

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Graham Merrett
U.S. Patent No.: 11,653,182 Attorney Docket No. 50095-0261IP1
Issue Date: May 15, 2023
Application No.: 17/959,687
Filing Date: October 4, 2022
Title: SERVER THAT SENDS A RESPONSE WHEN A MOBILE
 PHONE HAS AN ACTIVE STATUS WITH A PACKET
 SWITCHED MESSAGE SERVICE

DECLARATION OF DR. PATRICK TRAYNOR

I declare that all statements made herein on my own knowledge are true and that all statements made on information and belief are believed to be true, and further, that these statements were made with the knowledge that willful false statements and the like so made are punishable under Section 1001 of Title 18 of the United States Code.

Date: 28 August 2025

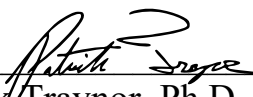
By: 
Patrick Traynor, Ph.D.

Table of Contents

I. QUALIFICATIONS AND BACKGROUND INFORMATION	4
II. LEGAL PRINCIPLES	10
A. Anticipation.....	10
B. Obviousness	11
III. OVERVIEW OF CONCLUSIONS FORMED	12
IV. BACKGROUND KNOWLEDGE ONE OF SKILL IN THE ART WOULD HAVE HAD PRIOR TO THE PRIORITY DATE OF THE '182 PATENT	12
V. INTERPRETATIONS OF THE '182 PATENT CLAIMS AT ISSUE	13
VI. THE '182 PATENT	13
A. Overview of the '182 Patent	13
B. Prosecution History of the '182 Patent.....	15
VII. OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES.....	16
A. Overview of Horvath	16
B. Overview of Tsampalis	21
C. Overview of Chatterjee	27
D. Overview of Kansal	28
E. Overview of Lin.....	30

VIII. GROUND 1: CLAIMS 1-30 ARE OBVIOUS IN VIEW OF THE
HORVATH-TSAMPALIS-CHATTERJEE-KANSAL COMBINATION.....30

- A. Combination of Horvath and Tsampalis.....31
- B. Combination of Horvath, Tsampalis, and Chatterjee40
- C. Combination of Horvath, Tsampalis, Chatterjee, and Kansal46
- D. Analysis with Respect to Claims 1-30.....49

IX. CONCLUSION.....128

DECLARATION OF DR. PATRICK TRAYNOR

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

I. QUALIFICATIONS AND BACKGROUND INFORMATION

1. My name is Patrick Gerard Traynor and I have been retained as an expert witness by Apple in the matter of Apple, Inc. (“Apple”) vs. HBCU Messaging US LP. 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. 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.

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 over 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 as Appendix A, 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:

- APPLE-1001 U.S. Patent No. 11,653,182 (“the ’182 Patent”)
- APPLE-1002 File History of U.S. Patent No. 11,653,182
- APPLE-1004 U.S. Pub. No. 2007/0254681 (“Horvath”)
- APPLE-1005 U.S. Pub. No. 2004/0203956 (“Tsampalis”)
- APPLE-1007 Chatterjee et al., “Instant Messaging and Presence Technologies for College Campuses.” IEEE Network, May/June 2005. (“Chatterjee”)
- APPLE-1008 U.S. Pub. No. 2005/0243978 (“Son”)
- APPLE-1009 UK Pub. No. 2432482 (“Beaumont”)
- APPLE-1010 U.S. Patent No. 9,408,077 (“David”)
- APPLE-1011 U.S. Patent No. 6,940,844 (“Purkayastha”)
- APPLE-1012 U.S. Patent No. 7,702,342 (“Duan”)
- APPLE-1013 U.S. Patent No. 8,819,145 (“Gailloux”)
- APPLE-1014 U.S. Pub. No. 2006/0286984 (“Bonner”)
- APPLE-1015 U.S. Pub. No. 2005/0197142 (“Major”)
- APPLE-1016 U.S. Pub. No. 2005/0037762 to Gurbani et al. (“Gurbani”)
- APPLE-1017 U.S. Patent No. 9,167,401 to Helferich (“Helferich”)
- APPLE-1018 U.S. Patent No. 6,430,604 (“Ogle”)
- APPLE-1019 PCT Pub. No. WO 2006/029331 (“Henderson”)
- APPLE-1020 U.S. Patent No. 7,236,472 (“Lazaridis”)

- APPLE-1025 Qi et al., 2004, July. “Multimedia Messaging Service.” Available at https://www.zte.com.cn/global/about/magazine/zte-communications/2004/1/en_68/162264.html (“Qi”)
- APPLE-1026 RFC 3261 – SIP: Session Initiation Protocol. Available at <http://www.faqs.org/rfcs/rfc3261.html>. June 2002.
- APPLE-1028 “How do I sign in to Messenger?” Yahoo! Messenger 6.0. 2004. Available at <https://web.archive.org/web/20040528072514/http://help.yahoo.com/help/us/messenger/win/signin/signin-03.html>
- APPLE-1032 U.S. Pub. No. 2008/0261577 (claiming priority to Provisional App. No. 60/913,187) (“Celik”)
- APPLE-1033 U.S. Provisional App. No. 60/913,187
- APPLE-1036 International Pub. No. WO 2007/052264 (“Agiv”)
- APPLE-1037 T-Mobile webpage <https://www.t-mobile.com/home-internet/the-signal/internet-help/the-complete-wifi-history>
- APPLE-1042 U.S. Pub. No. US 2008/0153459 (“Kansal”)
- APPLE-1043 RFC 2778 – A Model for Presence and Instant Messaging. Available at <https://datatracker.ietf.org/doc/html/rfc2778>. February 2000.
- APPLE-1044 RFC 3856 – A Presence Event Package for the Session Initiation Protocol (SIP). Available at <https://datatracker.ietf.org/doc/html/rfc3856>. August 2004.
- APPLE-1045 Trillian Pro v1.0 webpage (“Trillian”)
- APPLE-1046 U.S. Pub. No. 2007/0054627 (“Wormald”)
- APPLE-1047 U.S. Pub. No. 2008/0120427 (“Ramanathan”)
- APPLE-1048 U.S. Pub. No. 2002/0062345 (“Guedalia”)

- APPLE-1049 U.S. Patent No. 7,472,163 (“Ben-Yoseph”)
- APPLE-1050 U.S. Pub. No. 2005/0233737 (“Lin”)
- APPLE-1100 Complaint, *HBCU Messaging US LP v. Apple, Inc. et al.*, 1-24-cv-01199 (WDTX) (Oct. 7, 2024)
- APPLE-1101 Infringement Charts of the ’182 Patent
- APPLE-1103 U.S. Pub. No. 2007/0299930 (“Wendelrup”)

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, and at the direction of counsel, I have applied the July 24, 2007 filing date of the Australian Patent Application No. 2007903979 listed on the face of the ’182 Patent 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 July 24, 2007.

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 1-30 of the '182 Patent are obvious over Horvath in view of Tsampalis.

IV. BACKGROUND KNOWLEDGE ONE OF SKILL IN THE ART WOULD HAVE HAD PRIOR TO THE PRIORITY DATE OF THE '182 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 '182 Patent by the Critical Date (July 24, 2007) would have had at least a bachelor’s degree in computer science, electrical engineering, computer engineering, or a related field, with 2-3 years of industry experience in computer networking and

wireless telecommunications. 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 was such an individual at the time of the Critical Date. Moreover, I have taught, participated in organizations, and worked closely with many such persons over the course of my career.

V. INTERPRETATIONS OF THE '182 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 for the Petitioner that I should use July 24, 2007 as the point in time for claim interpretation purposes.

VI. THE '182 PATENT

A. Overview of the '182 Patent

24. The '182 Patent describes techniques for messaging over wireless networks in which a sending wireless device selects a transmission mode for

sending an outgoing message based on information indicating whether an intended recipient of the message is a subscriber of a service for receiving messages via a packet-switched bearer. APPLE-1001, Abstract, 2:30-3:2, 8:5-10:8. The Abstract summarizes the disclosed techniques as follows, for example:

A system may comprise a sending mobile phone that transmits SMS messages via a cellular network and packet switched messages via a packet switched message service (PSMS) and at least one server that supports the PSMS, maintains status information and queues messages for later delivery.

APPLE-1001, Abstract.

25. FIG. 3 is a flowchart that illustrates an example process for selecting a transmission mode for an outgoing message based on information about the recipient:

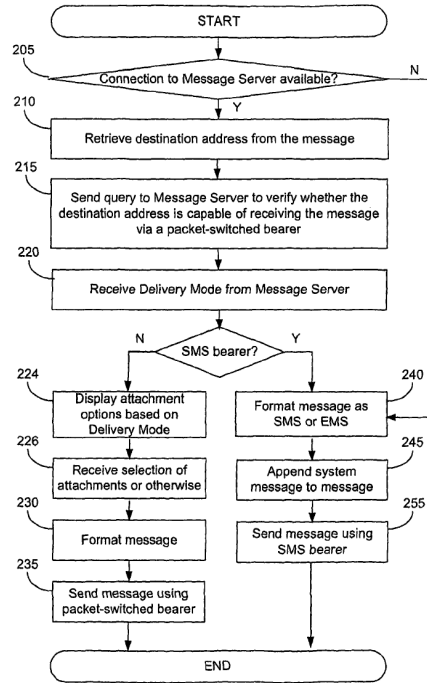


FIG. 3

APPLE-1001, FIG. 3

B. Prosecution History of the '182 Patent

26. During prosecution, the examiner allowed the claims without a prior art rejection¹ and did not consider any of the art applied in this Declaration. APPLE-1002.

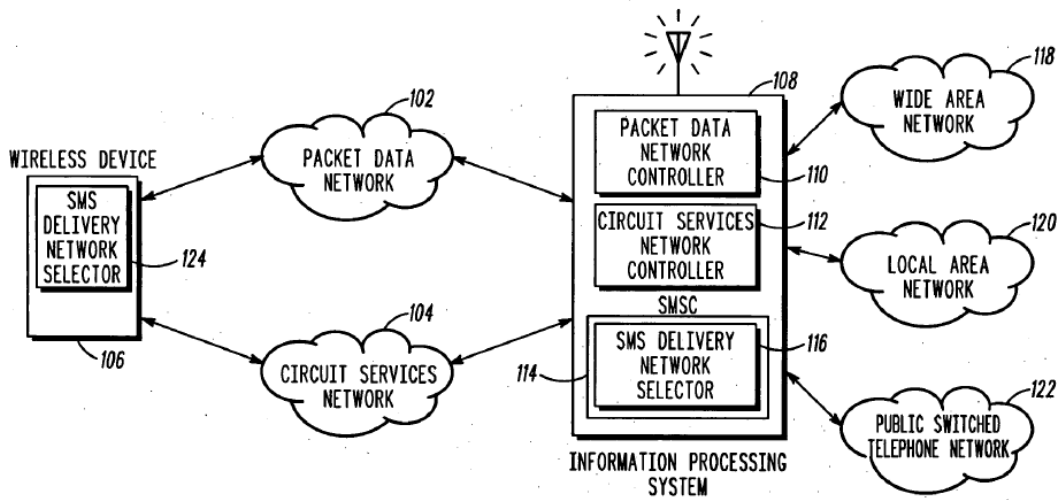
¹ The Office issued only a double patenting rejection of then pending claims 1-17 and 20, based on co-pending Application No. 17/959,697 (later issued as U.S. Patent No. 11,653,183), and claim 21, based on co-pending Application No. 17/959,697 in view of US2007/0299930 Wendelrup et al., for which Applicant filed a Terminal Disclaimer. APPLE-100261, 80, 94-102. The Office noted that

VII. OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES

A. Overview of Horvath

27. Horvath discloses a method and system for “transmitting short message service messages” with “a wireless device” over “a packet data network 102 and a circuit services network 104.” *See e.g.*, APPLE-1004, Title, [0001]-[0002], [0007], [0024]-[0026], [0033], FIGS. 1, 2. Horvath’s wireless device (*e.g.*, “wireless device 106”) is “a dual mode device capable of communicating on either the packet data network 102 or the circuit services network 104,” “based on [a] registration status of the wireless device.” APPLE-1004, [0007]-[0008], [0024], [0061], FIGS. 1 (below), 2, 4.

“[i]n an analogous field of endeavor, Wendelrup [APPLE-1103] discloses wherein the server is located outside of the cellular network (paragraph 0066, software which is downloaded remotely from a server either outside or inside the cellular network).” APPLE-1002, 101.

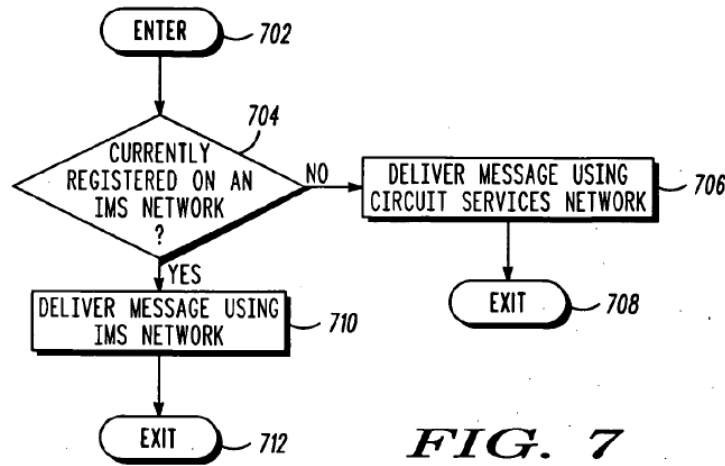


100
FIG. 1

APPLE-1004, FIG. 1

28. As shown in FIG. 1, wireless device 106 can function both as a sender device that sends messages destined for remote recipient device(s) and as a recipient device that receives message(s) sent from remote sender device(s). When wireless device 106 is instructed to send an SMS message (operating as a sender device), “the wireless device 106 first determines if it [*i.e.*, the sending wireless device] is registered on the packet data network 102,” and based on this determination, an “SMS delivery network selector 124” residing on the wireless device 106 “selects a network 102, 104 for the wireless device 106 to transmit [the] SMS message on.” APPLE-1004, [0050], [0062] (“[I]f the wireless device 106 is registered on the packet data network 102, the SMS delivery network selector 124 selects the packet data network 102 for transmission of the SMS message. If the

wireless device is not registered on the packet data network 102, the SMS delivery network selector 124 selects the circuit services network 104 for transmission of the SMS message.”), [0078], FIGS. 1, 4, 7.



APPLE-1004, FIG. 7 (Sender Device Perspective)

29. Although Horvath focuses on the selective use of packet switched or circuit switched bearers for delivery of SMS messages, Horvath notes that wireless device 106 can transmit other types of messages as well, including enhanced messaging service (“EMS”) messages, multimedia service (“MMS”) messages, and instant messages (“IM”). APPLE-1004, [0025], [0038]-[0039] (“An IMS system also includes application servers that host and execute services for the wireless device 106. A service for example, is SMS, MMS, ...and the like.”). A session initiation protocol (“SIP”) network operates atop the packet data network 102 to establish communication sessions and carry encapsulated SMS messages between wireless devices and a server when the circuit switched network 104 is not

used. *Id.* [0041], [0033] (“The SIP network is used for establishing instant messaging, ... and other real-time communications over the Internet.”), [0050], FIG. 5.

30. When a message is requested to be sent to a wireless device (e.g., wireless device 106) in Horvath’s system, the message request is first routed to a server system (e.g., information processing system 108) including a “Short Message Service Center (‘SMSC’ [114]).” APPLE-1004, [0045]-[0047], FIGS. 1-2. SMSC 114 includes an “SMS delivery network selector 116” that “selects either the packet data network 102 or the circuit services network 104 for delivery of a SMS message” based on whether the intended recipient of the message is currently registered on the packet data network 102. *Id.*, [0053], FIG. 3; *see also id.*, [0028], [0045]-[0047], FIGS. 1-2. SMSC 114, with SMS delivery network selector 116, determines the registration status of the recipient wireless device by checking whether the recipient is currently registered with an SIP network on the packet data network 102.² *Id.*, Abstract, [0002], [0006], [0008], [0028], [0033]-[0038], [0075]-

² The SIP network is supported by an “Internet Protocol multimedia subsystem” (IMS) core and is capable of transmitting rich **multimedia** data. APPLE-1004, [0034]; *see also* APPLE-1012 (describing IMS networks in further detail).

[0076], FIGS. 1, 2, 3, 6. By delivering messages to wireless devices over a packet data network rather than a circuit switched network when a recipient device is registered with the packet data network, Horvath's system reduces the amount of traffic transmitted over the circuit switched network, thereby freeing bandwidth for voice calls or other services on the circuit switched network. APPLE-1004, [0009], [0021], [0039], [0050].

31. FIG. 6 is a flowchart that illustrates "an exemplary process of a SMSC selecting either a circuit services network or a packet data network for delivery of a SMS message to a wireless device" (APPLE-1004, [0016]):

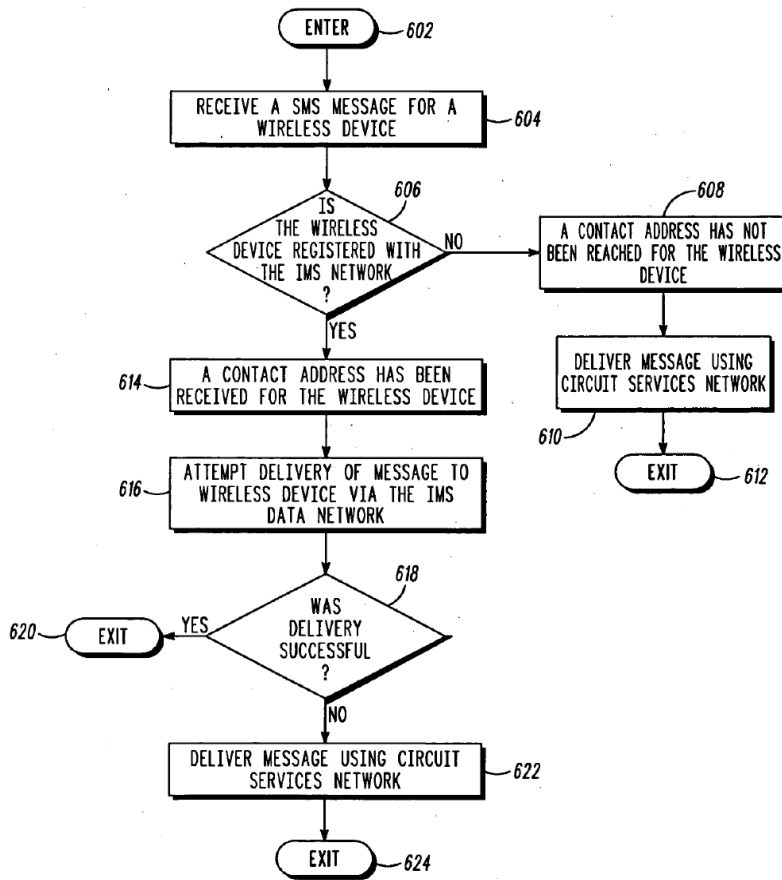


FIG. 6

APPLE-1004, FIG. 6 (Server Perspective)

B. Overview of Tsampalis

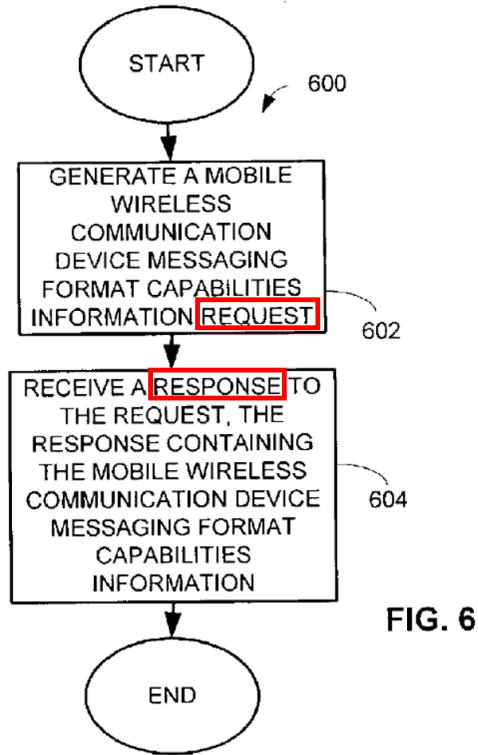
32. Tsampalis describes a “method and apparatus for providing wireless messaging” in which a first mobile wireless communication device 100 (*i.e.*, a sender device) obtains, either locally or via “a web server” or other “network element,” “messaging format capabilities information 110” of a second mobile wireless communication device 200 (*i.e.*, a recipient device) before the sender device sends a message. *See e.g.*, APPLE-1005, Title, Abstract, [0029]-[0039],

FIGS. 1, 2 (below, highlighting the local and remote messaging format capabilities determinator circuitries residing on the first wireless device), 5-7. The messaging format capabilities information 110 (MFCI) indicates the types of messages (*e.g.*, SMS, MMS, EMS) that the intended recipient device is capable of processing. APPLE-1005, [0022]-[0024].

