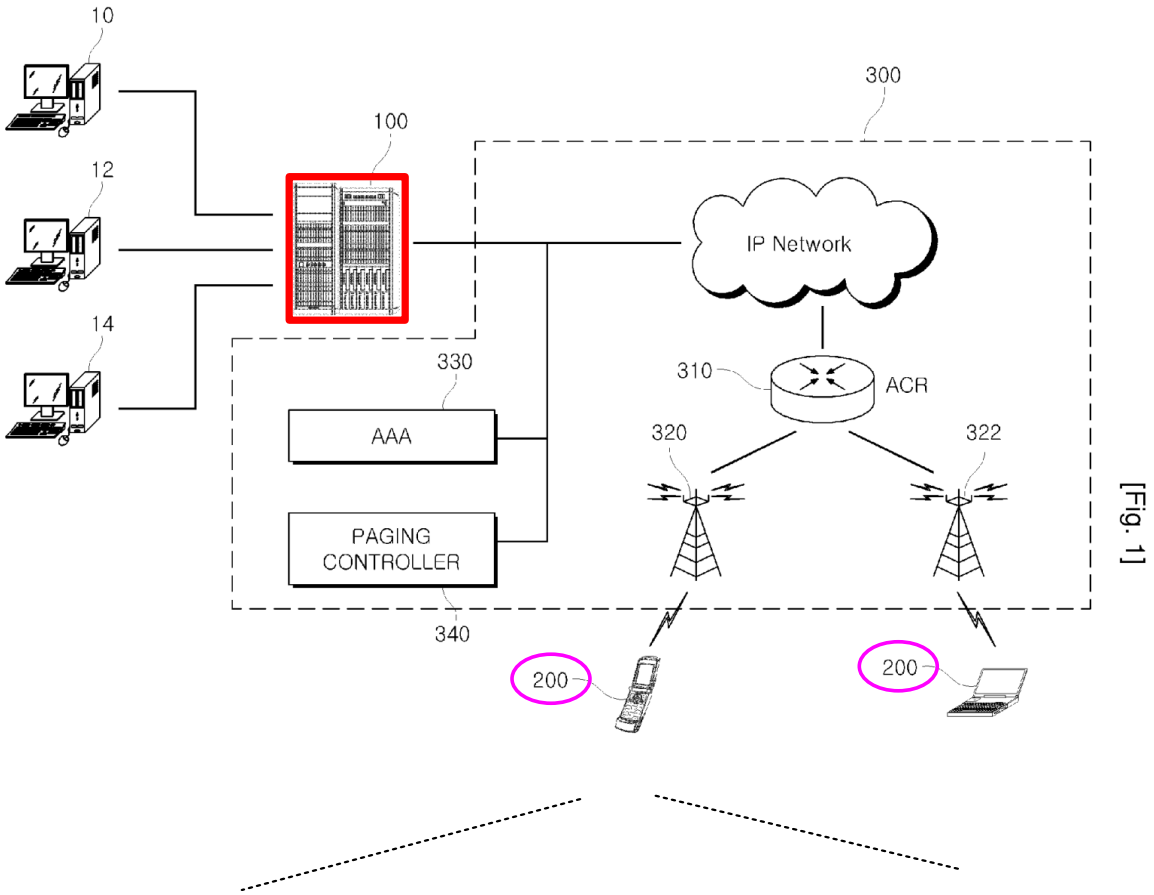
2. Houghton-Ogawa Combination

a) Implementing Houghton's Mobile Terminal with a Modem

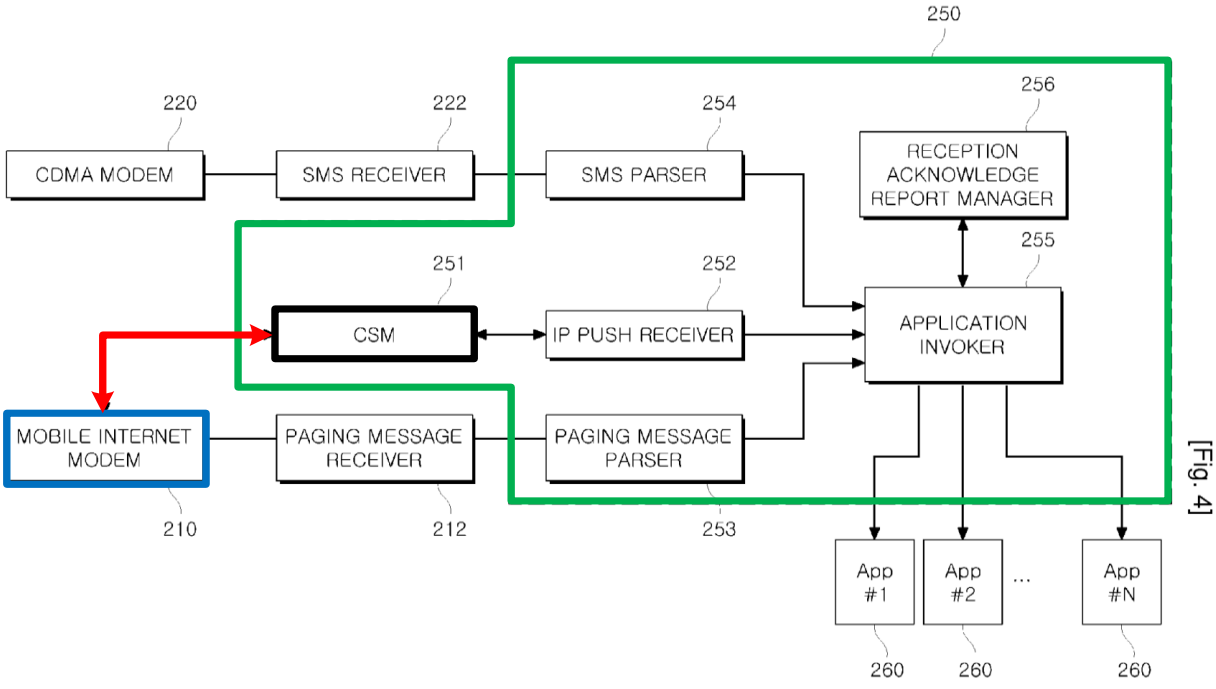
245. Houghton's mobile terminal is "located in [a] wireless network," and software on the terminal communicates with servers "over a data network 403, normally a wireless network capable of transmitting Internet Protocol (IP) packets." EX-1006, 11, 17. Houghton's terminal is also "equipped" to establish "a connection" to a "broadband network access point" via "a wireless communication network such as… Bluetooth, …Wi-Fi, Wi-Max or other personal area, local area, metropolitan, or large area network." *Id.*, 13-14.

246. While Houghton does not disclose details regarding how its mobile terminal facilitates communications over the wireless networks described in Houghton, using a modem for enabling communications with the wireless networks described in Houghton was well-known before the Critical Date. Lee, for example,

is a corroborating reference in the general technical field of push communications between network entities and applications executing of a user device. EX-1008, Abstract, ¶¶[1], [8], [44], [46], [55], [56]. In Lee, a service agent 250 (green in the figure below) on mobile terminal 200 (pink) receives messages from a service server 100 (red), and the mobile terminal 200 receives the messages through a mobile internet modem 210 (blue). *Id*., ¶¶[22-23], [27-28].



[Fig. 1]



[Fig. 4]

EX-1008, FIG. 1 (top, annotated), and FIG. 4 (bottom, annotated)

247. Using a modem to enable a user device to communicate over Houghton's wireless networks would have been a conventional and obvious way to implement what Houghton describes, and is nothing more than utilizing familiar, known components to achieve a predictable result of facilitating Houghton's communications. *See* EX-1008, ¶¶22-23. Moreover, a POSITA would have reasonably expected success in implementing Houghton's device with a modem because modems were a well-known, conventional way of achieving the wireless network communications Houghton describes.

b) Applying Ogawa's Symmetric Encryption Techniques

248. Houghton discloses using SSL for securing communication links between the push server 401 and push client 405. EX-1006, 20, 18. Houghton also describes "exchanging security keys" between the server and the client (EX-1006, 29) but does not provide details regarding the security key exchange. It was well-known (before the Critical Date) for data in messages transmitted between a server and a client to be encrypted using symmetric encryption, with a key that is shared between the server and the mobile terminal and stored in their respective memories. *See e.g.*, EX-1027, [0054]-[0060]; EX-1005, 3:44-53, 9:16-34; EX-1009, 3:25-27, 8:1-15. As discussed *supra* § IX.A.2 and further below, Ogawa also discloses details

regarding how to implement such symmetric encryption of messages sent between a server and a client. *See e.g.*, EX-1005, 3:44-53, 9:16-34.

249. A POSITA would have had multiple reasons to implement Ogawa's symmetric data encryption techniques with Houghton (which I have referred to here as "Houghton-Ogawa Message Encryption").

250. ***First,*** implementing the data encryption taught in Ogawa to Houghton's communicated messages would have achieved a "protected" push messaging system that beneficially "protect[s] the mobile terminals from hostile or unwanted contact common on the public Internet" (utilizing "exchang[ed] security keys"), consistent with Houghton's teachings. EX-1006, 17, 29.

251. ***Second,*** both references describe systems in the field of client-server communications, and Ogawa explains how an additional layer of symmetric encryption can be implemented for securing communications in server-client networked environments which already utilize, e.g., SSL, similar to those described in Houghton. In particular, Ogawa discloses using the SSL protocol to facilitate secure server-client communications (like Houghton), and then implementing an ***additional*** layer of encryption that involves exchanging a security key between server and client, storing the key at both, and using that key to encrypt and decrypt messages. EX-1005, 3:44-53, 3:60-4:4, 4:48-57, 5:59-65, 6:64-7:21, 9:16-34; *see also* EX-1009, 3:25-27, 8:1-5 (corroborating that that storing an encryption key on

both a server and a client device was well-known by the Critical Date). Given Ogawa's express teachings, the well-known use of symmetric data encryption in SSL-protected client-server environments like Houghton's, and the consistency between Ogawa's teachings and Houghton's teachings of security key exchange, a POSITA would have been motivated to implement Ogawa's encryption teachings of using a shared encryption key to encrypt Houghton's server-client communications.

252. ***Third,*** implementing the techniques described in Ogawa to Houghton's SSL-protected system would have beneficially enhanced security of data communications occurring over Houghton's network. Ogawa expressly teaches using two forms of encryption for client-server communications instead of one—data encryption to encrypt data sent over a secure communication channel (e.g., SSL-based connection)—which would have motivated the implementation of the same dual encryption techniques within Houghton's system.

253. ***Fourth,*** implementing Ogawa's data encryption into Houghton's system would have been nothing more than implementing known methods/techniques (symmetric encryption using a shared key as taught in Ogawa) to known systems/devices (the push server and mobile terminals with push clients taught in Houghton) to achieve predictable results (data encryption over messages transmitted on a secure SSL, as contemplated by Houghton).

254. Implementing Ogawa's encryption techniques in Houghton's system would have been predictable and straightforward, and a POSITA would have had a reasonable expectation of success in doing so, given (1) the similar client-server communication architectures taught by both references, (2) Houghton's teaching of key exchange for message encryption, and (3) Ogawa's (and the above-described corroborating references') provision of an exemplary implementation of such encryption using a symmetric/shared encryption key in the context of an SSL-protected network environment.

c) Ogawa's Decryption and Encryption Units

255. Ogawa teaches a "decryption unit" for decrypting received encrypted data as part of its symmetric encryption system. EX-1005, 5:59-6:9 ("[R]eceived shared key encrypted data will be decrypted using the shared encryption key 52 which was supplied to the decryption unit 33 and beforehand stored…"). A POSITA would have had reason to implement Ogawa's decryption unit as part of Houghton's push client to facilitate decryption of encrypted data received from the push server because Houghton's push client is responsible for receiving messages and distributing them to the correct mobile applications on the mobile terminal. Such an implementation would have beneficially allowed Houghton's push client to decrypt an encrypted message from the push server and obtain received information identifying the destination application to which the message should be routed.

256. Ogawa also teaches an encryption unit for encrypting (or "re-encrypt[ing]") data before transmitting it to another entity on the network (e.g., a server) or another part of the device, *e.g.*, storage. EX-1005, 5:59-6:9. As with the decryption unit, a POSITA would have had reason to implement the encryption unit as part of the Houghton's push client, because being able to securely transmit data to other components residing on the device such a storage unit, as disclosed in Ogawa, was a desirable feature that would have helped prevent, e.g., data theft.

257. A POSITA would have reasonably expected success in an implementation with Ogawa's encrypt and decrypt units incorporated into the push client on Houghton's mobile terminal, because the prior art elements of this system would each perform functions they performed prior to the combination—Houghton's system would continue to provide the push communications between push clients and push server using secure data connection C, and Ogawa's decrypt and encrypt units (implemented as part of the push client) would continue to facilitate encryption/decryption to secure the data received from the push server. Such a combination would have been well within a POSITA's capability to implement.

d) Storing Ogawa's Shared Encryption Key

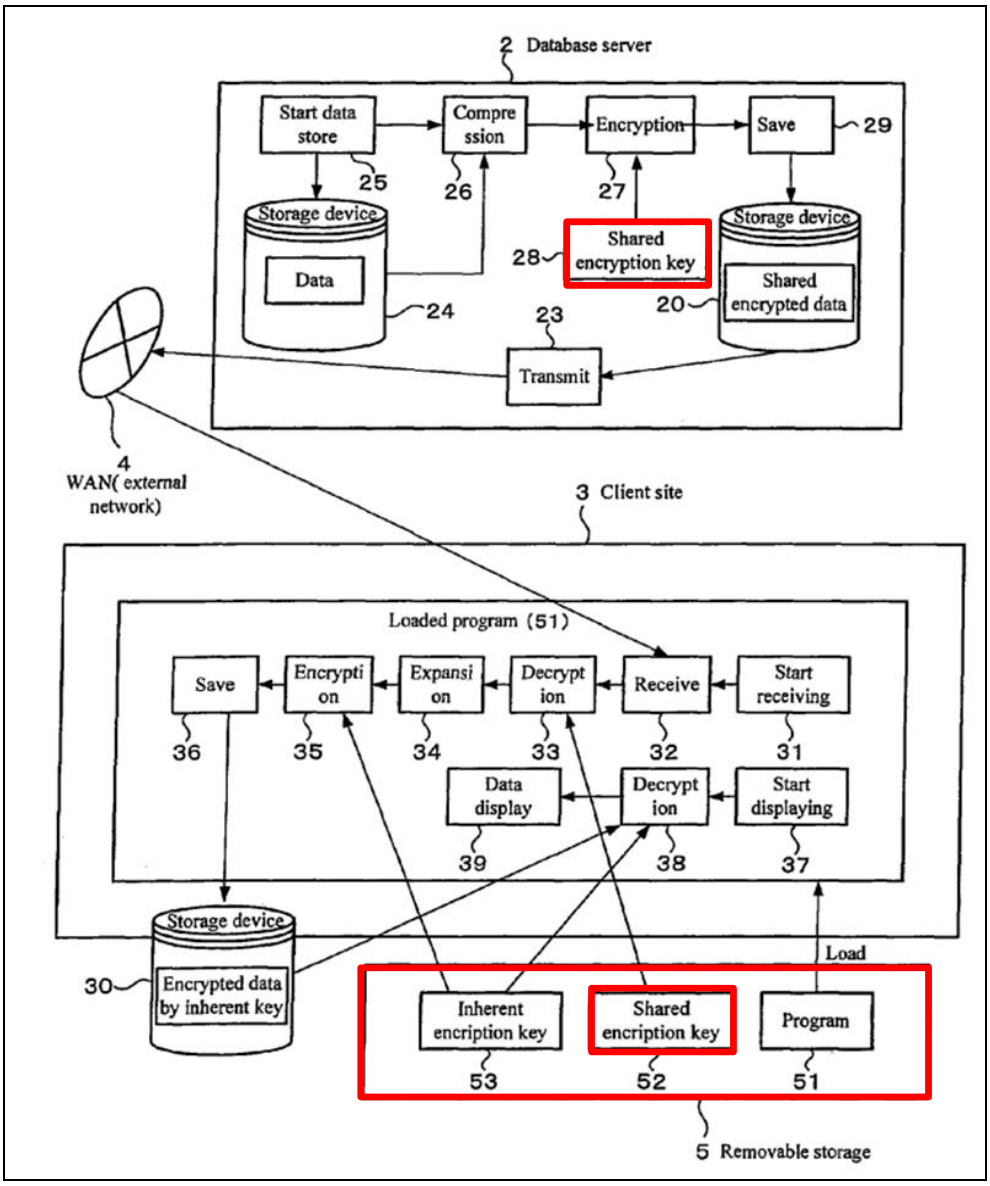
258. Houghton discloses that its mobile terminal is "capable of receiving and ***storing*** variables which configure behavior of the client," and discloses "***stored***"

"username, password, and security certificates." EX-1006, 22-23. A POSITA thus understood that Houghton's mobile terminal has memory. Alternatively, such an implementation would have been a conventional and obvious way to implement the "storing" that Houghton describes, and is nothing more than utilizing familiar, known components (memory) to achieve a predictable result of storing data on a mobile terminal.

259. Ogawa teaches the well-known technique of ensuring that each device/entity in a network environment that encrypts or decrypts communications using symmetric encryption ***stores*** the encryption key in memory connected to it. EX-1005, 3:18-34, 4:48-57, 5:59-65, 6:64-7:21, FIGS. 1, 7; *see also* EX-1009, 8:1-5, 3:25-27 (corroborating storage of an encryption key in a memory of the client device); EX-1006, 29, claim 3 (contemplating "exchanging security keys" between the server and the client). For symmetric encryption, there were a limited number of ways to ensure the same key was used by encrypting/decrypting devices, including (1) storage of the same key by each encrypting/decrypting device in persistent memory, and (2) generation of the same key at each device prior to performing the encrypting/decrypting operation, and storage of that key temporarily during the operation. In both ways, the key was stored during the encryption/decryption.

260. A POSITA would have had multiple reasons to store Ogawa's encryption key in the memory of Houghton's mobile terminal to facilitate decryption of encrypted messages received from Houghton's push server.

261. ***First***, an implementation in which the encryption key was stored in the Houghton mobile terminal's memory would have been a way to implement the symmetric encryption teachings of Ogawa, which discloses storing the shared encryption key in removable storage 5 that is connected to client site 3 and functions as a memory for client site 3, so that the key can be retrieved and used when needed to decrypt a message. EX-1005, 3:61-4:7, 5:41-47, 9:21-34, FIG. 7.



EX-1005, FIG. 7 (annotated)

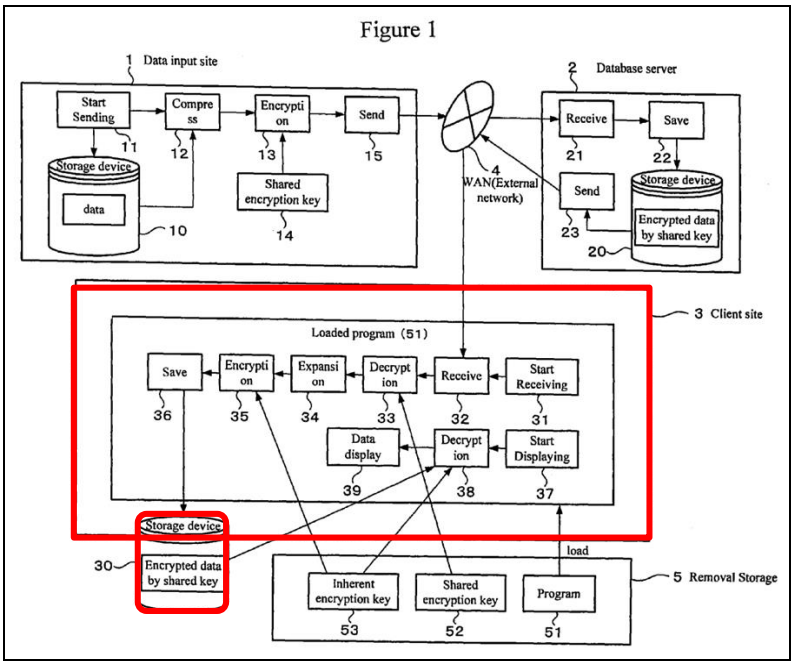
262. Storing Ogawa's encryption key in the memory of Houghton's mobile terminal (*i.e.*, the client site, in Ogawa's terminology) would have beneficially enabled the Houghton's push client (modified to include Ogawa's decryption and encryption units, as discussed above) to access the key and perform the decryption/encryption described in Ogawa.

263. ***Second***, such an implementation would have been nothing more than implementing a known method (storage of a symmetric/shared key in memory as taught by Ogawa and background references) to known systems (Houghton's push system, including a mobile terminal with memory) to achieve a predictable result of enabling Ogawa's symmetric encryption/decryption in Houghton's push system. *See e.g.*, EX-1009, 8:1-5, 3:25-27.

264. ***Third***, storing the shared key on a memory within Houghton's mobile terminal would have been an obvious, readily-implementable design choice that a POSITA would have known would facilitate storing of Ogawa's encryption key in a location accessible to the mobile terminal, as was necessary for symmetric encryption. That this design was well-known to POSITAs is corroborated by references like Qumei, which describes storing the "enciphering key" in an end-user device (*e.g.*, a mobile handset). EX-1009, 3:25-27.

265. Ogawa's removable storage 5 is part of the end-user device because it is connected to the client site 3 and functions as a memory for the client site 3 to store the shared key, and to retrieve it when needed to decrypt a message. EX-1005, 5:41-47. Ogawa further discloses that "the shared key encrypted data will be received by the [client site 3] from the database server 2 via network 4." EX-1005, 5:60-65. "This received shared key encrypted data will be decrypted using the shared encryption key 52 which was supplied to decryption unit 33 and beforehand

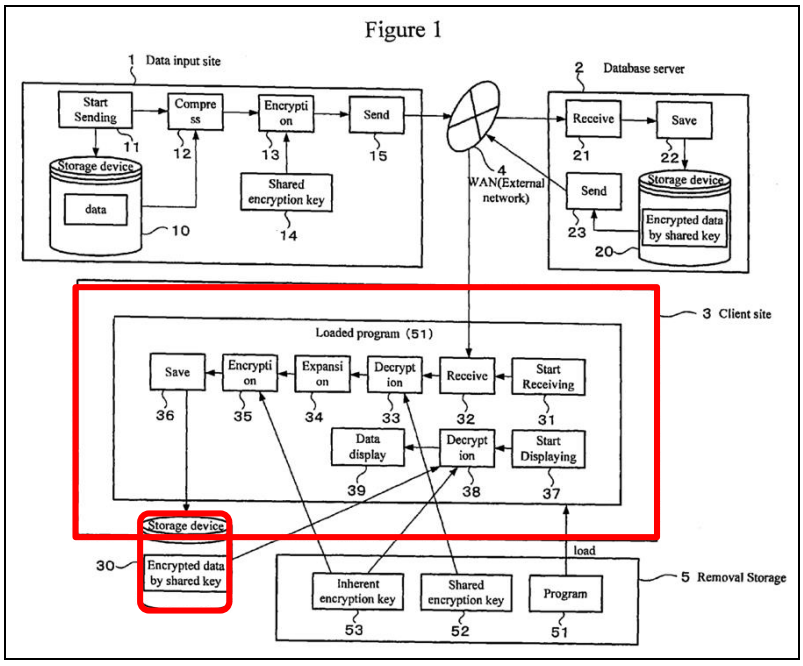
stored on the removable storage 5." *Id.*; *see also id.*, 6:64-7:21 ("When the removable storage 5 receives the encryption key from the client site 3 in step S15, it stores the encryption key into the memory device in the removable storage in step S16.").



EX-1005, FIG. 7 (annotated)

266. However, even if Ogawa's removable storage 5 were not considered part of the end-user device, having such memory resident on the end user device would have been obvious in view of Ogawa's teachings as well as the well-known use of storing encryption keys in memory resident in end-user device in the relevant timeframe (as also contemplated by Houghton). For example, Ogawa uses the removable memory 5 for mobility or group settings. EX-1005, 5:49-58. Removable memory 5 enhances mobility because it can be implemented "as a USB memory

device, flash drive, Zip disk, floppy disk, compact disc, miniSD, or even DVD RAM," attachable to the client 3 by being "physically coupled to the client site 3." EX-1005, 5:42-51. "A plurality of removable storage 5 devices may also be used, wherein each removable storage 5 contains the same program (or encryption key)…for encrypted data to be shared by members of a common group." *Id.*, 5:54-58. If such independent mobility or group settings are not required or needed for the intended environment, a POSITA would have found it obvious to simply store the shared key on a memory fixed to the client site 3, for example, on storage device 30.



EX-1005, FIG. 7 (annotated)

267. Alternatively, or additionally, storing the shared key on a memory installed/resident within the end user device would have been an obvious design choice that would be readily implemented to facilitate data storage, including storage

of the above-described shared encryption key. Qumei, for example, corroborates storing the "enciphering key" in the end-user device (e.g., a mobile handset), thus confirming that it would have been obvious to implement storage of the shared key within memory resident within the end-user devices. EX-1009, 3:25-27.

268. Storing the encryption key in the Houghton terminal's memory and enabling it to be retrieved from memory when needed would have been well within a POSITA's skill to implement, and a POSITA would have reasonably expected success in doing so, because this would have involved using components to perform the functions they performed prior to the combination.

e) Houghton-Ogawa

269. "Houghton-Ogawa" refers to the above-discussed encrypted push system that a POSITA would have been led to form based on Houghton and Ogawa.

270. Houghton-Ogawa implements Houghton's mobile terminal (which is configured to use the push system as described in Houghton) with a modem for wireless network communications. *Supra* § IX.B.2(a).

271. Houghton-Ogawa also implements Houghton's push server and mobile terminal so that the communication link between them is secured using SSL and transmitted messages are further encrypted using symmetric Houghton-Ogawa Message Encryption. *Supra* § IX.B.2(b).

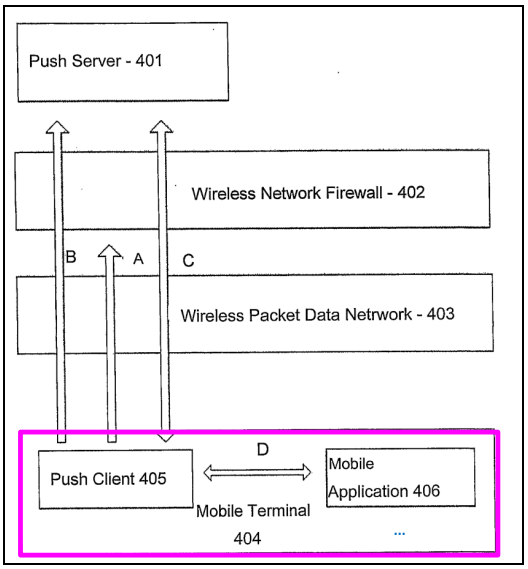
272. In Houghton-Ogawa, Ogawa's encrypt and decrypt units are implemented as part of the push client in Houghton's mobile terminal (*supra* § IX.B.2(c), and a common key is distributed to (and stored in the respective memories of) Houghton's mobile terminal and push server (*supra* § IX.B.2(d)).

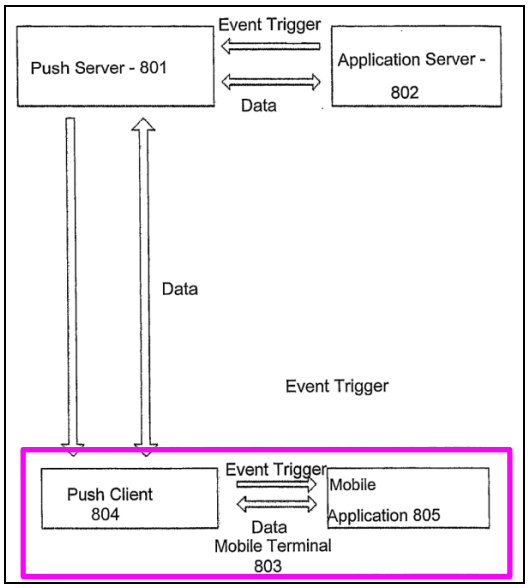
3. Claim Analysis

a) Claims 1 and 30

[1pre] An end-user device comprising:
[30pre] A method performed by an end-user device, the method comprising:

273. The '733 specification does not define any requirements for an "end-user device" (*see* EX-1001, 8:3-15, 8:60-9:15), using the term to include a "networked" device that has "services [for a user] delivered" to it. EX-1001, 5:65-6:28, 6:49-56. To the extent the preambles are limiting, a POSITA understood Houghton-Ogawa's mobile terminal 404/803 is an "end-user device," because it operates "under supervision" of a user and is a networked device to which services for the user are delivered. *See, e.g.*, EX-1006, 17, 12, 22.





EX-1006, FIG. 4 (annotated, left); FIG. 8 (annotated, right)

274. As described with reference to limitations [30a]-[30f] *infra*, Houghton-Ogawa's mobile terminal 404/803 performs claim 30's method.

[1a] a modem for enabling communication with a network system over a service control link provided by the network system over a wireless access network,

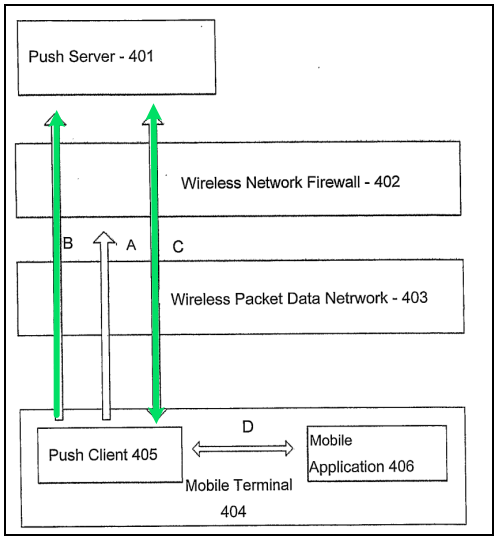
275. Element [1a] requires "a ***modem*** for enabling communication" taking place "over a wireless access network." The '733 specification uses "modem" to include "Wi-Fi" modems with which a device wirelessly communicates over an "access network, such as a… DSL wire line, cable DOCSIS wire line or fiber wire line configuration in place of the 3G or 4G access network connection." EX-1001, 25:29-45, 27:38-44, 29:52-67, 33:59-65. A POSITA understood Houghton-Ogawa's modem for connecting to a "wireless communication network such as… Wi-Fi" that provides access to a "broadband network" (*supra* § IX.B.2(a))—just like

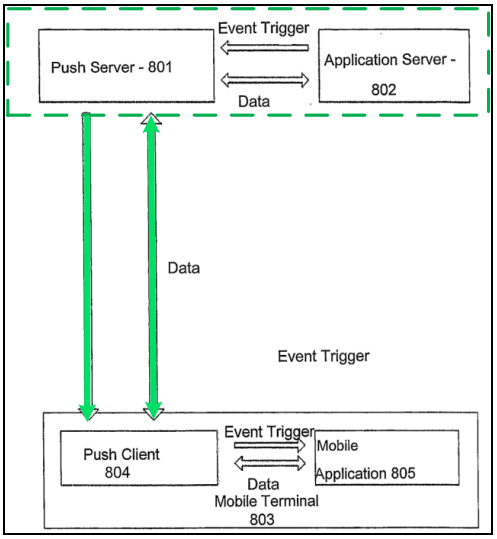
the ’733 Patent’s “Wi-Fi” modem that provides access to “DSL” and “cable” networks—is a “modem for enabling communication” taking place “over a wireless access network” as claimed.

276. Element [1a] also requires that the modem enable communication “with a ***network system*** over a service control link.” The ’733 specification never describes a “***network system***” in the context of a “service control link.”[5] According to the specification, a “service control link” is a “communication link” “between a device and ***the network***”—which, in the specification’s embodiments, is represented by “service controller 122.” EX-1001, 17:8-11, 68:20-37, FIGs. 16-20. As disclosed in the ’733 Patent, service control link 1653 is always shown to link the device to service controller 122. The specification says service controller 122 may “include[] one or more server functions,” and may be “implemented on multiple servers… or… on a single server.” EX-1001, 16:13-26. A POSITA thus understood that one or more servers performing one or more server functions would meet the claimed “network system.”

[5] The term “network systemS” is used in a different context in column 135 (lines 29-53), where it does not appear to be describing “communication” “over a service control link.”

277. In Houghton-Ogawa, mobile terminal 404/803's modem enables it to communicate with push server 401/801 and application server 802. EX-1006, 23.