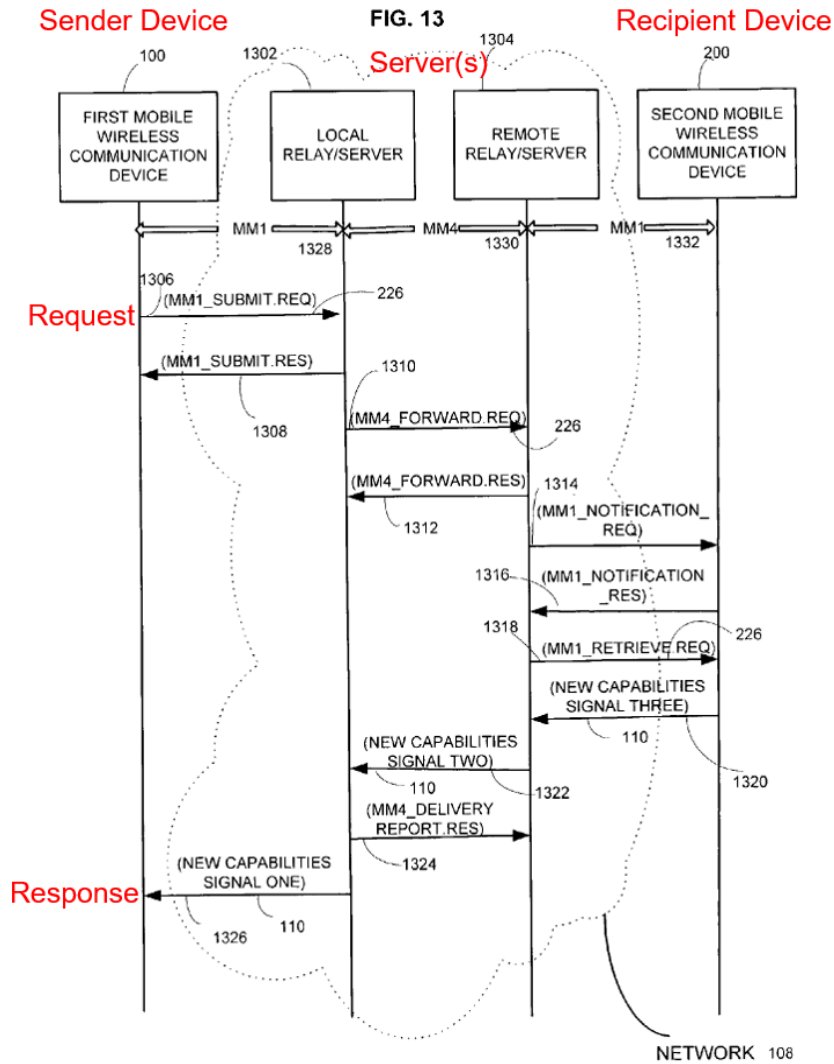
capabilities information **request**” to a remote web server, and “receiv[es] a **response** [e.g., from the web server] to the request where the response contains the second mobile wireless communication device messaging format capabilities information 110.” APPLE-1005, [0024], [0027], [0042] (both generation of the request and reception of the response “may be accomplished using the remote messaging format capabilities determinator circuitry 208” or “other suitable circuitry”), [0034], [0056]-[0057] (“request and retrieve the second mobile wireless communication device messaging format capabilities information 110,” “a second mobile wireless communication device messaging format request 226,” “new capabilities signal one 1326 [including] at least the second mobile wireless communication device messaging format capabilities information 110”), FIGS. 6 (below), 13 (below).

34. In some examples, Tsampalis explains that “the second mobile wireless communication device messaging format capabilities information 110 is stored” in “a network element within the network 108” such as “a web server.” *Id.*, [0039], [0057] (“note that some embodiments store the second mobile wireless communication device messaging format capabilities information 110 at the remote relay/server 1304, and for such embodiments, signals 1314, 1316, 1318 and 1320 are not used”). In such cases, the first (sender) device can retrieve the second

(recipient) device's MFCI 110 from a remote server using signaling like that shown in FIG. 13 (below). *Id.*; *see also id.*, [0056]-[0060], FIGS. 13-15.



APPLE-1005, FIG. 6 (Annotated)



APPLE-1005, FIG. 13 (Annotated)

35. Tsampalis further explains that the first (sender) device can store the second (recipient) device's MFCI 110 in a phonebook, and can use the second (recipient) device's MFCI 110 to select a suitable message format and corresponding transmission mode (e.g., an SMS, MMS, or EMS transmission) for sending the message based on the capabilities of the second (recipient) device.

APPLE-1005, [0041], [0060]-[0064], FIGS. 5, 16.

C. Overview of Chatterjee

36. Chatterjee provides a brief history of the development of instant messaging and presence (“IM&P”) technology and a summary of various standards, where “[i]nstant messaging is an application that enables networked users to send and receive short messages. Presence provides information about users’ reachability and willingness to accept/reject a brief chat session.” APPLE-1007, Abstract. Chatterjee explains, “IM systems, with the ability of providing presence information, enables a user to know the availability of other users. By using presence information, an IM system enables us to search for a specific user, check the user’s status, and send short messages.” APPLE-1007, page 4. According to Chatterjee, which was published back in 2005, “[p]opular IM applications include AOL™ Instant Messenger (AIM), ICQ™ (“I Seek You”), MSN™ or WindowsXP™ Messenger, and Yahoo™ Messenger.” APPLE-1007, page 4, Table 1 (below).

IM solutions	Characteristics	Vendor examples
Public services	Available to anybody; often free; use a centralized third-party server to relay messages	AOL Instant Messenger™, MSN Messenger™, Yahoo! Messenger™
Private services	IM systems designed for enterprise and corporate use; secure IM, message logging, enterprise-class service, corporate control	AOL Enterprise AIM™, Yahoo Messenger Enterprise™, Microsoft Messenger Connect for Enterprise™, IBM Lotus Sametime™
Collaboration tools	These collaborative systems include presence technology	IBM Lotus Sametime™, Groove Network Inc's Groove Workspace™
Carrier/network services	Convergence products that are now IM&P-enabled	Bantu Inc, Comverse Inc., DynamicSoft Inc., FaceTime Communications, Invertix Corp., NotePage Inc., PresenceWorks Inc., Vayusphere Inc.
Open source tools	Based on open source	Jabber Inc., Jabber.Org

■ Table 1. Instant messaging systems.

APPLE-1007, Table 1

D. Overview of Kansal

37. Like the Horvath-Tsampalis-Chatterjee combination, Kansal provides mobile messaging services for sending and receiving messages of different formats. APPLE-1042, Abstract, [0009], [0035] (“an IM application,” “an SMS application,” and “an MMS application”). Kansal describes arranging and correlating received messages of different types with a particular recipient.” APPLE-1042, [0009]; [0040]-[0043]; [0066]-[0069]. The wireless device can display a “messaging user interface” that “display[s] a messaging thread comprising correlated messages of different message types,” including “SMS messages, MMS messages, as well as, telephone messages, voicemail messages, fax messages, video conferencing messages, IM messages, and e-mail messages.” APPLE-1042, [0009], [0045]-[0046], [0054]-[0056], [0062]-[0064], [0070], [0077]-[0078], FIGs. 2-3 (shown below).

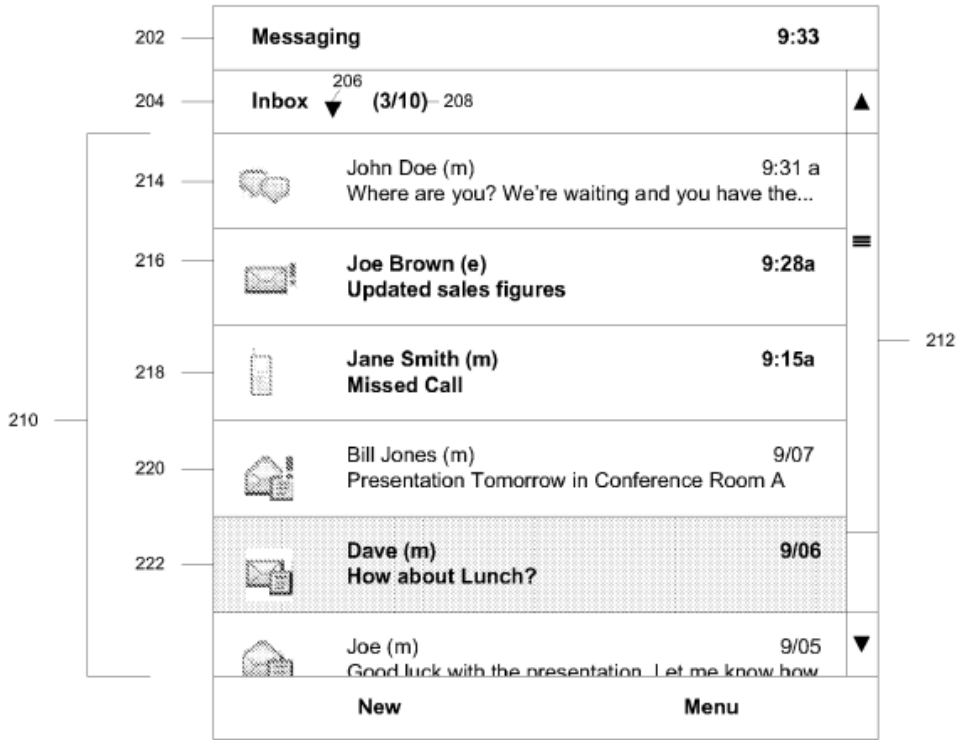


FIG. 2

APPLE-1042, FIG. 2

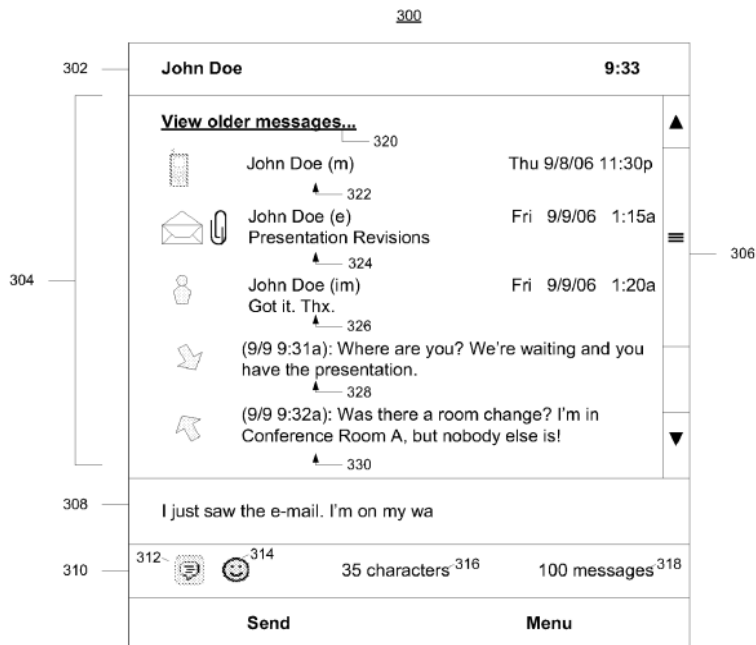


FIG. 3

APPLE-1042, FIG. 3

E. Overview of Lin

38. Lin discloses “a method for establishing a real-time session-based IM system or data exchange system between mobile devices over a digital mobile network system that supports data packet-based communications.” APPLE-1050, [0006]. As part of Lin’s method, “[t]he initiating mobile device [] transmits its IP address, including its TCP port number, the user's personal conference number and the user’s PIN (to authenticate the user as the moderator) in an SMS text message to [a] telephone number of [a] server 420.” *Id.*, [0017], FIG. 4; *see also id.*, Abstract, [0014]-[0016], FIGs.2-3.

VIII. GROUND 1: CLAIMS 1-30 ARE OBVIOUS IN VIEW OF THE HORVATH-TSAMPALIS-CHATTERJEE-KANSAL COMBINATION

A. Combination of Horvath and Tsampalis

39. Like the '182 Patent, Horvath describes selective transmission of wireless messages via different transmission bearers, including techniques for transmitting messages over either a packet data network or a circuit services network. APPLE-1001, 3:7-38; APPLE-1004, [0001], [0007], [0024]-[0026], [0050], [0061]-[0062], FIGS. 1, 4, 7; *supra*, Horvath Overview. Horvath is concerned with the circuit services network being “unnecessarily burdened with SMS traffic,” and proposes to ameliorate this problem by using a packet data network for the transmission of SMS messages by default whenever the sending and receiving devices are registered with a message delivery service on the packet data network (*e.g.*, registered with an SIP network). *See e.g.*, APPLE-1004, [0004], [0006]-[0009], [0021], [0039] (goal to provide “capacity relief on the circuit services network 104”), [0081] (desire to “provide dynamic optimization of the resources available” and to “optimiz[e] network resources”).

40. As described above, Horvath’s sender device determines whether to send an outgoing SMS message to a server system (*e.g.*, Information Processing System 108 / SMSC 114) over a packet data network or a circuit switched network based on whether the sender is currently registered with a session initiation protocol (“SIP”) network on the packet data network. *Supra*, Horvath Overview; APPLE-1004, [0004], [0074]-[0076], FIG. 6 (below). The server system in turn

determines whether to forward the SMS message to the intended recipient device over a packet data network or a circuit switched network based on whether the recipient is registered on the packet data network. *Id.*

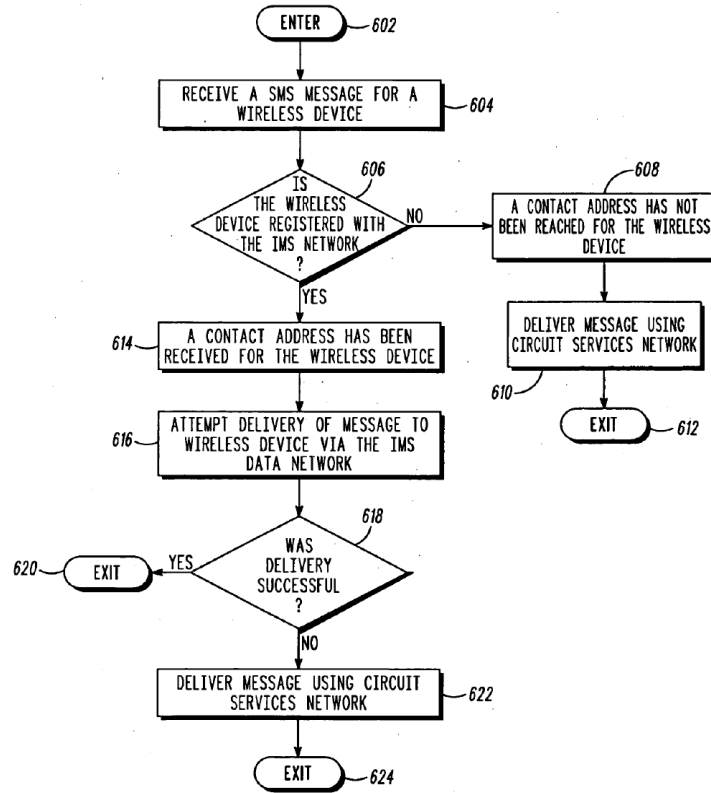


FIG. 6

APPLE-1004, FIG. 6 (Server Perspective)

41. By diverting SMS messages from the circuit switched network to the packet data network when a device is registered on a packet data network, Horvath’s system beneficially reduces load and “unnecessary overhead” on the circuit switched network. APPLE-1004, [0004], [0009]. Notwithstanding these benefits, however, a POSITA would have recognized that Horvath’s system was

still ripe for improvement. For example, although Horvath acknowledges additional messaging services apart from SMS (e.g., MMS, EMS, IM), Horvath provides little detail about the additional messaging services. APPLE-1005, [0025], [0039]. Additionally, a POSITA would have appreciated that some users did not necessarily subscribe to each of these messaging services and users often had limited messaging capabilities that precluded them from receiving or processing richer media formats beyond SMS (e.g., MMS, EMS, IM). Consequently, the sender risked sending a message in a format that the recipient would be incapable of processing or presenting to a user. This, in turn, resulted in failed message deliveries, re-transmission attempts that further burdened the network, increased processing load on messaging servers, and frustration by users who expected messages to be delivered in one format but which ultimately could not be delivered as expected. APPLE-1005, [0003]-[0004].

42. In view of these known problems with a multi-modal messaging environment like Horvath's in which different mobile device users subscribed to messaging services (e.g., SMS, MMS, EMS, IM), a POSITA would have turned to Tsampalis for specific guidance on how to improve the user experience and better manage and coordinate messaging formats in such an environment. *Supra*, Horvath Overview; Tsampalis Overview. In particular, Tsampalis describes an effective solution for improving messaging in such an environment by sharing the

recipient's messaging format capabilities information with the sender. *Supra*, Tsampalis Overview. A POSITA reviewing Horvath and Tsampalis would have found it obvious to implement Horvath's system in accordance with Tsampalis's suggestions for a sender device to obtain and use messaging format capabilities information of a recipient device to determine how to format and transmit an outgoing message to the recipient. Multiple reasons would have prompted a POSITA to combine Horvath's and Tsampalis's teachings in this manner well before the Critical Date of the '182 Patent (July 24, 2007).

43. First, a POSITA would have combined Horvath and Tsampalis such that the sender would obtain and use a recipient's messaging format capabilities information to enhance users' messaging experiences and ensure that the format of outgoing messages is compatible with the messaging format capability of the recipients' device before the message is sent. Tsampalis itself expressly acknowledges the benefits flowing from these techniques, noting that "the determining of the message capabilities of a target mobile wireless communication device before sending a message to such target device[] ... can enhance a user's experience by allowing a user to determine whether to attempt to send or modify a message based on the messaging capabilities of the intended recipient(s) of the message" and "by providing the user the ability to select a format in which to send a message based upon the messaging capabilities of the intended recipient(s) of the

message.” APPLE-1005, [0065]. Horvath also already considers the challenge of encoding in different network standards, which would further prompt a POSITA to combine with Tsampalis for teachings on formatting compatibility. *See e.g.*, APPLE-1004, [0050] (describing message encoding using “IS-637” versus very different “ANSI-41” standard).

44. Second, a POSITA would have sought to leverage Tsampalis-like messaging format capabilities information in Horvath’s system to permit the sender to make more frequent and reliable use of enhanced messaging formats such as MMS and IM. Enhanced messaging formats such as MMS and IM generally offer richer messaging capabilities than SMS, such as the ability to support extended character counts for longer messages and the ability to attach/include multimedia files with the message. APPLE-1007, Page 8 (“IM&P [*i.e.*, Instant Messaging and Presence] service is more media-rich than traditional applications such as mail, phone, and email. By using IM&P, we can deliver voice, video, and data together to various endpoints.”); APPLE-1025, Introduction (“The most significant characteristic of MMS is to support multimedia contents. It can send not only texts, but also images, videos and audios. Therefore, MMS applications are much richer than those of SMS.”). A POSITA would have understood that the enhanced messaging capabilities of MMS and IM were often desirable for situations where users desired to communicate more than the short,

text-based messages that could be accommodated by SMS. If the recipient's messaging capabilities are unknown, however, some senders are biased toward not using any of the enhanced messaging features of MMS or IM to ensure the message is successfully delivered to the recipient using a more basic service (e.g., SMS). But intentional avoidance of enhanced messaging features offered by MMS or IM is unnecessary if the recipient is in fact capable of receiving MMS or IM messages, and Tsampalis's proposal to share the recipients' messaging format capabilities information with the sender would allow a sender to use these rich messaging features more frequently and reliably with confidence that the recipient can successfully receive them.

45. Third, a POSITA would have sought to leverage Tsampalis-like messaging format capabilities information in Horvath's system to make better, more selective use of SMS when the recipient has limited messaging capabilities. As Tsampalis explains, some users do not subscribe to MMS and are incapable of receiving or processing messages other than SMS or similar text-based messages. APPLE-1005, [0061]-[0063]. By obtaining the recipients' messaging format capabilities information in advance of sending a message, the sender can ensure the message is appropriately sized and formatted according to the restrictions imposed by SMS and the limited messaging capabilities of the recipient. Likewise, the

sender can avoid making use of richer features associated with formats such as MMS or IM that the recipient could not receive or process.

46. Fourth, a POSITA would have been motivated to apply Tsampalis's teachings to Horvath in the manner described above to ensure the sender could recognize any incompatibilities between the format of an outgoing message and the messaging format capabilities of the intended recipient of the message *before* the message is sent. In addition to enhancing the user's experience, Tsampalis's approach to making use of messaging format capabilities information before a message is sent would beneficially reduce occurrences of failed message deliveries resulting from attempts to send incompatible message formats. It would likewise reduce network traffic and corresponding load on the system by reducing the number of re-transmission attempts stemming from failed message deliveries. APPLE-1005, [0003], [0004] (lamenting prior approaches where "the sending device is unaware of the incompatibility until after the message is bounced back" because "there is no opportunity for the sending device to change the content of the message, change the recipient list associated with the message, or choose not to send the message, before sending a message that will later be bounced back"); [0022]-[0023], [0025].

47. Fifth, a POSITA would have been motivated to apply Tsampalis-like messaging format capabilities information to Horvath's system to advance

Horvath's express objectives of reducing "unnecessary overhead for the system" and "dynamic optimization of [] resources." APPLE-1004, [0004], [0081]. For example, a POSITA would have appreciated that integration of Tsampalis's techniques in the combination would further optimize the sender's determination of a transmission mode (*e.g.*, whether to send an SMS, MMS, or IM, whether to attach any multimedia files, and/or whether to transmit over the packet data network or the circuit services network), while reducing unnecessary burden on the remote server by having the sender device process/format the outgoing message according to the selected transmission mode.

48. Sixth, a POSITA reviewing Horvath would have naturally looked to Tsampalis's techniques for sharing messaging format capabilities information because, like Horvath, Tsampalis describes communications networks that support multi-modal messaging formats, including "a cellular wireless network, internet or other suitable network." APPLE-1005, [0028]; *see also id.*, [0024]-[0027].

49. Seventh, a POSITA would have found it obvious to combine the teachings of Horvath with Tsampalis because the combination merely involves the application of a known technique to a known system to achieve predictable results. Tsampalis recognized a known problem with dynamic messaging environments like Horvath's in which users have different messaging format capabilities, and yet, Tsampalis's teachings would help address this problem in a straightforward

manner that was well within the skill of a POSITA. A POSITA would have further recognized that at the time of the claimed invention, some users were still charged on a per SMS basis, and being selective about how messages were sent could save costs for both the sender and the receiver. APPLE-1009, 1 (“Sending an SMS message to a mobile telephone carries an attached cost for sending the message over the mobile network...A user of a mobile device whilst in a location with WiFi (or other form of) internet access would authenticate with the remote registration server and this would indicate to the Routing System that it was possible for that mobile device to receive text messages via the internet rather than via GSM SMS messages offering substantial cost savings to the sending party. Replies could also be made over the internet providing further costs savings.”). Accordingly, the combination would have been obvious.

50. Likewise, a POSITA would have reasonably expected success implementing the combination, especially since the resulting system could be implemented with conventional software and hardware techniques (*e.g.*, general-purpose processors on mobile devices executing programmable instructions) with messaging formats (*e.g.*, SMS, MMS, IM) that were well-defined and commonly implemented by the Critical Date of the '182 Patent. Further, the techniques that would be integrated from Tsampalis in the Horvath-Tsampalis combination are fully compatible with Horvath's and would not disturb the ability of Horvath's

system to transmit or deliver SMS messages over either a packet-based or circuit switched network. Indeed, Horvath and Tsampalis both describe multi-modal wireless devices that are physically and logically compatible with each other. As discussed above, Horvath and Tsampalis are also both analogous art to the '182 Patent, each being in the same field of endeavor and reasonably pertinent to the problems said to be addressed by the '182 Patent. For example, like the '182 Patent, Horvath and Tsampalis both describe methods and systems for mobile messaging over wireless networks. *Id.*; *supra*, §VI.A, Horvath Overview, Tsampalis Overview.³

B. Combination of Horvath, Tsampalis, and Chatterjee

51. Horvath and Tsampalis each describe conventional mobile messaging services for wireless devices, including SMS, MMS, and EMS. APPLE-1004,

³ The overview of the Horvath-Tsampalis combination described in §VIII.A, the Horvath-Tsampalis-Chatterjee combination described in §VIII.B, and the Horvath-Tsampalis-Chatterjee-Kansal combination described in §VIII.C below are incorporated in the analysis of each claim element in Ground 1 below. For claim elements in which the Declaration cites Horvath's teachings alone, it is understood that those teachings are applicable in the combination and are not negated by the combination with Tsampalis, Chatterjee, and Kansal.

[0025] (“Text messaging standards such as Short Message Service (‘SMS’), Enhanced Messaging Service (‘EMS’), Multimedia Messaging Service (‘MMS’), and the like are also included in the networks 102, 104.”); APPLE-1005, [0002] [0024] (“FIG. 1 illustrates a mobile wireless communication device such as a cellular telephone, two-way pager, or other device employing non-real-time store-and-forward messaging (e.g., SMS, EMS, MMS).”). While SMS, MMS, and EMS feature prominently in Horvath and Tsampalis, a POSITA would have appreciated that additional services were also commonly used for messaging on wireless devices by the Critical Date. For example, Horvath notes that its “IMS system also includes application servers that host and execute services for the wireless device 106,” where the services can include “SMS, MMS, caller ID, call waiting, push-to-talk, voicemail, and the like.” APPLE-1005, [0039]. Horvath also explains that “[t]he SIP network is used for establishing instant messaging, telephone calls, and other real-time communications over the Internet.” *Id.*, [0033]. Notably, Horvath acknowledges the option for additional messaging services such as instant messaging, although Horvath leaves many of the implementations details of these additional services to a POSITA. A POSITA interested in pursuing additional messaging services as suggested by Horvath would have turned to references like Chatterjee for further detail about the capabilities of these services and how to implement them.

52. As discussed above, Chatterjee describes various frameworks for instant messaging and presence (“IM&P”) services that were in widespread use long before the Critical Date. *Supra*, Chatterjee Overview. A POSITA reviewing Chatterjee would have found it obvious to apply Chatterjee’s suggestions for implementing an IM&P service in the Horvath-Tsampalis system such that the wireless device (*e.g.*, wireless device 106) in the resulting Horvath-Tsampalis-Chatterjee system would be further configured to send and receive instant messages, and to send and receive presence information indicating the availability of devices for receiving IMs. In the combination, the messaging format capabilities information shared with the sender device based on Tsampalis’s teachings would further include an indication of whether the intended recipient of a message is capable of receiving IMs in addition to other messaging formats such as SMS, MMS, and EMS. Multiple reasons would have prompted a POSITA to implement the combination.

53. First, a POSITA would have implemented instant messaging in the combination system to “enable[] short message exchanges between online users ... in real time” and “independent of locale.” APPLE-1007, 4. Chatterjee explains that the “real-time” nature of instant messaging services “differentiates IM” from other conventional messaging services, and IM beneficially allows users to “engage in real-time discussions” that facilitate “collaboration” and “improve[d]

decision making.” APPLE-1007, 4, 8; *cf.* APPLE-1005, [0002], [0024] (describing SMS, MMS, and EMS as “non-real-time store-and-forward messaging”).

54. Second, a POSITA would have implemented instant messaging in the combination system to expand the capabilities of the device and keep current with the growing popularity of instant messaging in the timeframe leading up to the '182 Patent. APPLE-1007, 4 (“Although IM started as a consumer-grade technology, it was quickly adopted by many businesses that saw its advantages in enabling quick communications and providing presence information. ... This new phenomenon is now impacting schools and college campuses.”).

55. Third, a POSITA would have implemented instant messaging in the combination system to promote the ability of organizations to readily “distribute various information including emergency news, [] events, and other important announcements” to users of the IM service. APPLE-1007, 8. Chatterjee specifically observes that “[u]sing IM increases efficiency and productivity if it is ubiquitous (i.e., available on the cell phone and used extensively ...).” APPLE-1007, 10.

56. Fourth, a POSITA would have considered IM to be a desirable messaging format to implement in the combination system because it “is more media-rich than traditional applications such as mail, phone, and email,” and IMs can deliver not only text but also “voice, video, and data together to various

endpoints.” APPLE-1007, 8. Further, “the delivered messages” can “integrate ... with existing systems and infrastructure” thereby “sav[ing] both time and money.” APPLE-1007, 8.

57. Fifth, to the extent presence is not obvious given that it is part of the SIP standard, Chatterjee makes it explicit, as a POSITA would have implemented presence capabilities in the combination system to better inform users of the instant messaging service when other users are available to receive instant messages. APPLE-1044 (a 2004 RFC already establishing the availability of presence functionality for SIP), Abstract (“This document describes the usage of the Session Initiation Protocol (SIP) for subscriptions and notifications of presence”); APPLE-1007, 4 (“By using presence information, an IM system enables us to search for a specific user, check the user’s status, and send short messages. ... We are also aware, in this case, whether or not the user is open to communicating at this time.”).

58. Sixth, it would have been obvious in view of Chatterjee to extend Tsampalis’s messaging format capabilities information in the combination system to further indicate an intended recipient’s instant messaging capability (*e.g.*, in addition to SMS, MMS, EMS capabilities). A POSITA would have understood that identifying additional messaging capabilities of the intended recipient of a message, including information indicating whether the intended recipient is capable of receiving instant messages, would further Tsampalis’s goal of enabling

the sending device to select an optimal message format before sending a message, thereby enhancing the user's experience and reducing attempts to transmit a message in a format that the recipient is either incapable of receiving or that does not make best use of the recipients' messaging capabilities. APPLE-1005, [0065], [0003]-[0004]. Tsampalis identifies SMS, MMS, and EMS as "non-real-time store and-forward messaging format capabilities," but Tsamaplis does not restrict the messaging format capabilities information from further including other messaging formats. APPLE-1005, [0022] (describing non-real time store-and-forward as a mere example of messaging format capabilities information ("such as")). Indeed, a POSITA would have preferred to inform the sender of all messaging format capabilities of the recipient, including IM, to provide the sender with comprehensive information that would better allow the sender to optimize its selection of a format for messaging the recipient. *See also* APPLE-1007, 6 (describing known option for "store-and-forward" IM services).

59. Finally, a POSITA would have found it obvious to apply an IM&P service based on Chatterjee in combination with Horvath-Tsampalis because the combination merely involves the use of well-known techniques for instant messaging and presence to a known system to achieve predictable results. A POSITA would have reasonably expected success implementing the combination, especially since the resulting system could be implemented with conventional

software and hardware on mobile devices using IM&P services that were well-established by the Critical Date. APPLE-1007, 10 (describing IM “available on the cell phone”), 4 (IM has been “quickly adopted”). Notably, Horvath explicitly describes the option of using a SIP network for instant messaging, and Chatterjee expands on IM&P services such as SIMPLE that were specifically developed to operate on SIP networks, or Jabber that was capable of interfacing with an SIP server. APPLE-1007, 5-8, FIG. 2 (depicting “SIMPLE components”), FIG. 3 (depicting “Foreign IM gateway (Jabber to SIP)”). Chatterjee is also analogous art to the ’182 Patent and fully compatible with Horvath and Tsampalis, each being in the same field of endeavor and reasonably pertinent to the problems said to be addressed by the ’182 Patent. For example, like the ’182 Patent, Tsampalis describes methods and systems for mobile messaging over wireless networks (*e.g.*, using IM).

C. Combination of Horvath, Tsampalis, Chatterjee, and Kansal

60. As discussed above, the Horvath-Tsampalis-Chatterjee combination provides a wireless mobile device capable of messaging using different messaging services including, SMS, MMS, and IM. *Supra* §VIII.B. It would have been obvious to apply Kansal’s suggestion for a messaging UI to display messages formatted according to these different formats within a single application UI. To the extent Kansal does not explicitly describe its messaging and displaying

functions implemented by a same messaging application, a POSITA would have found it an obvious design choice. *See also* APPLE-1042, FIG. 1 (using term “IM App 135” without differentiating whether it can be implemented by a single IM application or multiple IM applications). Indeed, technologies for displaying messages of different formats on a unified interface by a single messaging application was well known by the Critical Date. APPLE-1045, 1-3 (describing “Trillian Pro v1.0” as a multi-protocol messaging application released back in 2002, which incorporated various IM protocols and SMS on mobile phones, “all within one new powerful and professional interface,” “Trillian’s universal connectivity allows you to chat on all major chat networks, including AIM, MSN, ICQ, Yahoo!, and IRC simultaneously,” while its “Mobile Integration” feature also integrating “SMS, Short Message Service, [which] is text messaging to & from cellular phones.”). In fact, multiple reasons would have prompted a POSITA to implement this combination.

61. First, a POSITA would have been motivated to apply Kansal’s suggested unified messaging user interface to the wireless device in the resulting combination to improve the user’s experience with mobile messaging services involving messages of different types (*e.g.*, SMS, MMS, IM). This would have predictably achieved Kansal’s stated goals to meet the “need for an improved apparatus and methods for providing enhanced mobile messaging services.

APPLE-1042, [0002]. For example, correlating messages in a manner that allows a user to view all messages of various types with a particular user at a glance in a single thread would be advantageous in allowing a user to see all messages sent to particular recipients or received from particular senders within a single interface without needing to navigate to different messaging applications or interfaces for each different message type. APPLE-1045, 1-2 (advertising the benefits of a multi-protocol messaging application with a single interface for providing “better experience,” “a powerful and efficient user experience.”); APPLE-1042, [0009], [0045]-[0046], [0054]-[0056], [0062]-[0064], [0070], [0077]-[0078], FIGs. 2-3.

62. Second, providing a single thread of messages would have predictably improved the user interface by providing additional contextual information for a user of the wireless device. For example, Kansal explains that the thread can be “sorted in various ways such as by time of receipt.” APPLE-1042, [0049]; *see* FIGs. 2-3. In addition to improving the user experience (as described in the first reason), Kansal’s UI suggestions would provide additional contextual information that would otherwise not be readily conveyed. For example, as shown in FIG. 3 of Kansal, the chronologically ordered communication events (*e.g.*, missed call at 218 and urgent email request at 216) would beneficially provide additional context for the later received text message (*e.g.*, at 214). APPLE-1042, FIG. 3. As another example, the same user interface in FIG. 3 includes a “message count 208”

indicating the number of messages and unread items across services. APPLE-1042, [0048]. A POSITA would have sought to implement Kansal's user interface to provide this additional contextual information to a user.

63. Third, Kansal's techniques are fully compatible with the types of messaging formats disclosed in each of Horvath, Tsampalis, and Chatterjee (e.g., SMS, MMS, IM), and these formats are expressly identified in Kansal as services that can be integrated within its messaging interface. *See supra* §§VII.A-D. Applying Kansal's suggestion for a unified messaging interface for each of these services in the context of references with the same services to obtain a substantially similar result would have been obvious. Moreover, Kansal is analogous art to both the '182 Patent and Horvath, Tsampalis, and Chatterjee, especially as each are in the same field of endeavor and reasonably pertinent to the problems said to be addressed by the '182 Patent (e.g., mobile messaging). A POSITA would have reasonably expected success implementing the combination as the messaging and communication protocols involved were all well known before the Critical Date.

D. Analysis with Respect to Claims 1-30

Element [1pre]: A system comprising:

64. To the extent the preamble is limiting, the Horvath-Tsampalis-Chatterjee-Kansal combination provides [1pre]⁴. For example, Horvath discloses a variety of methods and systems for wireless communication, such as wireless messaging. *See e.g.*, APPLE-1004, Title (“METHOD AND SYSTEM FOR DELIVERY OF SHORT MESSAGE SERVICE MESSAGES”), Abstract (“A method and device for transmitting at least one short messaging service message to at least one wireless device are disclosed.”), [0011] (“FIG. 1 is block diagram illustrating an exemplary wireless communication system...”) ⁵, [0021] (“the system of the present invention”); *see also* APPLE-1005, [0001] (“The invention relates generally to wireless communication systems and methods, and more particularly to methods and apparatus for providing wireless messaging.”), [0006] (“FIG. 1 is a block diagram illustrating one example of a system in accordance with one embodiment of the invention that provides the obtaining of mobile wireless

⁴ This Declaration incorporates the description of the Horvath-Tsampalis combination from §VIII.A, the Horvath-Tsampalis-Chatterjee combination from §VIII.B, and the Horvath-Tsampalis-Chatterjee-Kansal combination from §VIII.C into the analysis of each element of the Challenged Claims.

⁵ Emphasis added throughout unless otherwise noted.

communication device messaging format capabilities before sending a message to the mobile wireless communication device.”).

Element [1a]: a sending mobile phone that transmits short message service (SMS) messages via a cellular network and packet switched messages via a packet switched message service (PSMS); and

65. Horvath-Tsampalis-Chatterjee-Kansal renders obvious [1a]. For example, Horvath discloses “a wireless device such as a mobile phone” (e.g., “wireless device 106”) (***a sending mobile phone***⁶) capable of “transmitting short message service messages” (SMS) over “a packet data network 102 and a circuit services network 104.” See e.g., APPLE-1004, Title, [0001]-[0002], [0007], [0024]-[0026], [0033], FIGS. 1, 2; see also APPLE-1005, [0022] (“mobile wireless communication devices (e.g., cell phones...)”), [0024] (“a mobile wireless communication device such as a cellular telephone”); APPLE-1007, page 5 (“mobile IM&P services (IMPS)”), page 10 (IM “available on the cell phone”).

66. Horvath’s FIG. 4 (below) further shows an example “wireless device 106” that communicates on “either the packet data network 102 or the circuit services network 104.” APPLE-1004, [0014], [0060]-[0070]. “The SMS delivery network selector 124 selects a network 102, 104 for the wireless device 106 to transmit a SMS message on.” APPLE-1004, [0062].

⁶ Bold and italicized text corresponds to claim language.

Selects network 102 or 104 for transmission

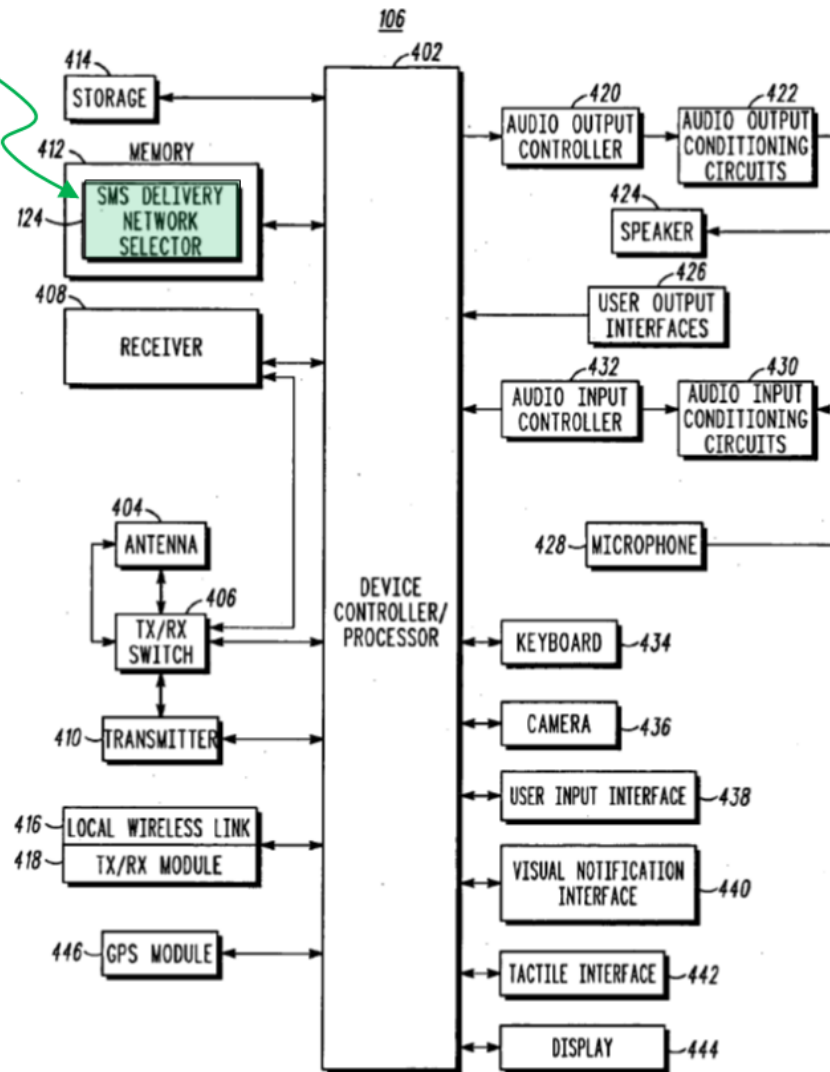
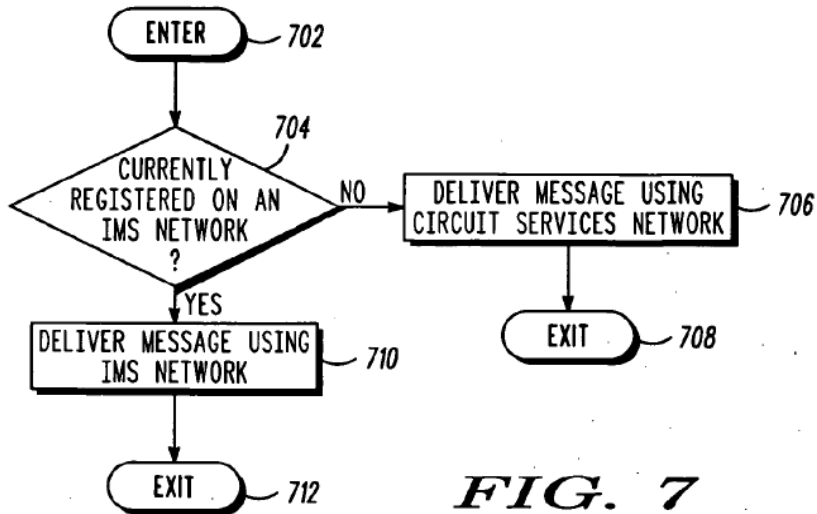


FIG. 4

APPLE-1004, FIG. 4

67. As shown in Horvath's FIG. 7, the sending mobile phone "select[s] a network for transmitting a SMS message based on what network the wireless

device is registered with.” APPLE-1004, [0007]-[0008], [0017], [0024], [0061], [0078]; *supra*, Horvath Overview.



APPLE-1004, FIG. 7 (Sender Device Perspective)

68. In more detail, wireless device 106 sends messages, *e.g.*, short message service (SMS) messages, “through a circuit services network” (*via a cellular network*) if wireless device 106 “is unregistered with” “a registrar associated with a session initiation protocol [SIP] network for communicating over a packet data network.” APPLE-1004, [0002], [0006]-[0007] (“determining, by the wireless device, whether it is currently registered with a registrar associated with a session initiation protocol network for communicating over a packet data network and a circuit services network....If the wireless device is unregistered with the registrar, the at least one short message service message is transmitted through a circuit services network to the at least one wireless device.”).

69. On the other hand, device 106 sends messages in “SIP packets” (*packet switched messages*) “through the session initiation protocol [SIP] network communicating over the packet data network,” *e.g.*, via “instant messaging” (*via a packet switched message service (PSMS)*) established by the “SIP network,” if device 106 “[is] registered with the [SIP] registrar” and subscribed to an instant messaging (IM) service. APPLE-1004, [0002], [0006]-[0007], [0017], [0024] (“In one embodiment, the packet data network 102 is an Internet Protocol (‘IP’) connectivity network, which provides data connections at much higher transfer rates than [*sic*] a traditional circuit services network.”), [0033] (“The SIP network is used for establishing instant messaging...and other real-time communications over the Internet.”), [0034] (“an Internet Protocol multimedia subsystem (‘IMS’) core that supports the SIP network. ... IMS uses a Voice-over-IP implementation and runs over the standard IP. The wireless device 106 can connect to the IMS network using different methods, which all use standard IP. For example, when a wireless device 106 wants to access the packet data network 102, the wireless device 106 registers with the IMS network. The basic functions of an IMS network should be known to those of ordinary skill in the art.”), [0037] (messages are sent over the SIP network in “**SIP packets**”), [0038] (“SIP message”), [0039] (“An IMS system also includes application servers that host and execute services for the wireless device 106. A service for example, is SMS, MMS, ...and the like.”),

[0041] (“the SMSC 114, which is acting as an SIP application server”), [0078], FIG. 7; APPLE-1007 (2005 publication providing an overview of “Instant Messaging and Presence Technologies” and various standards), page 4 (“At this time, a large number of IM systems exist in various Internet communities...”), page 7 (“the network packet with message Hello! sent from Alice@foobar.com to Bob@foobar.com is represented in Box 1. The network packet was captured on the source machine (Alice’s machine) using Ethereal Network Protocol Analyzer available at <http://www.ethereal.com>. The packet is not an exact illustration of all the details. It just gives an overview of how the information is stored and transferred on the network...”), Boxes 1 & 2, Table 1 (listing various “IM solutions” such as “AOL Instant Messenger™, MSN Messenger™, Yahoo! Messenger™”); *supra*, Horvath Overview, Chatterjee Overview, §VIII.B (Horvath-Tsampalis-Chatterjee combination).