EX-1006, FIG. 4 (annotated, left); FIG. 8 (annotated, right)

278. A POSITA understood that push server 401/801 and application server 802 (outlined with dashed-lines above) are a "network system," because (1) the specification only ever describes a "service control link" as connecting a device to a "network" that comprises one or more servers performing one or more server functions and thus the claimed "network system" encompasses at least that, and (2) the push server and application server are servers performing server functions. EX-1001, 16:13-26, FIGs. 16-20; EX-1006, 16-17, 23 ("An IP or other API (application programming interface) ***connection between application server 802 and push server 801*** simplifies the work and cost of creating application server 802 by taking care of network details already established for the COMMAND PUSH procedure.");

id. ("a data connection between application server 802 and mobile application 805 is established with the aid of [the] data connection in Figure 4, arrow C between push server 401/801 and push client 405/804."); *id*., 20 ("At any time after a connection is established between the client 405 and the server 401, the client may push a message to the server or the server may send a push message to the client. This is illustrated by means of the arrow C in Figure 4. These messages through a previously established, connection-oriented protocol such as TCP/IP, SSL, HTTP or HTTPS arrive quite rapidly."); *see also* discussion *infra* regarding [1e].

279. Regarding "***service control link***," the '733 specification does not set forth any requirements but says it "can provide an efficient and flexible control plane communication link" used for "***controlling***" some aspect of a "service" (*e.g.*, "data traffic, application usage, communication with certain network end points"). EX-1001, 7:23-33, 19:67-20:4, 25:46-53, 37:36-61, 68:19-58.

280. Houghton-Ogawa's data connection C is a "service control link," because it facilitates communication of commands/information relating to control of a service on the mobile terminal, as discussed below. *See*, *e.g.*, EX-1006, 20, 23. In Houghton-Ogawa, "push client software 405" on mobile terminal 404/803 "attempts to log into the push server 401 ***over a data network 403, normally a wireless network capable of transmitting Internet Protocol (IP) packets***." EX-1006, 17. Arrow B illustrates a login attempt." *Id*. After a connection is established between

client and server, "the client may push a message to the server or the server may send a push message to the client" through data connection C shown in Figure 4. EX-1006, 20.

281. Messages pushed from push server 401/801 to mobile terminal 404/803 over data connection C ***control*** the target application on the mobile terminal, e.g., by causing the application to start, changing operating state. For example, Houghton says the push server "push[es] messages to [the] mobile terminal located in the wireless network and thereby ***cause[s] programs to start to a specified operating state or, if already started, change operating state to the state indicated by the message*** thereby presenting a new application view to the user of the mobile terminal." *Id*.; EX-1006, 11. "***[T]he push messages may include, for example, a message stimulating, triggering or commanding the launch, display or shift to foreground of a user interface*** feature of the terminal such as an application…." EX-1006, 11, 29 (the push server sends "installation, updates, commands or data messages" to a push application); *see also* discussion *infra* regarding [1a2] (showing that data connection C, the claimed "service control link," supports "control plane communications").

282. Element [1a] also requires that the "service control link" be "***provided by the network system***." The '733 specification never describes how a "network system" "provide[s]" a "service control link." During prosecution, the examiner

rejected this limitation under §112 as indefinite. *See* EX-1002, 99-100. In response, Applicant argued this limitation "is supported at least by FIG. 16[,] illustrating service control link 1653 communicatively coupling service processor 115 and service controller 122," and the disclosures that "service controller 122…provides for network side of [the] communications with device 100." EX-1002, 76.

283. Based on Applicant's argument, a POSITA would have understood that Houghton-Ogawa's "service control link" (data connection C) "is provided by the network system" because (1) data connection C communicatively couples the push server and push client together, such that the push server uses transport functionalities associated with data connection C for communications transmitted to or received from push client 405, and (2) before the Critical Date, it was well-known for SSL-based communications between a mobile terminal and a server to be implemented such that both entities participate in maintaining the connection between them after being initiated by the mobile terminal. EX-1006, 18 (indicating that arrow C is established based on a "connection-oriented protocol such as TCP/IP, SSL, HTTP or HTTPS"), 20 ("At any time after a connection is established between the client 405 and the server 401, the client may push a message to the server or the server may send a push message to the client [through] arrow C").

284. Indeed, before the Critical Date, it was well known for TLS/SSL-based communications between a mobile terminal and a server to be initiated by the mobile

terminal. *See, e.g.*, EX-1011, 29:31-30:24 (describing that TLS requires a handshake phase and a data transfer phase, and in the handshake phase, the "client side initiates a TLS handshake by sending the server a ClientHello message"). It would have been obvious that the push server, as the other side of the communication would also be involved in providing the communication link because otherwise the link would be open ended and not linking two network entities.

[1a1] the service control link secured by an encryption protocol
[30a1] the service control link secured by an encryption protocol,

285. The '733 specification says that encryption protocols that may be used to secure its communication links include use of Transport Layer Security (TLS) running over Transport Control Protocol (TCP). EX-1001, 17:2-26, 87:62-88:79, 98:42-44; 99:26-29; 101:65-67. The specification uses TLS and Secure Socket Layer (SSL) interchangeably. *See, e.g.*, EX-1001, 98:42-44; 99:26-29; 101:65-67.

286. In Houghton-Ogawa, SSL is used to secure data connection C which facilitates communications between push server 401 and push client 405. *Supra* §§ IX.B.1, IX.B.2(b), IX.B.2(e); EX-1006, 20 (disclosing that communication link C between push client 405 and push server 401 is a "connection-oriented protocol such as TCP/IP, SSL, HTTP or HTTPS."), 18 ("Differences in wireless network terminal characteristics, individual push server availability and accessibility,…connection level stateful (such as TCP) and stateless (such as UDP) transport protocol availability (such as IP4, IP6, SSL, HTTP, HTTPS) and alternate

mobile terminal network settings mean that a sequence of connection establishment attempts and connection maintaining steps may required to be made using variations in relevant network parameters."). SSL and its successor TLS were well-known encryption protocols for providing secure communications between entities on a network. *See e.g.* , EX-1013, p. 3 ("Cryptographic security[:] SSL should be used to establish a secure connection between two parties."); EX-1005, 3:61-4:7 ("in network communications utilizing a conventional TCP/IP (Transmission Control Protocol/Internet Protocol) or UDP (User Datagram Protocol), ***encryption communication, such as*** IPsec (Internet Protocol Security) or ***SSL (Secure Socket Layer), is utilized to prevent some security risks presented during the exchange of data between network terminals***."); EX-1010, 1:38-42 ("A variety of ***cryptographic techniques*** are known for securing transactions in data networks. ***For example, the Secure Socket layer (SSL) protocol and its successor Transport Layer Security (TLS) provides a mechanism for securely sending data between a server and a client***."). Thus, in view of Houghton's disclosures of using SSL (and its associated encryption protocols) for the communication link between the mobile terminal and the push server, a POSITA would have understood or found obvious that Houghton's communication path C between these entities ***is secured by an encryption protocol***.

[1a2] [the service control link is] configured to support control-plane communications between the network system and a service control device link agent on the end-user device;
[30a2] the service control link supporting control-plane communications between a service control device link agent on the end-user device and the network element;

287. Element [1a2] requires that the service control link be "configured to support control plane communications between the network system and a service control device link agent on the end-user device." Element [30a2] recites that the service control link "support[s] control-plane communications" between the "service control device link agent" and a "***network element***."

288. The same "network element" recited in [30a2] is recited in [30c] and [30d1]. The '733 Patent broadly uses "network element" to mean any element that is part of a network, *e.g.*, a server. EX-1001, 23:46-54, FIGs. 1-8. A POSITA would have understood that Houghton-Ogawa's push server 401/801—which is a server in claim 1's "network system" (as discussed for [1a])—is also a "network element" as that term is used in the '733 Patent.

289. As discussed for [1a], Houghton-Ogawa's data connection C (the claimed "service control link") is how push server 401/801 (which is part of the claimed "network system" in [1a2] and is the "network element" in [30a2]) communicates with push client 405/804 on Houghton-Ogawa's mobile terminal 404/803 (the recited "end-user device").

290. A POSITA would have understood that Houghton-Ogawa's data connection C (the secure control link) is "configured to support control-plane communications" as claimed. The '733 Patent says a "control plane communication link" manages "aspects of device based network service policy implementation," including "policy settings for the device for network services, …such as access control settings, … user notification settings, user privacy settings, user preference settings, [etc.]" EX-1001, 8:60-9:15, 9:23-24. A POSITA understood control-plane communications to encompass communications "across a network" that "involv[e] supervision" of "device-based" "control" of "service[s]" delivered to a device, for example by "communicating…, controlling, monitoring, or verifying service policy." *Id*., 37:36-43, 68:19-28.

291. As discussed for [1a], Houghton discloses that communications between the push server and push client over data connection C include control information related to particular services. For example, data connection C facilitates transmission of messages (originating, *e.g.,* from a separate application server) that "cause programs to start to a specified operating state," "change operating state," or "trigger[] or command[] the launch, display or shift to foreground of a user interface." EX-1006, 11; *see also id.*, 14 ("In some cases a separate server such as a telecommunication service server, gaming environment server, and original equipment manufacturer device or business information system may notify the

[push] server directly of events or messages to be sent using an external application programming interface (API). Such a device connected by external API may also receive information including the results and responses of messages which the user has replied to by terminal software or web page interaction."), 21-22 ("The potential applications of the COMMAND PUSH include but are not limited to mobile applications for enterprise connectivity, back office integration, database access, scientific and industrial process and equipment monitoring and control, pictures transfer, mobile gaming, application data transfer, mobile electronic commerce, application alarms, reminders, multimedia interactivity, corporate calendaring, personal messaging and group messaging, etc."), 29 (claim 1: the push server sends "installation, updates, commands, or data messages" to a push application).

292. Houghton also discloses tailoring what service-related control information is sent based on the device that the server's push message is being sent to. Like the '733 Patent (EX-1001, 8:60-9:15), Houghton describes accounting for, e.g., "user preferences," "network connection preferences," and "security certificates" (i.e., authentication settings and admission control settings)—that a POSITA understood are specific to a device. EX-1006, 14, 21-22 (explaining that application servers may use the push server "to push an application command message to the push client," as discussed *supra* § IX.B.1, and that: "[t]he push server 701 may in combination with ***user preferences*** stored in either the push server 701

or push client 704… request the push client 704 to ***display or otherwise as appropriate for the mobile terminal***… ***notify the user*** asking permission for launching mobile application 705 prior to application launch. The preferred embodiment is for the behavior, language and content of this information to be configured on the server 701 ***based on the service and preferences of the individual receiving the message***... The server 701 may thus specify the ***network connection preferences, notification sounds, and other behavior of the client 704***. These changes facilitate the efficient and manageable operation of the entire system and can be used for automated remote maintenance of push client 704, mobile applications as 705, and configurable aspects of underlying mobile terminal 703, for example, ***changing the username, password, and security certificates*** stored in the mobile terminal."), 29.

293. Houghton also discloses that actions taken by mobile terminal 404/803 upon receiving such push messages are "***specified in the command C from the server 401***," and determined based on "***user preferences***." EX-1006, 21. For example, the push message may include "information ***specifying how upon receiving such a message the client 405 will notify*** and optionally ask the user if the action should be performed may optionally be included," which causes the push client in the mobile terminal to execute "appropriate automated actions and user interface media capabilities… ***as specified in the command C from the server 401***,"

e.g., "optionally proceed[ing] without audio, with network downloaded audio, or without first requesting confirmation from the user ***as specified by user preferences*** [on the device] and command details." EX-1006, 21. Thus, messages from Houghton's push server are used for device-based control of services delivered to the device in Houghton-Ogawa, and a POSITA understood Houghton-Ogawa's data connection C is "configured to support control plane communications" as claimed.

294. A POSITA would likewise have understood these communications are "between" the Houghton-Ogawa's push server (which is part of the claimed "network system" from element [1a] and is the network element in [30a2]) and "a ***service control device link agent*** on the end-user device," as claimed.

295. The '733 specification does not describe any "service control device link agent." It describes a "service control device ***link*** 1691," saying it is a "device side" component that may "provide an efficient and secure solution for transmitting and receiving service policy implementation, control, monitoring and verification information with other network elements." EX-1001, 37:43-62. And it uses the term "agent" to refer to any component—which may be "implemented entirely in software"—that performs some function (e.g., transmitting information for, *e.g.*, "control plane communication"). *Id.*, 15:58-16:2, 42:51-52, claim 26. The specification ***does not*** set forth any required function. Moreover, by the Critical Date, it was well-known that an agent performed function(s) on behalf of an entity

(e.g., a user, client, server, etc.). (citing EX-1029, 12). EX-1001, 16:2-12. This use of "agent" is consistent with Patent Owner's interpretation in litigation. EX-1021, 13-23 and 62 (where "agents" in recited in claim 1 is mapped to "client app[s]" on an alleged device); EX-1038, 17.

296. Houghton-Ogawa's push client 405/804 is "implemented in the form of a software run in a processor of the mobile terminal 404." EX-1006, 16. As discussed above, it facilitates communications with the push server using data connection C, and is used for transmission, controlling, and execution of a service on the device on behalf of the server. EX-1006, 21, FIG. 4. Houghton-Ogawa's push client 405/804 is thus a "service control device link agent," as claimed.

[1b] [the end-user device comprising:] a plurality of device agents communicatively coupled to the service control device link agent through an agent communication bus, each of the plurality of device agents identifiable by an associated device agent identifier; and
[30b] each of the plurality of device agents identifiable by an associated device agent identifier and communicatively coupled to the service control device link agent through an agent communication bus,

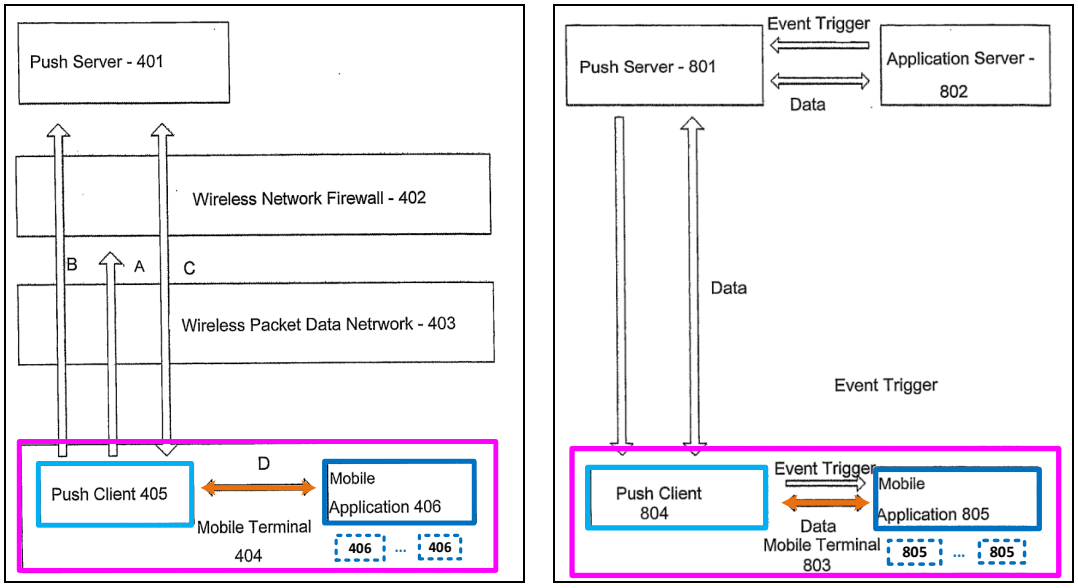
297. As discussed for [1a2], the '733 Patent uses the term "agent" to include a "component" implemented "entirely in software" that performs some function (e.g., transmitting information) on behalf of a client or server. EX-1001, 15:58-16:2, 42:51-52; EX-1029, 12; EX-1021, pp. 13, 14, 62; EX-1038, 17. A "***device*** agent" is an agent on a device.

298. In Houghton-Ogawa, push client 405/804 is communicatively coupled to multiple mobile applications 406/805. EX-1006, 21. Houghton discloses various examples of such applications, including, *e.g.*, "video game" and "messaging" applications described further below in the context of claims 15 and 20.

299. Push client 405/804 forwards a push message to the appropriate application (from among the multiple mobile applications) specified in the message. A push message includes "information ***specifying which mobile application 406 from a plurality of such applications*** may optionally be included [in the push message]." EX-1006, 21. "Upon receiving such a message, appropriate automated actions and user interface media capabilities of the mobile terminal as specified in the command C from the server 401 are executed ***by the push client 405***." *Id*. Thus, Houghton-Ogawa's mobile applications may be "***direct[ed]***" by a push server (using a push message) to perform functions related to the service, including "use of additional network resources either on the push server or other server" and "application data transfer." EX-1006, 21. Because the multiple mobile applications on the mobile terminal are implemented in software and each performs functions directed by and thus on behalf of, *e.g.*, an application server providing the user a service, a POSITA would have understood these mobile applications to be "a plurality of device agents," as claimed.

300. A POSITA would have likewise understood that push client 405/804 is communicatively coupled to these device agents "through an agent communication bus," as claimed.

301. In particular, Houghton discloses that push client 405/804 may "pass… command details" to specific mobile applications, and "may in turn at any time accept data D from each of a plurality of mobile applications 406." EX-1006, 21, FIG. 4.



EX-1006, Figure 4 (annotated, left); Figure 8 (annotated, right)

302. The arrows from Houghton Figures 4 and 8 above (highlighted orange) represent data communications in the mobile terminal between push client 405/804 and mobile applications 406/805. A POSITA would have understood that such communications would be "through an agent communication bus" as that term is used in the '733 patent. Per the '733 Patent, the "agent communication bus" can be

a communication link that facilitates communications with the device agents. EX-1001, 42:48-58; EX-1038, 24. Similarly, a POSITA would have found obvious that there would need to be a communication bus/link between push client and the applications to facilitate communications ("D") of the application-specific messages between the push client and the destination applications.

303. Alternatively, a POSITA would have had reason to implement the communication link between Houghton's push client and mobile applications in Houghton-Ogawa as a bus. Before the Critical Date, it was well-known to use a communication bus (*e.g.*, a "D-bus") to facilitate communications ("D") of the application-specific messages between the push client and the destination applications, as Houghton describes. *See, e.g.*, EX-1031, 10:56-62 ("Bus may be an example of a device inter-process communication channel used to send information between applications. As such, method calls made over the D-Bus may be serialized as a message addressed to a particular application. The particular application may then listen and perform the service requested and place an output back on the D-Bus addressed to the browser application."); EX-1008, ¶28, FIG. 4. Using such a bus in Houghton's mobile terminal would have been a conventional, obvious way to implement what Houghton describes, and is nothing more than utilizing familiar, known components (a bus) to achieve a predictable result of facilitating Houghton's push client and mobile applications to interface with one another. A POSITA would

have reasonably expected success doing so. Houghton-Ogawa's end-user device (mobile terminal 404/803) thus has "a plurality of device agents communicatively coupled to the service control device link agent through an agent communication bus," as claimed.

304. Each of Houghton-Ogawa's "device agents" is also "identifiable by" an "associated device agent identifier," as claimed.

305. The '733 specification does not describe any requirements for the claimed "associated device agent identifier." In Houghton-Ogawa, push messages are routed by the push client to specific mobile applications using "binary or text information" included in the message that "specif[ies] which mobile application 406 from a plurality of such applications" is the target of the push message. EX-1006, 21. A POSITA would have understood that the "information specifying which mobile application 406" to send messages to, as Houghton teaches, meant that each of Houghton-Ogawa's "device agents" was "identifiable by" an "associated device agent identifier," as claimed.

306. Alternatively, implementing Houghton's information specifying a particular application to be in the form of an "identifier" would have been a conventional and obvious way to implement what Houghton describes (EX-1006, 21), and is nothing more than utilizing a known technique (use of application identifier) to a known system (a push-based server-client system of Houghton) to

achieve a predictable result of accurately routing messages to applications based on their identifiers, as suggested by Houghton and as was well-known in the art before the Critical Date. For example, in the relevant context of push communications and associated environments, Lee discloses that the push message includes an "app_ID" that specifies a target application on the mobile terminal that is targeted as a destination for the push message. EX-1008, ¶22. A POSITA would have reasonably expected success doing so.

[1c] [the end-user device comprising:] memory configured to store an encryption key,

307. Per the '733 Patent, the "encryption key" recited in features [1c], [1c1], and [1d2] is used for encryption/decode functions that are applied in addition to the "encryption protocol" applied on the link, as recited in feature [1a1]. For example, the '733 Patent specifies that "[v]arious embodiments include ***two or three layers of encryption*** in the service control link, ***with one embodiment or layer*** being implemented in the ***encrypt functions (2408, 2428) and decode functions (2412, 2422), and another embodiment or layer implemented in the transport services stack (2410, 2420)***." EX-1001, 87:57-63. "For example, various known security encryption techniques can be implemented in ***the encrypt functions (2408, 2428), with*** public/private or ***completely private keys*** and/or signatures so that very strong levels of security for service processor control plane traffic can be achieved even

through the basic transport services (2410, 2420) implemented with standard secure or open Internet networking protocols, such as TLS or TCP." *Id*., 87:67-88:7.

308. Consistent with this disclosure, Houghton-Ogawa's mobile terminal includes memory that stores Ogawa's shared encryption key, which as discussed *supra* § IX.B.2(d) is used to secure Houghton-Ogawa's data connection C with a second layer of encryption beyond the SSL protocol. Houghton-Ogawa's end-user device thus includes "a memory configured to store an encryption key," as claimed. *See* EX-1006, 29 ("the push client, in response to receiving a push message…, forwards such application commands or data or ***stores*** such application installation or updates ***within the mobile terminal***"), *id.*, 22 ("user preferences [are] ***stored in*** either the push server 701 or push client 704."), *id*. ("the client 704 is also capable of receiving and ***storing*** variables which configure behavior of the client 704. The server 701 may thus specify the network connection preferences, notification sounds, and other behavior of the client 704. These changes…can be used for automated remote maintenance of push client 704, mobile applications as 705, and configurable aspects of underlying mobile terminal 703, for example changing the username, password, and security certificates ***stored in the mobile terminal***.").

309. Additionally, under Patent Owner's claim interpretation in litigation, the "encryption key" limitations recited in [1c], [1c1]/[30c], and [1d2]/[30d2] may be ***part of*** the "encryption protocol" that secures limitation [1a1]'s service control

link. EX-1021, pp. 3-13 and 24-34 (using the same features of the "security protocols" used in the targeted product to allege infringement of "encryption protocol" in [1a1] and "encryption key" in [1c]); EX-1038, 8, 29. In other words, Patent Owner asserts the "encryption key" limitation is satisfied by systems where encryption is performed using SSL (or similar) "encryption protocol" without an additional layer of encryption. *Id.* Even if the claims were interpreted in this manner, Houghton-Ogawa separately meets the claims under this interpretation.

310. To the extent the limitations recited in [1c], [1c1]/[30c], and [1d2]/[30d2] are interpreted to encompass encryption performed ***as part of*** a SSL-enabled encryption protocol that also meets limitation [1a1] (*i.e.*, single-layer encryption), Houghton-Ogawa's memory meets [1c] under this interpretation, because Houghton-Ogawa's data connection C is secured using SSL. *Supra* §§ IX.B.2(b); IX.B.2(e).

311. As noted for [1a1], SSL is used to secure Houghton-Ogawa's data connection C between the push server 401 and push client 405. EX-1006, 20. While Houghton does not describe the details of how SSL (or any other connection-oriented protocol, *e.g.*, TLS) is implemented, such details were well-known to a POSITA before the Critical Date. *See e.g.*, EX-1013, p. 3, EX-1014, p. 3. For example, it was well-known that SSL (and TLS) use ***symmetric*** encryption that involves using the ***same*** key at the source and destination of a message for

encryption and decryption. For example, Lu corroborates that, in TLS/SSL, the client and server generate and exchange keys that are used to encrypt/decrypt communications transmitted over a network channel. EX-1026, 29:31-30:24. A POSITA likewise understood that such keys were conventionally stored (at least temporarily) in the respective memories of the encrypting and decrypting entities. Thus, under Patent Owner's interpretation of the claims—which reads the claims onto systems that ***only*** secure client-server communication channels based on the symmetric encryption used in SSL/TLS—Houghton-Ogawa, which uses SSL (*supra* §§ IX.B.1, IX.B.2(b), IX.B.2(e)), includes "memory configured to store an encryption key," as required by limitation [1c] (under Patent Owner's interpretation).

[1c1] the encryption key shared between the service control device link agent and a service control server link element of the network system; [30c] …an encryption key shared between the service control device link agent and the network element…

312. Element [1c1] requires that the encryption key be "shared between the service control device link agent"—Houghton-Ogawa's push client 405/804, as discussed for [1a2]—"and a service control server link element of the network system." Element [30c] recites that the encryption key be "shared between the service control device link agent" and "the network element" (which is mapped to Houghton-Ogawa's push server, as discussed above in the context of [30a2]).

313. While the ’733 specification never describes element [1c1]’s “service control server link element of the network system,” it refers to a “service control server ***link*** 1638,” and says it is a “network side” component that may “provide[] an efficient and secure mechanism for transmitting and receiving service policy implementation, control, monitoring and verification information between the device agents (e.g., service processor agents/components) and other network elements (e.g., service controller agents/components).” EX-1001, 68:19-40.

314. As discussed for [1a], push server 401/801 is part of Houghton-Ogawa’s “network system.” A POSITA would have understood that Houghton-Ogawa’s push server “provides a mechanism for transmitting and receiving” “service policy… information” between “device agents” and other “network elements,” because: (1) Houghton discloses data connections between push server 401/801, push client 405/804 on mobile terminal 404/805, and application server 802 (EX-1006, FIGs. 4 and 8), (2) Houghton expressly describes using those data connections to “establish[]” “a data connection” “between” the “application server” and “mobile application” (*id.*, 23), (3) Houghton expressly describes “redirection” of data received from the mobile applications on the mobile terminal “***to other servers***” via the push server (*id.*, 21), and (4) as discussed above for [1a2] and below for [1e], Houghton’s connections are used for control-plane communications between Houghton-Ogawa’s application servers and mobile applications. EX-1006,

21-22. A POSITA would thus have understood that Houghton-Ogawa's push server—which can communicate with the Houghton-Ogawa mobile terminal's push client over data connection C—was a "service control server link element of the network system," as recited in [1c1].

315. In Houghton-Ogawa, Ogawa's encryption key is stored on the mobile terminal to enable the push client to decrypt data received from the push server on which the same encryption key is also stored. *Supra* § IX.B.2.(d); EX-1005, 5:59-65, 6:64-7:21, 9:16-34. As discussed *supra* § IX.B.2(d), before the Critical Date, this was well-known for symmetric encryption. *See* EX-1009, 8:3-5 ("Symmetric ciphering/enciphering may use one or multiple keys for both encryption and decryption"); EX-1013, 3.

316. A POSITA would have understood that the same key stored at both Houghton-Ogawa's mobile terminal and push server for Houghton-Ogawa Message Encryption—which is used by both Houghton-Ogawa's push client (the claimed "service control device link agent, as discussed for [1a2]) and push server (the claimed "service control server link element of the network system," as discussed for [1c1], and also the "network element" for [30c]) for encryption/decryption—was "***shared between***" those two claimed components, as required.

317. A POSITA would also have understood that under Patent Owner's interpretation of the claims—which covers systems that only secure client-server

communications using the single layer of symmetric encryption used in SSL/TLS—the key for Houghton-Ogawa's symmetric SSL/TLS encryption (*supra* §§ IX.B.1, IX.B.2(b), IX.B.3.(e)), by being stored temporarily at both the mobile terminal (with the push client) and the push server, was likewise "shared between" the push client and push server (under Patent Owner's interpretation).

[1d1] wherein the service control device link agent is configured to: receive, over the service control link, an encrypted agent message from the service control server link element,
[30d1] receiving, over a service control link, an encrypted agent message from a network element,

318. Element [1d1] requires the "service control device link agent" to be "configured to: receive, over the service control link, an encrypted agent message from the service control server link element." Element [30d1] recites "receiving" an encrypted agent message from claim 30's "network element."

319. In Houghton-Ogawa, push client 405/804 (the claimed "***service control device link agent***," as discussed for [1a2]) is configured to receive, over data connection C (the claimed "***service control link***," as discussed for [1a]), encrypted messages from the push server (the claimed "***service control server link element***" in claim 1, as discussed for [1c1], and "***network element***" in claim 30, as discussed for [30a2]). Such messages may come from application servers that are pushed to the push client via the push server, as discussed for [1a2]/[30a2]. *See also supra* § IX.B.1.

320. The ’733 specification never uses the term “encrypted agent message.” Based on the plain language of the claims, a POSITA would have understood the term to encompass an encrypted message sent to an agent. In Houghton-Ogawa, messages are encrypted both using Houghton-Ogawa Message Encryption and an SSL encryption protocol before they are transmitted to the push client. *Supra* §§ IX.B.2(b), IX.B.2(e).

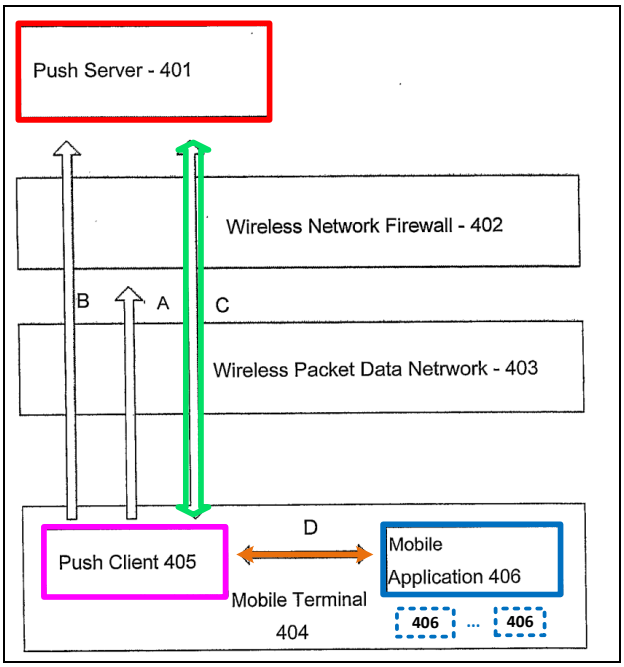
321. First, because the messages are encrypted using Houghton-Ogawa Message Encryption, a POSITA would have understood that, in Houghton-Ogawa, the service control device link agent is “configured to” “receive, over the service control link, an encrypted agent message from the service control server link element,” as claimed in claim 1 and that the message is received “from a network element,” as claimed in claim 30.

322. Additionally and alternatively, under Patent Owner’s interpretation of the claims—which covers systems with only the single layer of symmetric encryption used in SSL/TLS—Houghton-Ogawa’s symmetric SSL encryption (*supra* §§ IX.B.1, IX.B.2(b), IX.B.2(e)) alone also meets limitations [1d1] and [30d1], because SSL is a protocol for encrypting messages sent over the data connection to Houghton-Ogawa’s push client.

[1d2] [wherein the service control device link agent is configured to:] using the encryption key, obtain a decrypted agent message, [30d2] using [the] encryption key shared between the service control device link agent and the network element, obtaining a decrypted agent message

323. The claims require the service control device link agent to (or be configured to) "us[e]" the "encryption key" to "obtain[]" a "decrypted agent message." The '733 specification never uses the term "decrypted agent message." Based on the plain language of the claims, a POSITA would have understood the term to encompass a message sent to an agent that has been decrypted.

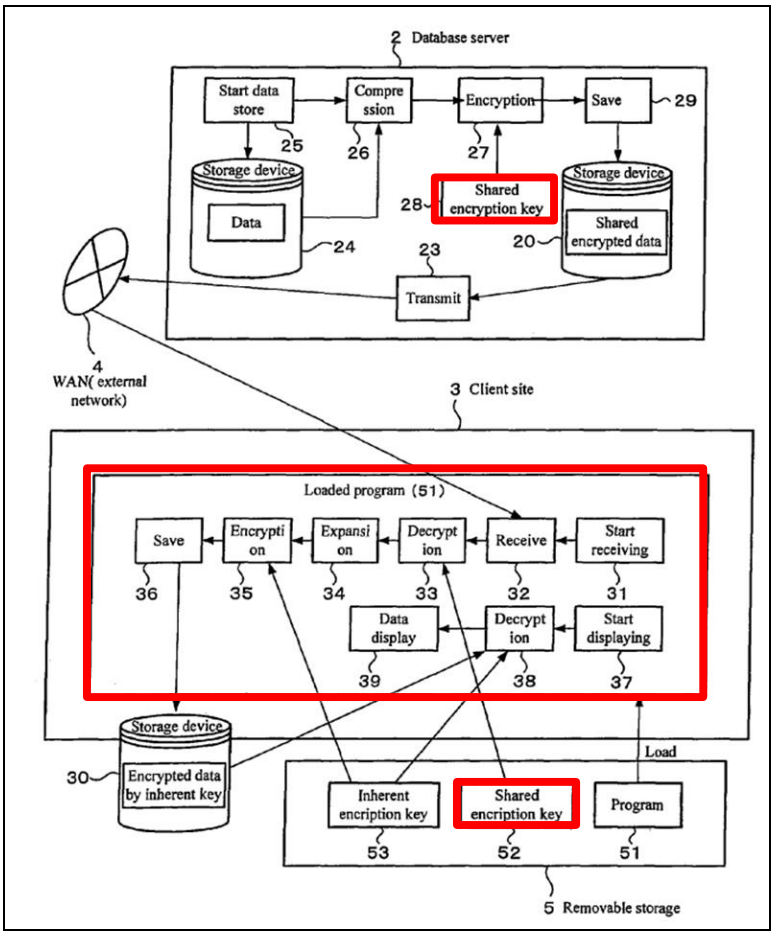
324. Houghton says that "[u]pon receiving… a message, ***appropriate automated actions*** and user interface media capabilities of the mobile terminal ***as specified in the command C*** from the server 401 ***are executed by the push client 405***," *e.g.*, "asking the user if the mobile application should be launched," "passing the command details (arrow D) to the specified mobile application, module or additional feature within the same application suite," "launching the application, module or feature," etc. EX-1006, 21.



EX-1006, FIG. 4 (annotated)

325. In Houghton-Ogawa, encrypted messages (e.g., received from the application server via the push server) are decrypted at the push client, which is implemented to use Ogawa's decrypt unit and shared encryption key to decrypt messages that were encrypted using Houghton-Ogawa Message Encryption. *Supra* §§ IX.B.2(b), IX.B.2. A POSITA understood that the push client decrypts the message ***before*** executing the actions specified by the message in order to process the message and determine what actions need to be taken. *See* EX-1006, 34 (claim 33: "***[T]he push client*** and push server establish a secure connection and ***unwrap such security*** on behalf of the mobile application"). Ogawa discloses that the message decryption at the client site is performed using the key shared between the client site and the sender of the message, e.g., server 2. *See* discussion re [1c1]

supra. More specifically, "at the client site 3, ***the shared key encrypted data will be received*** by the receive unit 32 ***from the database server 2*** via network 4." EX-1005, 5:59-67. "This received shared key encrypted data will be ***decrypted using the shared encryption key 52*** which was supplied to decryption unit 33 and beforehand stored on the removable storage 5." *Id*.; *see also id*., 6:64-7:21 (providing an example process for exchanging the shared key between the client site and a message sender (e.g., input site 1)). A POSITA would have understood that, in Houghton-Ogawa, the service control device link agent is thus configured to "us[e] the encryption key" of Ogawa to "obtain a decrypted agent message," as claimed.



EX-1005, FIG. 7 (annotated)

326. Additionally and alternatively, under Patent Owner's interpretation of the claims—which covers systems with only a single layer of symmetric encryption used in SSL/TLS—Houghton-Ogawa's symmetric SSL encryption (*supra* §§ IX.B.1, IX.B.2(b), IX.B.2(e)) alone also meets limitations [1d2] and [30d2], because messages encrypted using SSL must be decrypted using the same encryption key used to encrypt the message, and the result is a message for the agent that has been decrypted, *i.e.*, "a decrypted agent message" (under Patent Owner's interpretation). *See* EX-1009, 6:59-7:17, 7:34-40, 8:1-5 (corroborating using of symmetric

cryptography to decrypt the received encrypted messages, e.g., software/firmware updates to update the software/firmware on mobile handset 207).

[1d3] the decrypted agent message comprising a particular agent identifier and message content for delivery to a particular device agent of the plurality of device agents, the particular agent identifier identifying the particular device agent,

[30d3] the decrypted agent message comprising a particular agent identifier and message content for delivery to a particular device agent of a plurality of device agents on the end-user device, … [30d4] the particular agent identifier identifying the particular device agent,

327. The claims require that the "decrypted agent message" include "a particular agent identifier and message content for delivery to a particular device agent of" the "plurality of device agents," where "the particular agent identifier identifies the particular device agent."

328. In Houghton-Ogawa, the push client (the claimed "***service control device link agent***," discussed in the context of [1a2]) receives encrypted ***messages*** from the push server (as discussed in the context of [1d1]). As discussed in the context of [1d2], the push client decrypts those messages to obtain "decrypted agent message[s]," as claimed. The push client then uses the information included in the message, including "information specifying which mobile application 406 from a plurality of such applications" (the claimed "***plurality of device agents***," as discussed in the context of [1b]) the message is directed to, in order to push the message to the appropriate mobile application. EX-1006, 21.

329. As discussed in the context of [1b], a POSITA would have understood that Houghton-Ogawa's "information specifying which mobile application" to route the message to is, or would have been obvious to implement as, an "associated device agent identifier." A POSITA would have likewise understood that this information is also a "particular agent identifier" in Houghton-Ogawa's "decrypted message" that "identifies the particular device agent" to which the message should be delivered, as claimed.

330. Houghton-Ogawa's message also includes "binary or text information to be passed to the… specified mobile application," which, as further explained for [1e] *infra*, a POSITA would have understood (based on Houghton's teachings) to constitute message content and commands that are used by the application to execute and display content. EX-1006, 21; *see also* EX-1006, 8 (indicating that "rout[ing] commands or application-specific data to the mobile application" was conventional). While the '733 specification never uses the term "message content," a POSITA would have understood that the above-described "binary or text information," "commands," and "application-specific data" in the message is "content" in the message, and thus is "message content" that will likewise be delivered.

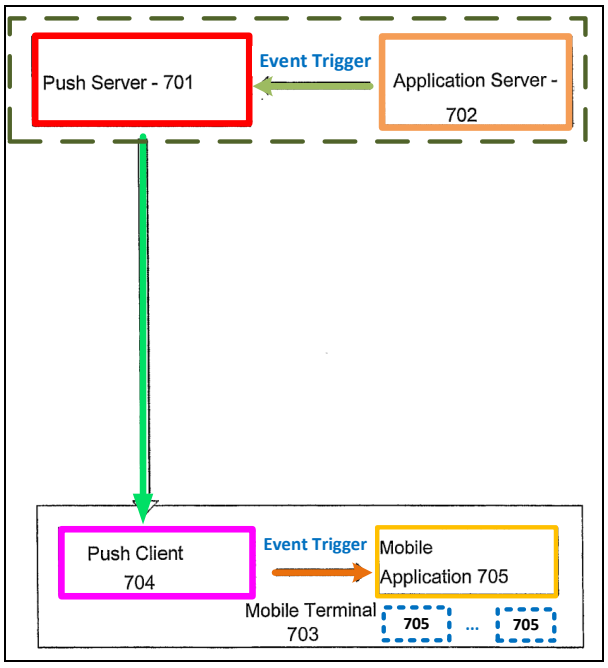
[1e] the message content [being] from a particular server of a plurality of servers communicatively coupled to the service control server link element, and [30e] the message content [being] from a particular server of a plurality of servers communicatively coupled to the network element; and

331. Element [1e] requires the "message content" to be "from a particular server of a plurality of servers communicatively coupled to the service control server link element." Element [30d1] recites that the "plurality of servers" be "communicatively coupled to" claim 30's "***network element***."

332. Houghton-Ogawa's push server is the claimed "service control server link element" in claim 1 (as discussed for [1c1]), and the claimed "network element" in claim 30 (as discussed for [30a2]). The "binary or text information," "commands," and "application-specific data" in Houghton-Ogawa's received message is "message content" as discussed in the context of [1d3].

333. Houghton discloses an ***application server*** (communicatively coupled to the push server) sending message content that triggers the push server to push the message to the push client on the mobile terminal, and ultimately to a mobile application that is also on the mobile terminal. "Figure 7 illustrates an example of an 'COMMAND PUSH' procedure" that a POSITA understood to be implemented in Houghton's Figure 4 system "wherein [Houghton's] ***push server***... is ***triggered by a trigger event*** as for example ***from an application server***… to push an application command message to the push client… and thereby initiate a mobile

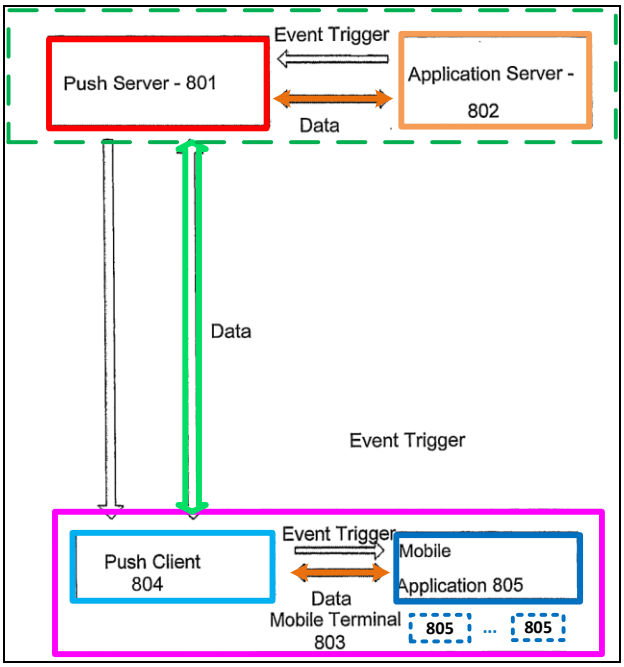
terminal client trigger event in a mobile application… from a plurality of such applications… on the terminal…" EX-1006, 21-22; *see also id.*, 23 (explaining that Figure 7 is an example of the embodiments shown in Figures 4 and 8). "***The trigger [event]*** mechanism ***may be***… an IP-triggered ***application launch and data transfer*** as in the case of mobile application launched by contact to a specified IP port." *Id.* "***The trigger event*** from [the] push client… to [the] mobile application… may optionally ***include commands*** or data affecting the aspect of visual presentation of mobile application…" *Id.* Figure 7, annotated below, shows that push client 704 delivers to mobile application 705 data of trigger event included in the message that the push server 701 received from application server 702.



EX-1006, Figure 7 (annotated)

334. A POSITA would have understood that "event trigger" messages sent from the application server to the push client includes content, *e.g.*, a command to launch or use particular mobile applications such as a display or audio application, that constituted "message content," as claimed.

335. A POSITA would also have understood that Houghton discloses message content being sent from the application server to a mobile application through the "data connection" between the two. *See* EX-1006, 9 ("Once such an IP connection is established between the server and one or more mobile terminals, the connection can be used to transfer messages to the mobile terminal, [e.g.,] … event trigger messages to launch or command a mobile application."). Houghton emphasizes that the connection between the application server and the application on the mobile terminal is a "data connection" for transmitting data. "Figure 8 illustrates an extension of the procedure in Figure 7,… with the additional step that a ***data connection between application server 802 and mobile application 805*** is established with the aid of the persistent managed, tested and configured data connection in Figure 4, arrow C between push server 401/801 and push client 405/804." EX-1006, 23. "***An IP*** or other API (application programming interface) ***connection between application server 802 and push server 801*** simplifies the work and cost of creating application server 802 by taking care of network details already established for the COMMAND PUSH procedure." *Id*.



EX-1006, Figure 8 (annotated)

336. Finally, a POSITA would have understood Houghton to expressly disclose that the illustrated application server is one of multiple servers in communication with the push server. EX-1006, 22 ("The push client… may in turn at any time accept data D from each of a plurality of mobile applications 406 and direct such to the push server 401, possibly for redirection ***through push server API to other servers***, mobile terminals, push clients and computing devices.").

337. Moreover, in view of Houghton's express disclosure of examples of different application servers—e.g., a telecommunication service server, gaming environment server—a POSITA would have understood Houghton to include multiple application servers, *e.g.*, with each application server providing a particular service and a particular application or applications on the mobile device, and sending

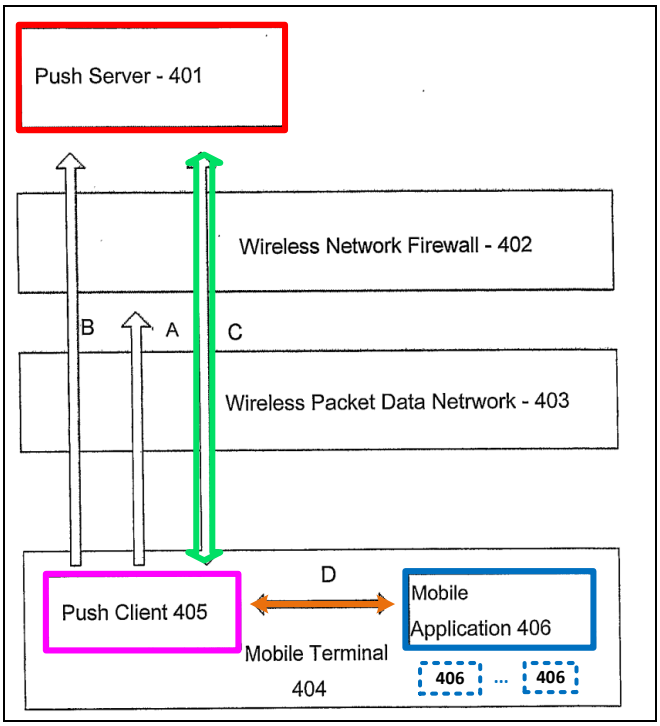
messages or event triggers corresponding to that particular service. For example, in Houghton, "a separate server such as a telecommunication service server, gaming environment server, and original equipment manufacturer device or business information system may notify the [push] server directly of events or messages to be sent". EX-1006, 14. Alternatively, such an implementation would have been a conventional and obvious way to implement what Houghton describes, and is nothing more than utilizing familiar, known components (multiple individual application servers corresponding individual services associated with individual mobile applications) to achieve a predictable result of providing a variety of services to a user through applications on a mobile terminal. A POSITA would be motivated to use multiple servers for providing the individual services because by doing so, a vulnerability or population of one server would not affect other or all individual services.

[1f] [wherein the service control device link agent is configured to:] based on the particular agent identifier, deliver the message content to the particular device agent over the agent communication bus.
[30f] delivering the message content to the particular device agent over the agent communication bus based on the particular agent identifier.

338. The claims require that the "service control device link agent" be "configured to," "deliver[] the message content to the particular device agent over the agent communication bus" "based on the particular agent identifier."

339. Houghton-Ogawa's push client is a "service control device link agent" (as discussed in the context of [1a2]). As discussed for [1b] and [1d3], the push message received from Houghton-Ogawa's push server includes "information ***specifying which mobile application 406*** from a plurality of such applications" the content of the push message is "to be passed to." EX-1006, 21. "Upon receiving such a message, appropriate automated actions and user interface media capabilities of the mobile terminal as specified in the command C from the server 401 are ***executed by the push client 405***," for example "playing a sound, asking the user if the mobile application should be launched," or "***passing the command details (arrow D) to the specified mobile application***." *Id*. Indeed, delivering message content based on the application identifier that was included in the push message was conventional even before Houghton. *See e.g.*, EX-1006, 8, 22, and 5; *see also* EX-1008, ¶28 ("The integrated push service agent 250…selectively invokes the application 260 compliant to the associated *application ID app_ID of the push information push_info to deliver the push data*.").

340. A POSITA also understood that such communication would occur "through the agent communication bus" (discussed in the context of [1b]). Houghton-Ogawa thus meets this element.



EX-1006, FIG. 4 (annotated)

b) Claim 2

[2] The end-user device recited in claim 1, wherein the particular server comprises a service usage history server, a policy management server, an access control integrity server, a network traffic analysis server, a beta test server, a service download control server, a billing event server, an activation server, a transaction server, an authentication server, or a content management server.

341. Claim 2 recites a list of alternative servers that claim 1's "particular server" may comprise, including "a service download control server" and "a content management server."

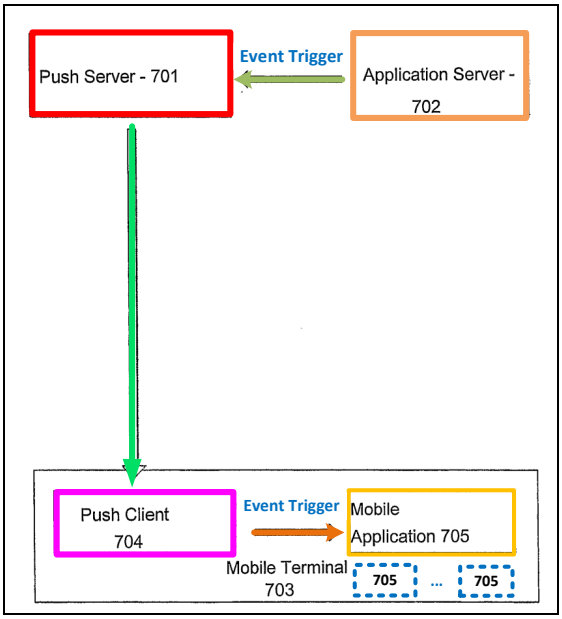
342. The '733 specification uses the term "service download control server" to encompass a server that "provides a download function to install and/or update

service software elements." EX-1001, 77:31-38. The '733 specification does not describe a "content management server," but a POSITA understood "content management" encompassed managing any aspect of delivery of data to an end-user. *Id.*, 16:53-54. A POSITA also understood that since the message includes the "content," management of the message delivery would be a form of "content management" as it would determine what happens to that content and where it ends up going.

343. Houghton teaches an application server triggering the pushing of "application installation, updates, commands, or data messages" in a message from the push server to the push client. EX-1006, 29. Thus, Houghton-Ogawa's application server comprises "***a server download control server***" by providing a download function to install and/or update service software elements, and "***a content management server***" because it manages or controls the delivery of data to the push client (and the mobile application). EX-1001, 77:31-38).

344. Houghton also says an application server can trigger the push server "to ***push an application command message*** to the push client." EX-1006, 21-22. "The ***trigger*** mechanism … may be an IP-triggered application launch and ***data transfer*** as in the case of mobile application launched by contact to a specified IP port." *Id.* The application server is "***a separate server*** such as a telecommunication service server, gaming environment server, and original equipment manufacturer device or

business information system may ***notify the [push] server directly of events or messages to be sent***." EX-1006, 14; *see also id*., 22 ("The ***trigger*** mechanism … may be an IP-triggered application launch and ***data transfer***). For this additional reason, Houghton-Ogawa's application server in Houghton-Ogawa comprises "***a content management server***," because it manages or controls the delivery of data to the push client (and the mobile application).



EX-1006, Figure 7 (annotated)

c) Claim 5

[5] The end-user device recited in claim 1, wherein the message content is based, at least in part, on a user preference.

345. Houghton says the push server may, based on "***user preferences*** stored in… the push server," "request the push client… to display or otherwise… notify the

user asking permission for launching [a] mobile application… prior to application launch." EX-1006, 22. Houghton also expressly discloses the "***behavior, language, and content***" of this user notification being "configured on" the push server "***based on*** the service and ***preferences of the individual*** receiving the message." *Id.*; *see also id*., 21 (the push message includes "***information*** specifying how upon receiving such a message the client 405 will notify and optionally ask the user if the action should be performed."). Thus, in Houghton-Ogawa, the message content sent from the push server—*e.g.*, in a message containing a specific notification for display to the user—is "based on" "user preference[s]," as claimed, *e.g.*, preferences regarding how the user likes to be notified.

d) Claim 7

[7] The end-user device recited in claim 1, wherein the message content comprises a service offer, an advertisement, or a transaction offer.

346. Claim 7 requires claim 1's "message content" to "comprise[]" one of various alternatives, including "a service offer" or "an advertisement."

347. The '733 specification does not ever use the term "service offer," but a POSITA would have understood it to encompass offering a choice about whether to accept a service. As discussed for claim 5, Houghton discloses message content from the push server that comprises information ultimately displayed to a user, *e.g.*, a notification asking permission to display or launch an application. The notification

is in the message, for example, as part of a trigger or command to display the notification. For example, "the ***push messages may include***, for example, ***a message stimulating, triggering or commanding the launch, display or shift to foreground of a user interface*** feature of the terminal." EX-1006, 11-12. Further, the "***push messages may include***, for example, ***messages triggering the mobile terminal to*** play a sound notifying the recipient of the application command or state change, or display notification providing event information from which the user may ***select or decline*** to display the application." *Id*. Through the presentation of the message/notification, the user will be ***offered the service of*** getting the application displayed. It is up to the user on whether to accept or decline this service offer.

348. Houghton also discloses other examples of services that may be offered to a user device through the push message technology. For example, "potential applications of the COMMAND PUSH include but are not limited to [services such as] mobile applications for enterprise connectivity, back office integration, *database access, scientific and industrial process and equipment monitoring and control, pictures transfer, mobile gaming, application data transfer, mobile electronic commerce, application alarms, reminders, multimedia interactivity, corporate calendaring, personal messaging and group messaging, etc.*" EX-1006, 22. Since COMMAND PUSH is "to push an application command message to the push client

704," it would have constituted an offer for a service that is included in the message. *Id*., 21-22.

349. A POSITA would have understood that a notification allowing a user to ***select or decline*** to display a mobile application is an ***offer*** to receive a ***service*** through one of Houghton's various mobile applications, which the user may accept or decline. Houghton-Ogawa thus includes messages with message content that constitutes "a service offer," as claimed.

350. Separately, Houghton discloses using its push message system for "mobile electronic commerce." EX-1006, 22. A POSITA would have understood that Houghton thus discloses transmission of advertisements, because advertisements were conventionally a major feature of mobile electronic commerce implementations. *See e.g.*, EX-1033, 1:66-2:6 ("[A] e-flyer contains a solicitation or advertisement and enables the extension of e-commerce sites, representing a subset of the respective catalogs of e-commerce sites in the form of Solicitations to shoppers."); EX-1034, [0048] ("Once the user has viewed the advertisement (e.g. clicked through the advertisement), the user may decide to purchase the goods and/or services corresponding to the advertisement. Thus, the user may solidify a purchase by communicating with the E-Commerce server 506.") Alternatively, an implementation in which Houghton's push system was used to transmit advertisements as part of its disclosed mobile electronic commerce application (EX-

1006, 22) would have been conventional and well within a POSITA's skill to implement. Houghton discloses its push messages including media or multimedia such as pictures, video, or audio. EX-1006, 14. Before the Critical Date, it was well-known to push digital advertisements in these media formats as part of mobile electronic commerce services, using, *e.g.*, communication protocols like WAP (*see* EX-1006, 1, 5, 9). And, before the Critical Date, it was well known for digital advertisements to be in the form of similar media (e.g., picture, audio, video) data files, and for such digital advertisement to be pushed to client devices through wireless communication protocols such as WAP, which is also leveraged in Houghton. *See* EX-1015, [0012] ("The advertisement system ***pushes*** the ***advertisement image data*** without any user involvement ***to the mobile terminal*** of the user who subscribed to receiving the advertisement."); *id*., [0105] ("the advertisement image data can be forwarded to the terminal ***by a WAP push technology***."). Thus, using Houghton's push system in Houghton-Ogawa to push advertisements would have been nothing more than utilizing familiar, known components (pushed message content, digital advertisements) to achieve a predictable result of facilitating use of Houghton's push messaging system in the context of a mobile electronic commerce system, and a POSITA would have reasonably expected success doing so.

e) Claim 8

[8] The end-user device recited in claim 1, wherein the message content comprises information from a third party configured to provide control of a service or a billing for a service.

351. As discussed for claim 2, Houghton-Ogawa's application server comprises a content management server and a service download control server.

352. A POSITA would have understood that Houghton-Ogawa's application server controls aspects of services delivered to a mobile terminal because it controls what data (for a specific service provided to the user by a specific mobile application) is pushed to the push client as message content—*e.g.*, service content, or updates to the application providing the service to the user. *See supra* discussion regarding claim 2. Because the data received by the push server from Houghton-Ogawa's application server that is pushed as message content to the client (which triggers the push server into, *e.g.*, forwarding the data) is used by the server to affect the service's content or update the application used to provide the user the service, a POSITA understood it includes information "***configured to*** provide control of a service," as claimed.

353. Further, a POSITA understood that data from the application server constitutes "information from a ***third party***" because the application server is separate from Houghton-Ogawa's push server, and the '733 Patent characterizes servers coupled to the service control server link element as providing "third party"

function. In the '733 Patent, (i) the billing server 1662 constitutes the "particular server" recited in claim 1 because it is a server that is communicatively coupled to service control server link element 1638, and (ii) billing server 1662 is a "third party" within the scope of claim 8 because as the '733 Patent specifies, billing server 1662 "***provides trusted third party function for certain ecommerce billing transactions***." *See* EX-1001, FIG. 16 and 77:39-47.

f) Claim 9

[9] The end-user device recited in claim 1, wherein the message content comprises an agent instruction, a setting value, an agent configuration, or a software update.

354. Claim 9 requires claim 1's "message content" to "comprise" one of several alternatives, including "a software update." Houghton says once "an IP connection is established between the server and one or more mobile terminals, the connection can be used to ***transfer messages*** [from the push server] to the mobile terminal"—including "application[] updates to replace or improve installed applications." EX-1006, 9, 34 (claim 29), 31 (claim 15). Such transfer (i.e., push) of messages "include[s] the sending of data files, new applications and ***applications updates*** to replace or improve installed applications." *Id*. Houghton also discloses that "an application[] is part of [a] software." EX-1006, 11-12. A POSITA understood such application updates are "***software updates***," as claimed, and that

such software updates are provided in push messages from the push server to the push client/mobile terminal.

g) Claim 10

[10] The end-user device recited in claim 1, wherein the message content comprises software or a media file.

355. As discussed for claim 9, in Houghton-Ogawa, application updates are sent using Houghton's push system. A POSITA understood "software updates" comprise "software," as claimed. *See also* EX-1006, 9, 29, 34 at claim 29 ("Once such an IP connection is established between the server and one or more mobile terminals, the connection can be used to ***transfer messages*** to the mobile terminal. [Example] interesting uses [for transfer of such messages] include the ***sending of data files, new applications and applications updates to replace or improve installed applications***."), 29 at claim 1 ("the ***push server sends***, in response to predetermined trigger events, at any time ***push application installation, updates, commands or data messages*** to be directed to a push application [on the mobile terminal]."), 31 at claim 15 ("the push server sends to the push client is new application code, application code updates or application data updates.").

356. Additionally, Houghton discloses message content directed to media-based applications (e.g., picture transfer, mobile gaming, multimedia interactivity, messaging). EX-1006, 21-22. For example, the applications "include but are not

limited to ***mobile applications for***…***pictures transfer***, ***mobile gaming***, application data transfer, mobile electronic commerce, application alarms, reminders, ***multimedia interactivity***, corporate calendaring, personal messaging and group messaging, etc." EX-1006, 22. Because the push message is application-specific (*see* the discussion above for [1b]) and the applications can be media-based, a POSITA would have understood that message content directed to such applications included media files. *See* EX-1006, 11-12 (***push messages may include***, for example, messages triggering the mobile terminal ***to play a sound notifying*** the recipient of the application command or state change, ***or display notification*** providing event information from which the user may select or decline to display the application."); *id*., 9 (indicating that the push message can include "data files"); EX-1015, [0012] (corroborating that pushing "image data [to a] mobile terminal" was known before the Critical Date). Thus, a POSITA understood that message content in Houghton-Ogawa may comprise "a media file" as claimed.

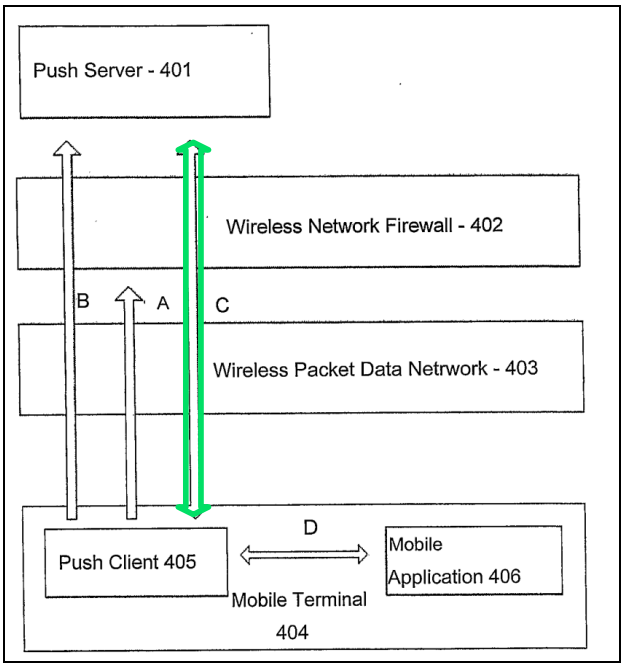
h) Claim 13

[13] The end-user device recited in claim 1, wherein the service control device link agent is further configured to send a device message to the service control server link element over the service control link.

357. Claim 13 requires that claim 1's "service control device link agent" (Houghton-Ogawa's push client, as discussed for [1a2]) "is further configured to

send a device message to the service control server link element" (Houghton-Ogawa's push server, as discussed for [1c1]) "over the service control link" (Houghton-Ogawa's data connection C, as discussed for [1a]). The '733 specification does not use the term "device message," but based on the claim's plain language, a POSITA understood the term to encompass any message from a device on the network, *e.g.*, the end-user device.

358. Per Houghton, "[a]t any time after a connection is established between the client 405 and the server 401, the [push] client may push a message to the [push] server." EX-1006, 20. "This is illustrated by means of the arrow C in Figure 4." *Id*.; *see also id*., 21 ("The ***push client 405*** may in turn at any time accept data D from each of a plurality of mobile applications 406 and ***direct such to the push server 401***.").



EX-1006, FIG. 4 (annotated)

359. A POSITA understood that a message from the push client on the mobile terminal was a "device message," as claimed.

i) Claim 14

[14] The end-user device recited in claim 13, wherein the device message comprises a service usage report or an integrity report.

360. As discussed for claim 10, messages sent from the push server to the push client in Houghton-Ogawa may include a media file such as pictures, mobile gaming, multimedia interactivity, and/or instructions to change the state of the destination application as presented on a user interface. *See also* EX-1006, 11-12, 22. A POSITA understood that presenting such content to a user on the user interface of a mobile terminal constitutes usage of a service.

361. As discussed above with respect to claim 10, the content of the push message (sent from the push server to the push client) can include media file such as pictures, mobile gaming, multimedia interactivity, and/or instructions to change the state of the destination application as presented on a user interface. EX-1006, 11-12, 22. Providing any of the media file and the instructions to the mobile terminal constitutes a service, and the mobile terminal presenting them on a user interface constitutes a ***service usage***. More specifically, the message content includes "***a message stimulating, triggering or commanding the launch, display or shift to foreground of a user interface*** feature of the terminal," to cause the mobile terminal to display content of the media file or to change the state of the destination application. EX-1006, 11-12. "In response to receiving such a message, a mobile terminal may spontaneously open…user interface feature of the terminal, [and i]f such application…is already operating in the mobile terminal, the action of such a message would instead stimulate the application…***to present itself to the foreground of the user interface*** and change state ***as specified in the application-specific message*** received from the server." *Id*.

362. Houghton says that after executing a function in response to push message received from the push server—*e.g.*, presenting the received media file or "changing the state of [a target application] as specified in the application-specific message" (EX-1006, 11-12, 22) "client 405 may also send a message to the server

401 (step 633), such as ***a command execution acknowledgement or result***." EX-1006, 26. Because this message from the mobile terminal includes information about the acknowledgement or result of executing the command for a particular service, it constitutes as a "service usage report," as claimed.

363. This is consistent with the disclosure of the '733 Patent. The '733 Patent does not provide a definition for a "service usage report." But as an example, it notes that "provid[ing] a service usage report, include[es] monitored service usage for the device 101." 57:37-46. A POSITA understood that client 405 sending the "*command execution acknowledgement or result*" conveys that the client 405 monitors the mobile terminal's usage of the service (e.g., presenting the media file or changing the state of the target application) delivered to the terminal.

364. Houghton also discloses its mobile terminal sending messages to the push server to "maintain[] an open path for network communication with the server." EX-1006, 15. The message "keeps the connection to the server open and ***tests the integrity of the connection*** while automatically reestablishing the connection as necessary." *Id*. A POSITA understood that this message from the mobile terminal constitutes an ***integrity report*** because the message provides information regarding the integrity of the connection between the client and server, and "upon failure to receive acknowledgement of" such a message, "the push client or the push server" "may choose to open a new connection." *Id*., 30; *see also id*., 11 ("the mobile

terminal maintains contact with the server by periodically testing the connection with a suitable keepalive message, [and] automatically re-establish the connection when the connection gets broken").