70. To be clear, Horvath’s traditional circuit services networks 104 include traditional “CDMA” or “GSM” type of cellular networks. APPLE-1004, FIGS. 1, 2, [0002] (“Traditionally, SMS messages are sent over circuit services networks such as Code Division Multiple Access (‘CDMA’) 1x networks.”), [0026] (“the circuit services network 104 may comprise Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA), Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), Frequency

Division Multiple Access (FDMA), Orthogonal Frequency Division Multiplexing (OFDM), or the like.”), [0039] (“The present invention is not limited to the IS-41 based circuit network. Other networks such as a GSM map circuit network can also be used.”); APPLE-1014, [0006] (“cellular network (*e.g.*, GSM-global system for mobile communications)”), [0047] (“other cellular network technologies (*e.g.*, UMTS, CDMA...)”).

Element [1b]: at least one server that supports the PSMS and maintains status information;

71. Horvath-Tsampalis-Chatterjee-Kansal renders obvious [1b]. A POSITA would have understood and found obvious that Horvath-Tsampalis-Chatterjee-Kansal’s remote server system (*e.g.*, “information processing system 108”) supports packet switched “instant messaging” service (***the PSMS***) and maintains status information. *See e.g.*, APPLE-1004, [0033], [0038], [0046], [0052], FIGS. 1 (below), 2, 3; APPLE-1007, pages 4, 5, 10, Table 1, FIG.1; *supra*, §§VII.C, VIII.B, Analysis of [1a]; *infra*, Analysis of [1k] (limiting PSMS).

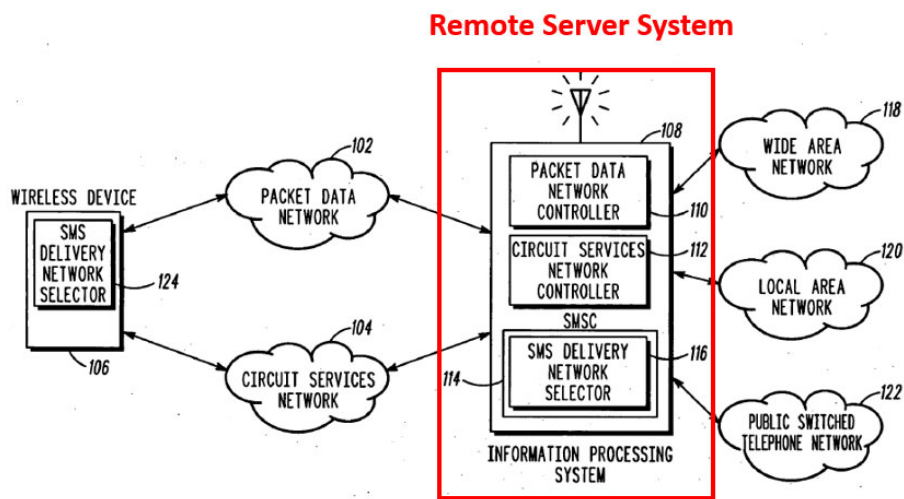


FIG. 1

APPLE-1004, FIG. 1 (Annotated)

72. In more detail, as discussed above, Horvath describes a set of remote servers, *e.g.*, a “Short Message Service Center (‘SMSC’ [114]),” a “proxy call session control function (‘P-CSCF’) 206,” an “interrogating/serving call session control function (‘I, S-CSCF’) 208,” and a “registrar such as a home subscriber server (‘HSS’),” which could be implemented as a single “information processing system” (*at least one server*). *Supra*, §§VII.A, VIII.A; APPLE-1004, Abstract, [0002], [0006], [0008], [0028], [0033]-[0038], [0075]-[0076], FIGS. 1, 2 (below), 3, 6. Horvath explains that “[a]lthough, the SMSC 114, C-CSCF 206, I, S-CSCF 208, and HSS 210 are shown as separate components, each respective component can reside on the same or separate information processing system.” APPLE-1004, [0038].

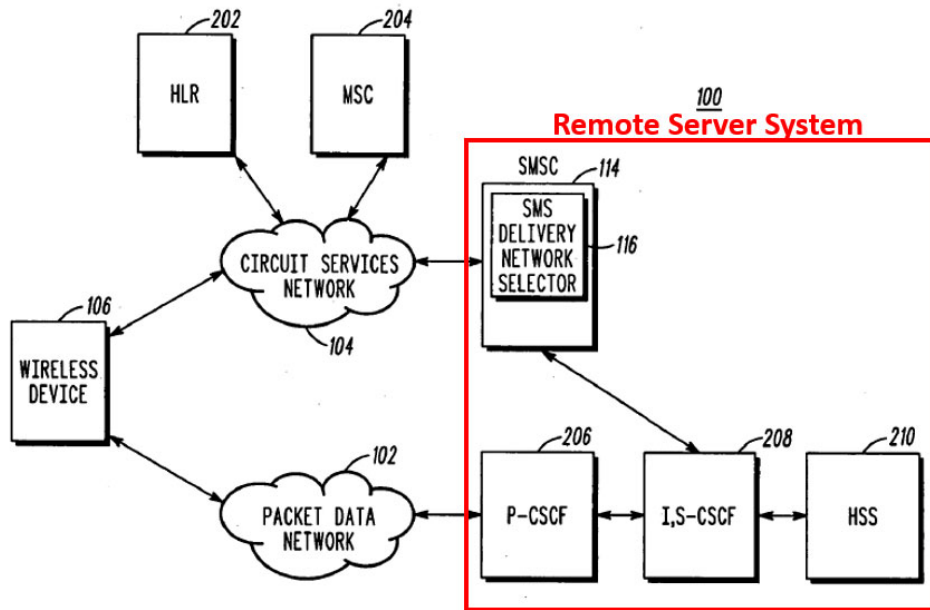


FIG. 2

APPLE-1004, FIG. 2 (Annotated)

73. Horvath’s remote server(s) supports “instant messaging” (*supports the PSMS*), as Horvath explains, “[t]he P-CSCF 206, I, S-CSCF 20S, and HSS 210 also comprise part of an Internet Protocol multimedia subsystem (‘IMS’) core that supports the SIP network,” which is “used for establishing instant messaging,” and “[i]n one embodiment, the SMSC 114 is also part of the IMS core.” APPLE-1004, [0033]-[0034].

74. Horvath further discloses “application server(s)” as part of the IMS system that provide messaging “services subscribed to by the wireless device 106,” such as “instant messaging” (IM) service, which is a type of packet switched message service (*PSMS*). APPLE-1004, [0033] (“The SIP network is used for

establishing instant messaging”), [0038], [0039] (“An IMS system also includes application servers that host and execute services for the wireless device 106. A service for example, is SMS, MMS...and the like. An application server interfaces with the S-CSCF component of the I, S-CSCF 20S using SIP.”).

75. Horvath explains that “[i]n one embodiment of the present invention, the SMSC 114 acts as an application server for transmitting/delivering SMS messages to the wireless device 106 through the packet data network 102 using the IMS network. In other words, the SMSC 114 includes SIP/IMS capabilities to deliver SMS messages to the wireless device 106.” APPLE-1004, [0039], [0041] (“the SMSC 114, which is acting as an SIP application server”).

76. Additionally, Chatterjee provides a brief history and summary of various IM and presence applications and standards, for example, “[a]mong IM clients, MSN Messenger™ was the dominant technology for IM followed by AIM™ and then Yahoo Messenger™.” APPLE-1007, page 10. Chatterjee further describes various servers that provide the IM and presence service. *See e.g.*, APPLE-1007, page 4 (“After AOL rolled out their service, Yahoo and MSN introduced their own products that enabled users to communicate with AIM servers.”), page 5 (“In 1998, Jabber project was initiated to build an IM client and server that could interact with the various proprietary systems by using a superset of all of the major consumer IM systems”), page 7 (“Jabber, through its

architecture (Fig. 3), uses a distributed network utilizing many interconnected servers...Jabber servers”), Table 1 (“Public services” as “IM solutions” “use a centralized third-party server to replay messages”), FIG. 3 (“SIP server,” “Jabber server[s]”).

77. Moreover, a POSITA would have understood and found obvious that Horvath-Tsampalis-Chatterjee-Kansal’s remote server(s) (e.g., “information processing system 108”) *maintains status information* (e.g., online presence status of whether a phone is online, offline, etc.) for its registered mobile phones that are subscribers of IM. *See e.g.*, APPLE-1007, Title (“instant messaging and presence technologies for college campuses”), Abstract (“Presence provides information about users’ reachability and willingness to accept/reject a brief chat session”), page 4 (“IM systems, with the ability of providing presence information, enables a user to know the availability of other users. By using presence information, an IM system enables us to search for a specific user, check the user’s status, and send short messages. Popular IM applications include AOL™ Instant Messenger (AIM), ICQ™ (“I Seek You”), MSN™ or WindowsXP™ Messenger, and Yahoo™ Messenger....there are times when we may need an instant response from one in a group of users. It takes a while just to find one of the users in that group, who might be available or not. In IM applications, if we have that group of users on our ‘buddy list,’ we can tell at a glance if any of them are logged onto the network, and

whether they have been active recently. We are also aware, in this case, whether or not the user is open to communicating at this time. If they are, we can send a quick IM and communicate further.”); *supra*, §§VII.C, VIII.B.

78. Indeed, providing presence status along with IM was a common practice well known in the field before the Critical Date to facilitate real time communication among subscribers. APPLE-1010, 8:52-54 (“Presence status indicates online status (e.g., offline, online and busy, online and available, etc.) for the destination user.”); APPLE-1019, page 9, lines 30-31 (“the client device can receive an automatic update of presence information from other client devices and/or a server”); APPLE-1020, 1:40-45 (“An instant messaging server keeps track of the online status of each of its subscribed users (often referred to as presence information), and when someone from a user’s buddy list is online, the service alerts that user and enables immediate contact with the other user.”); APPLE-1016, [0015] (“a wireless communication network 100 including a mobile switching center (MSC) 102”), [0025] (“The MSC 102 includes...an SMS connection and transmission module 208.”), [0026] (“The SMS connection and transmission module 208 examines the user profile 108 to determine the user selections for handling of SMS transmissions and to determine the conditions that prevail with respect to the telephone 104B. As noted above, these conditions may include status of the telephone 104B, for example, whether or not the telephone 104B is turned

off, previous notations by a user, for example, whether or not the user has indicated that he or she is away from the telephone, and status of a user's IM connection. If necessary to determine the disposition of the message, the connection and transmission module 208 also queries the wireless interface module 206 to determine the status of the telephone 104B.”), [0028].

Element [1c]: wherein: the sending mobile phone retrieves a destination address of a first message from the first message, wherein the destination address of the first message is a phone number of a first receiving mobile phone;

79. Horvath-Tsampalis-Chatterjee-Kansal renders obvious [1c]. A POSITA would have understood and found obvious that Horvath-Tsampalis-Chatterjee-Kansal's wireless device 106 (*the sending mobile phone*) *retrieves a destination address of a first message from the first message, wherein the destination address of the first message is a phone number of a first receiving mobile phone*, e.g., when the sender enters a phone number of a first recipient for a first active message that the sender is composing. See e.g., APPLE-1004, Abstract, [0040], [0072]-[0073]; APPLE-1005, [0024], [0027], [0033], [0046], [0064], FIGS. 4, 10.

80. For example, Horvath explains that the sending mobile phone, e.g., wireless device 106, sends messages to recipient wireless devices over one or more packet data networks 102 and/or circuit switched networks 104. APPLE-1004, [0050] (“wireless device 106[] ... is configured to transmit SMS messages to

another device”), [0078], FIG. 7. From Horvath’s disclosures in this regard, a POSITA would have understood that the sending mobile phone retrieves a destination address of a receiving mobile phone, especially since the intended recipient would need to be addressed in the message to be delivered to the desired receiving mobile phone.

81. Horvath discloses “information to identify” each wireless device registered to the remote server system, *e.g.*, a “destination address” (also referred to as “contact address” or “IMS contact address”), “such as a telephone uniform resource identifier (‘tel-URI’),” *e.g.*, “the telephone number assigned to the wireless device 106.” APPLE-1004, [0035] (“The HSS 210 also includes information to identify each registered wireless device 106 such as a telephone uniform resource identifier (‘tel-URI’) and/or a SIP uniform resource identifier (‘SIP-URI’). A tel-URI, for example is the telephone number assigned to the wireless device 106.”), [0045], [0050] (“In one embodiment, the destination address of the recipient device is a SIP URI formed out of the normal address (for example, tel:MDN).”), [0073] (“the contact address (for example, tel-URI) of the wireless device 106”), [0076] (“If the determination [of whether device 106 is registered on the packet data network], at step 606, is negative, then an IMS contact address, at step 608, does not exist for the wireless device 106....If the

determination, at step 606, is positive, an IMS contact address, at step 614, exists for the wireless device 106.”).

82. Horvath’s functionality for receiving information associated with a destination address of a recipient is maintained in the combination with Tsampalis, which similarly describes conventional addressing techniques where the sender receives phone numbers of intended messaging recipients while composing an active message. APPLE-1005, [0061] (“first mobile wireless communication device 100 will transparently contact the network talking to the address(es), (e.g., the MSISDN(s)), of the recipient(s)”). Tsampalis teaches that an “active message” being composed by a user of the sending mobile phone contains a “recipient ID” received from the user, *e.g.*, a phone number. APPLE-1005, FIG. 4 (below, showing “recipient ID” 402 list in the form of telephone numbers for each individual recipient list entry 408), [0032], [0033] (“As the active message recipient list 218 is populated with each recipient ID 402...”), [0046] (“Block 1008 demonstrates the method including the receiving of a next recipient ID 402 as the recipient ID is entered in the send message circuitry 106”), [0064] (“the user is composing a [text] message”), FIGS. 3-4 (showing phone numbers as recipient IDs), 7, 10.

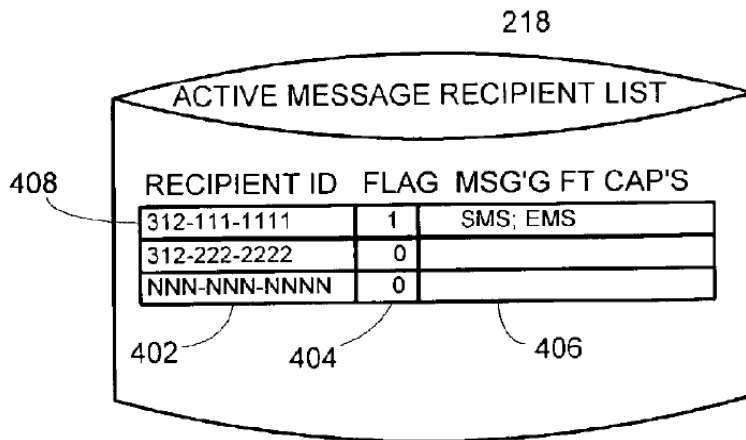
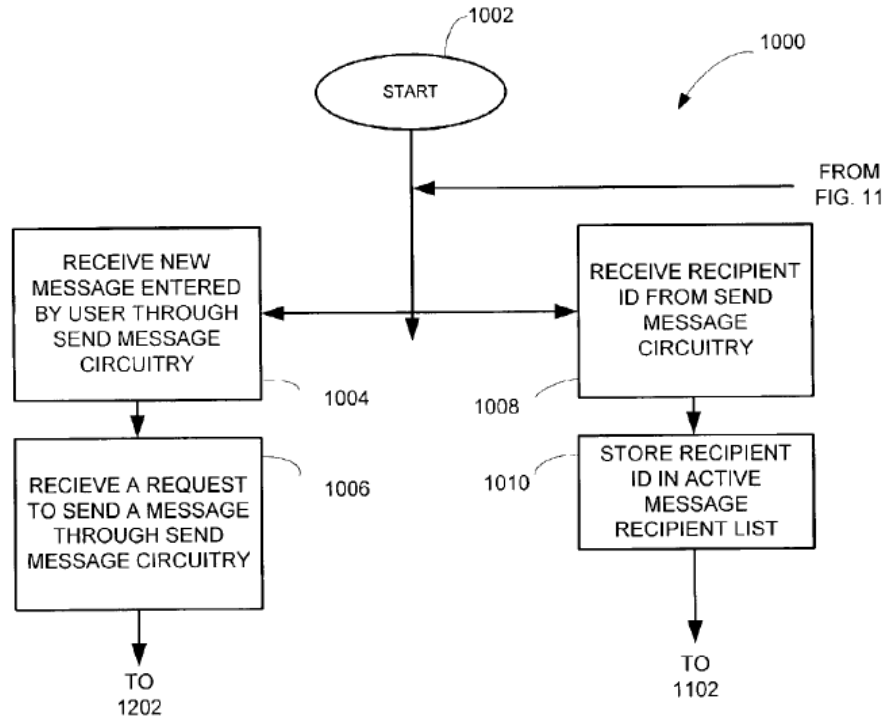


FIG. 4

APPLE-1005, FIG. 4

83. Tsampalis explains, referring to FIG. 10 (below), “[a]s shown in Block 1004, the method includes the receiving a new unformatted message 110 entered by a user” and “Block 1008 demonstrates the method including the receiving of a next recipient ID 402 as the recipient ID is entered in the send message circuitry 106.” APPLE-1005, [0046], FIG. 10.

FIG. 10



APPLE-1005, FIG. 10

84. These functions can be performed using Tsampalis’s “send message circuitry 106” or “other suitable circuitry,” “preferably software modules,” where steps (Blocks) 1004 and 1008 can be performed “in any chosen sequence.” APPLE-1005, [0046], [0024] (“the term circuitry includes at least the following: one or more processing devices executing software stored in memory, such as microprocessors, digital signal processors (DSPs), microcontrollers or alternatively discrete logic, state machines, or any suitable combination of hardware, software stored in memory and/or firmware. Further, in a preferred embodiment, the mobile

wireless communication device messaging format capabilities determinator circuitry 104 and the send messaging circuitry 106 are software modules executing on DSPs contained within a mobile wireless communication device.”), [0027] (the circuitry “is preferably software modules”).

85. From these and related descriptions, a POSITA would have understood and found obvious that the Horvath-Tsampalis-Chatterjee-Kansal’s sending mobile phone (“wireless device 106”) retrieves a destination address (*e.g.*, a phone number of a receiving mobile phone) of a first active message (*e.g.*, ***first message***) being composed by the user of the sending mobile phone from the first active message (***from the first message***) addressed to the first receiving mobile phone, using suitable circuitry such as software modules running on the sending mobile phone.

Element [1d]: the sending mobile phone sends first information representing the phone number of the first receiving mobile phone to the at least one server;

86. Horvath-Tsampalis-Chatterjee-Kansal renders obvious [1d]. As further described below, the sending mobile phone in the Horvath-Tsampalis-Chatterjee-Kansal combination determines whether the destination address corresponds to a subscriber of the instant messaging (IM) service through the remote server system supporting IM. *Supra*, §VIII.A, Analysis of [1b].

87. In the combination, Tsampalis confirms that it would have been obvious for the sending mobile phone to determine whether the destination address

corresponds to a subscriber of an IM service by sending a request to the remote server system and receiving a response from the server system indicating the same. *Supra*, §§VII.B, VIII.A. For example, based on Tsampalis’s express teachings, the sending mobile phone in the Horvath-Tsampalis-Chatterjee-Kansal combination would send a request to the remote server system for the recipient’s messaging format capabilities information and would receive a response that indicates whether the recipient indicated by the destination address (*e.g.*, phone number) is capable of receiving/processing IM messages—and thus whether the recipient is a subscriber of an IM service. *Id.*; APPLE-1005, [0022]-[0025], [0041], [0056]-[0065], FIGS. 5-6, 13; APPLE-1004, [0038] (“the services subscribed to by the device 106 can be provided”); APPLE-1007, page 5 (providing IM subscription examples that “[b]y January 1997, ICQ had 27,000 users with a growth rate of 100 percent per week. Meanwhile, America Online’s (AOL) Instant Messenger (AIM) increased its subscribers to ten million users”); *supra*, §§VII.B-C, VIII.A-B.

88. As described above with respect to [1c], Horvath discloses provision of “information to identify” each wireless device registered to the remote server system, *e.g.*, a “destination address” (also referred to as “contact address” or “IMS contact address”), “such as a telephone uniform resource identifier (‘tel-URI’),” *e.g.*, “the telephone number assigned to the wireless device 106.” APPLE-1004, [0035], [0045], [0050], [0073], [0076]. Further, Horvath describes that the home

subscriber server (“HSS”) 210 portion of the information processing system “comprises a database including profiles associated with each wireless device 106 registered with the IMS.” APPLE-1004, [0035]. “The HSS 210 also includes information to identify each registered wireless device 106 such as a telephone uniform resource identifier (‘tel-URI’) and/or a SIP uniform resource identifier (‘SIP-URI’).” *Id.* In other words, the HSS 210 includes a profile for each mobile device that may include both its telephone number (*i.e.*, “tel-URI”) and an SIP uniform resource identifier, which is an identifier for the SIP network. Thus, the profiles for each registered wireless device 106 is configured associate a user’s tel-URI and SIP-URI. A POSITA would have understood or at least found obvious that this allows a given device to query the remote server system (which includes the HSS) based on either the tel-URI or the SIP-URI. APPLE-1032, [0025] (“During the setup process, a user’s mobile communication device is preferably linked with the user’s account on a virtual community...the user’s user ID that is associated with the user’s virtual community account...”), [0029], [0033] (“the user is prompted to input the user’s ID that is associated with the selected virtual community. For example, the user can be prompted to input an e-mail address, telephone number, userID, member number, personal identification number, etc.”), supported by APPLE-1033, page 3 line 29 – page 4 line 31, page 14 lines 11-14; APPLE-1036, page 3 lines 25-28 (“MMS data flow starts with a subscriber using

an MMS client on the mobile phone to compose, address, and send an MMS message to one or more recipients. MMS addresses can be either E.164 phone numbers (e.g., '+18005551212') or RFC 2822 email addresses (e.g., 'you@yourdomain.com').”).

89. Thus, a POSITA would have found obvious that Horvath-Tsampalis-Chatterjee's sending mobile phone sends a first request (*first information*) including the phone number identifying (*representing the phone number of*) the first receiving mobile phone to the remote server system, such request containing a query for the messaging format capabilities information of the first receiver mobile phone, when such information is not already stored locally in the sending mobile phone. *supra*, §§VII.B, VIII.A.