365. Further, before the Critical Date, it was known that communications performed over SSL/TLS protocols would include integrity report or service usage reports. For example, it was well known for a user device to send an acknowledgement message when the user device received a communication from a server through a link supported by SSL/TLS. Such acknowledgement message constitutes an integrity report indicating that the user device is still actively communicating with the server and receiving the services offered by the server. As another example, "***video game actions or events, [and] messaging actions***" that "***push client makes the server aware of***" (as disclosed in Houghton), constitute integrity report because they indicate that the mobile terminal is still actively connected to the server, and also constitute a service usage report because they indicate what parts or forms of gaming or messaging services offered by the server the mobile terminal has used. EX-1006, 14.

j) Claim 15

[15] The end-user device recited in claim 13, wherein the device message comprises a user response.

366. As discussed above for claim 13, Houghton discloses a device message pushed from the mobile terminal to the push server. A POSITA would have understood—in the context of client-server environments where messages are transmitted between a user's mobile terminal and a server, as in Houghton—that messages from the mobile terminal conventionally included user responses to previously-received messages from the push server.

367. For example, Houghton teaches "client-side events" such as "***video game actions or events, [and] messaging actions***" that Houghton's "***push client makes the server aware of***." EX-1006, 14. A POSITA would have understood or found obvious that such information sent by the push client would be sent as content in messages from the mobile terminal, or would have found such an implementation an obvious, conventional utilization of familiar, known components (data transmitted as messages) to achieve a predictable result of facilitating client-server communications over the Internet. EX-1006, 1. A POSITA would also have understood that "video game actions or events" and "messaging actions" are examples of a "***user response***," as claimed, because they are sent by the push client in response to a user's action on the mobile terminal when using, *e.g.*, a "video

game" or "messaging" application. They are thus "device message[s]" that "comprise a user response," as claimed.

368. Additionally, Houghton says the push server may receive messages from another server (e.g., application server 802 in FIG. 8) that "notif[ies] the [push] server directly of events or messages to be sent [to the push client]." EX-1006, 14. Such triggering messages can include "responses of messages which ***the user has replied to*** by terminal software or web page interaction."

k) Claim 19

[19] The end-user device recited in claim 1, further comprising a user interface, and wherein the particular device agent is configured to assist in presenting a notification through the user interface, the notification [being] based on the message content.

369. Claim 19 requires claim 1's "end-user device" (Houghton-Ogawa's mobile terminal, as discussed for [1pre]) to include "a user interface," and requires "the particular device agent" (one of Houghton-Ogawa's mobile applications, *e.g.*, a "video game" or "messaging" application, as discussed for [1b] and [1d3]) to be "configured to assist in presenting a notification through the user interface, the notification being based on the message content."

370. Houghton's mobile terminal in Houghton-Ogawa has a user interface. *E.g.*, EX-1006, 11-12. Houghton discloses "a message stimulating, triggering or commanding the launch, display or shift to foreground of a user interface feature of

the terminal such as an application." EX-1006, 11-12. "In response to receiving such a message, a mobile terminal may… ***open…user interface feature of the terminal thereof to a designed application view*** or location, ***present new information of the availability of new information, a new feature or operating state***." *Id*. "If such application…is already operating in the mobile terminal, the action of such a message would instead stimulate the application…***to present itself to the foreground of the user interface*** and change state ***as specified in the application-specific message*** received from the server." *Id*. Houghton's application thus aids in presenting ("***is configured to assist in presenting***") itself and information ("***a notification***") "regarding new information[,] feature, or operating state" for the application through the user interface, in a way that is specified in Houghton's application-specific message ("***based on the message content***," as claimed). *See* discussion for [1d3] above.

l) Claim 20

[20a] The end-user device recited in claim 19, wherein the particular device agent is further configured to: assist in obtaining a user response to the notification, and send a first message to the service control device link [agent], the first message comprising the user response,

371. Claim 20 requires that "the particular device agent" (one of Houghton-Ogawa's mobile applications, *e.g.,* a "video game" or "messaging" application, as discussed in [1b] and [1d3]) is configured to "assist in obtaining a user response to

the notification" in claim 19 and "send a first message to the service control device link" agent (Houghton-Ogawa's push client, as discussed in [1a2]), "the first message comprising" a "user response."

372. As discussed for claim 19, the mobile applications in Houghton-Ogawa—*e.g.*, a "video game" or "messaging" application—are configured to assist in presenting "new information" received from the network through the user interface on Houghton-Ogawa's mobile terminal. And as discussed for claim 15, Houghton-Ogawa's push client is configured to send to the push server "video game actions or events" and "messaging actions" which are examples of "user response[s]" that correspond to a user's action on the mobile terminal when using, *e.g.*, a "video game" or "messaging" application.

373. A POSITA would have understood that user actions taken by the user when interacting with a "video game" or "messaging" application in Houghton-Ogawa would have included actions made in response to notifications presented through the user interface during use of the "video game" or "messaging" application. This is because a POSITA understood that, in the context of "video game" or "messaging" applications, the "game actions" or "messaging actions" disclosed in Houghton (EX-1006, 14) and described in the context of claim 15 would have included responses to the "new information" (described in the context of claim 19) that was presented to the user on the application.

374. For example, a user may send a message ("***user response***," as claimed) as a reply to "new information" (e.g., another user's message or an alert) in a message from another user that was presented with the assistance of the "messaging" application; or a user may take a game action ("***user response***," as claimed) responding to "new information" regarding a game (e.g., another user's chess move) that was presented with the assistance of a "video game" application. *See e.g.*, EX-1028, 729-730 ("when two users are playing chess remotely against each other using a chess application in their mobile terminals, the chess application can use a messaging system to transport the information about each move made by the user on the chessboard to the peer application."). A POSITA understood that these would have met the requirement of "assist[ing] in obtaining a user response to the notification" for two reasons.

375. ***First***, a POSITA understood that because the application assists with presenting the "new information" (discussed above for claim 19) that leads to the user's reaction/response, the application assists in obtaining the user's response to the notification.

376. ***Second***, a POSITA had several reasons to implement the user's response in Houghton-Ogawa to be submitted through the same application that presented the "new information." Implementing presentation of new information and obtaining user responses to that information in one application would have (1)

improved processing speed, which is desirable in video gaming applications and in messaging applications, (2) reduced traffic between separate device applications that would otherwise need to interact to perform both functions, and (3) reduced security risk that would otherwise be introduced due to the communications between the separate device components. A POSITA would have reasonably expected success with such an implementation because it was commonplace to implement applications to use a user interface for presenting information to and receiving input from a user.

377. Houghton-Ogawa also meets element [20a]'s requirement that the "particular device agent" (Houghton-Ogawa's mobile application) be configured to "send[] a first message to the service control device link agent," (Houghton-Ogawa's push client), where "the first message compris[es] the user response." Houghton teaches that its mobile application can send trigger messages to the push client, which in turn sends the trigger message to the push server, which in turn triggers the push server to send the push message to another server, e.g., an application server. EX-1006, 21; *see also* EX-1006, 14, 32; *see also supra* discussion regarding claim 15. Houghton also teaches that the trigger message can "include an alarm [or] notification" received from the mobile terminal. EX-1006, 21. A POSITA understood that in the context of a video game or a messaging application, such alarm or notification can include the user's actions (i.e., "user response" discussed

above) when using the application. For example, in a chess game application, the user's response includes "each move made by the user on the chessboard" presented on to the user. *See* EX-1028, 729-730.

[20b] and the service control device link agent is further configured to: using the encryption key, generate an encrypted device message comprising the user response, and send the encrypted device message to a service control server link element over the service control link.

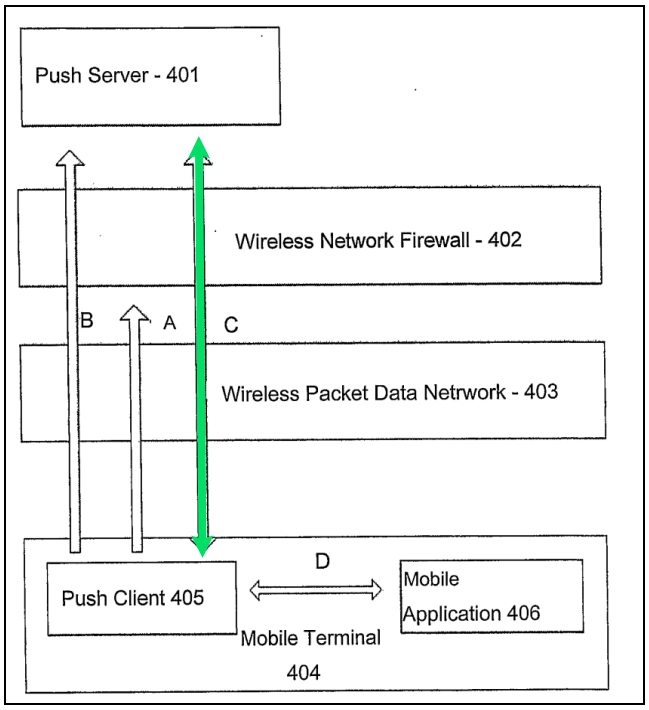
378. As discussed above for claim 15, Houghton discloses "client-side events"—*e.g.*, "video game actions or events, [and] messaging actions"—that the "push client makes the server aware of." As also discussed for claim 15, a POSITA would have understood that messages sent by the mobile terminal's push client to the push server containing this information are "device message[s]" that "comprise a user response."

379. As discussed for, *e.g.*, [1c]-[1c1], Houghton-Ogawa's push client (the "***service control device link agent***," as discussed for [1a2]), is configured to receive and decrypt encrypted messages received from Houghton-Ogawa's push server (the "***server control server link element***," as discussed for [1c1]) through data connection C (the "***service control link***," as discussed for [1a]). *See also supra* § IX.B.1. As also described for [1c]-[1c1], Houghton-Ogawa uses symmetric Houghton-Ogawa Message Encryption, where Ogawa's shared key (the "***encryption key***," as discussed

for [1c]) is stored at multiple network entities and used for encrypting and decrypting messages/content sent from one network entity to another. As discussed *supra* § IX.B.3(d), a POSITA had reason to implement Houghton-Ogawa's mobile terminal to encrypt data that it transmitted to other network entities, and thus a POSITA understood that messages transmitted from Houghton-Ogawa's push client to the push server were encrypted, where the push client on the mobile terminal (using its encryption unit) used the same symmetric encryption scheme discussed with respect to claim 1 to achieve device-side encrypting. Houghton-Ogawa's "service control device link agent" is thus "configured to: using the encryption key, generate an encrypted device message comprising the user response" (described above for [20a]), and "send the encrypted device message to a service control server link element over the service control link," as claimed.

380. Additionally and alternatively, this limitation is met under Patent Owner's interpretation of the claims—which covers systems that only secure client-server communications using symmetric encryption used in TLS/SSL. As discussed for, *e.g.*, [1c]-[1c1], it was well-known to symmetrically encrypt and decrypt a message transmitted through SSL protocols, and Houghton discloses two-way communications (arrow C) between the push server and push client that is secured using "a connection-oriented protocol such as… SSL." EX-1006, 20; *see also* discussion regarding claims 13, 15 above. A POSITA would have implemented

symmetric encryption/decryption for transmission of a message ***from*** the end-user device ***to*** the server through the ***same*** SSL-secured connection for the same reasons that would have motivated a POSITA to use symmetric encryption/decryption for messages transmitted in the other direction (discussed for claim 1). *See* EX-1009, 6:59-7:16, 8:1-5 (corroborating that (i) much like a server that encrypts messages before sending them out, client devices too can have enciphering sections to encrypt messages to be sent out, and that (ii) either of the client or server sides can use symmetric cryptography to cipher a message). Under Patent Owner's interpretation, encryption of the messages described above for [20a] using SSL and transmitting them to the push server over data connection C would likewise meet this limitation.



EX-1006, FIG. 4 (annotated)

m) Claim 21

[21] The end-user device recited in claim 1, wherein the service control link supports asynchronous transmissions by the service control server link element.

381. Claim 21 requires claim 1's "service control link" (data connection C, as discussed for [1a]) to "support[] asynchronous transmissions" by claim 1's "service control server link element" (Houghton-Ogawa's push server, as discussed for [1c1]). The '733 Patent uses the term "asynchronous" to encompass transmissions that occur in response to the server receiving a user request for the transmission, or as a result of polling. *See e.g.*, EX-1001, 38:19-32, 69:23-24. A POSITA thus understood that the term "asynchronous transmissions" encompasses transmissions by a server sent to a client in response to a request from the client.

382. In Houghton-Ogawa, the push server can transmit messages ***asynchronously*** because the messages can be sent out in response to (and after) receiving a trigger event from the push client. For example, as discussed above for claim 15, the messages may be pushed in response to a "client-side event" such as a user device's request, which is akin to the user request disclosed in the '733 patent. *Id*. EX-1006, 14 (indicating that sending the push messages are "***triggered [by] events…which that push client makes the server aware of***[;] ***the server in turn initiating a push command event***."). *id*.; *see also id*., p. 21, last full para ("The push message from the push server 401 may be triggered by any trigger event, local or remote, [such as] an alarm, notification, or measurement result received to the push

server 401 from another device or system."); *id*., p. 32, claim 22 (providing examples of trigger events). Accordingly, in Houghton-Ogawa, data connection C (the "***service control link***," as claimed) supports asynchronous transmission by the push server after the server receives a user request, consistent with how this term is used in the '733 specification. EX-1001, 38:19-32, 69:23-24.

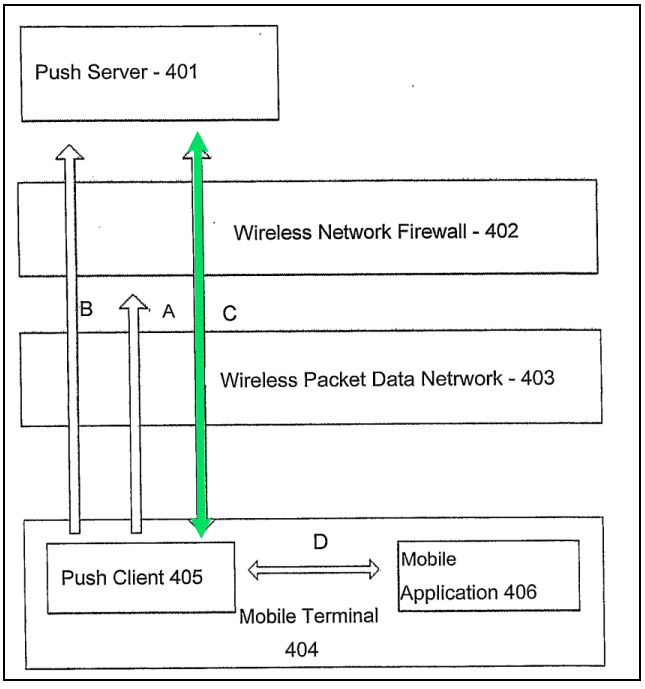
n) Claim 22

[22] The end-user device recited in claim 1, wherein the service control link supports periodic transmissions by the service control server link element.

383. Claim 22 requires that claim 1's "service control link" (Houghton-Ogawa's data connection C, as discussed for [1a]) "supports periodic transmissions" by "the service control server link element" (Houghton-Ogawa's push server, as discussed for [1c1]). Houghton expressly discloses "use of" a "***periodic***" messages used to ensure its connections are not "time expired" that are sent "from" the "server to the client." EX-1006, 19. These are "periodic transmissions," as claimed.

384. Additionally, the push client in Houghton "may send a periodic message (the arrow C in Figure 4) from the client 405 to the server 401 to the effect that [the connection does] not time expire." EX-1006, 26; see also id. 11 11 ("the mobile terminal maintains contact with the server by periodically testing the connection with a suitable keep alive message, a "ping", which resets timers in intervening operator stateful firewalls and/or NAT (network address translation)

firewalls."). "The client 405 may then wait for a reply or acknowledgement from the server 401, and if the acknowledgement is received (step 622), the client 405 returns to step 620 to await the next combined connection refresh and test." Id. "If the no acknowledgement is received, the client 405 may… simply re-attempt login to the server 401." EX-1006, 26. A POSITA would have understood that push client-initiated "periodic" messages, and the push server's acknowledgement messages to client-initiated periodic messages are each a "periodic transmission" (as claimed). EX-1006, 11. Because transmissions between Houghton-Ogawa's push server and push client take place through data connection C (see discussion regarding [1a]), a POSITA understood that data connection C "supports periodic transmissions," as claimed.



EX-1006, FIG. 4 (annotated)

o) Claim 26

[26] The end-user device recited in claim 1, wherein the particular device agent comprises software.

385. In Houghton-Ogawa, the particular device agent (e.g., mobile application 406/805) comprises software. A mobile application, as understood by a POSITA, is a software capable of performing a particular task (or set of tasks) on a mobile computing device. *See e.g.*, EX-1006, 9 ("Numerous ***mobile applications*** such as games and productivity ***software*** are now included with new mobile terminals."), 16, ("The mobile terminal 404 is preferably a commercially available mobile terminal, such as a portable phone or appliance capable of running software or personal digital assistant, which provides a platform for ***downloading application software*** over air or from a personal computer, installing the software in the terminal, and running the software in the terminal.").

386. Further, in the context of Houghton's disclosure, a POSITA understood the mobile application 406/805 on mobile terminal 404/803 includes software. As discussed above with respect to claim 9, Houghton discloses sending application updates to the mobile terminal to replace or improve the installed application over a wireless IP connection between the mobile terminal and a server. Additionally, Houghton discloses that the push client 804 uses an ***application*** *programming interface* (API) to connect to mobile applications 805. EX-1006, 23. An API is known for facilitating communications with software applications. *See* EX-1016,

1:24-32 ("***An API*** is a source code interface that a computer system or program library provides ***in order to support requests for services from a software application.***"); EX-1017, 1:54-2:5 ("The well-known application programming interface (API) is an abstract concept describing a set of functions or methods called by software.").

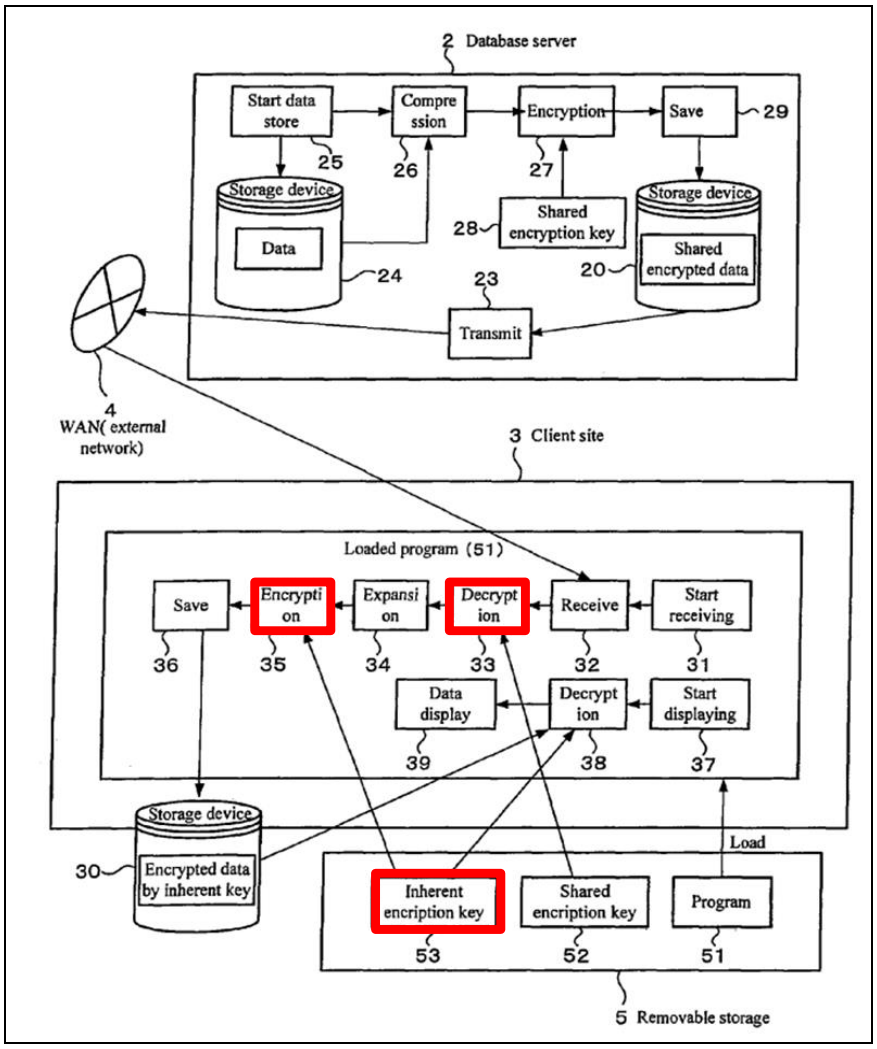
p) Claim 27

[27] The end-user device recited in claim 1, wherein the encryption key is a first encryption key, and the service control device link agent is further configured to encrypt the message content using a second encryption key before delivering the message content to the particular agent, the second encryption key shared by the service control device link agent and the particular agent.

387. Claim 27 calls the encryption key recited in claim 1 "a first encryption key," and requires claim 1's "service control device link agent" to be "configured to encrypt the message content using a ***second*** encryption key before delivering the message content to the particular agent."

388. Houghton's push client (the ***service control device link agent***, as discussed for [1a2]/[30a2]) is responsible for receiving a message from Houghton's push server, decrypting the message using a first encryption key, and sending message content to a destination application (the ***particular device agent***, as discussed for [1d3]/[30d3]-[30d4]).

389. As noted *supra* §IX.B.2(c), Ogawa discloses an encryption unit for re-encrypting data for, *e.g.*, transmission within the user device. EX-1005, 5:59-6:9. In Ogawa, a message received and decrypted at the client (using receive unit 32 and encryption unit 33) is converted back to its original format (using decompression/expansion unit 34), and encrypted again—before being transmitted within the client device, *e.g.*, for storage—by encryption unit 35, using an "inherent encryption key 53." EX-1005, 5:59-6:9, 5:24-25. Ogawa's inherent encryption key 53 is a second encryption key that is different from the first encryption key used to encrypt/decrypt data transmitted between the server and client.



EX-1005, FIG.7 (annotated)

390. Also as discussed *supra* §IX.B.2(c), a POSITA had reason to include the encryption functionality as part of Houghton's push client—*e.g.*, to secure decrypted received data before transmitting it to any other component on the user device—and would have reasonably expected success with such an implementation.

391. A POSITA would further have been motivated to implement Houghton-Ogawa's push client to secure/encrypt message content (received from, *e.g.*, the push server) using a different encryption key than the one used to decrypt

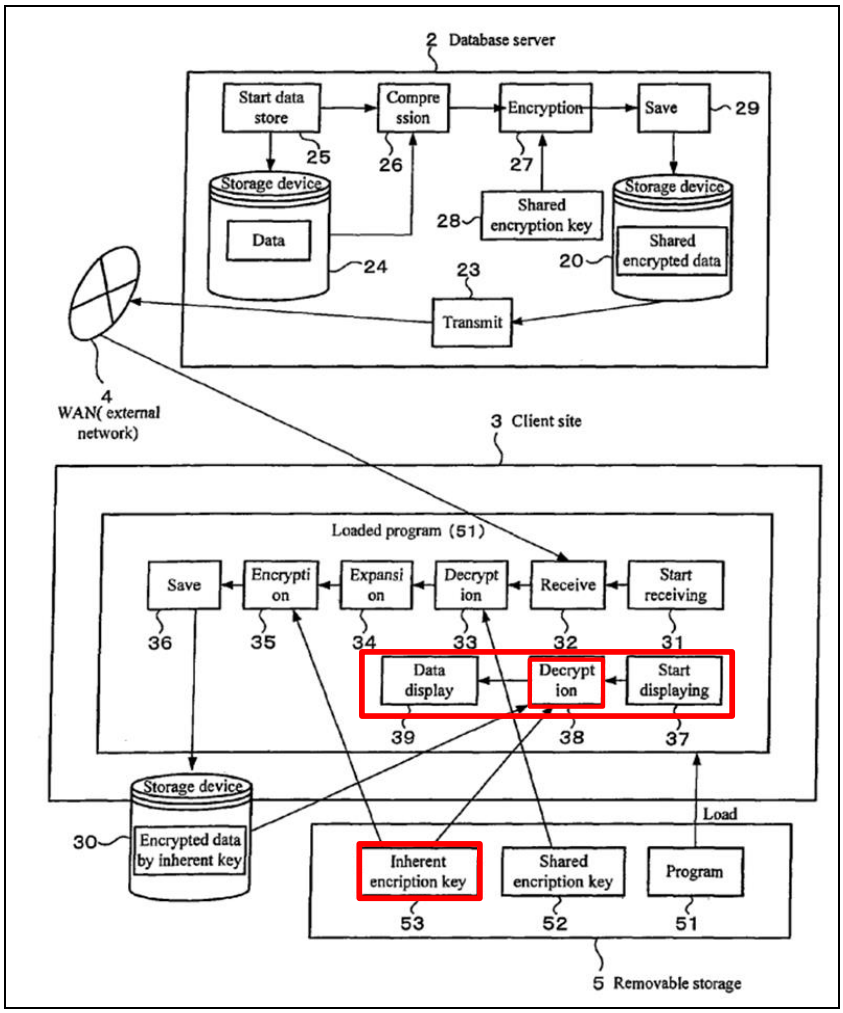
the received data (e.g., Ogawa's disclosed inherent key) prior to delivery to device storage or the destination application, as taught by Ogawa. EX-1005, 6:1-26. Such internal encryption within the device using an inherent key was expressly taught by Ogawa and would have improved security of the data in Houghton-Ogawa's user device when stored on the device or when transmitted within the terminal, and would have helped, *e.g.*, prevent unauthorized viewing or use of the data by rogue/unauthorized software on the device.

392. A POSITA would also have had reason to implement Houghton-Ogawa's push client such that it performed any intermediary functions/steps between decryption (e.g., by Ogawa's unit 33) and re-encryption (e.g., by Ogawa's unit 35) that were required to ensure that the destination (on the user device) received data with correct format and content. For example, the expansion unit 34 in Ogawa decompresses the decrypted data "to convert the data back to [its] original format" before re-encrypting that data at unit 35. EX-1005, 5:65-6:3. A POSITA would have reasonably expected success implementing Houghton-Ogawa's push client to perform the intermediary functions described in Ogawa, as discussed above—*e.g.*, by incorporating expansion unit 34—because the prior art components would continue to perform functions they performed prior to the combination. For example, the push client would continue to receive, decrypt, and send data to another component on the user device, and Ogawa's expansion and encryption units (as

implemented as part of the push client) would convert decrypted data into its original format before encrypting it for use within the user device.

393. Claim 27 also requires "the second encryption key" to be "shared by the service control link agent and the particular agent."

394. As noted for claim 19, Houghton-Ogawa's user device is capable of displaying messages to a user. As discussed below, a POSITA had reason to implement Houghton-Ogawa's user device such that it could display data that was encrypted using Ogawa's inherent key 53 (pursuant to Ogawa's teachings discussed above). Ogawa teaches using "display units 37-39" to "provide the necessary functionality for rendering decoded data to a display of" the client; in order to "render" data that is stored on the client on the display, Ogawa teaches decrypting the stored data by using the same inherent key 53 that encryption unit 34 used to encrypt the data for storage within the device. EX-1005, 5:24-30, 6:10-18.



EX-1005, FIG. 7 (annotated)

395. Based on Ogawa's express teachings, a POSITA would have had reason to implement Houghton-Ogawa's user device to incorporate Ogawa's display units 37-39 to be able to decrypt and display data decrypted using Ogawa's inherent key 53. A POSITA would have reasonably expected success doing so, because the prior art components would continue to perform functions they performed prior to the combination.

396. In such an implementation, for data received by the push client from the push server that was intended for immediate display to the user by Houghton's terminal (instead of, e.g., data intended for one of Houghton-Ogawa's mobile applications, *e.g.*, a "video game" or "messaging" application, as discussed for previous claims), a POSITA would have understood that Houghton-Ogawa's display units 37-39 themselves collectively constituted a destination application in the user device that performed display functions on behalf of an entity (e.g., client, server, another application, etc.), and thus constituted one of the "***plurality of device agents***" (identifiable by a "associated device agent identifier" in order to allow accurate routing of data intended for immediate display) for [1b], and ***a particular device agent***, for [1d3].

397. Because both the push client and Houghton-Ogawa's display units 37-39 use the same key for encryption and decryption, a POSITA would have understood that the inherent key (the claimed ***second encryption key***) is ***shared*** by encryption unit 35 in the push client (***the service control device link agent***, as claimed) and the destination display units 37-39 (***the particular agent***, as claimed).

q) Claim 28

[28] The end-user device recited in claim 1, wherein the service control device link agent is further configured to trigger a device transmission to maintain the service control link when a time between transmissions would otherwise cause the service control link to terminate.

398. The '733 Patent explains that a "transmission trigger is based on waiting for an amount of service usage, and also including a minimum transmission rate that triggers a transmission according to [for example,] ***a maximum time between transmissions clock*** to keep the service processor 115 in communication with the service controller 122 ***when little or no service usage is occurring***…." EX-1001, 38:19-25. Similarly, Houghton's push client sends periodic messages to the push server before a set expiration time: push client 405 periodically pings push server 401 with "***a suitable keep alive message***" to keep the data connection C (the "***service control link***") between the client and the server alive. EX-1006, 11, 26; *see also*, EX-1006, 27 ("***the push server 401 may receive a periodic message (the arrow C in Figure 4) from the client 405*** to the effect that the server updates the respective server object associated with a given client so ***that the connection, server socket or client socket is not time expired as being stale***."); *id*., 19 ("Use of ***a periodic message from the client to the server*** or server to the client ***to the effect that*** client socket, server socket, intermediate Network Address Translation (NAT) devices, intermediate firewalls, and intermediate gateway devices ***do not time expire the***

connection.”). A POSITA would have understood that if such pings are not sent before the connection time expired, the data connection would terminate.

r) Claim 29

[29] The end-user device recited in claim 1, wherein the service control link is configured to support control-plane communications using an Internet protocol.

399. Claim 29 requires claim 1’s “service control link” which “is configured to support control-plane communications” to be configured for such communications “using an Internet protocol.” As discussed for [1a1] and [1a2], data connection C (the “***service control link***”) supports control-plane communications. Houghton characterizes data connection C as being implemented using a “connection-oriented protocol such as TCP/IP, HTTP, or HTTPS.” EX-1006, 20; *see also id.*, 17 (disclosing “IP connection” for a connection of a mobile terminal to a network.). These were well-known secure Internet protocols. A POSITA thus understood that Houghton-Ogawa’s data connection C used an Internet Protocol as claimed. Alternatively, this would have been a conventional, obvious way to implement what Houghton describes, and is nothing more than utilizing familiar, known components to achieve a predictable, desirable result of enabling Houghton’s mobile terminal to send and receive data over the Internet. Before the Critical Date, these example protocols were known as secure Internet protocols, and as security protocols applied to known internet/network-based connections formed using such

Internet protocols. *See e.g.*, EX-1005, 3:43-53 ("the external wide area (WAN) tele communication network 4 is the global communications network, ***commonly referred to as the Internet***. The network components communicate via ***WAN 4*** through hyper text transfer protocol (***HTTP***)."), 3:61-4:7 ("in network communications [through network 4,] utilizing a conventional TCP/***IP*** (Transmission Control Protocol/***Internet Protocol***) or UDP (User Datagram Protocol), ***encryption communication, such as*** IPsec (Internet Protocol Security) or ***SSL (Secure Socket Layer),*** is utilized to prevent some security risks presented during the exchange of data between network terminals."). Thus, because communications in Houghton-Ogawa occur over data connection C, including control plane communications, Houghton-Ogawa meets the requirement that the claimed "***service control link***" (Houghton-Ogawa's data connection C) "is configured to support control-plane communications using an Internet Protocol," as claimed.

C. Ground 3: Claims 3, 4, 6, 11, 12, 16-18, 23, 24 Are Obvious Over Houghton-Ogawa, And Hwang

1. Hwang (EX-1007)

400. Hwang provides details regarding how to establish a roaming connection between a mobile device and a visited server when the terminal enters the roaming area of the server. EX-1007, [1], [35]. Like Houghton, Hwang is about

wirelessly providing services to end-user devices. While Houghton recognizes the need for a method to deliver "real time information, interactivity and rich media content, ***regardless of*** which mobile operator is being used and ***where the mobile user happens to be at that moment***," Houghton is silent on how to establish a roaming service for a mobile device that is on the move. EX-1006, pp. 10-11. Hwang, however, provides details regarding how to establish a roaming connection between a mobile device and a visited server when the terminal enters the roaming area of the server. EX-1007, [1], [35].

401. FIG. 8 (annotated below) illustrates a sequence of communications between a mobile terminal 800 and a Visited Service Provider (Visited SP) 810 when the terminal "arrives at the roaming area" of the Visited SP 810. EX-1007, [97], [100]. To start establishing a roaming connection with the Visited SP 810, mobile terminal 800 sends a request (803) to Visited SP 810 for roaming registration. EX-1007, [102-104]. Visited SP 810 sends back (806) a response including Roaming Service Allowed Scope that indicates the scope and charge of the roaming service. *Id*., [110-112]. If terminal 800 communicates (807) to the Visited SP that it agrees with the Roaming Service Allowed Scope, Visited SP 810 starts providing roaming services (809) to the terminal. *Id*., [113], [115].

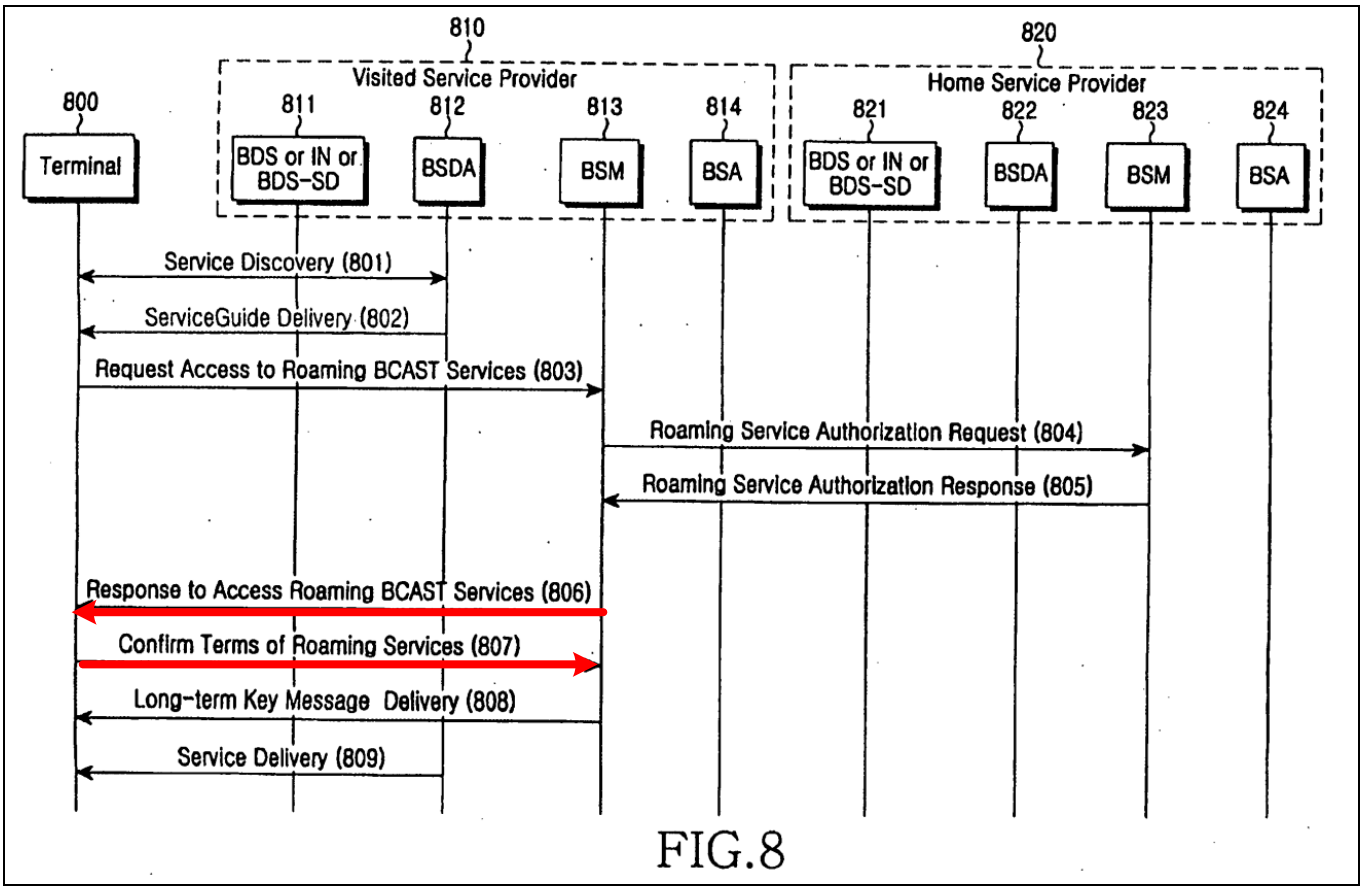


FIG.8

EX-1007, FIG. 8 (annotated)

2. Houghton-Ogawa and Hwang Combination

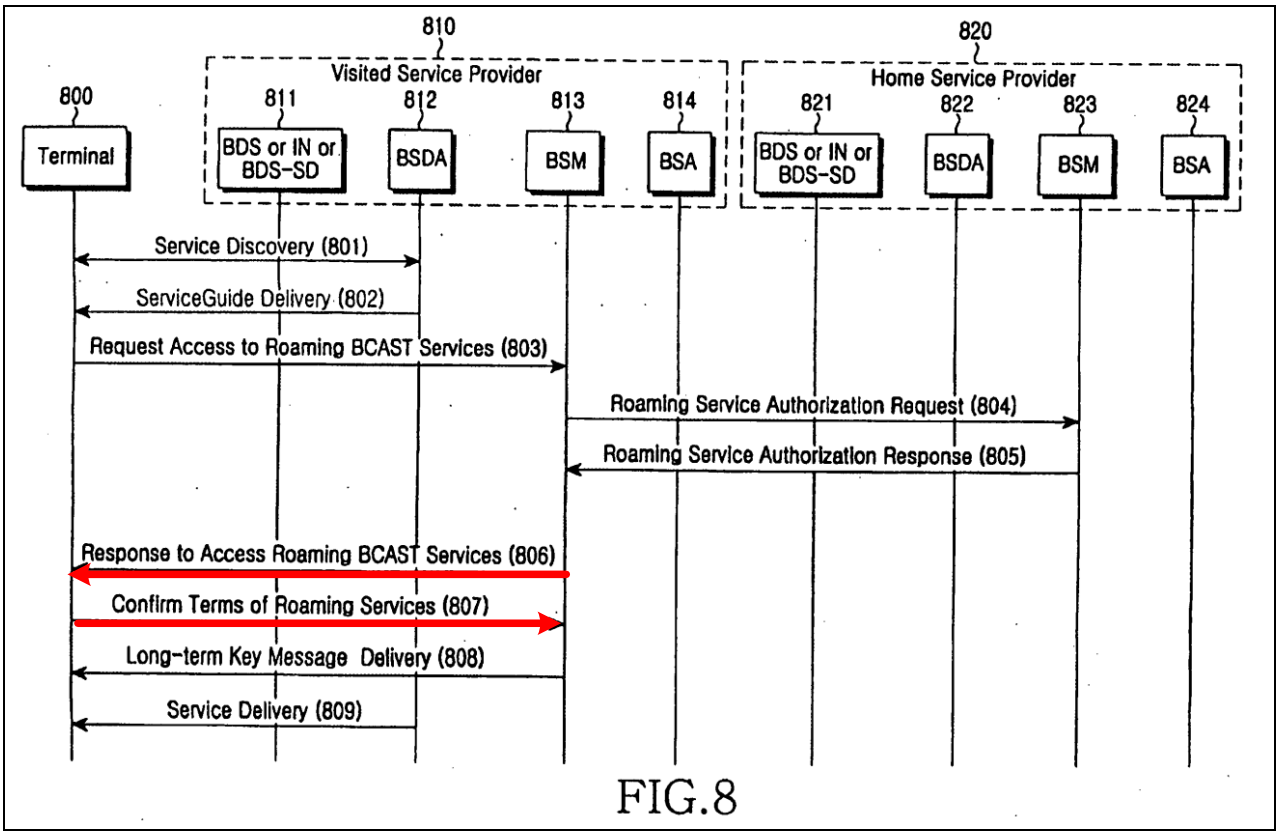
402. A POSITA would have found it obvious to combine the teachings of Houghton and Hwang, and would have been motivated to do so, for at least the reasons described below.

403. ***First***, a POSITA would have been motivated to apply the roaming initiation technique of Hwang to Houghton's push messaging system to enable the end-user to be able to receive and benefit from network services even while the end-user is away from his/her home network. Houghton recognizes the need for

delivering "real time information, interactivity and rich media content, ***regardless of*** which mobile operator is being used and ***where the mobile user happens to be at that moment***." EX-1006, 10-11. Houghton, however, does not explicitly disclose how to establish a roaming service for a mobile terminal that exits the user's home network. Recognizing the need to support roaming services in the context of Houghton's disclosures, a POSITA would thus have turned to roaming-related references, such as Hwang, for implementation details. *See* EX-1007, [35] ("According to…the present invention, there is provided a roaming service method in a mobile broadcasting system."); *id*., [97] ("FIG. 8 is a signaling diagram illustrating a roaming procedure.").

404. Hwang discloses a sequence of communications that happens between a user's mobile terminal—terminal 800 in Hwang—and a visited service provider (VSP) 810 before VSP 810 starts to provide roaming services to the user device. *Id*. Hwang discloses that VSP 810 sends a message (806) to terminal 800 to inform the terminal about the service terms ("reception rights") and charging policies associated with the roaming service. EX-1007, ¶¶[110-112]. In response (807), terminal 800 indicates "whether it agrees with the information in…the message received in step 806." *Id*., ¶[113]. After receiving such indication, VSP 810 starts providing roaming services to terminal 800. *Id*.

405. ***Second***, a POSITA understood that implementing Hwang's roaming initiation techniques to Houghton-Ogawa's system would have beneficially ensured that the user of Houghton-Ogawa's mobile terminal and push server agreed to the terms and billing policies of a visited network before the push server started providing any services (e.g., by sending messages) to the mobile terminal.



EX-1007, FIG. 8 (annotated)

406. ***Third,*** implementing these techniques in the form described in Hwang and within the service-providing environment disclosed in Houghton would have been nothing more than implementing a known method within known systems to achieve predictable results.

407. A POSITA would have reasonably expected success applying Hwang's roaming initiation technique to Houghton-Ogawa because Houghton provides the required infrastructure (a server that provides roaming services, and a mobile terminal device that uses the roaming services), and Hwang provides a known technique to establish an agreement between the visited service provider (e.g., implemented as part of Houghton-Ogawa's push server) and a roaming mobile terminal before any roaming services commence. Implementing these techniques in the form described in Hwang and within the service providing environment disclosed in Houghton would have amounted to implementing a known method within known systems to achieve predictable results.

408. Moreover, in the combination, the roaming authorization and messaging functionality of Hwang would readily achieve the goals of Hwang while enabling roaming services for Houghton—thus ensuring a reasonable expectation of success in the resulting combination. For example, the mobile terminal in Houghton sends request for connection to a server when the terminal wants to use the server's services. EX-1006, 18. Like the mobile terminal in Houghton, terminal 800 in Hwang requests connecting to a roaming server (Visited SP 810) when the terminal enters the area supported by that server. EX-1007, ¶¶[0100-102]. As discussed above, Hwang also discloses further communications between terminal 800 and the roaming server to reach an agreement regarding the roaming services before the

server starts providing such services (e.g., push services that push server in Houghton provides) to the terminal. The resulting combination—in which Houghton-Ogawa's push server is implemented to incorporate Hwang's roaming authorization and messaging functionality of Visited SP 810 as described above—is referred to herein as Houghton-Ogawa-Hwang.

3. Claim Analysis

(a) Claims 3-4

[3] The end-user device recited in claim 1, wherein the message content comprises information associated with a service usage.

[4] The end-user device recited in claim 3, wherein the information associated with the service usage comprises information about one or more of a service usage value, a projected service usage value, a service usage plan limit, a projected service usage overage, a projected service cost overage, a service plan period time duration, a service plan time remaining before end of period, and a service overage.

409. Claim 3 requires claim 1's "message content" to "comprise[] information associated with a service usage." Claim 4 requires the "information" to be "about one or more" of several alternatives, including "a service usage value," "a projected service usage value," or "a service usage plan limit."

410. The '733 Patent indicates that "service usage" can include usage of "roaming" services by the end-user device, and lists roaming costs as an example service usage. The patent notes that "the service usage counter can support

providing to the user ***the following service usage related data/reports:*** …projected costs, ***cost to roam, cost to roam options, and/or projected roaming costs***." EX-1001, 58:1-14; *see also id*., 53:7-10 ("the service monitor agent 1696 observes and possibly records or reports ***service usage categorized by network possibly including roaming networks***, paid service networks or free service network.").

411. Hwang discloses sending messages containing information about roaming service usage to end-user devices. A POSITA understood that the "Roaming Service Allowed Scope" sent as part of Hwang's message 806 is associated with "***service usage***," as claimed, because it includes the "reception rights" and charging policies to be applied to Houghton-Ogawa's mobile terminal for use of roaming services that Visited SP 810 provides. EX-1007, ¶¶[0112], [0108]. Information about the charging policies disclosed in Hwang also include "additional costs" associated with receiving the roaming services (which a POSITA understood constituted "***a service usage value***"), and "a change in the charging system" (which a POSITA understood constituted "***a projected service usage value***"). *Id*.; *see also id*., ¶[0121] ("If the BSM 813 of the Visited SP 810 can authorize the Terminal 800 to perform the roaming, it generates a response message taking into account ***the additional charge occurring during roaming*** and the change in the charging system using the subscription information of the Terminal 800, and transmits the response message to the terminal in step 908.").

412. A POSITA also understood that Hwang's "reception rights" constituted a "***service usage plan limit***," as claimed, because they indicate "which reception right the roaming Terminal 800 will have in the Visited SP 810," for example "a class of the service that the roaming-requested Terminal 800 can receive from the roaming-requested Visited SP 810." EX-1007, ¶¶[0112], [0108].

413. The information included in Hwang's message 806 is similar to the roaming information that the '733 patent says is sent from a roaming server, which does not require the information to be sent to a particular application, or otherwise be application-specific. *See e.g.*, EX-1001, 61:15-31 ("In some embodiments, billing information for roaming partners is provided. For example, ***a roaming server*** can include a roaming service cost data table for roaming service partners. In this example, ***when the device (e.g., device 101) connects to a roaming network provided by a roaming service partner, then the device can also receive the roaming service data rate based on the roaming service cost data table provided by the roaming server***."). Rather, information regarding the roaming service usage in the '733 Patent is directed to the device, as a whole, using the roaming service. Accordingly, a POSITA understood that Houghton-Ogawa-Hwang's message content (the content of message 806 pushed from VSP 810 to the mobile terminal) comprises information that meets claims 3 and 4.

(b) Claim 6, 11, and 12

[6] The end-user device recited in claim 1, wherein the message content comprises information associated with a roaming service usage or a roaming service cost.

[11] The end-user device recited in claim 1, wherein the message content comprises information associated with a service policy.

[12] The end-user device recited in claim 1, wherein the message content comprises service usage accounting information.

414. Claim 6 requires claim 1's "message content" to "comprise[] information as-sociated with a roaming service usage or a roaming service cost." Claim 11 requires the "message content" to "comprise[] information associated with a service policy." Claim 12 requires it to "comprise[]service usage accounting information."

415. In view of the discussion for claims 3-4, a POSITA understood that Houghton-Ogawa-Hwang includes message content (the content of message 806) comprising information associated with claim 6's "***roaming service usage***," because Hwang's "reception rights" information pertains to a mobile terminal's usage of the roaming service. This information is likewise associated with claim 6's "***roaming service cost***," because Hwang's message includes information related to additional costs and changes in the charging system due to use of the roaming service. The information is likewise associated with claim 11's "***service usage accounting information***," because Hwang's message includes information regarding the change

in the charging system due to using the roaming service, which a POSITA understood pertains to how usage of the service is quantified for the purpose of charging.

416. Houghton-Ogawa-Hwang also includes message content that comprises information associated with "***a service policy***" (e.g., reception rights or charging policies associated with the roaming services). As discussed above, VSP 810 sends (806) a message to the mobile terminal to inform the terminal's user about the service terms (e.g., charging policies) associated with the roaming service. A POSITA understood that this message includes details regarding policies associated with the roaming service, so that the user may accept or decline them in a response message (807). *See* EX-1007, ¶[0113] (In response (807), terminal 800 indicates "whether it agrees with the information in…the message received in step 806." "If the Terminal 800 does not agree with the additional cost occurring during roaming or the change in the charging system, the roaming service is not achieved." "However, if the Terminal 800 agrees, it proceeds to the next step."). Therefore, the message that the Visited SP 810 sends to terminal 800 is ***a service offer***, which Terminal 800 may accept or decline in the response message at step 807.

(c) Claims 16-18

[16] The end-user device recited in claim 15, wherein the user response comprises an acknowledgment of a roaming cost or a roaming usage.

[17] The end-user device recited in claim 15, wherein the user response comprises an acknowledgment of a service usage, a service cost, or a service overage.

[18] The end-user device recited in claim 15, wherein the user response comprises an indication that a user intends to purchase a service plan.

417. Claim 16 requires claim 15's "user response" to "comprise[] an acknowledgment of a roaming cost or a roaming usage." Claim 17 requires "an acknowledgment of a service usage, a service cost, or a service overage." Claim 18 requires "an indication that a user intends to purchase a service plan."

418. Hwang says VSP 810 sends (806) a message to the mobile terminal to inform it about the service terms such as charging policies associated with the roaming service. EX-1007, ¶¶[110-112]. The terminal's response (807) includes a "Roaming Confirm Status" "used for indicating whether" the user of the terminal has agreed with the terms on the Roaming Service Allowed Scope and "will roam to the Visited SP 810" "—*i.e.,* a "user response" as required by claim 15. EX-1007, ¶¶[0113-114]. Because message 807 includes a response indicating whether the user confirms (and thus acknowledges) terms of the Roaming Service Allowed Scope, and because Roaming Service Allowed Scope includes a service cost, a POSITA would have understood the user response to include an "***acknowledgement of a roaming coast or roaming usage***" (claim 16), and "***acknowledgment of a service***

usage" or ***"service cost***" (claim 17)—where the service is the roaming service. Further, a POSITA would understand that a user response agreeing to the Roaming Service Allowed Scope through message 807 meets claim 18's "***indication of an intention to purchase the service plan***," because the user confirms reception rights for the offered price.

(d) Claims 23-24

[23] The end-user device recited in claim 1, wherein the service control device link agent is further configured to send a device credential to the network system or receive the device credential from the network system during a service authorization sequence.

[24] The end-user device recited in claim 23, wherein the device credential comprises one or more of a phone number, an identification number, a security signature, a security credential, a subscriber identity module (SIM) identifier, a mobile equipment identifier (MEID), and a device identifier.

419. Claim 23 requires claim 1's "service control device link agent" (Houghton-Ogawa's push client) to be "configured to send" or "receive" a "device credential" to "the network system during a service authorization sequence." Claim 24 requires that the "device credential," comprise one of several alternatives, including a "device identifier." As discussed above for [1a], Houghton-Ogawa's push server is a part of a "network system," as claimed. The same is true of the push server when implemented to function as Hwang's VSP 810 (as discussed *supra*

§ X.C.2), because it is still a server providing performing one or more server functions in Houghton-Ogawa-Hwang's network.

420. Hwang uses a Terminal ID for each mobile terminal to keep track of which terminals have requested a roaming registration and identify each terminal's roaming authorization status. Roaming Request 803 sent from the mobile terminal to VSP 810 (implemented as the push server 401 in Houghton) includes the Terminal ID. EX-1007, ¶¶[0102-0103].

421. A POSITA would have understood that the Terminal ID is used "***during a service authorization sequence***," as claimed, because it is used to determine the whether the terminal is authorized to receive roaming services. The sequence includes the roaming request 803 received from the terminal, and subsequent communications between Visited SP 810 and Home SP 820 before responding (806) to the roaming request. In response the request, Visited SP 810 uses the terminal ID to send an inquiry (804) to the Home SP 820 to determine the Roaming Authorization Status of the terminal. EX-1007, ¶¶[0105-106]. Home SP 820 then responds with message 805 that includes a Roaming Authorization Status of the terminal, which is determined by retrieving subscription of the terminal, using the Terminal ID received as part of the inquiry 804. *Id*., ¶¶[0107-108].

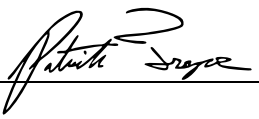
422. Because Houghton-Ogawa's push client 404 (the claimed "***service control device link agent***") exchanges communications with the push server, a

POSITA would have understood, in Houghton-Ogawa-Hwang, that push client 404 is configured to send a "***device credential***," as claimed in claim 23—Hwang's Terminal ID—to push server 401, which constitutes a "***device identifier***," as claimed in claim 24.

X. ADDITIONAL REMARKS

423. I currently hold the opinions set expressed in this declaration. But my analysis may continue, and I may acquire additional information and/or attain supplemental insights that may result in added observations.

424. I hereby declare 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 further declare that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of the Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patents issued thereon.

Dated: 22 January 2024 By: 

APPENDIX A

Patrick Gerard Traynor

Professor
Associate Chair for Research in CISE
John and Mary Lou Dasburgh Preeminent Chair in Engineering

Department of Computer & Information Science & Engineering (CISE)
University of Florida
E301 CSE Building, PO Box 116120
Gainesville, FL 32611 USA
traynor@cise.ufl.edu
http://www.cise.ufl.edu/∼traynor

Table of Contents

EDUCATIONAL BACKGROUND 4

EMPLOYMENT HISTORY 4

CURRENT FIELDS OF INTEREST 4

I. TEACHING 6
- A. Courses Taught . . . 6
- B. Continuing Education . . . 6
- C. Curriculum Development . . . 6
- D. Individual Student Guidance . . . 7
- E. Teaching Honors and Awards . . . 11

II. RESEARCH AND CREATIVE SCHOLARSHIP 12
- A. Thesis . . . 12
- B. Published Journal Papers (Refereed) . . . 12
- C. Published Books and Parts of Books . . . 14
- D. Edited Proceedings . . . 14
- E. Conference Presentations . . . 14
  - E.1. Conference Presentations with Proceedings (Refereed) . . . 14
  - E.2. Conference Presentations with Proceedings (Non-Refereed) . . . 20
  - E.3. Conference Presentations without Proceedings . . . 20
- F. Other . . . 20
  - F.1. Submitted Journal Papers . . . 20
  - F.2. Refereed Research Reports . . . 20
  - F.3. Software . . . 20
  - F.4. Published Papers (Non-Refereed) . . . 21
  - F.5. Books in Preparation . . . 21
  - F.6. Workshops and External Courses . . . 21
- G. Research Proposals and Grants (Principal Investigator) . . . 22
- H. Research Proposals and Grants (Contributor) . . . 24
- I. Research Honors and Awards . . . 25

III. SERVICE 27
- A. Professional Activities . . . 27
  - A.1. Memberships and Activities in Professional Societies . . . 27
  - A.2. Conference Committee Activities . . . 27
- B. On-Campus Committees . . . 28
  - B.1. University of Florida . . . 28
  - B.2. Georgia Tech . . . 29
- C. Special Assignments . . . 29
- D. Ph.D. Examining Committees . . . 29
- E. External Member of M.S. Examining Committee . . . 33
- F. Consulting and Advisory Appointments . . . 33
- G. Civic Activities . . . 33

IV. NATIONAL AND INTERNATIONAL PROFESSIONAL RECOGNITION 34
- A. Honors and Awards . . . 34
- B. Invited Conference Session Chairmanships . . . 34
- C. Professional Registration . . . 34
- D. Patents . . . 34
- E. Editorial and Reviewer Work for Technical Journals and Publishers . . . 35
- F. Expert Witness Services . . . 37

V. OTHER CONTRIBUTIONS 39
- A. Seminar Presentations (Invited Papers and Talks at Meetings and Symposia) . . . 39

B. Special Activities 43

EDUCATIONAL BACKGROUND

Degree	Year	University	Field
Ph.D.	2008	Pennsylvania State University State College, PA *Dissertation:* Characterizing the Impact of Ridigity on the Security of Cellular Telecommunications Networks *Advisors:* Thomas F. La Porta and Patrick D. McDaniel	Computer Science & Engineering
M.S.	2004	Pennsylvania State University State College, PA	Computer Science & Engineering
B.S.	2002	University of Richmond Richmond, VA *Minors:* Biology, Business Admin	Computer Science

EMPLOYMENT HISTORY

Title	Organization	Years
Professor	University of Florida	*August 2018–Present*
Associate Professor	University of Florida	*August 2014–July 2018*
Associate Professor	Georgia Institute of Technology	*March 2014–August 2014*
Assistant Professor	Georgia Institute of Technology	*2008–March 2014*
Research Assistant	Pennsylvania State University	*2004–2008*
Teaching Assistant	Pennsylvania State University	*2004*

CURRENT FIELDS OF INTEREST

My research focuses on the security of cellular/telephony networks and mobile systems. The security of these systems generally relies on their closed nature and trust in the honest behavior of users. However, with the recent disintegration of these assumptions and with over than six billion subscribers around the world, cellular and mobile systems represent the next great expansion in global critical infrastructure and, because of their unique characteristics, require new and different approaches to security.

Recognizing this, my research focuses on three specific themes: (1) developing efficient techniques to allow telephony providers and customers to authenticate the origin of incoming calls; (2) measuring and improving the security of emerging mobile financial systems and (3) efficient and strong privacy-preserving techniques for mobile devices. Additionally, I have significant expertise in fraud detection, particularly for payment systems.

I have a strong interest in solutions that can be deployed in both the short and long terms, and am actively engaging both industry and government in this capacity. My research, if successful, will help to not only improve the general security of networked devices, but also to maintain the historical reliability of telephony networks as they become the dominant digital access technology.

I. TEACHING

A. Courses Taught

Semester/Year	Course Number & Title	Number of Students	Comments
Fall 2022	CNT 5410 Computer and Network Security	75	New Topics
Fall 2021	CNT 5410 Computer and Network Security	45	New Topics
Fall 2019	CNT 5410 Computer and Network Security	28	New Topics
Fall 2018	CIS 6930 Cellular and Mobile Network Security	16	New Course
Fall 2017	CNT 5410 Computer and Network Security	27	New Topics
Fall 2016	CNT 5410 Computer and Network Security	60	New Topics
Spring 2016	CNT 5410 Computer and Network Security	13	New Topics
Spring 2015	CNT 5410 Computer and Network Security	12	New Topics
Fall 2014	CNT 5410 Computer and Network Security	30	New Course
Spring 2014	CS 6262 Network Security	55	New Projects
Fall 2013	CS 3251 Computer Networks I	73	Expanded Syllabus
Spring 2013	CS 6262 Network Security	65	All New Projects
	CS 8001 Information Security Seminar	20	New Speakers
Fall 2012	CS 8803 Cellular & Mobile Network Security	17	New Topics
	CS 8001 Information Security Seminar	20	New Speakers
Spring 2011	CS 8001 Information Security Seminar	20	New Speakers
Fall 2011	CS 6262 Network Security	27	Expanded Syllabus
	CS 8001 Information Security Seminar	35	New Speakers
Spring 2011	CS 3251 Computer Networks I	61	Expanded Syllabus
	CS 8001 Information Security Seminar	20	New Speakers
Fall 2010	CS 8803/4803 Cellular & Mobile Network Security	16	New Course
	CS 8001 Information Security Seminar	31	New Speakers
Fall 2009	CS 6262 Network Security	55	Expanded Syllabus
Spring 2009	CS 3251 Computer Networks I	45	Expanded Syllabus
Fall 2008	CS 8003 Destructive Research	10	New Course

Guest lecturer for CS 4235 (Introduction to Information Security) and CS 8803 (e-Democracy) in Fall 2008.

Advised ECE 4811/CS 4802 (Vertically Integrated Project) with Ed Coyle

B. Continuing Education

None.

C. Curriculum Development

CS 8803 Cellular and Mobile Network Security: *Fall 2010.* Developed an entirely new course around security issues facing cellular and mobile networks. Students learned about wireless basics, spectrum issues, core network architectures (GSM, ISDN, IMS, SIP), air interfaces (GSM, 3G), mobility management, authentication, mobile phone operating systems (Android, iPhone), Android security, congestion and denial of service, privacy and eavesdropping. Students also complete a research project and aim towards publishing this work at a major venue. My aim is for this class to become part of the regular offering of security courses and receive a non-8803 number. Semester projects were also judged and encouraged using a "venture capital" model, in which students had to pretend as if they were pitching their ideas for a start-up

company to potential investors.

CS 6262 Network Security: *Fall 2009.* Totally rewrote the syllabus and slide material, giving the class its first major overhaul in a number of years. While many old themes remain, new lecture blocks including Web Security, Cellular Security and Social Engineering were developed from scratch. This new course material was made available to all other faculty members teaching this class, who have since used my slides and syllabus.

CS 3251 Computer Networks I: *Spring 2009.* Modified undergraduate networking course to include a persistent focus on security at all layers of the protocol stack. I have also created new lectures focusing on the physical layer and cellular networks and new exams to include all of the abovementioned changes.

CS 8803 Destructive Research: *Fall 2008.* Developed course based around understanding how so-called secure systems have been defeated by attackers. With such knowledge, students would have the context to develop the next generation of more secure systems. I delivered more than 1/3 of the lectures in this seminar course and paid special focus on vulnerabilities in cellular networks, analog telecommunications and electronic voting. Students were also instructed on techniques for performing research, writing technical papers and making conference and lecture-style presentations. I have offered these slides to future 7001 classes to help impact a wider audience.

D. Individual Student Guidance

1. Research Scientists Supervised

None.

2. Ph.D. Students Graduated

Chaitrali Amrutkar Georgia Institute of Technology
Fall 2009–Fall 2013
Her research discovered vulnerabilities in mobile web browsers and developed techniques to detect malicious mobile web pages. Joined Oracle in Spring 2014.

Jasmine Bowers University of Florida
Fall 2015–Summer 2020
Her research focuses on mobile applications, and the development of tools for building secure systems. Now: Research Scientist, MITRE

Henry "Hank" Carter Georgia Institute of Technology
Fall 2010–Spring 2016
Developing techniques for secure function evaluation for privacy-preserving applications on constrained mobile devices. Now: Assistant Professor, Villanova University

Italo Dacosta Georgia Institute of Technology
Fall 2008–Summer 2012
Co-advised with Mustaque Ahamad. Research on scaling performance of SIP network components. Graduated Summer 2012, currently research scientist at EPFL.

David Dewey Georgia Institute of Technology
Fall 2011–Summer 2015
Investigated compiler techniques to remove software vulnerabilities from code. Now CTO of MailChimp.

Brad Reaves University of Florida
Fall 2014–Spring 2017
Develop strong authentication techniques for cellular networks. Now: Assistant Professor at North Carolina State University.

Nolen Scaife University of Florida
Fall 2014–Spring 2019
Developed techniques to detect credit card skimming. First: Assistant Professor at the University of Colorado Boulder. Now: Director, Global Cyber Intelligence at Walmart

Imani Sherman University of Florida
Fall 2018–Summer 2021
Developing usable interfaces against robocalls. Co-advised with Juan Gilbert. Now: Assistant Professor at the University of California, San Diego

Luis Vargas University of Florida
Fall 2016–Summer 2021
Developing techniques for network-based detection and mitigation of malware in a healthcare environment. Now: Data Scientist at the Alethia Group

Hadi Abdullah University of Florida
Fall 2016–Summer 2022
Evaluating the security of ML-driven voice interfaces. Now: Research Scientist at Visa Research

Christian Peeters University of Florida
Fall 2016–Summer 2022
Develop techniques to detect and defend against call and message interception attacks in cellular networks. Now: Research Scientist at Harbor Labs

2. Ph.D. Students Supervised

Logan Blue University of Florida
Fall 2016–Present
Investigating facial feature reconstruction from voice recordings.

Nathaniel Bennett University of Florida
Fall 2022–Present
Finding vulnerabilities in cellular core networks via fuzzing.

Cassidy Gibson University of Florida
Fall 2019–Present
Investigating weaknesses in web software.