Element [1e]: the at least one server, in response to receipt of the first information, sends a first response to the sending mobile phone when the phone number of the first receiving mobile phone is not identified as a subscriber of the PSMS;

90. Horvath-Tsampalis-Chatterjee-Kansal renders obvious [1e]. As discussed above, Horvath-Tsampalis-Chatterjee-Kansal's remote server system, in response to receipt of the first request (*first information*), sends a response (*a first response*) to the request back to the sending mobile phone, when the phone number of the first receiving mobile phone does not have the messaging format capabilities of instant messaging (*not identified as a subscriber of the PSMS*), for example, when the first receiving mobile phone does not have a subscription with

an IM service and registration to the packet data “SIP network” (supported by an “IMS core”) “used for establishing instant messaging.” *Supra*, Analysis of [1d]; APPLE-1004, [0033]-[0034] (an “IMS core” “supports the SIP network,” and “when a wireless device 106 wants to access the packet data network 102, the wireless device 106 registers with the IMS network”), [0038] (“the services subscribed to by the device 106 can be provided” by “application server(s)”), [0039] (“application servers that host and execute services for the wireless device 106...the SMSC 114 acts as an application server...the SMSC 114 includes SIP/IMS capabilities”), [0040]-[0041] (“the application servers that are to be notified that they are to provide services for the wireless device 106”), [0045] (“In one embodiment, when a SMS message request is received by the SMSC 114, the SMSC 114 first determines if the recipient wireless device 106 is registered on the packet data network 102. For example, in an IMS network, the SMSC 114 determines if a registration message for the recipient device has been received from the S-CSCF or if a contact address has been received for the recipient device 106.”), [0047] (“If the recipient device is not registered on the packet data network 102, the SMSC 114 delivers the SMS message to the recipient device through the traditional circuit services network method (for example, ANSI-41 procedures).”), [0073] (“notify specific application servers that the wireless device 106 has

registered with the packet data network 102”), [0076]; APPLE-1007, page 5; *supra*, §§VII.A-B, VIII.A.

91. In more detail, the improved system’s remote server(s) sends a response to the request made by the sending mobile phone, which includes information about the receiving mobile phone messaging format capabilities (*e.g.*, SMS/MMS/IM), thereby allowing the sending phone to obtain such information about the receiving phone prior to sending a message, in accordance with Tsampalis. *Supra*, §§VII.B, VIII.A, Analyses of [1c]-[1d]; APPLE-1004, [0033], [0035], [0039], [0050], [0072]-[0073], [0076]; APPLE-1005, [0033]-[0035] (sending mobile phone “determine[s] the message format capabilities of the corresponding recipient ID” of a receiving mobile phone, *e.g.*, through a remote server), [0045], [0056]-[0057], [0060]-[0065], FIGS. 4, 5, 6, 13.

92. A POSITA would have understood and found obvious that the Horvath-Tsampalis-Chatterjee-Kansal’s remote server(s) determines messaging service subscriptions information, *e.g.*, with instant messaging service(s), of the receiving mobile phone (*subscriber of the PSMS*), as it receives the request from the sending mobile phone, as Horvath explains that “[t]he HSS 210 [as part of the remote server(s)] comprises a database including profiles associated with each wireless device 106 registered with the IMS” and identified by their respective identifiers such as phone numbers, where “[a] profile, for example, includes

subscription related information.” APPLE-1004, APPLE-1004, [0031] (“Subscriber information... comprises access right(s) and/or a service(s) subscribed to by the wireless device 106.”), [0033], [0035]; *see also id.*, [0072]-[0073] (“the S-CSCF receives a profile associated with the wireless device 106 from the HSS 210 to authenticate the wireless device 106,” and at “regist[rati]on with the IMS core,” SMSC 114 is notified “of the contact address (for example, tel-URI) of the wireless device 106,” and “specific application servers” are also notified that “the wireless device has registered with the packet data network 102”).

93. Again, Tsampalis similarly teaches a remote server making determination of a receiving mobile phone (identified by a “recipient ID” such as phone number) messaging format capabilities information. APPLE-1005, [0033]-[0035], [0045], [0056]-[0057], [0060]-[0065], FIGS. 4, 5, 6, 13. To be clear, a POSITA would have understood and found obvious that such messaging format capabilities information reflects the receiving mobile phone’s subscription(s) with the messaging service(s) that support the corresponding messaging format(s) as well as necessary registration to network(s) supporting the corresponding messaging format(s).

94. Thus, in the combined system of Horvath-Tsampalis-Chatterjee-Kansal, when the response from the remote server (*first response*) indicates that the receiving mobile phone’s (*first receiving mobile phone*) messaging format

capabilities information does not include a format of IM, then the phone number of the receiving mobile phone (*first receiving mobile phone*) is not identified as a subscriber of the IM service (*the PSMS*). APPLE-1004, [0031].

95. To be clear, a mobile phone needs both access to the packet data network and subscription with an instant messaging service (*e.g.*, that the SIP network establishes and supports) to send or receive instant messages. APPLE-1004, [0033] (“The SIP network is used for establishing instant messaging...and other real-time communications over the Internet.”); APPLE-1007, page 7 (IM transmitted as “network packet”), Boxes 1-2; APPLE-1005, [0002] (“non-real-time store-and-forward messaging” such as “SMS,” “EMS,” and “MMS” messaging), [0022], [0024].

Element [1f]: after the first response is received by the sending mobile phone, the sending mobile phone sends the first message as an SMS message to the first receiving mobile phone;

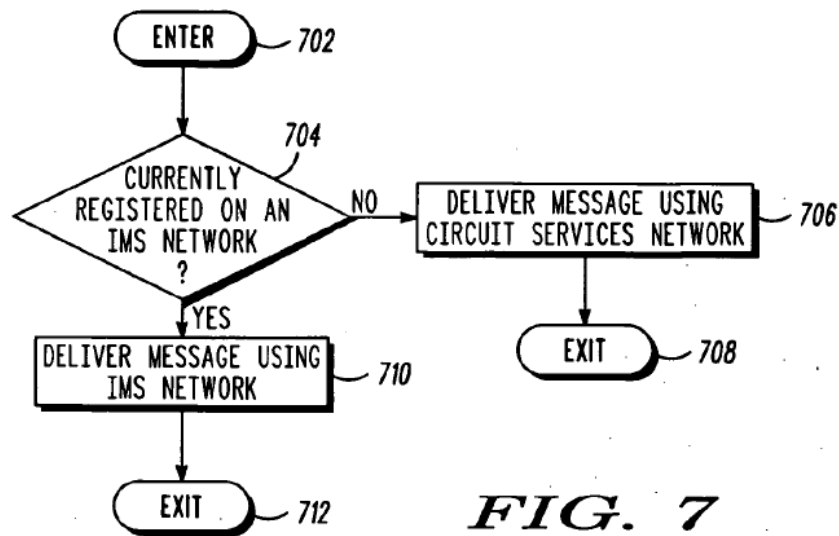
96. Horvath-Tsampalis-Chatterjee-Kansal renders obvious [1f]. A POSITA would have understood and found obvious that after the first response (indicating the first receiving mobile phone is not a subscriber of instant messaging, as described with respect to [1e], *supra*) is received by the sending mobile phone, the sending mobile phone sends the first message ***as an SMS message*** to the first receiving mobile phone.

97. To be clear, the first receiving mobile phone could be registered and connected to the packet data network but not subscribed to any IM service, in which case the SMS message could be sent as packeted data over the packet data network both upstream (from sending mobile phone to the remote server system) and downstream (from the remote server system to the recipient mobile phone); while if the first receiving phone is not registered with the packet data network or registered but lost connection, then the SMS message is first sent as data packet upstream then relayed by the remote server system over the circuit services network downstream. *Supra*, §§VII.A, VIII.A, Analysis of [1e].

98. As discussed above, the Horvath-Tsampalis-Chatterjee-Kansal's sending mobile phone determines and selects a transmission mode shaped by at least messaging format and transmission network (*e.g.*, whether to send an SMS, MMS, or IM, and whether to transmit over the packet data network or the circuit services network) for sending an outgoing message to a receiving mobile phone. *Supra*, §VIII.A; APPLE-1004, Abstract, [0004], [0006]-[0009], [0024]-[0026], [0028], [0033]-[0039], [0045], [0050], [0061]-[0063], [0074]-[0076], [0078], [0080]-[0081], FIGS. 1-4, 6-8; APPLE-1005, Abstract, [0004], [0022], [0024], [0027], [0033]-[0035], [0039], [0041]-[0042], [0045], [0056]-[0057], [0060]-[0065], FIGS. 2, 5, 6, 9, 13. The determination of transmission mode is based on

various factors including the sending mobile phone's network registration status and the receiving mobile phone messaging format capabilities.

99. Again, Horvath discloses the sending mobile phone determining a transmission network, and associated messaging format, for sending an outgoing message to the receiving mobile phone, based on various factors including a mobile phone's (the sending phone) registration with a packet data network and subscription with certain messaging service(s). APPLE-1004, [0050], [0062], [0078], FIGS. 1, 4, 7 (below); *supra*, §§VII.A, VIII.A, Analysis of [1e].



APPLE-1004, FIG. 7 (Sender Device Perspective)

100. Also discussed above, in the improved system of Horvath-Tsampalis-Chatterjee-Kansal, the sending mobile phone makes a more dynamic and optimized transmission mode determination based further on the receiving mobile phone's messaging format capabilities information, which the sending mobile

phone receives prior to sending a message in a compatible messaging format, in accordance with Tsampalis. *Supra*, §§VII.B, VIII.A, Analyses of [1d]-[1e]; APPLE-1004, [0004], [0081]; APPLE-1005, [0065].

101. For example, when the first receiving mobile phone has SMS messaging format capabilities but not IM (*not identified as a subscriber of the PSMS*, as recited in [1e]), then at least in one case the sending mobile phone sends the first message *as an SMS message*, which is a compatible format between the sending phone and the first receiving phone, instead of an IM message (an incompatible format in this case) to the first receiving mobile phone. *Supra*, §VIII.A, Analysis of [1e].

Element [1g]: the sending mobile phone retrieves a destination address of a second message from the second message, wherein the destination address of the second message is a phone number of a second receiving mobile phone;

102. Horvath-Tsampalis-Chatterjee-Kansal renders obvious [1g]. According to the same procedure described above with respect to [1c], a POSITA would have understood and found obvious that when the user of Horvath-Tsampalis-Chatterjee-Kansal's sending mobile phone composes *a second active message* addressed to *a second receiving mobile phone*, the sending mobile phone retrieves the destination address from the second active message being composed, wherein the destination address of the second active message is the phone number of the second receiving mobile phone. *Supra*, Analysis of [1c]; APPLE-1004,

[0027] (“The packet data network 102 and the circuit services network 104 support any number of wireless devices 106. The support of the networks 102, 104 includes support for mobile telephones, smart phones...”), [0029], [0031] (“the wireless communication system 100 comprises one or more wireless devices 106”); APPLE-1005, [0009] (“an active message recipient list”), [0032]-[0040], [0062]-[0063] (scenarios where “there is one remote recipient” “or where there are multiple remote recipients”), FIG. 4.

103. More specifically, Horvath describes that at least the HSS 210 portion of the remote server system includes “profiles associated with each wireless device 106 registered with the IMS,” which a POSITA would have understood or at least found obvious to mean that there were many wireless devices within the system and that each wireless device would have been configured to send messages to any of the other wireless devices within the system. APPLE-1004, [0035]; *see also id.*, [0039] (“the SMSC 114 includes SIP/IMS capabilities to deliver SMS messages to the wireless device 106”). This is further confirmed by Tsampalis, which describes that a wireless device may send multiple messages, each of which may indicate one or more recipient IDs. *See* APPLE-1005, [0046] (“For example, the user may begin by entering one recipient ID, typing one paragraph of the message, entering a second recipient ID, and entering a second paragraph of the message”); *see also id.*, [0036] (“Upon detection of a request to send the message 112, a

process begins which includes the looping through of the recipient IDs 402 in the active message recipient list 218 to send messages to each designated recipient”). From these teachings, a POSITA would have understood or at least found obvious that the user of Horvath-Tsampalis-Chatterjee-Kansal’s sending mobile phone would have sent multiple messages (including a *first message* and a *second message*) to multiple different recipients (including a *first receiving mobile phone* and a *second receiving mobile phone*).

Element [1h]: the sending mobile phone sends second information representing the phone number of the second receiving mobile phone to the at least one server;

104. Horvath-Tsampalis-Chatterjee-Kansal renders obvious [1h]. According to the same procedure described above with respect to [1d], a POSITA would have understood and found obvious that Horvath-Tsampalis-Chatterjee-Kansal’s sending mobile phone sends a second request (*second information*) representing the phone number of the second receiving mobile phone to the remote server(s), the second request including a query of messaging format capabilities information of the second receiving mobile phone. *Supra*, Analyses of [1d]-[1e], [1g].

Element [1i]: the at least one server, in response to receipt of the second information and conditioned on the phone number of the second receiving mobile phone being identified as a subscriber of the PSMS and the second receiving mobile phone having an active status with the PSMS, sends a second response to the sending mobile phone;

105. Horvath-Tsampalis-Chatterjee-Kansal renders obvious [1i]. Following the same procedure as described above with respect to [1e], Horvath-Tsampalis-Chatterjee-Kansal's remote server(s), in response to receipt of the second request (*second information*), sends *a second response* to the sending mobile phone, the second response containing the second receiving mobile phone's messaging format capabilities information. *Supra*, §§VII.B, VIII.A, Analysis of [1e].

106. As also discussed above, Horvath-Tsampalis-Chatterjee-Kansal's remote server(s) maintains presence status information for all registered IM subscribers. *Supra*, Analysis of [1b]. A POSITA would have found obvious that a response would have further included the presence status of the inquired receiving mobile phone with IM (*status with the PSMS*) if the receiving mobile phone is a subscriber of IM, as explained in more detail below.

107. Again, the improved method and system of Horvath-Tsampalis-Chatterjee-Kansal makes more dynamic and optimized transmission mode determinations (and selections), based on not only the network registration status and messaging format capabilities of the sending mobile phone, but also at least the messaging format capabilities of the receiving mobile phone, by the sending mobile phone obtaining such information about the receiving mobile phone prior to sending a message, in accordance with Tsampalis. *Supra*, §§VII.B, VIII.A,

Analyses of [1d]-[1e]; APPLE-1004, [0004], [0081]; APPLE-1005, [0004], [0026], [0062], [0065].

108. As discussed above, based on Horvath, a POSITA would have understood and found obvious that the subscriber status of the second receiving mobile phone is determined through identifying information, *e.g.*, the phone number of the second receiving mobile phone, as part of a profile stored in the remote server(s) (*e.g.*, the HSS 210) at registration, such profile also contain “subscription related information. APPLE-[0033]-[0035], [0038]-[0041] (“subscriber profile”). Consistent with Horvath, Tsampalis teaches determining a recipient device’s messaging format capabilities, which reflect subscriptions to various messaging services, through “recipient ID” such as the phone number. APPLE-1005, [0033]-[0035] (sending device “determine[s] the message format capabilities of the corresponding recipient ID” of a receiving mobile phone, *e.g.*, through a remote server), [0045], [0056]-[0057], [0060]-[0065], FIGS. 4, 5, 6, 13.

109. Based on the teachings of Chatterjee, a POSITA would have found obvious that the status of the receiving mobile phone is another factor that would be relevant to a user’s optimized transmission determination in the Horvath-Tsampalis-Chatterjee-Kansal system. For example, Chatterjee describes that “[p]resence provides information about users’ reachability and willingness to accept/reject a brief chat session.” APPLE-1007, 1. Like message format

capability, a POSITA would have at least found obvious that such presence information would have been useful to a user of a sending mobile device in determining whether and when to send message to a given recipient mobile device. Thus, when a receiving mobile phone (*e.g.*, second receiving mobile phone) is registered with the SIP/IMS packet data network and subscribed to an instant messaging service (*the second receiving mobile phone being identified as a subscriber of the PSMS*), the status (*e.g.*, offline/inactive, online/active) of the receiving mobile phone with instant messaging also affects its messaging capabilities using IM, *i.e.*, whether it is capable of sending or receiving IM messages at the moment (*e.g.*, when the receiving mobile phone is offline, an instant message would not be delivered to it successfully). *Supra*, §§VII.C, VIII.A-B, Analyses of [1b], [1e].

110. As discussed above, a POSITA would have found it obvious to configure the sending mobile phone in the Horvath-Tsampalis-Chatterjee-Kansal combination to determine whether a receiving mobile phone has an active status (*e.g.*, online and available), in accordance with Chatterjee. *Supra*, §§VII.C, VIII.B. Although Horvath describes examples that focus on SMSC 114 receiving information about the recipient's current registration status, it would have been obvious for the sending mobile phone also to request and receive from a remote server (*e.g.*, HSS 210 or SMSC 114) the recipient's presence status on the SIP

network. As discussed above, by the Critical Date of the '182 Patent, it was well known how to implement an IM client that polled a server for the current registration status (*e.g.*, presence information) of another IM client, and a POSITA would have possessed motivation to poll a server for such information before sending an IM to ensure the recipient was available to receive the message and participate in a real-time IM session. *Supra*, §§VII.C, VIII.B, Analysis of [1b]. Tsampalis's teaching to provide the recipient's messaging capabilities information in a response to the sender also underscores the obviousness of allowing the sender to poll the server for the recipient's current presence status, *e.g.*, through the same response, because it shows how the sender can use information about the recipient to more effectively tailor messaging strategies to the recipient.

111. Thus, a POSITA would have found obvious that in the combined system, in response to receipt of the second request (*second information*), and conditioned on the phone number of the second receiving mobile phone being *identified as a subscriber of* instant messaging (*the PSMS*) (having both registration with the packet data network and subscription with an instant messaging service) and the second receiving mobile phone *having an active status with* instant messaging (*the PSMS*), the remote server(s) sends *a second response* to the sending mobile phone, where the second response contains IM messaging format capabilities information and represents an active status of the second

receiving mobile phone with IM, together indicating that the second receiving mobile phone is online and capable of IM.

Element [1j1]: after the second response is received by the sending mobile phone, the sending mobile phone sends the second message as a packet switched message, via a wireless local area network (WLAN) and the PSMS, to the second receiving mobile phone,

112. Horvath-Tsampalis-Chatterjee-Kansal renders obvious [1j1]. A POSITA would have understood and found obvious that, after the second response indicating that the second receiving mobile phone is capable of instant messaging is received by the sending mobile phone, the sending mobile phone sends the second message as an instant message (*a packet switched message*), via the packet data network, such as “an 802.11 network” (*a wireless local area network (WLAN)*), and the IM service (*PSMS*), to the second receiving mobile phone.

113. Specifically, Horvath teaches that, “if the wireless device 106 is registered on the packet data network 102, the SMS delivery network selector 124 selects the packet data network 102 for transmission of the” message. APPLE-1004, [0062]. Horvath teaches that the packet data network 102 may include an SIP network, which is “used for establishing instant messaging.” APPLE-1004, [0033], [0046] (“the SMSC 114 delivers the SMS message to the recipient device through the packet data network 102 via the SIP network”). And as described in Section VIII.B, *supra*, the messaging format capabilities information shared with the sender device based on Tsampalis’s and Chatterjee’s teachings would further

include an indication of whether the intended recipient of a message is capable of receiving IMs in addition to other messaging formats such as SMS, MMS, and EMS. Thus, where the sender and receiver were both capable of communicating via an instant messaging service established by Horvath's SIP network, a POSITA would have at least found obvious that the user could select to send the message as an instant message (*a packet switched message*) via the IM service (*PSMS*), consistent with the teachings of Tsampalis. See APPLE-1005, [0037] ("If the user chooses to send the active message 216 in a format of the recipient list messaging format capabilities 406, the active message 216 is formatted in the selected messaging format capability, (e.g., message 112), and is sent to the second mobile wireless communication device 200").

114. Further, a POSITA would have understood or at least found obvious that the packet data network 102 would have been *a wireless local area network (WLAN)*. Specifically, Horvath teaches that "packet data network 102 is an Internet Protocol ('IP') connectivity network, which provides data connections at much higher transfer rates than [*sic*] a traditional circuit services network," and can comprise "an 802.11 network." APPLE-1004, [0024]. A POSITA would have understood and found obvious that a common type of 802.11 network was a wireless LAN. APPLE-1011, 5:1-33 ("WLAN capabilities including...technology version (such as 802.11[[])"), 6:27-32 ("WLAN 802 protocols...IEEE 802

networks”), FIG. 5B; APPLE-1009, 1 (“New generation mobile phones in addition to GSM capability also have the ability to access the internet via 802.11 g, b and other related wireless protocols.”), 3 (“The mobile GSM device would have an operating system capable of running an application which could subscribe and log into a registration server when the device gained access to the internet via a route such as bluetooth [*sic*], Wifi (802.11b,g or other)...”), 4 (“Wi-Fi is an abbreviation for wireless fidelity and is used to refer generically to any type of wireless network based on the IEEE 802.11 standard or similar form of IP based wireless communication”); APPLE-1037 (“When did Wi-Fi become popular? ... 2004: The first Wi-Fi-certified devices (cell phones, PDAs and TVs) hit the market.”); *see also* APPLE-1004, [0033]-[0034] (“The wireless device 106 can connect to the IMS network using different methods, which all use standard IP.”).

Element [1j2]: wherein at the time the packet switched message is sent, the second receiving mobile phone is not connected to the at least one server, wherein the packet switched message is queued until the second receiving mobile phone connects to the at least one server;

115. Horvath-Tsampalis-Chatterjee-Kansal renders obvious [1j2]. A POSITA would have understood or at least found obvious that, when Horvath-Tsampalis-Chatterjee-Kansal’s second receiving mobile phone became disconnected from the IM service implemented by Horvath’s SIP network (*PSMS*), the second message would not have been able to be delivered to the second receiving mobile phone. *Supra*, §§VII.A-D, VIII.A-B, Analyses of [1e], [1i].