Ryon Kennedy University of Florida
Fall 2020–Present
Finding vulnerabilities in cellular core networks via fuzzing.

Seth Layton University of Florida
Fall 2020–Present
Detecting deepfakes in audio samples.

Allison Lu University of Florida
Fall 2022–Present
Measuring repeatability in computer security.

Daniel Olszewski University of Florida
Fall 2019–Present
Removing unwanted/insecure features from software.

Tyler Tucker University of Florida
Fall 2021–Present
Evaluating the security of Bluetooth/cellular radios.

Kevin Warren University of Florida
Fall 2019–Present
Detecting deepfake audio through linguistic information.

3. Ph.D. Students - Other

Saurabh Chakradeo Georgia Institute of Technology
Fall 2010–Spring 2013
Research exploring malicious mobile applications. Left to join Facebook.

Brendan Dolan-Gavitt Georgia Institute of Technology
Spring 2009
Research project on using kernel type graphs to detect dummy structures.

Eric (Yu) Liu Georgia Institute of Technology
Fall 2008
Research on the spread of malcode through cellular infrastructure.

Chaz Lever Georgia Institute of Technology
Fall 2011–Spring 2014
Developing techniques to measure the spread of malware in cellular networks. Left Georgia Tech to create a startup.

Frank Park Georgia Institute of Technology
Fall 2008–Spring 2010
Research on multi-factor authentication using cellular phones. Left program after failing comprehensive exam to join startup.

Ferdinand Schober Georgia Institute of Technology
Fall 2009–Summer 2010
Developed mechanisms for smart networks and smart mobile devices to fight infection and provide remote remediation. Returned to Microsoft.

4. M.S. Students Supervised

Chaitrali Amrutkar Georgia Institute of Technology
Fall 2008–Spring 2009
Research on improving performance of security critical functions in IMS cellular core. Completed her Ph.D with me at GT.

Logan Blue University of Florida
Fall 2015–Spring 2016
Investigated problems of cellular and network security.

David Dewey Georgia Institute of Technology
Fall 2009–Spring 2010
Research on security issues caused by transitive trust assumptions in the Windows COM infrastructure. Completed his Ph.D. with me at GT.

Christopher Grayson Georgia Institute of Technology
Fall 2012–Fall 2013
Developed continuous authentication mechanisms using the multitude of sensors available on a mobile phone. Now at Bishop Fox Consulting (industry).

Young Seuk Kim Georgia Institute of Technology
Fall 2012–Fall 2013
Performed research that compared the security vulnerabilities found in the traditional and mobile web.

Daniel Komaromy Georgia Institute of Technology
Fall 2008–Summer 2009
Research on building a real-time streaming audio system using attribute-based crypto for broadcast encryption.

Nigel Lawrence Georgia Institute of Technology
Fall 2011–Spring 2012
Discovered hijacking attacks in SNMPv3, a widely used and thought to be secure network management protocol. Now at Solute (industry).

Philip Marquardt Georgia Institute of Technology
Fall 2009–Present
Research on developing an iPhone application to prevent individuals from being profiled by Shopper Loyalty Programs. First with MIT Lincoln Labs, now Raytheon

Rishikesh Naik Georgia Institute of Technology
Fall 2008–Spring 2010
Research on converting expensive cryptographic primitives (e.g., Secure Function Evaluation) into efficient applications for mobile phones. Now with Cisco Systems.

Ashish Nautiyal CISE
Fall 2015–Spring 2016
Research on connecting telephone calls to the larger authentication infrastructure.

Nilesh Nipane Georgia Institute of Technology
Fall 2008–Spring 2010
Research on creating provably anonymous networks on a base of secure function evaluation. Now with VMWare.

Walter "Nolen" Sciafe Georgia Institute of Technology
Spring 2012–Spring 2014
Developed the OnionDNS architecture, which prevents domain delisting attacks by leveraging a Tor hidden service. Joined Ph.D. program at UF.

Tyler Tucker University of Florida
Fall 2018–Spring 2021
Evaluating the security of Bluetooth radios.

5. M.S. Special Problems Students

Siddhant Deshmukh University of Florida
Fall 2016–Present
Developed tools for analysis of mobile digital financial services.

Chinmay Gangakhedkar Georgia Institute of Technology
Spring 2009
Research on multi-factor authentication using mobile phones.

Christopher Grayson Georgia Institute of Technology
Spring 2013
Research on continuous authentication using mobile phones.

Aarushi Karnany University of Florida
Fall 2016–Present
Developed tools for analysis of mobile digital financial services.

Rohit Matthews Georgia Institute of Technology
Spring 2011
Developed mobile phone-based tools for measuring performance and reachability throughout the Internet.

Ashwin Narasimhan Georgia Institute of Technology
Spring 2009
Research on developing efficient security mechanisms for the IMS cellular core.

Aamir Poonawalla Georgia Institute of Technology
Spring 2010
Helped develop a call provenance infrastructure, which included both networking and machine learning components.

Erin Reddick Georgia Institute of Technology
Fall 2008–Fall 2009
Research on IPTV security with GTRI.

Lalanthika Vasudevan Georgia Institute of Technology
Spring 2009
Research on developing efficient security mechanisms for the IMS cellular core.

6. Undergraduate Special Problems Students

Ethan Shernan Georgia Institute of Technology
Spring 2014
Developed an infrastructure for detecting billing bypass fraud attacks.

Young Seuk Kim Georgia Institute of Technology
Fall 2011–Spring 2012
Developed a mobile phone application for taking measurements of cellular networks.

Dane Van Dyck Georgia Institute of Technology
Summer 2009
Research on virtualization support for mobile phones.

E. Teaching Honors and Awards

1. Georgia Institute of Technology, CETL "Thanks For Being A Great Teacher" Award, Fall 2013.
2. Georgia Institute of Technology, CETL "Thanks For Being A Great Teacher" Award, Fall 2012.
3. United State Army Signal Corps, "Helmet" Award, 2010.
4. Georgia Institute of Technology, CETL "Thanks For Being A Great Teacher" Award, Spring 2009.
5. Pennsylvania State University CSE Graduate Student Teaching Award, 2005

II. RESEARCH AND CREATIVE SCHOLARSHIP

A. Thesis

1. Patrick Gerard Traynor. *Characterizing the Impact of Rigidity on the Security of Cellular Telecommunications Networks*. PhD thesis, The Pennsylvania State University, May 2008.

B. Published Journal Papers (Refereed)

1. Cassidy Gibson, Vanessa Frost, Katie Platt, Washington Garcia, Luis Vargas, Sara Rampazzi, Vincent Bindschaedler, Patrick Traynor, and Kevin Butler. Analyzing the Monetization Ecosystem of Stalkerware. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2022.

2. Bradley Reaves, Luis Vargas, Nolen Scaife, Dave Tian, Logan Blue, Patrick Traynor, and Kevin Butler. Characterizing the Security of the SMS Ecosystem with Public Gateways. *ACM Transactions on Privacy and Security (TOPS)*, 22(1), 2018.

3. Patrick Traynor, Kevin Butler, Jasmine Bowers, and Bradley Reaves. FinTechSec: Addressing the Scurity Challenges of Digital Financial Services. *IEEE S&P Magazine*, 15(5):85–89, 2017.

4. Nolen Sciafe, Henry Carter, Rachel Jones, Lyrissa Lidsky, and Patrick Traynor. OnionDNS: A Seizure-Resistant Top-level Domain. *International Journal of Information Security (IJIS)*, 2017.

5. Bradley Reaves, Jasmine Bowers, Nolen Scaife, Adam Bates, Arnav Bharatiya, Patrick Traynor, and Kevin Butler. Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World. *ACM Transactions on Privacy and Seurity (TOPS)*, 2017.

6. Henry Carter and Patrick Traynor. OPFE: Outsourcing Computation for Private Function Evaluation. *International Journal of Information and Computer Security (IJICS)*, 2017.

7. Stephan Heuser, Bradley Reaves, Praveen Kumar Pendyala, Henry Carter, Alexandra Dmitrienko, William Enck, Negar Kiyavash, Ahmad-Reza Sadeghi, and Patrick Traynor. Phonion: Practical Protection of Metadata in Telephony Networks. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2017.

8. Bradley Reaves, Jasmine Bowers, Sigmond A. Gorski III, Olabode Anise, Rahul Bobhate, Raymond Cho, Hiranava Das, Sharique Hussain, Hamza Karachiwala, Nolen Scaife, Byron Wright, Kevin Butler, William Enck, and Patrick Traynor. *droid: Assessment and Evaluation of Android Application Analysis Tools. *ACM Computing Surveys (CSUR)*, 2016.

9. Chaitrali Amrutkar, Young Seuk Kim, and Patrick Traynor. Detecting Mobile Malicious Webpages in Real Time. *IEEE Transactions on Mobile Computing (TMC)*, To Appear 2016.

10. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Outsourcing Secure Two-Party Computation as a Black Box. *Journal of Security and Communication Networks (SCN)*, To Appear 2016.

11. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Secure Outsourced Garbled Circuit Evaluation for Mobile Devices. *Journal of Computer Security (JCS)*, 24(2):137–180, 2016.

12. Adam Bates, Kevin Butler, Micah Sherr, Clay Shields, Patrick Traynor, and Dan Wallach. Accountable Wiretapping -or- I Know They Can Hear You Now. *Journal of Computer Security (JCS)*, 23(2):167–195, 2015.

13. Henry Carter, Chaitrali Amrutkar, Italo Dacosta, and Patrick Traynor. For Your Phone Only: Custom Protocols for Efficient Secure Function Evaluation on Mobile Devices. *Journal of Security and Communication Networks (SCN)*, 7(7):1165–1176, 2014.

14. Chaitrali Amrutkar, Patrick Traynor, and Paul van Oorschot. An Empirical Evaluation of Security Indicators in Mobile Web Browsers. *IEEE Transactions on Mobile Computing (TMC)*, 14(5), 2015.

15. Andrew Harris, Seymour Goodman, and Patrick Traynor. Privacy and Security Concerns Associated with Mobile Money Applications in Africa. *Washington Journal of Law, Technology & Arts*, 8(3), 2013.

16. Italo Dacosta, Saurabh Chakradeo, Mustaque Ahamad, and Patrick Traynor. One-Time Cookies: Preventing Session Hijacking Attacks with Stateless Authentication Tokens. *ACM Transactions on Internet Technology (TOIT)*, 12(1), 2012.

17. Cong Shi, Xiapu Luo, Patrick Traynor, Mostafa Ammar, and Ellen Zegura. ARDEN: Anonymous netwoRking in Delay tolErant Networks. *Journal of Ad Hoc Networks*, 10(6):918–930, 2012.

18. Patrick Traynor. Characterizing the Security Implications of Third-Party EAS Over Cellular Text Messaging Services. *IEEE Transactions on Mobile Computing (TMC)*, 11(6):983–994, 2012.

19. Italo Dacosta, Vijay Balasubramaniyan, Mustaque Ahamad, and Patrick Traynor. Improving Authentication Performance of Distributed SIP Proxies. *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, 22(11):1804–1812, 2011.

20. Patrick Traynor, Chaitrali Amrutkar, Vikhyath Rao, Trent Jaeger, Patrick McDaniel, and Thomas La Porta. From Mobile Phones to Responsible Devices. *Journal of Security and Communication Networks (SCN)*, 4(6):719 – 726, 2011.

21. Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Brent Waters. Secure Attribute-Based Systems. *Journal of Computer Security (JCS)*, 18(5):799–837, 2010.

22. Patrick Traynor, Kevin Butler, William Enck, Kevin Borders, and Patrick McDaniel. malnets: Large-Scale Malicious Networks via Compromised Wireless Access Points. *Journal of Security and Communication Networks (SCN)*, 2(3):102–113, 2010.

23. Patrick Traynor. Securing Cellular Infrastructure: Challenges and Opportunities. *IEEE Security & Privacy Magazine*, 7(4), 2009.

24. Kevin Butler, Sunam Ryu, Patrick Traynor, and Patrick McDaniel. Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems. *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, 20(12):1803–1815, 2009.

25. Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta. Mitigating Attacks On Open Functionality in SMS-Capable Cellular Networks. *IEEE/ACM Transactions on Networking (TON)*, 17(1), 2009.

26. Patrick Traynor, Michael Chien, Scott Weaver, Boniface Hicks, and Patrick McDaniel. Non-Invasive Methods for Host Certification. *ACM Transactions on Information and System Security (TISSEC)*, 2008.

27. Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta. Exploiting Open Functionality in SMS-Capable Cellular Networks. *Journal of Computer Security (JCS)*, 16(6):713–742, 2008.

28. Patrick Traynor, Raju Kumar, Heesook Choi, Sencun Zhu, Guohong Cao, and Thomas La Porta. Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks. *IEEE Transactions on Mobile Computing (TMC)*, 6(6), 2007.

C. Published Books and Parts of Books

1. Andrew Harris, Frank S. Park, Seymour Goodman, and Patrick Traynor. *Emerging Privacy and Security Concerns for Digital Wallet Deployment*. Privacy in America: Interdisciplinary Perspectives. Scarecrow Press, July 2011.

2. Kevin Butler, William Enck, Patrick Traynor, Jennifer Plasterr, and Patrick McDaniel. *Privacy Preserving Web-Based Email*. Algorithms, Architectures and Information Systems Security, Statistical Science and Interdisciplinary Research. World Scientific Computing, November 2008.

3. Patrick Traynor, Patrick McDaniel, and Thomas La Porta. *Security for Telecommunications Networks*. Number 978-0-387-72441-6 in Advances in Information Security Series. Springer, August 2008.

D. Edited Proceedings

None.

E. Conference Presentations

E.1. Conference Presentations with Proceedings (Refereed)

1. Christian Peeters, Tyler Tucker, Anushri Jain, Kevin Butler, and Patrick Traynor. LeopardSeal: Detecting Call Interception via Audio Rogue Base Stations. In *Proceedings of the ACM International Conference on Mobile Systems, Applications and Services (MobiSys)*, 2023.

2. Tyler Tucker, Hunter Searle, Kevin Butler, and Patrick Traynor. Blue's Clues: Practical Discovery of Non-Discoverable Bluetooth Devices. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2023.

3. Hadi Abdullah, Aditya Karlekar, Saurabh Prasad, Muhammad Sajidur Rahman, Logan Blue, Luke Bauer, Vincent Bindschaedler, and Patrick Traynor. Attacks as Defenses: Designing Robust Audio CAPTCHAs Using Attacks on Automatic Speech Recognition Systems. In *Symposium on Network and Distributed System Security (NDSS)*, 2023.

4. Daniel Olszewski, Sandeep Sathyanarayana, Weidong Zhu, Kevin Butler, and Patrick Traynor. HallMonitor: A Framework for Identifying Network Policy Violations in Software. In *IEEE Conference on Communications and Network Security (CNS)*, 2022.

5. Hadi Abdullah, Aditya Karlekar, Vincent Bindschaedler, and Patrick Traynor. Demystifying Limited Adversarial Transferability in Automatic Speech Recognition Systems. In *Proceedings of the International Conference on Learning Representations (ICLR)*, 2022. (Acceptance rate: 32%).

6. Logan Blue, Kevin Warren, Hadi Abdullah, Cassidy Gibson, Luis Vargas, Jessica O'Dell, Kevin Butler, and Patrick Traynor. Who Are You (I Really Wanna Know)? Detecting Audio DeepFakes Through Vocal Tract Reconstruction. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2022. (Acceptance rate: 17.2%).

7. Grant Hernandez, Marius Muench, Dominik Maier, Alyssa Milburn, Shinjo Park, Tobias Scharnowski, Tyler Tucker, Patrick Traynor, and Kevin R. B. Butler. FirmWire: Transparent Dynamic Analysis for Cellular Baseband Firmware. In *Symposium on Network and Distributed System Security (NDSS)* , 2022. (Acceptance rate: 16.2%).

8. Christian Peeters, Christopher Patton, Imani N. Sherman, Daniel Olszewski, Thomas Shrimpton, and Patrick Traynor. SMS OTP Security (SOS): Hardening SMS-Based Two Factor Authentication. In *ACM Asia Conference on Computer and Communications Security (ASIACCS)*, 2022. (Acceptance rate: 18.2%).

9. Hadi Abdullah, Muhammad Sajidur Rahman, Christian Peeters, Cassidy Gibson, Washington Garcia, Vincent Bindschaedler, Thomas Shrimpton, and Patrick Traynor. Beyond L_p Clipping: Equalization based Psychoacoustic Attacks against ASRs. In *The Asian Conference on Machine Learning (ACML)*, 2021.

10. Imani Sherman and Daniel Delgado and Juan Gilbert and Jaime Ruiz and Patrick Traynor. Characterizing User Comprehension in the STIR/SHAKEN Anti-Robocall Standard. In *Proceedings of the Annual Research Conference on Comunications Information and Internet Policy (TPRC 49)*, 2021.

11. Hadi Abdullah, Kevin Warren, Vincent Bindschaedler, Nicolas Papernot, and Patrick Traynor. The Faults in our ASRs: An Overview of Attacks against Automatic Speech Recognition and Speaker Identification Systems. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2021. (Acceptance rate: 12.1%).

12. Hadi Abdullah, Muhammad Sajidur Rahman, Washington Garcia, Logan Blue, Kevin Warren, Anurag Swarnim Yadav, Tom Shrimpton, and Patrick Traynor. Hear "No Evil", See "Kenansville": Efficient and Transferable Black-Box Attacks on Speech Recognition and Voice Identification Systems. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2021. (Acceptance rate: 12.1%).

13. Imani Sherman, Jasmine Bowers, Liz-Laure Laborde, Juan E. Gilbert, Jaime Ruiz, and Patrick Traynor. Truly Visual Caller ID? An Analysis of Anti-Robocall Applications and their Accessibility to Visually Impaired Users. In *IEEE International Symposium on Technology and Society (IEEE ISTAS)*, 2020.

14. Imani Sherman, Jasmine Bowers, Keith McNamara, Juan Gilbert, Jaime Ruiz, and Patrick Traynor. Are You Going to Answer That? Measuring User Responses to Anti-Robocall Application Indicators. In *Proceedings of the ISOC Network & Distributed Systems Security Symposium (NDSS)*, 2020. (Acceptance rate: 17.4%).

15. Joseph Choi, Dave Tian, Grant Hernandez, Christopher Patton, Benjamin Mood, Thomas Shrimpton, Patrick Traynor, and Kevin Butler. A Hybrid Approach to Secure Function Evaluation Using SGX. In *Procedings of the ACM ASIA Conference on Computer and Communications Security (ASIACCS'19)*, 2019. (Acceptance Rate: 17.0% for full papers).

16. Vanessa Frost, Dave Tian, Christie Ruales, Patrick Traynor, and Kevin Butler. Examining DES-based Cipher Suite Support within the TLS Ecosystem. In *Proceedings of the ACM ASIA Conference on Computer and Communications Security (ASIACCS'19)*, 2019. (Acceptance Rate: 22.0% for all papers).

17. Dave Tian, Joseph Choi, Grant Hernandez, Patrick Traynor, and Kevin Butler. A Practical Intel SGX Setting for Linux Containers in the Cloud. In *Proceedings of the ACM Conference on Data and Application Security and Privacy (CODASPY'19)*, 2019. (Acceptance rate: 23.5%).

18. Nolen Scaife, Jasmine Bowers, Christian Peeters, Grant Hernandez, Imani Sherman, Lisa Anthony, and Patrick Traynor. Kiss from a Rogue: Evaluating Detectability of Pay-at-the-Pump Card Skimmers. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2019. (Acceptance rate: 12.0%).

19. Jasmine Bowers, Imani Sherman, Kevin Butler, and Patrick Traynor. Characterizing Security and Privacy Practices in Emerging Digital Credit Applications. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2019. (Acceptance rate: 25.6%).

20. Hadi Abdullah, Washington Garcia, Christian Peeters, P. Traynor, K. Butler, and J. Wilson. Practical Hidden Voice Attacks against Speech and Speaker Recognition Systems. In *Proceedings of the ISOC Network & Distributed Systems Security Symposium (NDSS)*, 2019. (Acceptance Rate: 17.1%).

21. Lius Vargas, Logan Blue, Vanessa Frost, Christopher Patton, N. Scaife, K. Butler, and P. Traynor. Digital Healthcare-Associated Infection Analysis of a Major Multi-Campus Hospital System. In *Proceedings of the ISOC Network & Distributed Systems Security Symposium (NDSS)*, 2019. (Acceptance Rate: 17.1%).

22. Dominik Wermke, Nicolas Huaman, Yasemin Acar, Bradley Reaves, Patrick Traynor, and Sascha Fahl. A Large Scale Investigation of Obfuscation Use in Google Play. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2018. Acceptance Rate: 20.1%.

23. Nolen Scaife, Christian Peeters, and Patrick Traynor. Fear the Reaper: Characterization and Fast Detection of Card Skimmers. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2018. Acceptance Rate: 19.0%.

24. Dave (Jing) Tian, Grant Hernandez, Joseph Choi, Vanessa Frost, Christie Raules, Kevin Butler, Patrick Traynor, Hayawardh Vijayakumar, Lee Harrison, Amir Rahmati, and Mike Grace. ATtention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2018. Acceptance Rate: 19.0%.

25. Logan Blue, Hadi Abdullah, Luis Vargas, and Patrick Traynor. 2MA: Verifying Voice Commands via Two Microphone Authentication. In *ACM Asia Conference on Computer and Communications Security (ASIACCS)*, 2018. (Acceptance Rate: 20.0%).

26. Nolen Scaife, Christian Peeters, Camilo Velez, Hanqing Zhao, Patrick Traynor, and David Arnold. The Cards Aren't Alright: Detecting Counterfeit Gift Cards Using Encoding Jitter. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2018. (Acceptance Rate: 10.4%).

27. Christian Peeters, Hadi Abdullah, Nolen Scaife, Jasmine Bowers, Patrick Traynor, Bradley Reaves, and Kevin Butler. Sonar: Detecting SS7 Redirection Attacks Via Call Audio-Based Distance Bounding. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2018. (Acceptance Rate: 10.4%).

28. Tyler Ward, Joseph Choi, Kevin Butler, John M. Shea, Patrick Traynor, and Tan Wong. Privacy Preserving Localization Using a Distributed Particle Filtering Protocol. In *IEEE MILCOM*, 2017. (Acceptance Rate: 56%).

29. Bradley Reaves and Logan Blue and Hadi Abdullah and Luis Vargas and Patrick Traynor and Thomas Shrimpton. AuthentiCall: Efficient Identity and Content Authentication for Phone Calls. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2017. (Acceptance Rate: 16.3%).

30. Jasmine Bowers and Bradley Reaves and Imani N. Sherman and Patrick Traynor and Kevin Butler. Regulators, Mount Up! Analysis of Privacy Policies for Mobile Money Applications. In *Proceedings of the USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2017. (Acceptance Rate: 26.5%).

31. Bradley Reaves, Logan Blue, and Patrick Traynor. AuthLoop: End-to-End Cryptographic Authentication for Telephony over Voice Channels. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2016. (Acceptance Rate: 15.5%).

32. Dave Tian, Nolen Scaife, Adam Bates, Kevin Butler, and Patrick Traynor. Making USB Great Again with USBFILTER. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2016. (Acceptance Rate: 15.5%).

33. Bradley Reaves, Dave Tian, Logan Blue, Patrick Traynor, and Kevin Butler. Detecting SMS Spam in the Age of Legitimate Bulk Messaging. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2016. (Acceptance Rate: 35.0%).

34. Nolen Scaife, Henry Carter, Patrick Traynor, and Kevin Butler. CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. In *IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2016. (Acceptance Rate: 17.6%).

35. Bradley Reaves, Nolen Scaife, Dave Tian, Logan Blue, Patrick Traynor, and Kevin Butler. Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2016. (Acceptance Rate: 13.0%).

36. Benjamin Mood, Debayan Gupta, Henry Carter, Kevin Butler, and Patrick Traynor. Frigate: A Validated, Extensible, and Efficient Compiler and Interpreter for Secure Computation. In *Proceedings of the IEEE European Symposium on Security and Privacy*, 2016. (Acceptance Rate: 17.3%).

37. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Outsourcing Secure Two-Party Computation as a Black Box. In *Proceedings of the International Conference on Cryptology and Network Security*, 2015. (Acceptance Rate: 52.9%).

38. Nolen Sciafe, Henry Carter, and Patrick Traynor. OnionDNS: A Seizure-Resistant Top-level Domain. In *Proceedings of the IEEE Conference on Communications and Network Security (CNS)*, 2015. (Acceptance Rate: 28.1%).

39. Bradley Reaves, Nolen Scaife, Adam Bates, Patrick Traynor, and Kevin Butler. Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2015. (Acceptance Rate: 15.7%).

40. Bradley Reaves, Ethan Shernan, Adam Bates, Henry Carter, and Patrick Traynor. Boxed Out: Blocking Cellular Interconnect Bypass Fraud at the Network Edge. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2015. (Acceptance Rate: 15.7%).

41. David Dewey, Bradley Reaves, and Patrick Traynor. Uncovering Use-After-Free Conditions In Compiled Code. In *Proceedings of the International Conference on Availability, Reliability and Security (ARES)*, 2015. (Acceptance Rate: 22%).

42. Ethan Shernan, Henry Carter, Dave Tian, Patrick Traynor, and Kevin Butler. More Guidelines Than Rules: CSRF Vulnerabilities from Noncompliant OAuth 2.0 Implementations. In *Proceedings of the International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA)*, 2015. (Acceptance Rate: 22.7%).

43. Henry Carter, Charles Lever, and Patrick Traynor. Whitewash: Outsourcing Garbled Circuit Generation for Mobile Devices. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2014. (Acceptance Rate: 19.9%).

44. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Secure Outsourced Garbled Circuit Evaluation for Mobile Devices. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2013. (Acceptance Rate: 16.2%).

45. Chaitrali Amrutkar, Matti Hiltunen, Shobha Venkataraman, Kaustubh Joshi, Patrick Traynor, Trevor Jim, and Oliver Spatscheck. Why is My Smartphone Slow? On The Fly Diagnosis of Poor Performance on the Mobile Internet. In *Proceedings of The 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2013. (Acceptance Rate: 19.6%).

46. Saurabh Chakradeo, Brad Reaves, Patrick Traynor, and William Enck. MAST: Triage for Market-scale Mobile Malware Analysis. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2013. (Acceptance Rate: 15.0%)(Best Paper).

47. Charles Lever, Manos Antonakakis, Brad Reaves, Patrick Traynor, and Wenke Lee. The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2013. (Acceptance rate: 18.8%).

48. Chaitrali Amrutkar, Kapil Singh, Arunabh Verma, and Patrick Traynor. VulnerableMe: Measuring Systemic Weaknesses in Mobile Browser Security. In *Proceedings of the International Conference on Information Systems Security (ICISS)*, 2012. (Acceptance rate: 25%) (Best Paper - SAIC Student Paper Competition (GT)) (Finalist - CSAW AT&T Applied Security Research Best Paper Competition 2012).

49. Chaitrali Amrutkar, Patrick Traynor, and Paul van Oorschot. A Measurement Study of SSL Indicators on Mobile Browsers: Extended Life, or End of the Road? In *Proceedings of the Information Security Conference (ISC)*, 2012. (Acceptance rate: 32%) (Best Student Paper).

50. Italo Dacosta, Mustaque Ahamad, and Patrick Traynor. Trust No One Else: Detecting MITM Attacks Against SSL/TLS Without Third-Parties. In *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, 2012. (Acceptance Rate: 20.2%).

51. Adam Bates, Kevin Butler, Micah Sherr, Clay Shields, Patrick Traynor, and Dan Wallach. Accountable Wiretapping -or- I Know They Can Hear You Now. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2012. (Acceptance Rate: 17.8%).

52. Yacin Nadji, Jon Giffin, and Patrick Traynor. Automated Remote Repair for Mobile Malware. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2011. (Acceptance Rate: 18.5%).

53. Nilesh Nipane, Italo Dacosta, and Patrick Traynor. "Mix-In-Place" Anonymous Networking Using Secure Function Evaluation. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2011. (Acceptance Rate: 18.5%).

54. Philip Marquardt, Arunabh Verma, Henry Carter, and Patrick Traynor. (sp)iPhone: Decoding Vibrations From Nearby Keyboards Using Mobile Phone Accelerometers. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2011. (Acceptance Rate: 13.9%).

55. Philip Marquardt, David Dagon, and Patrick Traynor. Impeding Individual User Profiling in Shopper Loyalty Programs. In *Proceedings of the International Conference on Financial Cryptography and Data Security (FC)*, 2011. (Acceptance Rate: 35.1%).

56. David Dewey and Patrick Traynor. No Loitering: Exploiting Lingering Vulnerabilities in Default COM Objects. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2011. (Acceptance Rate: 20.1%).

57. Vijay Balasubramaniyan, Aamir Poonawalla, Mustaque Ahamad, Michael Hunter, and Patrick Traynor. PinDr0p: Using Single-Ended Audio Features to Determine Call Provenance. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2010. (Acceptance Rate: 17.2%).

58. Patrick Traynor, Joshua Schiffman, Thomas La Porta, Patrick McDaniel, Abhrajit Ghosh, and Farooq Anjum. Constructing Secure Localization Systems with Adjustable Granularity. In *IEEE Global Communications Conference (GLOBECOM)*, 2010. (Acceptance Rate: 35.6%).

59. Patrick Traynor. Characterizing the Security Implications of Third-Party EAS Over Cellular Text Messaging Services. In *Proceedings of the Second IEEE International Conference on Security and Privacy in Communication Networks (SecureComm)*, 2010. (Acceptance Rate: 25.0%).

60. Kapil Singh, Samrit Sangal, Nehil Jain, Patrick Traynor, and Wenke Lee. Evaluating Bluetooth as a Medium for Botnet Command and Control. In *Proceedings of the International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA)*, 2010. (Acceptance Rate: 30.7%).

61. Italo Dacosta and Patrick Traynor. Proxychain: Developing a Robust and Efficient Authentication Infrastructure for Carrier-Scale VoIP Networks. In *Proceedings of the USENIX Annual Technical Conference (ATC)*, 2010. (Acceptance Rate: 17.0%).

62. Frank S. Park, Chinmay Gangakhedkar, and Patrick Traynor. Leveraging Cellular Infrastructure to Improve Fraud Prevention. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2009. (Acceptance Rate: 19.0%).

63. Patrick Traynor, Michael Lin, Machigar Ongtang, Vikyath Rao, Trent Jaeger, Thomas La Porta, and Patrick McDaniel. On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2009. (Acceptance Rate: 18.4%).

64. Brendan Dolan-Gavitt, Abhinav Srivastava, Patrick Traynor, and Jonathon Giffin. Robust Signatures for Kernel Data Structures. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2009. (Acceptance Rate: 18.4%).

65. Italo Dacosta, Vijay Balasubramaniyan, Mustaque Ahamad, and Patrick Traynor. Improving Authentication Performance of Distributed SIP Proxies. In *Proceedings of the Conference on Principles, Systems and Applications of IP Telecommunications (IPTComm)*, 2009. (Acceptance Rate: 43.3%).

66. Patrick Traynor, Kevin Butler, William Enck, and Patrick McDaniel. Realizing Massive-Scale Conditional Access Systems Through Attribute-Based Cryptosystems. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2008. (Acceptance Rate: 17.7%).

67. Patrick Traynor, Patrick McDaniel, and Thomas La Porta. On Attack Causality in Internet-Connected Cellular Networks. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2007. (Acceptance Rate: 12.3%).

68. Sunam Ryu, Kevin Butler, Patrick Traynor, and Patrick McDaniel. Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems. In *Proceedings of the IEEE International Symposium on Security in Networks and Distributed Systems (SSNDS)*, 2007. (Acceptance Rate: 40%).

69. Luke St. Clair, Lisa Johansen, William Enck, Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Trent Jaeger. Password Exhaustion: Predicting the End of Password Usefulness. In *Proceedings of the International Conference on Information Systems Security (ICISS)*, 2006. (Invited Paper).

70. Kevin Butler, William Enck, Jennifer Plasterr, Patrick Traynor, and P. McDaniel. Privacy-Preserving Web-Based Email. In *Proceedings of the International Conference on Information Systems Security (ICISS)*, December 2006. (Acceptance Rate: 30.4%).

71. Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Brent Waters. Secure Attribute-Based Systems. In *Proceedings of the Thirteenth ACM Conference on Computer and Communications Security (CCS)*, November 2006. (Acceptance Rate: 14.8%).

72. Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta. Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks. In *Proceedings of the Twelfth Annual ACM International Conference on Mobile Computing and Networking (MobiCom)*, September 2006. (Acceptance Rate: 11.7%).

73. Patrick Traynor, Michael Chien, Scott Weaver, Boniface Hicks, and Patrick McDaniel. Non-Invasive Methods for Host Certification. In *Proceedings of the Second IEEE International Conference on Security and Privacy in Communication Networks (SecureComm)*, August 2006. (Acceptance Rate: 25.4%).

74. Patrick Traynor, JaeShung Shin, Barat Madan, Shashi Phoha, and Thomas La Porta. Efficient Group Mobility for Heterogeneous Sensor Networks. In *Proceedings of the IEEE Vehicular Technology Conference (VTC Fall)*, September 2006. (Acceptance Rate: 58%).

75. Patrick Traynor, Raju Kumar, Hussain Bin Saad, Guohong Cao, and Thomas La Porta. LIGER: Implementing Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks. In *Proceedings of the 4th ACM International Conference on Mobile Systems, Applications and Services (MobiSys)*, June 2006. (Acceptance Rate: 15.4%).

76. Patrick Traynor, Guohong Cao, and Thomas La Porta. The Effects of Probabilistic Key Management on Secure Routing in Sensor Networks. In *Proceedings of the 2006 IEEE Wireless Communications and Networking Conference (WCNC)*, April 2006. (Acceptance Rate: 38.8%).

77. Patrick Traynor, Heesook Choi, Guohong Cao, Sencun Zhu, and Thomas La Porta. Establishing Pair-Wise Keys In Heterogeneous Sensor Networks. In *Proceedings of the 25th Annual IEEE Conference on Computer Communications (INFOCOM)*, April 2006. (Acceptance Rate: 18%).

78. William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta. Exploiting Open Functionality in SMS-Capable Cellular Networks. In *Proceedings of the Twelfth ACM Conference on Computer and Communications Security (CCS)*, November 2005. (Acceptance Rate: 15%).

Removed for external version.

E.2. Conference Presentations with Proceedings (Non-Refereed)

None.

E.3. Conference Presentations without Proceedings

1. Patrick Traynor. Work in Progress Presentations: Fine-Grained Secure Localization for 802.11 Networks. 15th USENIX Security Symposium (SECURITY), August 2006.

2. Patrick Traynor. Work in Progress Presentations: Fundamental Limitations of Sensor Network Security. ACM/USENIX Fourth International Conference on Mobile Systems Applications and Services (MobiSys), June 2006. (Award: Most Entertaining WIP).

3. Patrick Traynor, Heesook Choi, Guohong Cao, and Thomas La Porta. Poster Session: Probabilistic Unbalanced Key Distribution and Its Effects on Distributed Sensor Networks. Workshop on Wireless Security (WiSe), October 2004.

F. Other

F.1. Submitted Journal Papers

None.

F.2. Refereed Research Reports

None.

F.3. Software

1. *GSM Air Interface Simulator:* Developed a full voice, data and SMS capable simulator for the wireless portion of a GSM network. Models communications down to the timeslot for highest possible accuracy. Used in the majority of our work on cellular security.

2. *Malicious Telephony Load Tester:* Built a system on top of the TM1 Telecom Database testing suite to allow for a comparison of malicious traffic of varying composition.

F.4. Published Papers (Non-Refereed)

1. Patrick Traynor. Characterizing the Limitations of Third-Party EAS Over Cellular Text Messaging Services. Technical report, 3G Americas Whitepaper, 2008.

2. Lisa Johansen, Kevin Butler, William Enck, Patrick Traynor, and Patrick McDaniel. Grains of SANs: Building Storage Area Networks from Memory Spots. Technical Report NAS-TR-0060-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, 2007.

F.5. Books in Preparation

None.

F.6. Workshops and External Courses

1. Luis Vargas, Patrick Emami, and Patrick Traynor. On the Detection of Disinformation Campaign Activity with Network Analysis. In *Proceedings of the 2020 ACM SIGSAC Cloud Computing Security Workshop*, CCSW '20, 2020.

2. Siddhant Deshmukh, Henry Carter, Grant Hernandez, Patrick Traynor, and Kevin Butler. Efficient and Secure Template Blinding for Biometric Authentication. In *IEEE Workshop on Security and Privacy in the Cloud (SPC)*, 2016.

3. Debayan Gupta, Benjamin Mood, Joan Feigenbaum, Kevin Butler, and Patrick Traynor. Using Intel Software Guard Extensions for Efficient Two-Party Secure Function Evaluation. In *Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC)*, 2016.

4. Chaitrali Amrutkar and Patrick Traynor. Rethinking Permissions for Mobile Web Apps: Barriers and the Road Ahead. In *Proceedings of the ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, 2012.

5. Nigel Lawrence and Patrick Traynor. Under New Management: Practical Attacks on SNMPv3. In *Proceedings of the USENIX Workshop on Offensive Technologies (WOOT)*, 2012.

6. Andrew Harris, Frank S. Park, Seymour Goodman, and Patrick Traynor. Emerging Privacy Concerns for Digital Wallet Deployment. In *Proceedings of the Workshop on Making Privacy in America*, 2009.

7. Patrick Traynor. Privacy and Security Concerns for Personal and Mobile Health Devices. In *Proceedings of the Workshop to Set A Research Agenda for Privacy and Security of Healthcare Technologies*, 2009.

8. Kevin Butler, William Enck, Harri Hursti, Stephen McLaughlin, Patrick Traynor, and Patrick McDaniel. Systemic Issues in the Hart InterCivic and Premier Voting System: Reflections Following Project EVEREST. In *Proceedings of the USENIX/ACCURATE Electronic Voting Technology (EVT) Workshop*, 2008.

G. Research Proposals and Grants (Principal Investigator)

1. Approved and Funded

1. **Testing Audio Deep Fake Detectors**
   Sponsor: Bank of America
   Investigator(s): Patrick Traynor (PI), Kevin Butler
   Amount: *$274,000 over 2 years*
   Awarded: August 2021

2. **Deploying Defenses for Cellular Networks Using the AWARE Testbed**
   Sponsor: Department of Homeland Security: CISA:
   Investigator(s): Patrick Traynor (PI), Kevin Butler, Guofei Gu, Radu Stoleru, Walter Magnussen, P. R. Kumar
   Amount: *$3,100,000 over 4 years*
   Awarded: October 2019

3. **SaTC:CORE:Medium: Securing the Voice Processing Pipeline Against Adversarial Audio**
   Sponsor: NSF Secure and Trustworthy Cyberspace
   Investigator(s): Patrick Traynor (PI), Thomas Shrimpton, Vincent Bindschaedler
   Amount: *$1,199,999 over 4 years*
   Awarded: October 2019

4. **Artus Protocol STTR Phase II**
   Sponsor: Office of Naval Research
   Investigator(s): Patrick Traynor (PI), Kevin Butler
   Amount: *$800,000 over 4 years*
   Awarded: August 2019

5. **Evaluating the Security of QR Code-Based Payments**
   Sponsor: Discover Financial
   Investigator(s): Patrick Traynor (PI)
   Amount: *$50,000 over 1 year*
   Awarded: September 2018

6. **Workshop: Addressing the Technical Security Challenges of Emerging Digital Financal Services**
   Sponsor: NSF Secure and Trustworthy Cyberspace
   Investigator(s): Patrick Traynor (PI), Kevin Butler
   Amount: *$50,000 over 1 year*
   Awarded: September 2017

7. **Designing Strong End-to-End Authentication Mechanisms for Modern Telephony Systems**
   Sponsor: NSF Secure and Trustworthy Cyberspace
   Investigator(s): Patrick Traynor (PI)
   Amount: *$500,000 over 3 years*
   Awarded: July 2016

8. **Digital Healthcare-Associated Infection: Measurement, Defense and Prevention in a Modern Digital Healthcare Ecosystem**
   Sponsor: National Science Foundation
   Investigator(s): Patrick Traynor (PI), Kevin Butler, Shigang Chen
   Amount: *$1,200,000 over 4 years*
   Awarded: June 2016

9. **Evaluating and Improving Security in Emerging Branchless Banking Systems**
   Sponsor: NSF Secure and Trustworthy Cyberspace
   Investigator(s): Patrick Traynor (PI)
   Amount: *$500,000 over 3 years*
   Awarded July 2015

10. **Prevention and Detection of Disallowed Connections in Mobile and Pervasive Systems**
    Sponsor: CISE-ECE Harris Endowed Seed Fund Program
    Investigator(s): Patrick Traynor (PI), Renato Figueiredo (PI)
    Amount: *$40,000 over 1 year*
    Awarded December 2014

11. **Mobile Excursion Study Support**
    Sponsor: Hanscom AFB Electronic Systems Command Development Planning Division (ESC/XR)
    Investigator(s): Patrick Traynor (PI), Mustaque Ahamad, Jeff Evans, Chuck Bokath
    Amount: *$280,000 over 3 months*
    Awarded July 2012

12. **Characterizing the Security Limitations of Accessing the Mobile Web**
    Sponsor: NSF Secure and Trustworthy Cyberspace
    Investigator(s): Patrick Traynor (PI) and William Enck (NC State)
    Amount: *$334,000 over 3 years*
    Awarded July 2012

13. **Mitigating Attacks on Mobile Devices and Critical Cellular Infrastructure**
    Sponsor: US Department of Defense - Defense University Research Instrumentation Program (DURIP)
    Investigator(s): Patrick Traynor (PI), Jon Giffin, Mustaque Ahamad
    Amount: *$210,081 over 1 year*
    Awarded June 2011

14. **Characterizing and Implementing Efficient Primitives for Privacy-Preserving Computation**
    Sponsor: DARPA PROgramming Computation on EncryptEd Data (PROCEED) – Broad Agency Announcement
    Investigator(s): Patrick Traynor (PI) and Kevin Butler (UOregon)
    Amount: *$580,000 over 4 years*
    Awarded May 2011

15. **Security for Converged IMS Networks**
    Sponsor: US Department of Defense
    Investigator(s): Patrick Traynor (PI), Mustaque Ahamad and Russ Clark
    Amount: *$242,401 over 1 year*
    Awarded August 2010

16. **CAREER: Protecting User Data on Lost, Stolen and Damaged Mobile Phones**
    Sponsor: NSF Trustworthy Computing
    Investigator(s): Patrick Traynor (PI)
    Amount: *$400,000 over 5 years*
    Awarded: May 2010

17. **Provably Anonymous Networking Through Secure Function Evaluation**
    Sponsor: NSF Trustworthy Computing
    Investigator(s): Patrick Traynor (PI)
    Amount: *$200,000 over 2 years*
    Awarded: July 2009

18. **Characterizing and Mitigating Device-Based Attacks in Cellular Telecommunications Networks**
Sponsor: NSF Trustworthy Computing
Investigator(s): Patrick Traynor (PI) and Jonathon Giffin
Amount: *$450,000 over 3 years*
Awarded: July 2009

2. Pending

Removed for external version.

H. Research Proposals and Grants (Contributor)

1. Approved and Funded

1. **SaTC: Frontier: Securing the Future of Computing for Marginalized and Vulnerable Populations**
Sponsor: NSF SaTC
Investigator(s): Kevin Butler (PI), Patrick Traynor, Tadayoshi Kohno, Franzi Roesner, Apu Kapadia, Eakta Jain.
Amount: *$7,500,000 for 5 years*
Awarded October 2022

2. **ROCKY: Reliable Obfuscated Communications Kit for everYone**
Sponsor: DARPA Resilient Anonymous Communication for Everyone (RACE) – Broad Agency Announcement
Investigator(s): Thomas Shrimpton (PI), Patrick Traynor, Kevin Butler, Vincent Bindschaedler, Nadia Heninger
Amount: *$1,600,000 over 4 years*
Awarded May 2019

3. **WiFiUS: Collaborative Research: SELIOT: Securing Lifecycle of Internet-of-Things**
Sponsor: NSF CNS WiFiUS
Investigator(s): Gene Tsudik (PI), Patrick Traynor
Amount: *$300,000 for 2 years*
Submitted December 2016

4. **Cloud-based Oblivious Spectrum Mapping and Allocation**
Sponsor: NSF CNS EARS
Investigator(s): John Shea (PI), Tan Wong, Patrick Traynor
Amount: *$532,952 for 2 years*
Submitted May 2016

5. **DURIP: Developing Research Capability in Cyber-Physical Systems at the University of Florida**
Sponsor: Small
Investigator(s): Kevin Butler (PI), Patrick Traynor, My Thai
Amount: *$200,000 for 2 years*
Submitted: June 2015

6. **Securing the New Converged Telephony Landscape**
Sponsor: NSF TWC: Small
Investigator(s): Mustaque Ahamad (PI) and Patrick Traynor
Amount: *$500,000 for 3 years*
Submitted: December 2012

7. **Facilitating Free and Open Access to Information on the Internet**
   Sponsor: NSF Trustworthy Computing
   Investigator(s): Nick Feamster (PI), Wenke Lee, Patrick Traynor, Hans Klein, Roger Dingledine, Michael Freedman and Edward W. Felten
   Amount: *$1,500,000 for 4 years*
   Awarded: June 2011

8. **Monitoring Free and Open Access to Information on the Internet**
   Sponsor: Google Focus Program
   Investigator(s): Nick Feamster (PI), Wenke Lee, Mustaque Ahamad, Patrick Traynor, Henry Owen, Ellen Zegura, Zvi Galil
   Amount: *$1,000,000 for 2 years*
   Awarded: November 2011

9. **Dynamic-attribute-based Disclosure of Health Information in Emergency Care Scenarios**
   Sponsor: Health Systems Institute (HSI) Seed Grant Program
   Investigator(s): Doug Blough (PI), Mustaque Ahamad, Patrick Traynor and Jim Jose
   Amount: *$50,000 over 1 year*
   Awarded: August 2009

10. **Federal Cyber Service Scholarships at Georgia Tech**
    Sponsor: NSF SFS Scholarships
    Investigator(s): Seymour Goodman (PI), Patrick Traynor
    Amount: *$1,250,682 over 5 years*
    Awarded: June 2009

11. **Security for IMS-Enabled Converged Applications**
    Sponsor: US Department of Defense
    Investigator(s): Mustaque Ahamad (PI), Patrick Traynor (PI), Michael Hunter, Russ Clark
    Amount: *$146,121 for 1 year*
    Awarded: August 2008

2. Pending

Removed for external version.

I. Research Honors and Awards

1. Fellow, Center for Financial Inclusion at Accion, 2017.
2. Sloan Research Fellow, Alfred P. Sloan Foundation, 2014.
3. Best Paper, The ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec); Budapest, Hungary, 2013.
4. Best Student Paper, The Information Security Conference (ISC); Passau, Germany, 2012
5. Lockheed Inspirational Young Faculty Award, 2012
6. Best Demo, "Is Browsing the Internet on Your Mobile Phone Secure?" Chaitrali Amrutkar (Ph.D Advisee), CoC Research Day, 2011
7. Best Poster, "(sp)iPhone: Decoding Vibrations From Nearby Keyboards Using Mobile Phone Accelerometers" Arunabh Verma, Henry Carter (MS, Ph.D Advisees), CoC Research Day, 2011
8. National Science Foundation CAREER Award, 2010

9. Pennsylvania State University Alumni Association Dissertation Award, 2007
10. Pennsylvania State University CSE Graduate Research Assistant Award, 2007
11. AT&T Wireless Fellowship, 2005

III. SERVICE

A. Professional Activities

A.1. Memberships and Activities in Professional Societies

1. Senior Member, Association for Computing Machinery (ACM)
2. Senior Member, Institute of Electrical and Electronics Engineers (IEEE)
3. Member, USENIX Advanced Computing Systems Association (USENIX)

A.2. Conference Committee Activities

1. Program co-Chair, *IEEE Symposium on Security and Privacy (OAKLAND)*: 2023, 2024
2. Program co-Chair, *USENIX Security Symposium (SECURITY)*: 2019
3. Program co-Chair, *Network and Distributed System Security Symposium (NDSS)*: 2017, 2018
4. Program Chair, *USENIX Workshop on Offensive Technologies (WOOT)*: 2016
5. Program Chair, *ACM Conference on Wireless Network Security (WiSec)*: 2014
6. Program Co-Chair, *Annual Computer Security Applications Conference (ACSAC)*: 2012, 2013
7. Program Chair, *USENIX Workshop on Hot Topics in Security (HotSec)*: 2012
8. Chair Invited Talks Committee, *USENIX Security Symposium (SECURITY)*: 2014
9. Workshops Chair, *IEEE Conference on Communications and Network Security (CNS)*: 2016
10. Program Committee, *USENIX Security Symposium (SECURITY)*: 2008, 2009, 2010, 2013, 2015-2018, 2020-2022
11. Program Committee, *IEEE Symposium on Security and Privacy (OAKLAND)*: 2009-2014, 2022.
12. Program Committee, *ACM Conference On Computer and Communications Security (CCS)*: 2009, 2013-2015, 2017
13. Program Committee, *Network and Distributed System Security Symposium (NDSS)*: 2010, 2013-2016, 2020-2021
14. Program Committee, *IEEE European Symposium on Security and Privacy (Euro S&P)*: 2016
15. Program Committee, *Annual Computer Security Applications Conference (ACSAC)*: 2008, 2009, 2010, 2011, 2015
16. Program Committee, *ACM Conference on Wireless Network Security (WiSec)*: 2009, 2010, 2013, 2015-2021
17. Program Committee, *International Conference on Financial Cryptography and Data Security (FC)*: 2010, 2013
18. Program Committee, *USENIX Symposium on Operating Systems Design and Implementation (OSDI)*: 2016.
19. Program Committee, *ICST Conference on Security and Privacy in Communication Networks (SecureComm)*: 2009, 2010
20. Program Committee, *Privacy Enhancing Technologies Symposium (PETS)*: 2015, 2016

21. Program Committee, *International World Wide Web Conference (WWW)*: 2016
22. Program Committee, *USENIX Workshop on Hot Topics in Security (HotSec)*: 2011
23. Program Committee, *ACM SIGCOMM Workshop on Networking, Systems, and Applications on Mobile Handhelds (MOBIHELD)*: 2010
24. Program Committee, *International Workshop on Mobile Security (WMS)*: 2010
25. Program Committee, *European Symposium on Research in Computer Security (ESORICS)*: 2009, 2011
26. Program Committee, *IEEE Conference on Mobile Ad-hoc and Sensor Systems (MASS)*: 2009, 2010
27. Program Committee, *Information Security Conference (ISC)*: 2010
28. Program Committee, *IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT)*: 2009
29. Program Committee, *Computer Security Architecture Workshop (CSAW)*: 2008
30. Program Committee, *IWCMC Computer and Network Security Symposium*: 2009
31. Program Committee, *IARIA International Conference on Internet Monitoring and Protection (ICIMP)*: 2009
32. Program Committee, *IEEE Workshop on Network Security and Privacy (NSP)*: 2008
33. Program Committee, *IEEE International Workshop on Wireless and Sensor Networks Security (WSNS)*: 2008, 2009
34. Program Committee, *IEEE Conference on Sensor Networks, Ubiquitous and Trustworthy Computing (SUTC)*: 2008
35. Program Committee, *ACM Conference on Computer and Communications Security, Industry and Government Track (CCS I&G)*: 2006, 2007
36. Program Committee, *Workshop on Secure Network Protocols (NPSec)*: 2006
37. Program Committee, *International Conference on Information Systems Security (ICISS)*: 2006, 2009, 2010
38. Program Committee, *IEEE LCN Workshop on Network Security (WNS)*: 2006, 2007, 2008

B. On-Campus Committees

B.1. University of Florida

1. Member, Computer and Information Science and Engineering Steering Committee, 2015-2017.
2. Member, Graduate Recruiting Committee, 2015-2017.
3. Chair, Computer and Information Science and Engineering Industrial Advisory Board, 2014-2015.

B.2. Georgia Tech

1. Member, Massive Open Online Master's (MOOMS) Investigation Committee, 2012-2013.
2. Chair, School of Computer Science Ph.D. Review Committee, 2012.
3. Member, School of Computer Science Ph.D Review Committee, 2011.
4. Faculty Advisor, Grey H@T - Georgia Tech Undergraduate Security Club, 2011-2014.
5. Member, School of Computer Science Ph.D. Review Committee, 2011.
6. Member, School Advisory Committee, School of Computer Science, 2011-2013.
7. Member, School of Computer Science Chair Recruiting Committee, 2011.
8. Member, School of Computer Science Faculty Recruiting Committee, 2010, 2011.
9. Chair, College of Computing Ph.D. Welcome Weekend Committee, 2009, 2010, 2011 (co-chair).
10. Member, College of Computing Ph.D. Recruiting Committee, 2009.
11. Member, Georgia Tech Computer and Network Usage Security Policy (CNUSP) Evaluation Group, 2009.

C. Special Assignments

None.

D. Ph.D. Examining Committees

Ph.D. Examining Committees

1. Bradley Reaves, Department of Computer and Information Science and Engineering, University of Florida, Summer 2017.
   Advisor: Professor Patrick Traynor.
2. Adam Bates, Department of Computer and Information Science and Engineering, University of Florida, Spring 2016.
   Advisor: Professor Kevin Butler.
3. Benjamin Mood, Department of Computer and Information Science and Engineering, University of Florida, Spring 2016.
   Advisor: Professor Kevin Butler.
4. Henry Carter, College of Computing, Georgia Tech, Fall 2015.
   Advisor: Professor Patrick Traynor.
5. David Dewey, College of Computing, Georgia Tech, Fall 2015.
   Advisor: Professor Patrick Traynor.
6. Lateef Yusuf, College of Computing, Georgia Tech, Spring 2014.
   Advisor: Professor Umakishore Ramachandran.
7. Chaitrali Amrutkar, College of Computing, Georgia Tech, Summer 2013.
   Advisor: Professor Patrick Traynor.
8. Long Lu, College of Computing, Georgia Tech, Summer 2013.
   Advisor: Professor Wenke Lee.

9. Manos Antonakakis, College of Computing, Georgia Tech, Summer 2012.
   Advisor: Professor Wenke Lee.

10. Junjie Zhang, College of Computing, Georgia Tech, Summer 2012.
    Advisor: Professor Wenke Lee.

11. Italo Dacosta, College of Computing, Georgia Tech, Summer 2012.
    Advisor: Professor Patrick Traynor.

12. Virendra Kumar, College of Computing, Georgia Tech, Summer 2012.
    Advisor: Professor Alexandra Boldyreva.

13. Anirudh Ramachandran, College of Computing, Georgia Tech, Summer 2011.
    Advisor: Professor Nick Feamster.

14. Vijay Balasubramaniyan, College of Computing, Georgia Tech, Summer 2011.
    Advisor: Professor Mustaque Ahamad.

15. Kapil Singh, College of Computing, Georgia Tech, Summer 2011.
    Advisor: Professor Wenke Lee.

16. Abhinav Srivastava, College of Computing, Georgia Tech, Summer 2011.
    Advisor: Professor Jon Giffin.

17. Adam O'Neill, College of Computing, Georgia Tech, Summer 2010.
    Advisor: Professor Alexandra Boldyreva.

18. David Cash, College of Computing, Georgia Tech, Fall 2009.
    Advisor: Professor Alexandra Boldyreva.

External Member of Ph.D. Research Committee

None.

External Member of Ph.D. Examining Committee

1. Shannon Eggers, Department of Materials Sciences and Engineering - Nuclear Engineering Program, University of Florida, Fall 2016.
   Advisor: Professor Kelly Jordan.

2. Ed Carlisle, Department of Electrical and Computer Engineering, University of Florida, Summer 2016.
   Advisor: Professor Alan George.

3. Claudio Marforio, Department of Computer Science, Swiss Federal Institute of Technology Zurich (ETH Zurich), Fall 2015.
   Advisor: Professor Srdjan Capkun.

4. Nils Ole Tippenhauer, Department of Computer Science, Swiss Federal Institute of Technology Zurich (ETH Zurich), Spring 2012.
   Advisor: Professor Srdjan Capkun.

5. Bongkyoung Kwon, School of Electrical and Computer Engineering, Georgia Tech, Summer 2009.
   Advisor: Professor John Copeland.

Ph.D. Thesis Proposal Committees

1. Bradley Reaves, Department of Computer and Information Science and Engineering, Spring 2016.
   Advisor: Professor Patrick Traynor.
2. Maliheh Shirvanian, University of Alabama, Birmingham, Spring 2016.
   Advisor: Professor Nitesh Saxena.
3. Benjamin Mood, Department of Computer and Information Science and Engineering, Fall 2015.
   Advisor: Professor Kevin Butler.
4. Adam Bates, Department of Computer and Information Science and Engineering, Fall 2015.
   Advisor: Professor Kevin Butler.
5. Lateef Yusuf, College of Computing, Georgia Tech, Spring 2013.
   Advisor: Professor Umakishore Ramachandran.
6. Long Lu, College of Computing, Georgia Tech, Spring 2013.
   Advisor: Professor Wenke Lee.
7. Chaitrali Amrutkar, College of Computing, Georgia Tech, Fall 2012.
   Advisor: Professor Patrick Traynor.
8. Junjie Zhang, College of Computing, Georgia Tech, Fall 2011.
   Advisor: Professor Wenke Lee.
9. Italo Dacosta, College of Computing, Georgia Tech, Fall 2011.
   Advisor: Professor Patrick Traynor.
10. Manos Antonakakis, College of Computing, Georgia Tech, Fall 2011.
    Advisor: Professor Wenke Lee.
11. Abhinav Srivastava, College of Computing, Georgia Tech, Spring 2011.
    Advisor: Professor Jon Giffin.
12. Vijay Balasubramaniyan, College of Computing, Georgia Tech, Fall 2010.
    Advisor: Professor Mustaque Ahamad.
13. Kapil Singh, College of Computing, Georgia Tech, Fall 2010.
    Advisor: Professor Wenke Lee.
14. Anirudh Ramachandran, College of Computing, Georgia Tech, Fall 2010.
    Advisor: Professor Nick Feamster.
15. Adam O'Neill, College of Computing, Georgia Tech, Spring 2010.
    Advisor: Professor Alexandra Boldyreva.
16. David Cash, College of Computing, Georgia Tech, Spring 2009.
    Advisor: Professor Alexandra Boldyreva.

Ph.D. Qualifying Exam Committees—Georgia Tech

1. Byoungyoung Lee, College of Computing, Georgia Tech, Spring 2013.
   Advisor: Professor Wenke Lee.
2. Yizheng Chen, College of Computing, Georgia Tech, Spring 2013.
   Advisor: Professor Wenke Lee.

3. Xinyu Xing, College of Computing, Georgia Tech, Spring 2013.
   Advisor: Professor Wenke Lee.

4. Brad Reaves, College of Computing, Georgia Tech, Spring 2013.
   Advisor: Professor Patrick Traynor.

5. Chaz Lever, College of Computing, Georgia Tech, Spring 2013.
   Advisor: Professor Patrick Traynor.

6. Terry Nelms, College of Computing, Georgia Tech, Spring 2012.
   Advisor: Professors Mustaque Ahamad and Roberto Perdesci.

7. Saurabh Chakradeo, College of Computing, Georgia Tech, Spring 2012.
   Advisor: Professor Patrick Traynor.

8. Henry Carter, College of Computing, Georgia Tech, Spring 2012.
   Advisor: Professor Patrick Traynor.

9. David Dewey, College of Computing, Georgia Tech, Spring 2012.
   Advisor: Professor Jon Giffin.

10. Chaitrali Amrutkar, College of Computing, Georgia Tech, Fall 2011.
    Advisor: Professor Patrick Traynor.

11. Yacin Nadji, College of Computing, Georgia Tech, Fall 2011.
    Advisor: Professor Wenke Lee.

12. Yogesh Mundada, College of Computing, Georgia Tech, Fall 2011.
    Advisor: Professor Nick Feamster.

13. Hyojoon Kim, College of Computing, Georgia Tech, Fall 2011.
    Advisor: Professor Nick Feamster.

14. Ikpeme Erete, College of Computing, Georgia Tech, Spring 2011.
    Advisor: Professor Alex Orso.

15. Chaitrali Amrutkar, College of Computing, Georgia Tech, Spring 2011.
    Advisor: Professor Patrick Traynor.

16. Brendan Dolan-Gavitt, College of Computing, Georgia Tech, Spring 2011.
    Advisor: Professor Wenke Lee and Professor Jon Giffin.

17. Sam Burnett, College of Computing, Georgia Tech, Fall 2010.
    Advisor: Professor Nick Feamster.

18. Cong Shi, College of Computing, Georgia Tech, Fall 2010.
    Advisor: Professor Mostafa Ammar and Professor Ellen Zegura.

19. Partha Kanuparthy, College of Computing, Georgia Tech, Fall 2010.
    Advisor: Professor Constantine Dorvolis.

20. Long Lu, College of Computing, Georgia Tech, Spring 2010.
    Advisor: Professor Wenke Lee.

21. Virendra Kumar, College of Computing, Georgia Tech, Spring 2009.
    Advisor: Professor Alexandra Boldyreva.

22. Frank Park, College of Computing, Georgia Tech, Spring 2009.
    Advisor: Professor Patrick Traynor.

23. Italo Dacosta, College of Computing, Georgia Tech, Fall 2008.
Advisor: Professor Mustaque Ahamad and Professor Patrick Traynor.

24. Adam O'Neill, College of Computing, Georgia Tech, Fall 2008.
Advisor: Professor Alexandra Boldyreva.

E. External Member of M.S. Examining Committee

M.S. Thesis Defense Committees None.

F. Consulting and Advisory Appointments

1. Skim Reaper, *Co-Founder and CEO*, 2019-Present.
2. CryptoDrop Anti-Ransomware, *Co-Founder and CEO*, 2017-2018.
3. Pindrop Security, *Research Fellow and Co-Founder*, Spring 2012 - Spring 2014.
4. United States Army (via US Falcon), *Information Assurance Officer Training Program*, Spring 2010.
5. 3G Americas, *Characterizing the Limitations of Third-Party EAS over Cellular Text Messaging Systems*, Fall 2008.

G. Civic Activities

None.

IV. NATIONAL AND INTERNATIONAL PROFESSIONAL RECOGNITION

A. Honors and Awards

1. Fellow, Kavli Foundation, 2017.
2. Fellow, Center for Financial Inclusion at Accion, 2016.
3. Sloan Research Fellow, Alfred P. Sloan Foundation, 2014.

B. Invited Conference Session Chairmanships

1. Session Chair, *Work-in-Progress* at the *USENIX Security Symposium (SECURITY)*, 2016.
2. Session Chair, *Mobile Security* at the *USENIX Security Symposium (SECURITY)*, 2013.
3. Poster Chair, *USENIX Security Symposium (SECURITY)*, 2010, 2011.
4. Session Chair, *Privacy and Anonymity* at the *USENIX Workshop on Hot Topics in Security (HotSec)*, 2011.
5. Session Chair, *Security of Authentication and Protection Mechanisms* at the *IEEE Symposium on Security & Privacy (OAKLAND)*, 2011.
6. Session Chair, *Information Abuse* at the *IEEE Symposium on Security & Privacy (OAKLAND)*, 2010.
7. Session Chair, *RFID Security* at the *ACM Conference on Computer and Communications Security (CCS)*, 2009.
8. Session Chair, *Browser Security Session* at the *USENIX Security Symposium (SECURITY)*, 2009.
9. Session Chair, *Information Security Session* at the *IEEE Symposium on Security and Privacy (OAKLAND)*, 2009.
10. Session Chair, *Work-in-Progress* at the *IEEE Symposium on Security and Privacy (OAKLAND)*, 2009.
11. Session Chair, *Work/Opinions-in-Progress* at the *ISOC Network and Distributed Systems Security (NDSS) Symposium*, 2009.
12. Session Chair, *Privacy Session* at the *USENIX Security Symposium (SECURITY)*, 2008.

C. Professional Registration

None.

D. Patents

1. Patrick G. Traynor, Christian Peeters, Bradley G. Reaves, Hadi Abdullah, Kevin Butler, Jasmine Bowers, Walter N. Scaife, "Detecting SS7 Redirection Attacks With Audio-Based Distance Bounding", United State Patent # 11,265,717, Filed March 2019, Issued March 2022.
2. Patrick G. Traynor, Logan E. Blue, Luis Vargas, "Method and Apparatus for Differentiating Between Human and Electronic Speaker for Voice Interface Security", United State Patent # 11,176,960, Filed June 2019, Issued November 2021.
3. Patrick G. Traynor, Bradley G. Reaves, Logan E. Blue Practical End-to-End Cryptographic Authentication for Telephony Over Voice Channels, United State Patent # 11,329,831, Filed November 2018, Issued May 2022.