Instead of abandoning the second message completely, a POSITA would have understood and found obvious that the remote server(s) queues the second message, in at least one case until the second receiving mobile phone connects to the remote server(s). Indeed, it was a known problem that mobile devices connected to wireless networks often experienced “unreliable” connections in which “[n]etworking equipment between two connected users may frequently fail and recover.” APPLE-1047, [0007]. “In environments where network connections are unreliable, messages sent by real-time messaging clients often fail to get delivered to the recipient.” *Id.* “If the user's connection frequently disconnects and reconnects, the user may see multiple error messages, contributing to a poor experience for the user.” *Id.* One known way for a real-time messaging system to deal with these issues is to utilize a message cache that “caches any messages sent while the connection is unavailable.” *See, e.g.*, APPLE-1047, [0017]; APPLE-1046, [0035] (“...the application server maintains the online status of the user despite the user being temporarily disconnected. Any messages directed to the user during this time may be temporarily stored in a memory and then sent to the second device once the second device has logged in the application server.”); APPLE-1048, [0053] (describing that when a receiving user is disconnected, the message of a sending user “may be received and deposited in a Message Cache 124 within the Presence Server 110” and if the receiving user reconnects, “all

messages stored in the Message Cache 124 may be relayed”). “[B]y caching the messages, the reliable messaging system can send the messages to the receiving participant once the connection is restored.” APPLE-1047, [0017].

116. Accordingly, a POSITA would have at least found it obvious that, when *the second receiving mobile phone is not connected to the at least one server*, the IM message (*packet switched message*) *is queued until the second receiving mobile phone connects to the at least one server*.

Element [1k]: the PSMS is a service for sending and receiving packet switched messages other than SMS, enhanced message service (EMS) and multimedia message service (MMS) messages; and

117. Horvath-Tsampalis-Chatterjee-Kansal renders obvious [1k]. Horvath-Tsampalis-Chatterjee-Kansal’s “instant messaging” (IM) is a packet switched message service (*the PSMS*) that is for sending and receiving packet switched messages other than SMS, EMS, and MMS messages, over the packet data network (*e.g.*, the “SIP network” / “IMS network”). APPLE-1004, [0033] (“The SIP network is used for establishing instant messaging...”). For example, Chatterjee explains that IM messages can be formatted using formats for, among others, the SIP/SIMPLE or Jabber/XXMP standards. APPLE-1007, 8 (Box 1, Box 2). Each of SIP/SIMPLE and Jabber/XXMP are different formats from the SMS/MMS/EMS message formats. Accordingly, a POSITA would have at least found it obvious that the IM service (*PSMS*) implemented by Horvath’s SIP

network would have been *for sending and receiving packet switched messages other than SMS, EMS and MMS messages*. APPLE-1008, [0004] (“Message services for mobile communication terminals can be broadly divided into instant message (IM) services, multimedia message services (MMS), and short message services (SMS).”); APPLE-1009, page 3 (“The mobile GSM device would have an operating system capable of running an application which could subscribe and log into a registration server when the device gained access to the internet via a route such as bluetooth, Wifi (802.11b,g or other), ...The mobile device would register with the remote registration server and this registration would inform the Routing System that the message could be sent via the internet based connection rather than via the GSM network if required. The registration server could be either a dedicated solution using normal web based protocols such as http post or get, or via SIP, SMPP or other protocol”); APPLE-1021, 9:57-64 (“MM [Message Managers] 245 represents any of a variety of applications configured to transmit, receive, and/or otherwise process messages and other network content, including, but not limited to SMS, MMS, IM, email, VOIP, browsers, or the like, and to enable telecommunication with another user of another networked device.”), 10:3-50 (“MM 245 may further include an IM application that is configured to initiate and otherwise manage an instant messaging session, including, but not limited to AOL Instant Messenger, Yahoo! Messenger, NET Messenger Server, ICQ, and the

like. In one embodiment, the IM application within MM 245 may be configured to employ a SIP/RTP to integrate IMNOIP features. For example, the IM application may employ SIMPLE (SIP for Instant Messaging and Presence Leverage), APEX (Application Exchange), Prim (Presence and Instant Messaging Protocol), Open XML-based XMPP (Extensible Messaging and Presence Protocol), more commonly known as Jabber and OMA (Open Mobile Alliance)'s IMPS (Instant Messaging and Presence Service) created specifically for mobile devices, or the like.”).

Element [11]: content of the SMS message and content of the packet switched message is displayed by a same messaging client.

118. Horvath-Tsampalis-Chatterjee-Kansal renders obvious [11]. As discussed above in Sections IV.A.1(f)-(g), the combination implements Kansal's messaging user interface, which displays a message thread of various types including “SMS messages” and “IM messages” (*packet switched message*) within a single messaging client interface at the mobile wireless device. APPLE-1042, [0046]; *see also id.*, [0009]; [0045]-[0046]; [0054]-[0056]; [0062]-[0064]; [0070]; [0077]-[0078]. FIGs. 2, 3 (shown below).

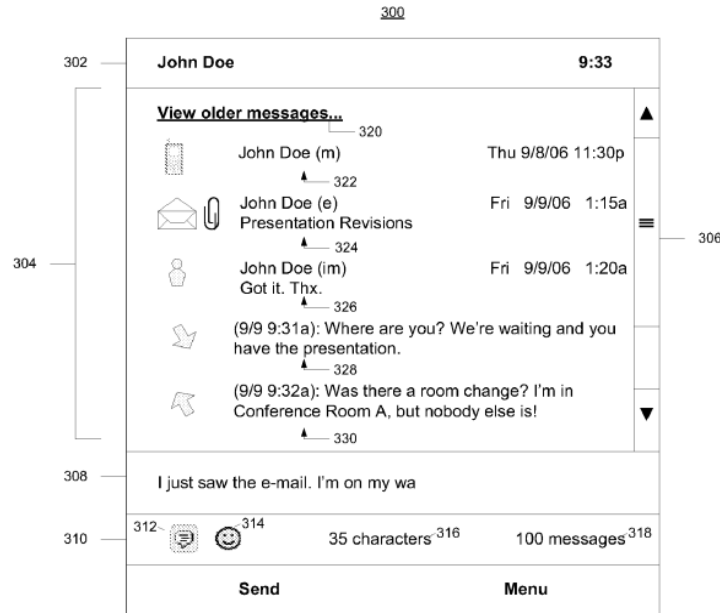


FIG. 3

APPLE-1042, FIG. 3

Claim [2]: *The system of claim 1, wherein the second receiving mobile phone has an active status with the PSMS in at least one case when the second receiving mobile phone is not connected to the at least one server.*

119. Horvath-Tsampalis-Chatterjee-Kansal renders obvious Claim [2]. As described above with respect to [1j2], it was a known problem that mobile devices connected to wireless networks often experienced “unreliable” connections in which “[n]etworking equipment between two connected users may frequently fail and recover.” APPLE-1047, [0007]. For at least temporary disconnections, it was further known to delay changing status to avoid the poor user experience of seeing constant disconnection and error messages. *See, e.g.,* APPLE-1047, [0016] (“delay displaying any error message to the user for a certain amount of time while the

reliable messaging system attempts to restore the connection,” so that “real-time communication appears more reliable to the user, because the user will see fewer delivery errors when a connection can be reestablished”); APPLE-1046, [0035] (“...the application server maintains the online status of the user despite the user being temporarily disconnected. Any messages directed to the user during this time may be temporarily stored in a memory and then sent to the second device once the second device has logged in the application server.”). Based on these common practices, it would have at least been obvious to a POSITA the *second receiving mobile phone has an active status with the IM service (PSMS) in at least one case when the second receiving mobile phone is not connected to the at least one server* (e.g., during temporary disconnections due to unreliable wireless network service).

Claim [3]: The system of claim 1, wherein the second receiving mobile phone has an active status with the PSMS in at least one case when the second receiving mobile phone is connected to the at least one server and the second receiving mobile phone has an active status with the PSMS in at least one case when the second receiving mobile phone is not connected to the at least one server.

120. Horvath-Tsampalis-Chatterjee-Kansal renders obvious Claim [3]. As discussed above with respect to [2], for at least temporary disconnections, it was known to delay changing status to avoid the poor user experience of seeing constant disconnection and error messages. *See, e.g.,* APPLE-1047, [0016] (“delay displaying any error message to the user for a certain amount of time while the

reliable messaging system attempts to restore the connection,” so that “real-time communication appears more reliable to the user, because the user will see fewer delivery errors when a connection can be reestablished”); APPLE-1046, [0035] (“...the application server maintains the online status of the user despite the user being temporarily disconnected. Any messages directed to the user during this time may be temporarily stored in a memory and then sent to the second device once the second device has logged in the application server.”). This means that the IM service (*PSMS*) would show an active status for a user both when the user’s mobile device is connected to the remote server that provides access to the SIP network hosting the IM service (*the second receiving mobile phone has an active status with the PSMS in at least one case when the second receiving mobile phone is connected to the at least one server*) and also when the mobile device is temporarily disconnected to the remote server (*the second receiving mobile phone has an active status with the PSMS in at least one case when the second receiving mobile phone is not connected to the at least one server*).

Claim [4]: The system of claim 1, wherein the second receiving mobile phone has an inactive status with the PSMS subsequent to a plurality of messages being queued for the second receiving mobile phone; wherein the PSMS routes at least some messages between PSMS subscribers according to an email address

121. Horvath-Tsampalis-Chatterjee-Kansal renders obvious Claim [4]. A POSITA would have understood and found obvious that during a period between when a receiving mobile phone (e.g., the second receiving mobile phone) goes

offline and when its status changes from active to inactive, the sending mobile phone continues to send messages using instant messaging (*the PSMS*) while the remote server(s) queues these received messages for the second receiving mobile phone. *Supra*, Analyses of [1]2] and Claim [2].

122. Upon the expiration of that time period, which is defined by a certain event (*e.g.*, a user input), a specified time period, or by another threshold parameter such as a certain maximum number of messages being queued (*e.g.*, due to limited storage capacity), depending on the design, the status updates from active to inactive (*the second receiving mobile phone has an inactive status with the PSMS subsequent to a plurality of messages being queued for the second receiving mobile phone*). *Supra*, Analyses of Claims [2]-[3]; APPLE-1009, FIG. 2 (“If the mobile device is not subscribed via IP, messages would be **either be queued until** the mobile device registers over an IP based route **or after a set period** the messages would be routed as a GSM SMS message.”), page 2 (“if the handset is not registered with the registration server, the message will be queued for IP based delivery **within a specified time period.**”); APPLE-1010, 8:51-9:12, 11:24-36 (“The presence status 405 presented in the unified inbox view 400 **may be updated** continuously, **periodically, or upon user input.**”); APPLE-1017, 34:66-35:33 (“the message may be held until the mobile phone is on line. In other words, when the user is logged in or when the presence of the user is detected, the

message is delivered.”); APPLE-1049, Abstract (describing techniques for “[d]istinctively treating digital communications sent by bulk message senders” by “providing a set of bulk sender behavior policies and monitoring compliance by a bulk message sender with the set of policies”), 2:15-35 (“The bulk sender behavior policies may include a requirement that the bulk sender ... not send more than a predetermined amount of digital communications that are returned to the bulk message sender as undeliverable over a predetermined time interval” and “accept more than a predetermined amount of digital communications that are returned to the bulk message sender as undeliverable over a predetermined time interval.”), 2:36-58 (“The bulk sender behavior policies may further include a requirement that the bulk message sender not send future e-mails to an e-mail address of a recipient if an e-mail sent to the e-mail address is designated as undeliverable to a permanent delivery failure.”), 7:47-58, 11:15-33 (“mailbox ... may be full and unable to accept more emails”), 32:14-40); *generally id.*, 4:31-6:9.

123. Moreover, as discussed above, Horvath describes “profiles associated with each wireless device 106 registered with the IMS” stored on the database HSS including “information to identify each registered wireless device 106,” such as a telephone number” and “IP address” of the wireless device 106, which is bond with the “SIP address” by the S-CSCF during “SIP registrations.” APPLE-1004, [0035], [0038] (“The S-CSCF retrieves device profiles from the HSS 210. The S-

CSCF also handles SIP registrations which allows the S-CSCF to bind the location of the wireless device 106 (for example, the IP address of the device) and the SIP address.”).

124. A POSITA would have understood and found obvious that other than telephone number and IP address, the information used to identify each registered wireless device 106 stored in the HSS and bond with the SIP address during registration include “e-mail type of addresses.” APPLE-1005, [0061]; APPLE-1004, [0050] (“the destination address of the recipient device is a SIP URI formed out of the normal address (for example, tel:MDN)”); APPLE-1026, §4 (“SIP URIs are defined in Section 19.1. It has a similar form to an email address, typically containing a username and a host name. In this case, it is sip:bob@biloxi.com, where biloxi.com is the domain of Bob’s SIP service provider.”), §19.1 (“The ‘sip:’ and ‘sips:’ schemes follow the guidelines in RFC 2396 [5]. They use a form similar to the mailto URL... The formal syntax for a SIP or SIPS URI is presented in Section 25. Its general form, in the case of a SIP URI, is: sip:user:password@host:port;uri-parameters?headers”); APPLE-1021, 10:3-50 (“an IM application that is configured to initiate and otherwise manage an instant messaging session, including, but not limited to AOL Instant Messenger, Yahoo! Messenger, NET Messenger Server, ICQ, and the like”); APPLE-1028 (archived webpage from 2004 showing sign-in requirements for Yahoo! Messenger 6.0: “The

application will request a **Yahoo! ID** and password each time it is started....If you don't have a Yahoo! D, click the Get Yahoo! ID button to create a free Yahoo! Account.”); APPLE-1032, [0017] (“virtual communities (e.g., communities hosted on social networking sites such as...Instant Messenger, ICO...”), [0025] (“the user ID that is associated with the user’s virtual community account (e.g., an e-mail address”), FIGS. 2 (“UserID (e.g., e-mail address) for this account”), 5, supported by APPLE-1033, page 3, lines 4-5, page 4, lines 2-6; APPLE-1036, page 3 lines 25-28 (“MMS data flow starts with a subscriber using an MMS client on the mobile phone to compose, address, and send an MMS message to one or more recipients. MMS addresses can be either E.164 phone numbers (e.g., ‘+18005551212’) or RFC 2822 email addresses (e.g., ‘you@yourdomain.com’).”).

125. A POSITA would have further understood and found obvious that when the second receiving mobile phone has an inactive status, the instant messaging service (*the PSMS*), through the remote server(s), routes at least some messages between the instant messaging subscribers according to the email address(es) of one or more recipients (*an email address*).

Claim [5]: The system of claim 1, wherein the status information maintained by the at least one server is maintained in accordance with an undelivered message queue.

126. Horvath-Tsampalis-Chatterjee-Kansal renders obvious Claim [5]. As discussed above, a POSITA would have found obvious that the status information

maintained by Horvath-Tsampalis-Chatterjee-Kansal's remote server(s) is maintained in accordance with a period defined by either a specific event (e.g., user input) or a relevant threshold parameter such as a specified time or a maximum number of undelivered messages being queued (*an undelivered message queue*). *Supra*, Analyses of Claims [2]-[4].

Claim [6]: The system of claim 1, wherein the second receiving mobile phone has an inactive status with the PSMS when an inactivity parameter associated with the second receiving mobile phone exceeds a threshold.

127. Horvath-Tsampalis-Chatterjee-Kansal renders obvious Claim [6]. As discussed with respect to [2], it was a known problem that mobile devices connected to wireless networks often experienced “unreliable” connections in which “[n]etworking equipment between two connected users may frequently fail and recover.” APPLE-1047, [0007]. For at least temporary disconnections, it was further known to delay changing status to avoid the poor user experience of seeing constant disconnection and error messages. *See, e.g.*, APPLE-1047, [0016] (“delay displaying any error message to the user for a certain amount of time while the reliable messaging system attempts to restore the connection,” so that “real-time communication appears more reliable to the user, because the user will see fewer delivery errors when a connection can be reestablished”); APPLE-1046, [0035] (“...the application server maintains the online status of the user despite the user being temporarily disconnected. Any messages directed to the user during this time

may be temporarily stored in a memory and then sent to the second device once the second device has logged in the application server.”). However, after the user’s device had been disconnected for longer than the certain amount of time (*an inactivity parameter associated with the second receiving mobile phone exceeds a threshold*), a POSITA would have found it obvious that *the second receiving mobile phone has an inactive status with the IM service (PSMS)*. See APPLE-1047, [0016], [0020] (“If the receiving participant is disconnected, the sending participant may receive other responses, such as ‘480 Temporarily Unavailable’ or ‘504 Server Timeout,’...”).

Claim [7]: The system of claim 1, wherein the second receiving mobile phone has an active status with the PSMS after a message queued for the second receiving mobile phone is delivered to the second receiving mobile phone.

128. Horvath-Tsampalis-Chatterjee-Kansal renders obvious Claim [7]. As described with respect to [1j2], it was a known problem that mobile devices connected to wireless networks often experienced “unreliable” connections in which “[n]etworking equipment between two connected users may frequently fail and recover.” APPLE-1047, [0007]. One known way for a real-time messaging system to deal with these issues is to utilize a message cache that “caches any messages sent while the connection is unavailable.” See, e.g., APPLE-1047, [0017]; APPLE-1046, [0035]; APPLE-1048, [0053].

129. As discussed with respect to [2], for at least temporary disconnections, it was further known to delay changing status to avoid the poor user experience of seeing constant disconnection and error messages. *See, e.g.*, APPLE-1047, [0016] (“delay displaying any error message to the user for a certain amount of time while the reliable messaging system attempts to restore the connection,” so that “real-time communication appears more reliable to the user, because the user will see fewer delivery errors when a connection can be reestablished”); APPLE-1046, [0035] (“...the application server maintains the online status of the user despite the user being temporarily disconnected. Any messages directed to the user during this time may be temporarily stored in a memory and then sent to the second device once the second device has logged in the application server.”). Accordingly, for messages sent to a receiving mobile device during a temporary disconnection, a POSITA would have found it obvious to store the messages in a message cache until the receiving mobile device was able to reconnect and keep the status active throughout the process. Because the active status never changed, *the second receiving mobile phone has an active status with the PSMS after a message queued for the second receiving mobile phone is delivered to the second receiving mobile phone.*

130. To be clear, the claim language reciting “*after*” does not imply causality or otherwise require that the status have been anything other than

“active” before a message queued for the second receiving mobile phone is delivered to the second receiving mobile phone. Nor does the word “*after*” impose a limit to how long after, it could be immediately after, or it could be any time after the number of undelivered messages comes back to below the threshold, before the status is updated to active again, depending on design choice.

Claim [8]: The system of claim 1, wherein the second receiving mobile phone has an active status with the PSMS at a point in time subsequent to a message queued for the second receiving mobile phone being delivered to the second receiving mobile phone.

131. Horvath-Tsampalis-Chatterjee-Kansal renders obvious Claim [8]. *Supra*, Analysis of Claim [7]. Note that “*at a point in time subsequent to*” recited here is similarly unbound as “*after*” recited in Claim [7].

Claim [9]: The system of claim 1, wherein the second receiving mobile phone has an active status with the PSMS when the second receiving mobile phone is connected to the at least one server and the second receiving mobile phone remains active for a time period after the second receiving mobile phone is not connected to the at least one server, after which the second receiving mobile phone has an inactive status with the PSMS, wherein a plurality of undelivered messages are queued for the second receiving mobile phone during the time period.

132. Horvath-Tsampalis-Chatterjee-Kansal renders obvious Claim [9]. As described with respect to [1j2], it was a known problem that mobile devices connected to wireless networks often experienced “unreliable” connections in which “[n]etworking equipment between two connected users may frequently fail and recover.” APPLE-1047, [0007]. As described with respect to [2] and [6], for

at least temporary disconnections, it was further known to delay changing status to avoid the poor user experience of seeing constant disconnection and error messages. *See, e.g.*, APPLE-1047, [0016] (“delay displaying any error message to the user for a certain amount of time while the reliable messaging system attempts to restore the connection,” so that “real-time communication appears more reliable to the user, because the user will see fewer delivery errors when a connection can be reestablished”); APPLE-1046, [0035] (“...the application server maintains the online status of the user despite the user being temporarily disconnected. Any messages directed to the user during this time may be temporarily stored in a memory and then sent to the second device once the second device has logged in the application server.”). Accordingly, it would have been obvious to a POSITA that *the second receiving mobile phone has an active status with the IM service (PSMS) when the second receiving mobile phone is connected to the remote server (at least one server) connecting the receiving device to the SIP network implementing the IM service, and the second receiving mobile phone remains active for a time period after the second receiving mobile phone is not connected to the at least one server.* However, after the user’s device had been disconnected for longer than the “certain amount of time” (*a time period after the second receiving mobile phone is not connected to the at least one server*), a POSITA

would have found it obvious that *the second receiving mobile phone has an inactive status with the* IM service (*PSMS*).

133. Further, as discussed with respect to [1j2], one known way for a real-time messaging system to deal with unreliable connection issues is to utilize a message cache that “caches any messages sent while the connection is unavailable.” *See, e.g.*, APPLE-1047, [0017]; APPLE-1046, [0035]; APPLE-1048, [0053]. Correspondingly, a POSITA would have found it obvious that *a plurality of undelivered messages are queued for the second receiving mobile phone during* the time while the receiving mobile device attempts to reconnect (*the time period*).

Claim [10]: The system of claim 1, wherein: the sending mobile phone sends the SMS message to the first receiving mobile phone in accordance with the first response; the sending mobile phone sends the packet switched message to the second receiving mobile phone in accordance with the second response.

134. *Supra*, §VIII.A, Analyses of [1j1], [1f].

Claim [11]: The system of claim 4, wherein at least one of the plurality of messages queued for the second receiving mobile phone is a picture message.

135. Horvath-Tsampalis-Chatterjee-Kansal renders obvious Claim [11]. For example, Horvath, Tsampalis and Chatterjee all disclose messaging text as well as multimedia messages, which include images, audio (*i.e.*, voice) and video messages. APPLE-1004, [0025] (“...Multimedia Messaging Service (‘MMS’), and the like are also included in the networks 102, 104.”), [0029] (“Each of these

networks 118, 120, 122 has the capability of sending data, for example, a multimedia text message to the wireless devices 106.”), [0034] (“an Internet Protocol multimedia system (‘IMS’)”), [0068] (“a received multimedia message may include a sequence of colored lights to be displayed to the user as part of the message.”), [0069] (“a multimedia message received by the wireless device 106 may include a video media component that provides a vibration during playback of the multimedia message”); APPLE-1005 (description focusing on MMS and SMS messaging format capabilities); APPLE-1007, page 8 (“IM&P service is more media-rich than traditional applications such as mail, phone, and email. By using IM&P, we can deliver voice, video, and data together to various endpoints...We can search for images from our database and transmit them through IM&P services.”).