4. Walter Nolen Scaife, Patrick G. Traynor and Christian Peeters, "Payment Card Overlay Skimmer Detection", United States Patent # 10,496,914, Filed October 2017, Issued December 2019. (See also # 10,936,928)

5. Patrick G. Traynor, David P. Arnold, Walter Nolen Scaife, Christian Peeters, and Camilo Valez Cuervo, "Detecting counterfeit magnetic stripe cards using encoding jitter", United States Patent # 10,803,261, Filed May 2017, Issued October 2020.

6. Patrick G. Traynor, Bradley Reaves, Logan Blue, Luis Vargas, Hadi Abdullah, and Thomas Shrimpton, "Identity and content authentication for phone calls", United States Patent # 10,764,043, Filed Apr 2017, Issued September 2020.

7. Walter Nolen Scaife, Henry Carter, Patrick G. Traynor and Kevin R. B. Butler. "Malware Detection Through User Data Transformation Monitoring", United States Patent # 10,685,114. Filed September 2015, Issued June 2020.

8. Vijay A. Balasubramaniyan, Mustaque Ahamad, Patrick G. Traynor. "Using Single-Ended Audio Features to Automatically Determine Voice Call Provenance", United States Patent, #9,037,113 June 2010, Issued May 2015. (See also #9,516,497 and #10,523,809)

9. Patrick G. Traynor, Byungsuk Kim and Farooq Anjum. "Secure Localization for 802.11 Networks with Fine Granularity", United States Patent, #8,107,400, Filed July 2008, Issued January 2012.

E. Editorial and Reviewer Work for Technical Journals and Publishers

Associate Editor:

- *ACM Transactions on Information and System Security (TISSEC)* 2015-present

Guest Editor:

Journals

- *IEEE Security and Privacy Magazine (S&P)* 2013

Reviewer for:

Journals

- *ACM Transactions on Information and System Security (TISSEC)* 2008, 2009, 2010, 2011, 2012, 2013
- *IEEE Transactions on Dependable and Secure Computing (TDSC)* 2012, 2013
- *IEEE Security and Privacy Magazine (S&P)* 2010, 2011
- *Communications of the ACM (CACM)* 2010
- *Journal of Anesthesia & Analgesia* 2009
- *IEEE Transactions on Mobile Computing (TMC)* 2008, 2010, 2011, 2012, 2013
- *IEEE Transactions on Internet Technology (TOIT)* 2009, 2010
- *ACM Mobile Computing and Communications Review (MC2R)* 2008
- *IEEE/ACM Transactions on Networking (TON)* 2007, 2008
- *Journal of Pervasive and Mobile Computing (PMC)* 2009, 2010

- *IEEE Transactions on Parallel and Distributed Systems (TPDS)* 2005, 2009, 2010
- *IEEE Transactions on Computers (TOC)* 2010
- *Journal of Security and Communication Networks (SCN)* 2008
- *IEEE Communications Letters (CL)* 2007, 2009
- *IEEE Transactions on Wireless Communications (TWC)* 2007
- *Pervasive and Mobile Computing (PMC)* 2007
- *IEEE Transactions on Software Engineering (TSE)* 2007, 2008
- *Journal of Wireless Networks (WiNet)* 2006, 2007, 2008, 2009
- *Journal of Wireless Communications and Mobile Computing* 2006
- *ACM Computing Surveys (ACMCS)* 2006
- *Information Processing Letters (IPL)* 2006
- *IEEE Transactions on Very Large Scale Integration Systems (TVLSIS)* 2006

Conferences and Workshops

- *ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2011
- *ACM Conference on Computer and Communications Security (CCS)*, 2008, 2011
- *IEEE Symposium on Security and Privacy (OAKLAND)* 2007, 2008
- *Computer Security Foundations (CSF)*, 2011
- *IFIP Conference on Data and Applications Security (DBSec)* 2008
- *Financial Cryptography (FC)* 2007, 2008
- *International Conference on VLSI Design (VLSI)* 2007
- *Annual Computer Security Applications Conference (ACSAC)* 2005, 2006, 2007
- *USENIX Workshop on Hot Topics in Security (HotSec)* 2007
- *International Conference on Information Systems Security (ICISS)* 2007
- *IEEE International Conference on Computer Engineering & Systems (ICCES)* 2007
- *International Workshop on Security (IWSec)* 2006, 2007
- *USENIX Security Symposium (SECURITY)* 2006, 2007
- *IEEE Sarnoff Symposium (SARNOFF)* 2007
- *International Conference on New Technologies, Mobility and Security (NTMS)* 2007
- *IEEE Infocom (INFOCOM)* 2007
- *Network and Distributed System Security Symposium (NDSS)* 2007
- *International Workshop on Storage Security and Survivability (IWSSS)* 2006
- *ACM Conference on Computer and Communications Security (CCS)* 2006

- *IEEE GLOBECOM (GLOBECOM)* 2006
- *International Conference on Mobile and Ubiquitous Systems: Networks and Services (MOBIQUITOUS)* 2006
- *IFIP Conference on Data and Applications Security (DBSec)* 2006
- *Emerging Trends in Information and Communications Security (ETRICS)* 2006
- *International Conference on Applied Cryptography and Network Security (ACNS)* 2006
- *ACM Symposium on Access Control Models and Technology (SACMAT)* 2006
- *IEEE Conference on Communication Systems Software & Middleware (COMSWARE)* 2006
- *International Conference on Cryptology in India (IndoCrypt)* 2005
- *IEEE Symposium on New Frontiers in Dynamic Spectrum Access (DySPAN)* 2005
- *European Symposium on Research in Computer Security (ESORICS)* 2005

F. Expert Witness Services

1. *Epic Games, Inc. & Anor v Google LLC & Ors - Federal Court of Australia Proceeding NSD 190 of 2021:* Expert witness for the Defense (via Corrs Chambers Westgarth). Status: Ongoing. *January 2023 - Present*.
2. *Telefonaktiebolaget LM Ericsson vs Apple, Inc:* Expert witness for the Defendant, Non-Infringement and Invalidity (via WilmerHale LLP). Status: Settled. *February 2022 - December 2022*.
3. *Wepay Global Payments, LLC v. Bank of America N. A.,:* Expert Witness for the Defendant (via WilmerHale LLP) Status: Dismissed. *September 2022 - November 2022*.
4. *Apple vs. R.N Nehushtan Trust Ltd.:* Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Status: Submitted to PTAB. *August 2022 - Ongoing*.
5. *Apple/Microsoft vs. Zipit Wireless:* Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Status: Settled. *May 2021 - November 2022*.
6. *Blackberry Inc v MobileIron, Inc:* Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Verdict: Settled. *January 2021 - March 2021*.
7. *Apple Inc v Seven Networks, LLC:* Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Verdict: Three of four petitions instituted by PTAB. Fourth rejected via discretion, case settled. *August 2019 - November 2020*.
8. *mSIGNIA, Inc. v. InAuth, Inc.:* Expert Witness for the Defendant for Inter Partes Review, Non-Infringement and Invalidity (via Quinn Emanuel Urquhart and Sullivan, LLP). Verdict: Dismissed with prejudice. *October 2017 - December 2018*.
9. *Huawei v. T-Mobile:* Expert Witness for the Defendant for Non-Infringement (via WilmerHale LLP, Alston & Bird LLP) Verdict: Settled *June 2016 - December 2017*.
10. *Telefonaktiebolaget LM Ericsson v Apple:* Expert Witness for the Defendant for Non-Infringement, Invalidity (via WilmerHale LLP). Verdict: Settled *June 2015 - December 2015*.
11. *Mayfonk v Nike:* Expert Witness for the Plaintiff for Infringement (via Paul Hastings). Verdict: Settled. *June 2015 - November 2015*.

12. *Maxim Integrated Products v Bank of the West:* Expert Witness for the Defendant for Non-Infringement (via Paul Hastings LLP). Verdict: Dismissed with prejudice. *January 2014 - August 2014.*

13. *Maxim Integrated Products v Comerica Inc, et al:* Expert Witness for the Defendant for Non-Infringement (via McKenna, Long & Aldridge LLP). Verdict: Settled. *June 2014 - August 2014.*

14. *William Grecia v. Apple Inc. et al:* Expert Consultant for the Defendant for Invalidity (via Kirkland & Ellis LLP). Verdict: Closed in initial pleadings, dismissed with prejudice. *July 2014 - August 2014.*

15. *Intertrust Technologies Corp. v. Apple Inc.:* Expert Consultant for Defendant for Invalidity and Non-Infringement (via Kirkland & Ellis LLP). Verdict: Settled. *October 2013 - February 2014.*

16. *Maxim Integrated Products v KeyCorp Bank:* Expert Witness for the Defendant for Non-Infringement (via Calfee, Halter & Griswold LLP) Verdict: Settled. *April 2013 - June 2013.*

17. *Intellectual Ventures LLC vs. Check Point; et al.:* Expert Consultant for the Plantiff for Infringement (via Susman Godfrey LLP), Verdict: Infringement on 2 of 4 patents. *October 2012 - February 2015.*

V. OTHER CONTRIBUTIONS

A. Seminar Presentations (Invited Papers and Talks at Meetings and Symposia)

1. Keynote: Well, It Worked on My Computer: Reproducibility, Tech Transfer, and Computer Security Research. National Science Foundation Secure and Trustworthy Cyberspace (SaTC) Vision 2.0 Workshop, March 2023. University of Texas at Dallas.

2. Humans vs The Computer Interfaces: Separating Deepfakes/Bots from People Using Psychoacoustics. UCLA Electrical and Computer Engineering Distinguished Seminar, February 2023. University of California, Los Angeles.

3. Keynote: Exploiting the Gaps Between Human and Machine Understanding of Audio: Frameworks, Attacks, and Defenses. ISCA Symposium on Security and Privacy in Speech Communication (SPSC), November 2021. Virtual.

4. The State of Voice Cloning Technology. Federal Trade Commission (FTC) Workshop on Voice Cloning Technologies, January 2020. Washington, DC.

5. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. North Carolina State University Department of Computer Science Colloquium, January 2020. Raleigh, NC.

6. Moving from research to practice: How to maximize the impact of SaTC projects. National Science Foundation Secure and Trustworthy Cyberspace (SaTC) PI Meeting, October 2019. Alexandria, VA.

7. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. Purdue University Computer Science Excellence Lecture Series, October 2019. West Lafayette, IN.

8. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. Bank of America - Colloquium Series, March 2019. Charlotte, NC.

9. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. CISPA – Helmholtz Center for Information Security, Saarland University, February 2019. Saarbrücken, Germany.

10. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. University of Maryland - Distinguished Colloquium, February 2019. College Park, MD.

11. Responsible Finance for the Digital Client. Foromic Conference, October 2018. Barranquilla, Colombia.

12. Panel: Authentication Challenges for New Interfaces, Devices, and Wireless Networks. ACM Conference on Security and Privacy in Wireless and Mobile Networks, June 2018. Stockholm, Sweeden.

13. Sonar: Detecting SS7 Redirection Attacks Via Call Audio-Based Distance Bounding. CyberSecurity@KAIST Workshop - KAIST, June 2018. Daejon, South Korea.

14. Why Caller-ID Spoofing Is So Easy (and Why End-To-End Solutions Are the Way Forward). IEEE Workshop on Technology and Consumer Protection (ConPro'18), May 2018. San Francisco, CA.

15. Panel: The Future of Cybersecurity. SEC Academic Conference - Auburn University, May 2018. Auburn, AL.

16. Sound Principles: Verifying Voice Commands in an IoT World. IoT Security Workshop - Aalto University, September 2017. Helsinki, Finland.

17. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Eurecom Institute, September 2017. Sophia Antipolis, France.

18. Panel: Infrastructure Stability. ITU-T Focus Group Digital Financial Services, December 2016. Geneva, Switzerland.

19. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. ETH Zurich, December 2016. Zurich, Switzerland.

20. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. University of Richmond, October 2016. Richmond, Virginia.

21. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Indiana University, September 2016. Bloomington, Indiana.

22. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Aalto University Computer Science Department Forum, August 2016. Helsinki, Finland.

23. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. KAIST Information Security Seminar - Korean Advanced Institute of Science and Technology, June 2016. Daejeon, South Korea.

24. Updated Mobile Money Vulnerability Report. International Telecommunications Union Digital Financial Services Working Group Workshop, May 2016. Washington, DC.

25. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. UF Eye Opener Discovery Breakfast - University of Florida, May 2016. Gainesville, FL.

26. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Illinois Science of Security (SoS) Lablet Speaker Series - University of Illinois, Urbana-Champaign, April 2016. Urbana-Champaign, Illinois.

27. New Trends in Cybersecurity:Vulnerabilities in Branchless Banking Systems. United States Departments of State and Justice - Cybersecurity and Cybercrime Workshop for Lusophone Africa, September 2015. Maputo, Mozambique.

28. New Trends in Cybersecurity:Vulnerabilities in Branchless Banking Systems. United States Departments of State and Justice - ECCAS Cybersecurity and Cybercrime Workshop, August 2015. Kinshasa, Democratic Republic of Congo.

29. Chasing Telephony Security: Where the Wild Things... Are? University of Florida - Department Colloquium, January 2014. Gainesville, FL.

30. Chasing Telephony Security: Where the Wild Things... Are? Verizon Wireless RNC/Data Center, October 2013. Alpharetta, GA.

31. Chasing Telephony Security: Where the Wild Things... Are? University of Waterloo - CrySP Speaker Series on Privacy, October 2013. Waterloo, ON, Canada.

32. Analyzing Malicious Traffic in Cellular Networks. GSM Association's (GSMA) Mobile Malware Community Workshop, July 2013. Mountain View, CA.

33. Threats to Mobile Devices. US Federal Trade Commission (FTC) Public Forum - Invited Speaker, June 2013. Washington, D.C.

34. Chasing Telephony Security: Where the Wild Things... Are? University of Wisconsin - Madison, Security Seminar, March 2013. Madison, WI.

35. The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers. Invited Talk: Centre for Secure Information Technologies (CSIT) Queen's University, March 2013. Belfast, Northern Ireland.

36. Chasing Telephony Security: Where the Wild Things... Are? Stanford Security Seminar, March 2013. Stanford, CA.

37. Chasing Telephony Security: Where the Wild Things... Are? University of California, Berkeley, Security Group, March 2013. Berkeley, CA.

38. Chasing Telephony Security: Where the Wild Things... Are? Carnegie Mellon University CyLab Seminar, February 2013. Pittsburgh, PA.

39. Chasing Telephony Security: Where the Wild Things... Are? University of Oregon Department of Computer Science Colloquium, November 2012. Eugene, OR.

40. Chasing Telephony Security: Where the Wild Things... Are? University of Washington Department of Electrical Engineering, Network Security Lab (NSL): Invited Talk, November 2012. Seattle, WA.

41. Needles and Haystacks: Digging for Ground Truth on Mobile Malware. ZISC Workshop on Secure Mobile and Cloud Computing, ETH Zurich, June 2012. Zurich, Switzerland.

42. Panel: Advice for Early Career Faculty. CRA Career Mentoring Workshop, February 2012. Washington, D.C.

43. Research Challenges in Cellular and Mobile Network Security. US-China Software Workshop (Co-Sponsored by NSF and NSFC), September 2011. Beijing, China.

44. Mobile Security: Understanding Risks to Critical Infrastructure. Invited Talk: US Department of State East African Workshop on Cyberspace Security, July 2011. Nairobi, Kenya.

45. Tomorrow's Issues: Solving the Mobile Security Threat. Invited Talk: Centre for Secure Information Technologies (CSIT) Queen's University, March 2011. Belfast, Northern Ireland.

46. PinDr0p: Using Single-Ended Audio Features to Determine Call Provenance. Invited Talk: MITRE Corporation, March 2011. Burlington, MA.

47. Defeating Session Hijacking Attacks with Disposable Web Credentials. Invited Talk: Facebook, February 2011. Palo Alto, CA.

48. Understanding the Disruptive Potential of Malware in Cellular Networks. Invited Talk: RSA Conference, February 2011. San Francisco, CA.

49. Panel: Voice Security – Now Just a False Sense of Security and Privacy. Invited Panelist: Mobile Security Symposium, February 2011. San Francisco, CA.

50. Understanding the Disruptive Potential of Malware in Cellular Networks. Invited Talk: Concordia University, May 2010. Montreal, QC, Canada.

51. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Qualcomm Research, March 2010. San Diego, CA.

52. Privacy and Security Concerns for Personal and Mobile Health Devices. Invited Talk: Workshop to Set A Research Agenda for Privacy and Security of Healthcare Technologies, October 2009. Indianapolis, IN.

53. Considerations for EAS Over Cellular Text Messaging Services. 3G Americas Webinar, July 2009.

54. University Telephony Research Panel. Conference on Principles, Systems and Applications of IP Telecommunications (IPTCOMM), July 2009.

55. The Evolving Mobile Landscape: Emerging Security Threats. Mobile Security eConference, SC Magazine, June 2008.

56. Characterizing the Impact of Rigidity on the Security of Cellular Networks. University of Washington, February 2009. Seattle, WA.

57. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Microsoft Research, February 2009. Redmond, WA.

58. Next Year's Problems. Secure Computing (SC) Magazine Webinar, November 2008.

59. Panel: Embedded Systems and their Increasing Impact on Infrastructure Security. Workshop on Embedded Systems Security (WESS), October 2008.

60. Can you DoS me now? Security Issues in Cellular Networks. Georgia Institute of Technology, September 2008. Atlanta, GA.

61. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Georgia Institute of Technology, April 2008. Atlanta, GA.

62. Characterizing the Impact of Rigidity on the Security of Cellular Networks. AT&T Research Labs, April 2008. Florham Park, NJ.

63. Characterizing the Impact of Rigidity on the Security of Cellular Networks. University of Arizona, March 2008. Tucson, AZ.

64. Cellular Networks Security Panel. USENIX Security Symposium, August 2007. Boston, MA.

65. malnets:Large-Scale Malicious Networks via Compromised Access Points. The Pennsylvania State University - ACM Club Invited Speaker, October 2006. State College, PA.

66. malnets:Large-Scale Malicious Networks via Compromised Access Points. The University of Michigan, October 2006. Ann Arbor, MI.

67. Exploiting Open Functionality in SMS-Capable Cellular Networks. The University of Michigan, October 2006. Ann Arbor, MI.

68. Exploiting Open Functionality in SMS-Capable Cellular Networks. High Technology Crime Investigation Association (HTCIA), September 2006. Pittsburgh, PA.

69. Trends in Security: Critical Engineering in the Large. Schlumberger Innovate IT! Workshop, May 2006. Cambridge, MA.

70. Exploiting Open Functionality in SMS-Capable Cellular Networks. InfraGard Pittsburgh Chapter General Meeting, September 2006. Pittsburgh, PA.

71. Exploiting Open Functionality in SMS-Capable Cellular Networks. InfraGard Pittsburgh Chapter General Meeting, September 2006. Pittsburgh, PA.

B. Special Activities

Presentations to Lay Media

1. How technology can fight digital fakery. The Babbage Podcast/The Economist https://shows.acast.com/theeconomistbabbage/episodes/babbage-how-to-detect-a-deepfake, January 2023.
2. Deepfake audio has a tell and researchers can spot it. Ars Technica https://arstechnica.com/information-technology/2022/09/researchers-use-fluid-dynamics-to-spot-deepfake-voices/, September 2022.
3. This security tool could help stop the problem of ransomware in its tracks. TheJournal.ie https://www.thejournal.ie/ransomware-researchers-stop-2875032-Jul2016/, July 2016.
4. Researchers Unleash Ransomware Annihilation. BankInfoSecurity - http://www.bankinfosecurity.com/researchers-unleash-ransomware-annihilation-a-9255, July 2016.
5. CryptoDrop Stops Ransomware by Stopping its Encryption. Security Intelligence - https://securityintelligence.com/news/cryptodrop-stops-ransomware-by-stopping-its-encryption/?utm_source=tfeed&utm_medium=twitter, July 2016.
6. Ransomware 'stopped' by new software. BBC - http://www.bbc.com/news/technology-36772461, July 2016.
7. Researchers create effective anti-ransomware solution. Help Net Security - https://www.helpnetsecurity.com/2016/07/12/anti-ransomware-solution/, July 2016.
8. Florida U boffins think they've defeated all ransomware. http://www.theregister.co.uk/2016/07/12/ransomware_defeated/, July 2016.
9. This Anti-Ransomware Tool Could Save You Hundreds of Pounds. Huffington Post - http://www.huffingtonpost.co.uk/entry/anti-ransomware-tool-save-hundreds-pounds_uk_57838beee4b0935d4b4b30ba, July 2016.
10. Researchers develop method to stop 100% of ransomware before it encrypts all files. Myce - http://www.myce.com/news/researchers-develop-method-stop-100-ransomware-encrypts-files-79873/, July 2016.
11. Desarrollan una solución para detener el ransomware. ComputerHoy - http://computerhoy.com/noticias/software/desarrollan-solucion-detener-ransomware-47972, July 2016.
12. Why your antivirus software can't stop ransomware. Futurity - http://www.futurity.org/ransomware-computer-files-1198242-2/, July 2016.
13. CryptoDrop Gives Users Hope to Prevent Ransomware Infections in the Future. Softpedia - http://news.softpedia.com/news/cryptodrop-gives-users-hope-to-prevent-ransomware-infections-in-the-future-506187.shtml, July 2016.

14. Could this be the answer to the ransomware threat?, Consumer Affairs. Consumer Affairs - https://www.consumeraffairs.com/news/could-this-be-the-answer-to-the-ransomeware-threat-071116.html, July 2016.

15. Extortion extinction: Researchers develop a way to stop ransomware. Phys.org - http://phys.org/news/2016-07-extortion-extinction-ransomware.html, July 2016.

16. Researchers Develop A Way To Stop Ransomware By Watching The Filesystem. Slashdot - https://yro.slashdot.org/story/16/07/08/2242244/researchers-develop-a-way-to-stop-ransomware-by-watching-the-filesystem, July 2016.

17. Mohul Ghosh. Trak.in - Digital Money Apps In India Are Unsafe and Unsecured – Researchers. http://trak.in/tags/business/2015/08/17/digital-money-apps-india-unsafe-unsecured/, August 2015.

18. Richard Handford. Mobile World Live - Survey finds security holes in mobile money apps. http://www.mobileworldlive.com/money/news-money/survey-finds-security-holes-in-mobile-money-apps/#.Vc27Y-QTmSQ.twitter, August 2015.

19. JENNIFER VALENTINO-DEVRIES. Wall Street Journal - Researchers Find Security Flaws in Developing-World Money Apps. http://blogs.wsj.com/digits/2015/08/11/researchers-find-security-flaws-in-developing-world-money-apps/, August 2015.

20. Jonathon Cheng. Wall Street Journal - Samsung Phone Studied for Possible Security Gap. http://online.wsj.com/news/articles/SB10001424052702304244904579276191788427198, December 2013.

21. N. V. The Economist - The Threat in the Pocket. http://www.economist.com/blogs/babbage/2013/10/difference-engine-0?fsrc=scn/fb/wl/bl/thethreatinthepocket, October 2013.

22. Antone Gonsalves. ComputerWorld - Let's Dump Anti-Virus and Move On:. http://blogs.computerworld.com/mobile-security/22969/lets-dump-av-and-move, October 2013.

23. Mathew J. Schwartz. InformationWeek - Google: Don't Fear Android Malware. http://www.informationweek.com/security/mobile/google-dont-fear-android-malware/240162399, October 2013.

24. Kirsten Doyle. ITWeb - Android Threat Exaggerated, or is it? http://www.itweb.co.za/index.php?option=com_content&view=article&id=68055, October 2013.

25. Danielle Walker. SC Magazine - Mobile malware prevalence expands, but privacy-abusing apps should be top of mind. http://www.scmagazine.com/mobile-malware-prevalence-expands-but-privacy-abusing-apps-should-be-top-of-mind/article/300597/, June 2013.

26. Jim Burress. WABE NPR - Mobile Web Browsers Full of Security Risks, Tech Professor Finds. http://wabe.org/post/mobile-web-browsers-full-security-risks-tech-professor-finds, December 2012.

27. Mark Huffman. Consumer Affairs - Georgia Tech: mobile browsers fail safety test. http://www.consumeraffairs.com/news/georgia-tech-mobile-browsers-fail-safety-test-120612.html, December 2012.

28. Matthew J. Schwartz. Information Week - Blame Screen Size: Mobile Browsers Flunk Security Tests. http://www.informationweek.com/security/mobile/blame-screen-size-mobile-browsers-flunk/240143999, December 2012.

29. Jon Gold. Network World - Ga. Tech researchers: Mobile Browsers need better HTTPS indicators. http://www.networkworld.com/news/2012/120512-mobile-browsers-264846.html, December 2012.

30. United Press International. Study: Most mobile Web browsers unsafe. http://www.upi.com/Science_News/Technology/2012/12/05/Study-Most-mobile-Web-browsers-unsafe/UPI-73431354743353/#ixzz2EGtQsuLd, December 2012.

31. Suzanne Choney. Mobile browser woes can fool even experts: report . http://www.nbcnews.com/technology/mobile-browser-woes-can-fool-even-experts-report-1C7451203, December 2012.

32. Meghan Kelly. VentureBeat - 3 hot security startups to watch. http://venturebeat.com/2012/02/27/3-security-startups-to-watch-at-the-2012-rsa-conference/, February 2012.

33. Jacob Goodwin. Government Security News - RSA 2012 – Pindrop Security can distinguish a fraudulent phone call from a real one. http://www.gsnmagazine.com/node/25721?c=communications, February 2012.

34. Matt Liebowitz. Phone hack logs keystrokes from nearby computers. MSNBC.com - http://www.msnbc.msn.com/id/44993238/ns/technology_and_science-security/#.TqU5MNSjPh4, October 2011.

35. Jacob Aron. iPhone keylogger can snoop on desktop typing. New Scientist - http://www.newscientist.com/article/dn21059-iphone-keylogger-can-snoop-on-desktop-typing.html, October 2011.

36. iPhone Keylogger Can Snoop on Desktop Typing. Slashdot - http://mobile.slashdot.org/story/11/10/18/2346222/iphone-keylogger-can-snoop-on-desktop-typing, October 2011.

37. Robert Lemos. Smart Phones Could Hear Your Password. Technology Review - http://www.technologyreview.com/computing/38913/?p1=A2, October 2011.

38. Kevin McCaney. Bad vibrations: How smart phones could steal PC passwords. Government Computer News - http://gcn.com/articles/2011/10/18/smart-phone-sensors-steal-keystrokes.aspx, October 2011.

39. PhysOrg. Turning iPhone into spiPhone: Smartphones' accelerometer can track strokes on nearby keyboards. PhysOrg.com - http://www.physorg.com/news/2011-10-iphone-spiphone-smartphones-accelerometer-track.html, October 2011.

40. Brid-Aine Parnell. Securo-boffins call for 'self-aware' defensive technologies. The Register - http://www.theregister.co.uk/2011/09/14/self_aware_cyber_security_technologies_should_be_a_top_priority/, September 2011.

41. Clay Dillow. 'PinDr0p' Tech Uses Unique Noise Fingerprints to Trace Calls. Popular Science - http://www.popsci.com/technology/article/2010-10/pindr0p-tech-tags-phone-calls-unique-fingerprints-trace-call-paths-across-networks, October 2010.

42. Lewis Page. Voice-routing call fingerprint system fights vishing. The Register - http://www.theregister.co.uk/2010/10/06/voice_fingerprints, October 2010.

43. Science Daily. Voice Phishing: System to Trace Telephone Call Paths Across Multiple Networks Developed. http://www.sciencedaily.com/releases/2010/10/101005121820.htm, October 2010.

44. Brian Kalish. To Text or Not to Text During Emergencies. NextGov.com - http://www.nextgov.com/nextgov/ng_20100914_5986.php?oref=topnews, September 2010.

45. Ki Mae Heussner. 'Operation Chokehold': Fake Steve Jobs Rallies iPhone Users to Cripple AT&T Network. ABC News - http://abcnews.go.com/Technology/GadgetGuide/fake-steve-jobs-rallies- iphone-users-cripple-att/story?id=9355447, December 2009.

46. Bob Brown. Researchers Set Their Sights on iPhones, Mobile Malware. PC World Magazine - ihttp://www.pcworld.com/article/182005/iphone_worms_mobile_malware.html?tk=rss, November 2009.

47. MacGregor Campbell. Botnets show their disruptive potential. New Scientist Magazine - http://www.newscientist.com/article/mg20427347.000-mobile-botnets-show-their-disruptive-potential.html, November 2009.

48. Angela Moscaritolo. Remote repair for infected phones in development. SC Magazine - http://www.scmagazineus.com/remote-repair-for-infected-phones-in- development/article/157504/, November 2009.

49. Bob Brown. iPhone worms, other smartphone malware in researchers' sights. Network World - http://www.networkworld.com/news/2009/111109-smartphone-security-georgia -tech.html?hpg1=bn, November 2009.

50. Urvaksh Karkaria. GT researchers work to secure cellphones. Atlanta Business Chronicle - http://atlanta.bizjournals.com/atlanta/blog/atlantech/2009/11/cellphone.html, November 2009.

51. Making Carriers Shoulder Smartphone Security. http://mobile.slashdot.org/story/09/11/11 /2318247/Making-Carriers-Shoulder-Smartphone-Security?art_pos=31, November 2009.

52. Ben Meyer. Georgia Tech to Lead Fight Against Cell Phone Hackers. NBC 11 Atlanta - http://www.11alive.com/news/local/story.aspx?storyid=132505&catid=3, July 2009.

53. Illena Armstrong. Safeguarding your mobile networks. SC Magazine - http://www.scmagazineus.com/Safeguarding-your-mobile-networks/article/138289/, June 2009.

54. Kelli B. Grant. Four Free Cellphone Apps to Help Manage Your Money. SmartMoney Magazine - http://www.smartmoney.com/Spending/Deals/4-Great-Free-Finance-Apps-for-Cellphones/, June 2009.

55. Amanda Hoffstrom. Technology's limitations in alerting campus danger. UWire Magazine - http://www.uwire.com/Article.aspx?id=3738798, February 2009.

56. Laura Sydell. Compromise Allows Obama To Keep BlackBerry. National Public Radio - http://www.npr.org/templates/story/story.php?storyId=99790788, January 2009.

57. Dennis Carter. Questions abound as emergency alert flops Virginia Tech's text-message alert system failed when the sound of gunfire was heard on campus; officials scramble to understand why. eSchool News - http://www.eschoolnews.com/iphone/top-story/index.cfm?i=56122#_56122, November 2008.

58. Jessica Bauer. Study: Text alerts may fail in real emergency. Diamondback Online - http://media.www.diamondbackonline.com/media/storage/paper873/news/2008/10/14/News/Study.Text.Alerts.May.Fail.In.Real.Emergency-3485509.shtml, October 2008.

59. Associated Press. Hackers Expected To Start Targeting Cell Phones. http://cbs5.com/watercooler/Cell.Phones.Hackers.2.840909.html, 2008.

60. Associated Press. College alert systems unreliable, study says. http://www.ajc.com/search/content/metro/stories/2008/09/25/college_campus_alerts.html, 2008.

61. Lee Shearer. Study: Campus alerts unreliable. Athens Banner Herald http://www.onlineathens.com/stories/092508/uga_336494829.shtml, 2008.

62. Bill Ray. 3G Americas warns against text warning systems. The Register - http://www.theregister.co.uk/2008/09/18/emergency_text/, 2008.

63. 3G Americas. 3G Americas Highlights New Research Report on Use of Cellular Text Messaging for Emergency Alert Services. 3G Americas http://www.3gamericas.org/English/news_room/DisplayPressRelease.cfm?id=3400&s=ENG, 2008.

64. Evan Koblentz. Web Exclusive: From Messaging to Management Duty. Wireless Week - http://www.wirelessweek.com/Messaging-to-Management-Duty.aspx, 2008.

65. Christopher Beam. How Do You Intercept a Text Message? Turn your cell phone into a spy gadget. Slate Magazine http://www.slate.com/id/2161402/, 2007.

66. Jamming Cellphones with Text Messages. Slashdot http://it.slashdot.org/it/05/10/05/1839217.shtml?tid=215&tid=172, 2005.

67. Cell phone networks at risk? CNN http://money.cnn.com/2005/10/05/technology/hacker_cellphones/, 2005.

68. John Schwartz. Text Hackers Could Jam Cellphones, a Paper Says. The New York Times http://www.nytimes.com/2005/10/05/technology/05phone.html?ex=1286164800&en=d917b9cd43dfaa31&ei=5090&partner=rssuserland&emc=rss, 2005.