136. Based on these and related descriptions, a POSITA would have found obvious that, in the combined system, at least one of the plurality of IM messages queued for the second receiving mobile phone contain image(s) (*is a picture message*). APPLE-1008, [0002] (multimedia contents transmitted by using an instant messaging (IM) client”).

Claim [12]: The system of claim 4, wherein at least one of the plurality of messages queued for the second receiving mobile phone is a video message.

137. *Supra*, Analysis of Claim [11].

Claim [13]: The system of claim 4, wherein at least one of the plurality of messages queued for the second receiving mobile phone is a voice message; wherein the messaging client does not provide a voice message attachment option during a period of time between when the first information is received by the messaging client and when the second information is received by the messaging client; wherein the messaging client provides a voice messaging attachment option at a time subsequent to when the second information is received by the messaging client.

138. Horvath-Tsampalis-Chatterjee-Kansal renders obvious Claim [13]. As discussed above, at least one of the plurality of messages queued for the second receiving mobile phone in Horvath-Tsampalis-Chatterjee-Kansal is an audio multimedia (*voice*) message. *Supra*, Analysis of Claim [11].

139. Chatterjee explains that the IM service “is more media-rich” because it can be used to deliver “deliver voice, video, and data together.” APPLE-1007, 8, 11 (“integrated voice, video, and data services in IM systems.”). These teachings are supplemented by Kansal’s express disclosure for including a selectable menu item to “Record Sound” as an option to add a voice recording attachment to a message. APPLE-1042, [0073], FIG. 5; *see also id.*, [0074]-[0078] (“add media”), [0060], FIG. 3 (314). Like Chatterjee, Kansal explains that this message (e.g., the message with the voice recording attachment) can be an IM message. APPLE-1042, [0078] (“the user may compose a message in one format (e.g., SMS) and then convert or send the message in another format (e.g., MMS, e-mail, IM, etc.)”); *see also id.* [0045] (“the messaging UI used to display the message thread generally may be supported by a particular messaging application such as ... IM

application 135”). [0064] (“using various types of messages”); [0071] (“the embodiments, however, are not limited in [the SMS] context.”). Tsampalis also recognized that some messaging formats are capable of handling multimedia attachments while others are not, and that “any attached/inserted multimedia files” to be sent as an SMS message “will be lost.” APPLE-1005, [0062].

140. Kansal explains that “the messaging UI 500 may automatically or seamlessly convert” between messaging formats based on whether a user has attached a media file to the message. APPLE-1042, [0077]-[0078]. However, Kansal’s ability to seamlessly convert messaging formats assumes that the user currently subscribes to a messaging service having a messaging format capable of handling multimedia attachments (*e.g.*, MMS, IM). Before the user subscribes to the IM service, if the user were only subscribed to SMS, the voice recording or other media file could not be attached to an SMS message. APPLE-1005, [0062]; APPLE-1042, [0077]. In this context, it would have been obvious not to provide the option to add to the SMS message a voice attachment (Sound Recording) before the user subscribes to the IM service or other service capable of handling media attachments. For example, Tsampalis describes the option of removing a media file from a composed/active message before it is sent as an SMS, but a POSITA would have recognized that the options of (i) permitting the attachment of a media file (*e.g.*, voice attachment) during message composition that would be

removed before sending (*e.g.*, sending as an SMS message), or (ii) preventing the attachment of a media file during message composition in the first instance would be a matter of obvious design choice. For example, a POSITA would have chosen the latter option in at least some cases to provide an earlier indication to the user that the message will not be able to be sent with a voice attachment. A POSITA would have desired to restrict attachments during message composition if either the sender or receiver had limited messaging capabilities since the attachments could not be delivered in either case. Thus, it would have been obvious to provide the option of adding a voice attachment if the receiver is a subscriber of either MMS or IM, and not to provide that option if the receiver is not a subscriber of either. In fact, imposing restrictions/constraints on message attachments was well known before the Critical Date. APPLE-1054, [0011] (“attachment constraints can be specified”), [0022]-[0025]. Thus, when the first response indicates the first receiving mobile phone as non-subscriber of either any IM service (*the PSMS*) or MMS (and only capable of text-only SMS), then the sending mobile phone does not provide multimedia attachment option, knowing any such attachment will be lost; while when the second response indicates the second receiving mobile phone as a subscriber of IM (thus capable of receiving multimedia files), then the sending mobile phone provides such attachment option.

Claim [14]: The system of claim 1, wherein the messaging client displays an indication of a bearer used for transmission of the packet switched message, prior to transmission of the packet switched message.

141. Horvath-Tsampalis-Chatterjee-Kansal renders obvious Claim [14].

142. As discussed above in Sections IV.A.1(f)-(g), the combination implements Kansal’s messaging user interface, which displays a message thread of various types including “SMS messages” and “IM messages” within a single messaging client interface at the mobile wireless device. APPLE-1042, [0046]; *see also id.*, [0009]; [0045]-[0046]; [0054]-[0056]; [0062]-[0064]; [0070]; [0077]-[0078]. FIGs. 2, 3 (shown below).

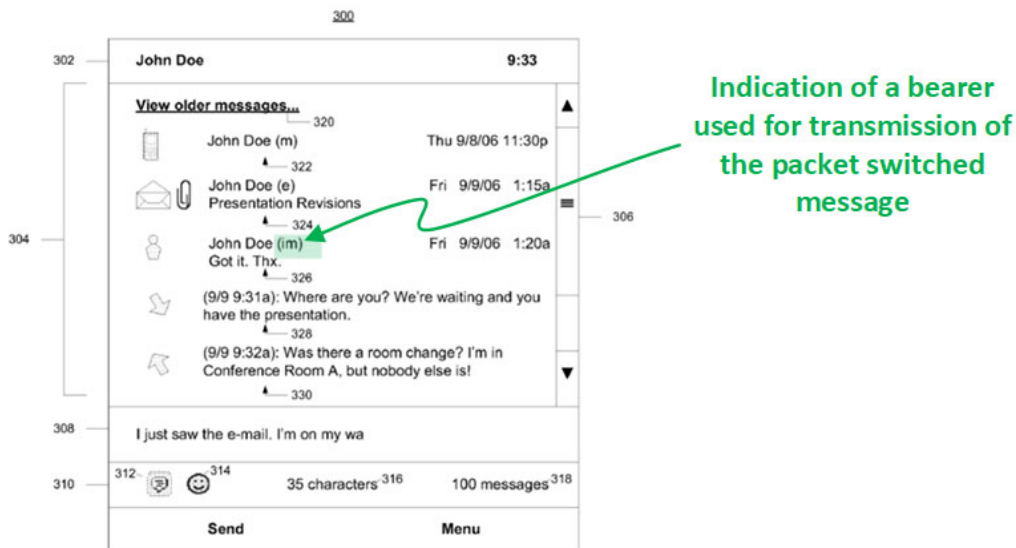


FIG. 3

APPLE-1042, FIG. 3

143. As annotated above, the interface described by Kansal *displays an indication of a bearer used for transmission of the packet switched message. Id.;*

In light of these teachings, it would have at least been obvious to a POSITA to display this information to the sender *prior to transmission of the packet switched message*, as that would help the user know which bearer they have selected for delivery. As described in Section IV.A.1(b), Tsampalis describes determining messaging format capabilities so that a user may select their preferred messaging format for delivering a message. APPLE-1005, [0037] (“If the user chooses to send the active message 216 in a format of the recipient list messaging format capabilities 406, the active message 216 is formatted in the selected messaging format capability, (e.g., message 112), and is sent to the second mobile wireless communication device 200”). A POSITA would have been motivated to display the messaging format information to the user while they were composing a message and prior to transmission—consistent with Tsampalis and Kansal—because it would have helped the user keep track of the format they selected and help them ensure they are utilizing the format they intended.

Claim [15]: The system of claim 1, wherein the messaging client displays an indication of a bearer used for transmission of the SMS message, prior to transmission of the SMS message.

144. *Supra*, Analysis of Claim [14].

Claim [16]: The system of claim 1, wherein at the time the packet switched message is sent, the second receiving mobile phone has an active status with the PSMS; wherein the second response communicates a different query result than the first response.

145. *Supra*, Analyses of [1e] (the first response indicating the first receiving mobile phone is not a subscriber and thus incapable of instant messaging), [1i] (the second response indicating the second receiving mobile phone is a subscriber and has an active status, thus capable of instant messaging), [1j1] (at the time the packet switched instant message is sent, the second receiving mobile phone has an active status with instant messaging).

Element [17pre1]: A method performed by

146. *Supra*, Analysis of [1pre].

Element [17pre2]: a sending mobile phone that transmits short message service (SMS) messages via a cellular network and packet switched messages via a packet switched message service (PSMS), the method comprising:

147. *Supra*, Analysis of [1a].

Element [17a]: authenticating a phone number of the sending mobile phone with the PSMS;

148. Horvath-Tsampalis-Chatterjee-Kansal renders obvious [17a]. For example, Horvath describes authenticating its wireless devices 106 (***the sending mobile phone***) *e.g.*, through authenticating an identifier such as a phone number of wireless device 106, both during registration with the SIP/IMS network and for transmitting subsequent messages. APPLE-1004, FIG. 5 (“S-CSCF authenticates and registers the wireless device” at step 508), [0035] (“The HSS 210 comprises a database including profiles associated with each wireless device 106 registered with the IMS. A profile, for example, includes subscription related information.

The **HSS 210** also performs **authentication and authorization** of the wireless device 106....The HSS 210 also includes **information to identify** each registered wireless device 106 such as a telephone uniform resource identifier ('tel-URI') and/or a SIP uniform resource identifier ('SIP-URI'). A tel-URI, for example is the **telephone number assigned to the wireless device 106.**"), [0036], [0040]; *supra*, Analysis of [1c].

149. In more detail, Horvath explains the SIP registration process for the wireless device 106 with the S-CSCF component of the remote server(s), during which "authentication and authorization" of the wireless device 106, through the database HSS containing "profiles associated with each wireless device 106" identified by *e.g.*, "the telephone number assigned to the wireless device 106," is also performed. APPLE-1004, [0035]-[0036], [0038] (The S-CSCF also handles **SIP registrations** which allows the S-CSCF to bind the location of the wireless device 106...and the SIP address"), [0040] ("The wireless device 106 registers with the S-CSCF component of the I, S-CSCF 208. When the S-CSCF receives a registration request from the wireless device 106, the **S-CSCF contacts the HSS 210 for authentication and authorization** of the wireless device 106. Upon being authenticated by the S-CSCF, a security association between the wireless device 106 and the P-CSCF, in one embodiment, is established."), [0041], [0072]-[0073], [0076], FIGS. 2, 5.

150. Once registration is complete, the P-CSCF of the remote server(s) “authenticate[s] subsequent messages:”

The P-CSCF 206 is a SIP proxy and is the first contact point for a wireless device 106 registered in the IMS network. In one embodiment, the wireless device 106 locates its respective P-CSCF 206 via a dynamic host configuration protocol (“DHCP”). The wireless device 106 is assigned to a specific P-CSCF 206 for the duration of the device’s subscription to the IMS network. All signaling messages are intercepted by the P-CSCF 206 allowing the P-CSCF 206 to inspect the messages. The P-CSCF 206 authenticates the wireless device 106 and is trusted by the other IMS components, which therefore do not perform further authentication of the wireless device 106. For example, after successful registration of a wireless device 106 with the S-CSCF component of the I, S-CSCF 208, security keys are sent to the P-CSCF 206, which allows it to setup a security association with the wireless device 106. The P-CSCF 206 can **authenticate subsequent messages** allowing the other network entities such as the I, S-CSCF 208 to trust the messages. Other functions of the P-CSCF 206 should be known to those of ordinary skill in the art.

APPLE-1004, [0036].

151. Through authentication with the remote server(s), wireless device 106 is also authenticated with the instant messaging service (*authenticating...with the PSMS*). APPLE-1004, [0033], [0038]-[0039] (“An application server [providing messaging service(s) such as instant messaging] interfaces with the S-CSCF component of the I, S-CSCF 20S using SIP.”), [0041] (“A subscriber profile sent

to the S-CSCF includes the filter criteria which are used by the S-CSCF to determine the application servers that are to be notified that they are to provide services for the wireless device 106. In one embodiment, part of the filter criteria includes conditions such that, when the conditions are satisfied, the S-CSCF notifies the SMSC 114 that the wireless device 106 has registered with the packet data network 102.... The SMSC 114 does not have to authenticate the wireless device 106 because the S-CSCF 206 has already done so.”), [0073]; APPLE-1007, 4 (“Instant messaging (IM)...enables [message] exchanges in real time”), 7, Boxes 1 & 2; *supra*, Analyses of [1k]-[11].

152. Horvath’s teachings in this regard are consistent with conventional techniques for authentication, *e.g.*, through a phone number, of a mobile phone for using SIP-based messaging service (such as instant messaging), by the Critical Date. APPLE-1009, pages 1 (“A user of a mobile device whilst in a location with WiFi (or other form of) internet access would **authenticate with the remote registration server** and this would indicate to the Routing System that it was possible for that mobile device to receive text messages via the internet rather than via GSM SMS messages offering substantial cost savings to the sending party.”), 3 (“The registration server could be either a dedicated solution using normal web based protocols such as http post or get, or via SIP, SMPP or other protocol which allows authentication with a remote device.”), 5 (“A Routing System consisting of

a gateway system containing a registration server capable of authenticating remote mobile devices via IP and **identifying the device via a unique identifier which can be related to the devices GSM mobile number** via lookup in a database or other information storage system”), 6 (“A Routing System utilising [*sic*] of Software capable of being installed and operated on a mobile device which authenticates with a remote database to signify it’s accessibility via an IP based route.”); APPLE-1043, §3 (“INSTANT MESSAGE SERVICE...May require authentication of SENDER USER AGENTS and/or INSTANT INBOXES...PRESENCE SERVICE...May require authentication of PRESENTITIES, and/or WATCHERS”); *see also* APPLE-1004, [0033] (“The SIP network is used for establishing instant messaging...and other real-time communications over the Internet.”); *supra*, §§VII.C, VIII.B. When the phone number of the first mobile wireless device (e.g., tel-URI) is registered in SIP or other network implementing the IM service, it would have been obvious for that phone number to be authenticated according to Horvath’s teachings. APPLE-1004, [0035].

Element [17b]: sending first information representing a phone number of a first receiving mobile phone to a server of the PSMS;

153. Horvath-Tsampalis-Chatterjee-Kansal renders obvious [17b]. *Supra*, Analyses of [1b] (Horvath-Tsampalis-Chatterjee-Kansal’s remote server(s) supports the PSMS), [1d]; APPLE-1004, [0039] (“the SMSC 114 acts as an

application server”), [0041] (“the SMSC 114...acting as an SIP application server”).

Element [17c]: receiving a first response when the phone number of the first receiving mobile phone is not identified as a subscriber of the PSMS;

154. *Supra*, Analysis of [1e].

Element [17d]: sending, after the first response is received by the sending mobile phone, an SMS message to the first receiving mobile phone;

155. *Supra*, Analysis of [1f].

Element [17e]: sending second information representing a phone number of a second receiving mobile phone to the server;

156. *Supra*, Analysis of [1h].

Element [17f]: receiving a second response, when the phone number of the second receiving mobile phone is identified as a subscriber of the PSMS and when the second receiving mobile phone has an active status with the PSMS; and

157. *Supra*, Analysis of [1i].

Element [17g]: sending a message, after the second response is received by the sending mobile phone, via a wireless local area network (WLAN) and the PSMS, to the second receiving mobile phone;

158. *Supra*, Analysis of [1j1] (“a message” of [17g] corresponds to “the second message” of [1j1]).

Element [17h]: wherein the second response communicates different information than the first response;

159. *Supra*, Analyses of [1e]/[17c] (first response indicating the first receiving mobile phone is not a subscriber, thus incapable of instant messaging)

and [1i]/[17f] (second response indicating the second receiving mobile phone is a subscriber and has an active status, thus capable of instant messaging).

Element [17i]: wherein the PSMS is a service for sending and receiving packet switched messages other than SMS, enhanced message service (EMS) and multimedia message service (MMS) messages;

160. *Supra*, Analysis of [1k].

Element [17j]: wherein the SMS message sent to the first receiving mobile phone and the message sent to the second receiving mobile phone are originated via a same messaging client.

161. *Supra*, Analysis of [1l].

Element [18pre]: The method of claim 17, further comprising:

162. *Supra*, Analysis of [1pre] and Claim [17].

Element [18a]: sending third information representing a phone number of the second receiving mobile phone to the server;

163. Horvath-Tsampalis-Chatterjee-Kansal renders obvious [18a]. As discussed above, Horvath-Tsampalis-Chatterjee-Kansal's sending mobile phone retrieves a destination address of an active message from the active message being composed by the user of the sending mobile phone, wherein the destination address of the active message is a phone number of a receiving mobile phone, and the sending mobile phone sends a request to the remote server(s). *Supra*, Analyses of [1c]-[1d] (regarding composing a first message addressed to a first receiving mobile phone and sending first information in the form of a first request) and [1g]-

[1h] (regarding composing a second message addressed to a second receiving mobile phone and sending second information in the form of a second request).

164. A POSITA would have found obvious that at least in one instance, the user of the sending mobile phone composes a third active message addressed to the second receiving mobile phone when the second receiving mobile phone does not have an active status with instant messaging (*the PSMS*), e.g., due to loss of connection with the remote server(s) for a long enough period for its status to change to inactive. *Supra*, Analyses of [1b]-[1d], [1g]-[1i], [1j2]. The sending mobile phone sends a third request (*third information*) representing the phone number of the second receiving mobile phone to the remote server(s) querying the messaging format capabilities information and active/inactive status of the second receiving mobile phone.

Element [18b]: receiving a third response, when the phone number of the second receiving mobile phone is identified as a subscriber of the PSMS and when the second receiving mobile phone does not have an active status with the PSMS;

165. Horvath-Tsampalis-Chatterjee-Kansal renders obvious [18b]. As discussed above, at least in one instance, the user of the sending mobile phone composes a third active message addressed to the second receiving mobile phone when the second receiving mobile phone does not have an active status. *Supra*, Analysis of [18a]. A POSITA would have understood and found obvious that in such instance, Horvath-Tsampalis-Chatterjee-Kansal's remote server(s) sends a

third response to the sending mobile phone (*receiving a third response*) indicating that the second receiving mobile phone is a subscriber of instant messaging (*the PSMS*) and that the second receiving mobile phone does not have an active status with instant messaging. *Id.; supra*, Analyses of [1b], [1i].

Element [18c]: and sending, after the third response is received, an SMS message to the second receiving mobile phone;

166. Horvath-Tsampalis-Chatterjee-Kansal renders obvious [18c]. A POSITA would have found obvious that when the third response indicates that the second receiving mobile phone does not have an active status, thus not capable of sending or receiving instant messages, at least in one instance the sending mobile phone sends the third message as an SMS message to the second receiving mobile phone, after learning from the received third response that any instant messages cannot be received by the second mobile phone. *Supra*, Analysis of [18b].

Element [18d]: wherein the third response communicates a same query result as the first response, and the third response communicates a different query result than the second response.

167. Horvath-Tsampalis-Chatterjee-Kansal renders obvious [18d]. As discussed above, the third response communicates a same query result as the first response, both indicating a lack of instant messaging capabilities of a receiving mobile phone, which is different from the query result of the second response which indicates an existence of instant messaging capabilities of a receiving mobile phone. *Supra*, Analyses of [1e], [1i], Analysis of [18b].

Claim [19]: The method of claim 18, further comprising: sending, after the third response is received, a multimedia message service (MMS) message to the second receiving mobile phone.

168. Horvath-Tsampalis-Chatterjee-Kansal renders obvious Claim [19]. As discussed above, the Horvath-Tsampalis-Chatterjee-Kansal's wireless devices are capable of various messaging formats through subscriptions to various messaging services, e.g., SMS, EMS, MMS (multimedia message service), and IM. *Supra*, §VII.A; APPLE-1004, [0025] ("Text messaging standards such as Short Message Service ('SMS'), Enhanced Messaging Service ('EMS'), Multimedia Messaging Service ('MMS'), and the like are also included in the networks 102, 104."), [0039]; *see also* APPLE-1005, [0002], [0024], [0056]-[0064].

169. A POSITA would have understood and found obvious that at least in one instance, the sending mobile phone, after the third response is received indicating a lack of instant messaging capabilities on the second receiving mobile phone due to an inactive status with the instant messaging service, a multimedia message service (MMS) message to the second receiving mobile phone. *Supra*, Analysis of Claim [18].

Claim [20]: The method of claim 17, wherein when the second response is received, the second receiving mobile phone is offline from the PSMS, wherein the PSMS routes at least some messages between PSMS subscribers according to an email address.

170. *Supra*, Analyses of Claims [2], [4] and [17].

Claim [21]: The method of claim 17, wherein the server is located outside of the cellular network, wherein the PSMS receives and queues messages addressed to a message recipient when the message recipient is not connected to the PSMS.

171. Horvath-Tsampalis-Chatterjee-Kansal renders obvious Claim [21]. Horvath-Tsampalis-Chatterjee-Kansal's remote server(s) is located outside of the circuit services network (*cellular network*) with "an interface to the packet data network 102 and the circuit services network 104." *Supra*, Analysis of [1a]; APPLE-1004, [0058], FIGS. 1-3.

172. A POSITA would have understood and found obvious that Horvath-Tsampalis-Chatterjee-Kansal's instant messaging service (*the PSMS*), *e.g.*, through the remote server(s), receives and queues messages addressed to a message recipient for later delivery if the outgoing messages cannot be delivered to the message recipient, *e.g.*, when the message recipient is not connected to instant messaging. *Supra*, Analysis of Claim [1].

Element [22pre1]: A method performed by

173. *Supra*, Analysis of [1pre].

Element [22pre2]: a sending mobile phone that transmits short message service (SMS) messages via a cellular network and packet switched messages via a packet switched message service (PSMS), the method comprising:

174. *Supra*, Analysis of [17pre2], Analysis of [1a].

Element [22a]: sending first information representing a phone number of a first receiving mobile phone to a server of the PSMS;

175. *Supra*, Analysis of [1d].

Element [22b]: receiving a first response when the phone number of the first receiving mobile phone is not identified as a subscriber of the PSMS;

176. *Supra*, Analysis of [1e].

Element [22c]: sending, after the first response is received by the sending mobile phone, an SMS message to the first receiving mobile phone;

177. *Supra*, Analysis of [1f].

Element [22d]: sending second information representing a phone number of a second receiving mobile phone to the server;

178. *Supra*, Analysis of [1h].

Element [22e]: receiving a second response, when the phone number of the second receiving mobile phone is identified as a subscriber of the PSMS and when the second receiving mobile phone has an active status with the PSMS;

179. *Supra*, Analysis of [1i].

Element [22f]: sending a message, after the second response is received by the sending mobile phone, via a wireless local area network (WLAN) and the PSMS, to the second receiving mobile phone;

180. *Supra*, Analysis of [1j1] (*a message* of [22f] corresponds to *the second message* of [1j1]).

Element [22g]: sending third information representing the phone number of the second receiving mobile phone to the server;

181. *Supra*, Analysis of [18a].

Element [22h]: receiving a third response, when the phone number of the second receiving mobile phone is identified as a subscriber of the PSMS and when the second receiving mobile phone does not have an active status with the PSMS; and

182. *Supra*, Analysis of [18b].

Element [22i]: sending, after the third response is received by the sending mobile phone, an SMS message to the second receiving mobile phone;

183. *Supra*, Analysis of [18c].

Element [22j]: wherein the second response communicates different information than the third response; and

184. *Supra*, Analysis of [18d].

Element [22k]: wherein content of the SMS message sent to the first receiving mobile phone, content of the message sent via the WLAN and the PSMS to the second receiving mobile phone and content of the SMS message sent to the second receiving mobile phone is displayed by a same messaging applicaion [sic] client;

185. *Supra*, Analysis of [11].

Element [22l]: wherein the PSMS routes at least some messages between PSMS subscribers according to an email address.

186. *Supra*, Analysis of Claim [4].

Claim [23]: The method of claim 22, wherein the sending mobile phone is authenticated to the PSMS via SMS.

187. Horvath-Tsampalis-Chatterjee-Kansal renders obvious Claim [23]. As discussed above, Horvath-Tsampalis-Chatterjee-Kansal's sending mobile phone is authenticated to instant messaging both at SIP registration and during subsequent messaging. *Supra*, Analysis of [17a]. A POSITA would have understood and found obvious that at least prior to the completion of the SIP registration with the IP-based packet data network, the sending mobile phone does not have access to the SIP or Internet protocol, such that the sending mobile phone is authenticated via SMS protocol. Moreover, it was known to POSITAs to authenticate a device

initiating an IM session through SMS text message between the user and the IM server. *See, e.g.*, APPLE-1050, [0006], [0017] (“The initiating mobile device [] transmits...to *authenticate* the user as the moderator) in an SMS text message to [a] telephone number of [a] server 420”), FIG. 4; *see also id.*, Abstract, [0014]-[0016], FIGs. 2-3

Claim [24]: The method of claim 22, wherein content of the message sent via the WLAN to the second receiving mobile phone and content of the SMS message sent to the second receiving mobile phone is displayed in a same interface.

188. *Supra*, Analysis of [11].

Element [25pre1]: A method performed by

189. *Supra*, Analysis of [1pre].

Element [25pre2]: a sending mobile phone that transmits short message service (SMS) messages via a cellular network and packet switched messages via a packet switched message service (PSMS), the method comprising:

190. *Supra*, Analysis of [17pre2].

Element [25a]: retrieving, by a messaging client, a destination address of a first message from the first message, wherein the destination address of the first message represents a phone number of a first receiving mobile phone;

191. *Supra*, Analysis of [1c].

Element [25b]: sending first information representing the phone number of the first receiving mobile phone to a server of the PSMS;

192. *Supra*, Analysis of [1d].

Element [25c]: receiving a first response when the phone number of the first receiving mobile phone is not identified as a subscriber of the PSMS;

193. *Supra*, Analysis of [1e].

Element [25d]: sending, after the first response is received by the sending mobile phone, the first message as an SMS message to the first receiving mobile phone;

194. *Supra*, Analysis of [1f].

Element [25e]: retrieving, by the messaging client, a destination address of a second message from the second message, wherein the destination address of the second message is a phone number of a second receiving mobile phone;

195. *Supra*, Analysis of [1g].

Element [25f]: sending second information representing the phone number of the second receiving mobile phone to the server;

196. *Supra*, Analysis of [1h].

Element [25g]: receiving a second response, when the phone number of the second receiving mobile phone is identified as a subscriber of the PSMS and when the second receiving mobile phone has an active status with the PSMS;

197. *Supra*, Analysis of [1i].

Element [25h]: sending the second message, after the second response is received by the sending mobile phone, via a wireless local area network (WLAN) and the PSMS, to the second receiving mobile phone;

198. *Supra*, Analysis of [1j1].

Element [25i]: sending third information representing the phone number of the second receiving mobile phone to the server;

199. *Supra*, Analysis of [18a].

Element [25j]: receiving a third response, when the phone number of the second receiving mobile phone is identified as a subscriber of the PSMS and when the second receiving mobile phone does not have an active status with the PSMS; and

200. *Supra*, Analysis of [18b].

Element [25k]: sending, after the third response is received by the sending mobile phone, an SMS message to the second receiving mobile phone;

201. *Supra*, Analysis of [18c].

Element [25l]: wherein the second response communicates different information than the third response

202. *Supra*, Analysis of [18d].

Element [25m]: wherein content of the SMS message sent to the first receiving mobile phone, content of the second message and content of the SMS message sent to the second receiving mobile phone is displayed by a same messaging client.

203. *Supra*, Analysis of [11].

Claim [26]: The method of claim 25, wherein: the SMS message sent to the first receiving mobile phone is sent in accordance with the first response; the second message is sent in accordance with the second response; the SMS message sent to the second receiving mobile phone is sent in accordance with the third response; the server is located outside of a cellular network.

204. *Supra*, Analyses of [1f] (the SMS message sent to the first receiving mobile phone is sent in accordance with the first response), [1j1] (the second message is sent in accordance with the second response); Analysis of [18c] (the SMS message sent to the second receiving mobile phone is sent in accordance with the third response), Analysis of Claim [21] (the server is located outside of a cellular network) and Analysis of Claim [25].

Claim [27]: The method of claim 25, wherein the first information represents a plurality of phone numbers, wherein the messaging client provides a single interface for sending and receiving both text and multimedia messages.

205. Horvath-Tsampalis-Chatterjee-Kansal renders obvious Claim [27]. For example, Tsampalis teaches “the use of an active message recipient list” having a plurality of recipients in a single active message, each recipient having a

“recipient ID” that the user enters in the form of phone numbers for the same active message that the use composes. See e.g., APPLE-1005, [0004] (“list of delivery recipients” for “a message”), [0009], [0032], [0055] (“groups of recipients”), FIG. 4 (below). Thus, a POSITA would have understood and found obvious that in at least one case the first information represents a plurality of phone numbers, when the first message is addressed to a plurality of recipients each identified by their respective phone number. *Supra*, Analyses of [1c]-[1d].

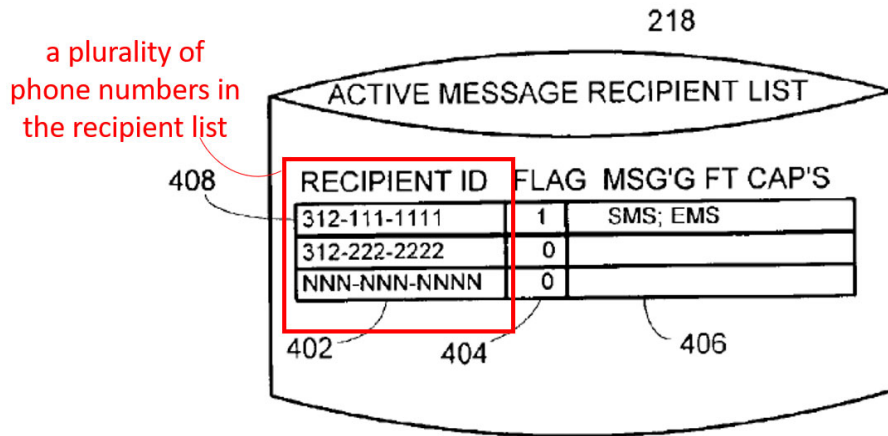


FIG. 4

APPLE-1005, FIG. 4 (Annotated)

206. Additionally, a POSITA would also have understood and found obvious that the messaging service application supporting IM (*messaging client*) operative on the Horvath-Tsampalis-Chatterjee-Kansal’s mobile phone provides a single interface for sending and receiving both text and multimedia messages, as

the IM service supports both text and multimedia messages. *Supra*, Analysis of Claim [11].

Claim [28]: The method of claim 25, wherein at the time when a status of the second receiving mobile phone is determined by the PSMS, the second receiving mobile phone is not connected to the PSMS.

207. *Supra*, Analyses of [1b] (server supports instant messaging (***the PSMS***) and maintains status), [1i] (second receiving mobile phone having an active status when it is online), Analysis of Claim [2] (second receiving mobile phone having an active status in at least one case when the second receiving mobile phone loses connection, before status updates to reflect the change (***determined by the PSMS***)), Analyses of [18a]-[18b] (second receiving mobile phone's status is determined by the instant messaging service to be inactive, *e.g.*, when the second receiving mobile phone is offline or disconnected for a long enough time), and Analysis of Claim [25].

Claim [29]: The method of claim 25, wherein the messaging client displays an indication of a bearer used for transmission of the second message sent to the second receiving mobile phone, prior to the sending of the second message to the second receiving mobile phone.

208. *Supra*, Analysis of Claim [14].

Claim [30]: The method of claim 25, wherein the messaging client displays an indication of a bearer used for transmission of the SMS message sent to the first receiving mobile phone, prior to the sending of the SMS message to the first receiving mobile phone.

209. *Supra*, Analysis of Claim [15].

IX. CONCLUSION

210. For all the reasons I have noted in the foregoing paragraphs, claims 1-20 of the '182 Patent are obvious in view of the references discussed above.

211. 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.

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

1889 Museum Rd,

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	12
II. RESEARCH AND CREATIVE SCHOLARSHIP	13
A. Thesis	13
B. Published Journal Papers (Refereed)	13
C. Published Books and Parts of Books	15
D. Edited Proceedings	15
E. Conference Presentations	15
E.1. Conference Papers with Proceedings (Refereed)	15
E.2. Conference Presentations with Proceedings (Non-Refereed)	22
E.3. Conference Presentations without Proceedings	22
F. Other	22
F.1. Submitted Journal Papers	22
F.2. Refereed Research Reports	23
F.3. Software	23
F.4. Published Papers (Non-Refereed)	23
F.5. Books in Preparation	23
F.6. Workshops and External Courses	23
G. Research Proposals and Grants (Principal Investigator)	24
H. Research Proposals and Grants (Contributor)	26
I. Research Honors and Awards	28
III. SERVICE	29
A. Professional Activities	29
A.1. Memberships and Activities in Professional Societies	29
A.2. Conference Committee Activities	29
B. On-Campus Committees	30
B.1. University of Florida	30
B.2. Georgia Tech	31
C. Special Assignments	31
D. Ph.D. Examining Committees	31
E. External Member of M.S. Examining Committee	35
F. Consulting and Advisory Appointments	35
G. Civic Activities	35
IV. NATIONAL AND INTERNATIONAL PROFESSIONAL RECOGNITION	36
A. Honors and Awards	36
B. Invited Conference Session Chairmanships	36
C. Professional Registration	36
D. Patents	36
E. Editorial and Reviewer Work for Technical Journals and Publishers	37
F. Expert Witness Services	39
V. OTHER CONTRIBUTIONS	41
A. Seminar Presentations (Invited Papers and Talks at Meetings and Symposia)	41

B. Special Activities 45

EDUCATIONAL BACKGROUND

Degree	Year	University	Field
Ph.D.	2008	Pennsylvania State University State College, PA <i>Dissertation:</i> Characterizing the Impact of Ridigity on the Security of Cellular Telecommunications Networks <i>Advisors:</i> 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 <i>Minors:</i> Biology, Business Admin	Computer Science

EMPLOYMENT HISTORY

Title	Organization	Years
Associate Chair for Research	University of Florida	August 2018–Present
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 2024	CNT 4007 Computer Networks 1	310	Revamped Course
Fall 2023	CIS 6930 Cellular and Mobile Network Security	19	New Topics
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

University of Florida

CNT 4007 Computer Networks 1: *Fall 2024.* Provided the first major overhaul to this course in a number of years. While I have relied on the same book used by other faculty, I have created new homeworks, projects, and slides to better represent the current state of computer networks. I have also significantly expanded the discussion of security in this course.

CIS 6930 Cellular and Mobile Network Security: *Fall 2018, 2023.* 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 (2G-5G), 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. 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.

CNT 5410 Computer and Network Security: *Fall 2014-2022.* 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.

Georgia Tech In addition to the above courses, I also developed the following course while serving as a faculty member at Georgia Tech.

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

Hadi Abdullah University of Florida

Fall 2016–Summer 2022

Evaluating the security of ML-driven voice interfaces. Now: Research Scientist at Visa Research

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.

- Logan Blue** University of Florida
Fall 2016–Summer 2022
Investigated biological feature reconstruction from voice recordings. Now: Research Scientist at Harbor Labs
- 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.
- Cassidy Gibson** University of Florida
Fall 2019–Spring 2025
Investigated compiler techniques to remove software vulnerabilities from code. Now CTO of MailChimp.
- 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
- 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

2. Ph.D. Students Supervised

Nathaniel Bennett University of Florida

Fall 2022–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.

Ryon Kennedy University of Florida

Fall 2020–Spring 2023

Finding vulnerabilities in cellular core networks via fuzzing. Left to join UFIT.

Eric (Yu) Liu Georgia Institute of Technology

Fall 2008

Research on the spread of malware 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 University of Florida

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. (Acceptance rate: 24%).
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 Security Challenges of Digital Financial Services. *IEEE S&P Magazine*, 15(5):85–89, 2017.
4. Nolen Scaife, 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 Security (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 Papers with Proceedings (Refereed)

1. Cassidy Gibson and Daniel Olszewski and Natalie Grace Brigham and Anna Crowder and Kevin R. B. Butler and Patrick Traynor and Elissa M. Redmiles and Tadayoshi Kohno. Analyzing the AI Nudification Application Ecosystem. In *Proceedings of the USENIX Security Symposium (Security)*, 2025.
2. Tyler Tucker, Nathaniel Bennett, Martin Kotuliak, Simon Erni, Srdjan Capkun, Kevin Butler, and Patrick Traynor. Detecting IMSI-Catchers by Characterizing Identity Exposing Messages in Cellular Traffic. In *Symposium on Network and Distributed System Security (NDSS)*, 2025. (Acceptance Rate 16.1%).
3. Magdalena Pasternak, Kevin Warren, Daniel Olszewski, Susan Nittroueri, Patrick Traynor, and Kevin Butler. Characterizing the Impact of Audio Deepfakes in the Presence of Cochlear Implant Simulated Audio. In *Symposium on Network and Distributed System Security (NDSS)*, 2025. (Acceptance Rate 16.1%).
4. Anna Crowder, Daniel Olszewski, Patrick Traynor, and Kevin R. B. Butler. I Can Show You the World (of Censorship): Extracting Insights from Censorship Measurement Data Using Statistical Techniques. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, December 2024. (Acceptance Rate 21.8%).
5. Kevin Childs, Cassidy Gibson, Anna Crowder, Kevin Warren, Carson Stillman, Elissa Redmiles, Eakta Jain, Patrick Traynor, and Kevin Butler. "I Had Sort of a Sense that I Was Always Being Watched... Since I Was": Examining Interpersonal Discomfort From Continuous Location-Sharing Applications. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2024. (Acceptance Rate 16.9%).
6. Nathaniel Bennett, Weidong Zhu, Benjamin Simon, Ryon Kennedy, William Enck, Patrick Traynor, and Kevin Butler. RANsacked: A Domain-Informed Approach for Fuzzing LTE and 5G RAN-Core Interfaces. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2024. (Acceptance Rate 16.9%).
7. Kevin Warren, Tyler Tucker, Anna Crowder, Daniel Olszewski, Allison Lu, Caroline Fedele, Magdalena Pasternak, Seth Layton, Kevin Butler, Carrie Gates, and Patrick Traynor. Better Be Computer or I'm Dumb": A Large-Scale Evaluation of Humans as Audio Deepfake Detectors. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2024. (Acceptance Rate 16.9%).

8. K. Virgil English, Nathaniel Bennett, Seaver Thorn, Kevin Butler, William Enck, and Patrick Traynor. Examining Cryptography and Randomness Failures in Open-Source Cellular Cores. In *Proceedings of the ACM Conference on Data and Application Security and Privacy (CODASPY)*, 2024. (Acceptance rate: 21.3%)(Best Paper).
9. Seth Layton, Tyler Tucker, Daniel Olszewski, Kevin Warren, Carrie Gates, Kevin Butler, and Patrick Traynor. SoK: The Good, The Bad, and The Unbalanced: Measuring Structural Limitations of Current Deepfake Datasets. In *Proceedings of the USENIX Security Symposium (Security)*, 2024. (Acceptance Rate 18.3%).
10. Imani Munyaka, Daniel Delgado, Juan Gilbert, Jaime Ruiz, and Patrick Traynor. “I used to live in Florida”: Exploring the Impact of Spam Call Warning Accuracy on Callee Decision-Making. In *Symposium on Usable Security and Privacy (USEC)*, 2024.
11. Jianliang Wu, Patrick Traynor, Dongyan Xu, Dave (Jing) Tian, and Antonio Bianchi. Finding Traceability Attacks in the Bluetooth Low Energy Specification and Its Implementations. In *Proceedings of the USENIX Security Symposium (Security)*, 2024. (Acceptance Rate 18.3%).
12. Daniel Olszewski, Allison Lu, Carson Stillman, Kevin Warren, Cole Kitroser, Alejandro Pascual, Divyajyoti Ukirde, Kevin Butler, and Patrick Traynor. “Get in Researchers; We’re Measuring Reproducibility”: A Reproducibility Study of Machine Learning Papers in Tier 1 Security Conferences. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2023. (Acceptance rate: 19.8%).
13. 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. (Acceptance rate: 21%).
14. 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. (Acceptance rate: 14%).
15. 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. (Acceptance rate: 16%).
16. 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.
17. 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%).
18. 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%).
19. 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%).

20. 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%).
21. 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.
22. 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 Communications Information and Internet Policy (TPRC 49)*, 2021.
23. 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%).
24. 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%).
25. 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.
26. 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%).
27. 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 *Proceedings of the ACM ASIA Conference on Computer and Communications Security (ASIACCS’19)*, 2019. (Acceptance Rate: 17.0% for full papers).
28. 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).
29. 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%).
30. 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%).
31. 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%).

32. 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%).
33. 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%).
34. 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%.
35. 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%.
36. 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%.
37. Luis Vargas, Gyan Hazarika, Rachel Culpepper, Kevin Butler, Thomas Shrimpton, Doug Szajda, and Patrick Traynor. Mitigating Risk while Complying with Data Retention Laws. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2018.
38. Logan Blue, Luis Vargas, and Patrick Traynor. Hello, Is It Me You're Looking For? Differentiating Between Human and Electronic Speakers for Voice Interface Security. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2018.
39. 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%).
40. 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%).
41. 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%).
42. 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%).
43. 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%).
44. 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%).

45. 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%).
46. 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%).
47. 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%).
48. 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%).
49. 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%).
50. 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%).
51. 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%).
52. Nolen Scaife, 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%).
53. 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%).
54. Bradley Reaves, Ethan Sherman, 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%).
55. 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%).
56. Ethan Sherman, 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%).
57. 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%).
58. 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%).

59. 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%).
60. 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).
61. 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%).
62. 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).
63. 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).
64. 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%).
65. 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%).
66. 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%).
67. 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%).
68. 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%).
69. 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%).
70. 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%).
71. Vijay Balasubramaniyan, Aamir Poonawalla, Mustaque Ahamad, Michael Hunter, and Patrick Traynor. PinDrOp: 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%).

72. 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%).
73. 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%).
74. 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%).
75. 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%).
76. 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%).
77. 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%).
78. 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%).
79. 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%).
80. 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%).
81. 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%).
82. 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%).
83. 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).
84. 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%).
85. 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%).

86. 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%).
87. 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%).
88. 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%).
89. 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%).
90. 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%).
91. 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%).
92. 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.

- 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

- Artus Protocol STTR Phase II - Extension**
Sponsor: Office of Naval Research
Investigator(s): Patrick Traynor (PI), Kevin Butler
Amount: *\$300,000 over 2 years*
Awarded: *August 2023*
- Testing Audio Deep Fake Detectors**
Sponsor: Bank of America
Investigator(s): Patrick Traynor (PI), Kevin Butler
Amount: *\$150,000 over 1 year*
Awarded: *August 2023*
- 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*
- 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*
- 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*
- 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*
- 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*
- Workshop: Addressing the Technical Security Challenges of Emerging Digital Financial Services**
Sponsor: NSF Secure and Trustworthy Cyberspace

Investigator(s): Patrick Traynor (PI), Kevin Butler
Amount: \$50,000 over 1 year
Awarded: September 2017

9. **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
10. **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
11. **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
12. **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
13. **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
14. **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
15. **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
16. **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

17. **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
18. **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
19. **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
20. **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 Kanuparth, 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, Byungsook 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. *ByteDance Ltd. vs CellSpin Soft, Inc.:* Expert witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Status: Ongoing. *February 2024 - Present.*
2. *Bank of America, N.A., vs PACid:* Expert witness for the Plaintiff for Inter Partes Review (via McNish PLLC). Status: Settled. *December 2023 - March 2024.*
3. *Microsoft vs Proxense, LLC:* Expert witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Status: Ongoing. *November 2023 - Present.*
4. *Samsung vs Headwater Research LLC:* Expert witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Status: Ongoing. *August 2023 - Present.*
5. *Advanced Coding Technologies LLC v. ByteDance PTE. Ltd., and TikTok PTE. Ltd.:* Expert witness for the Defense for Non-Infringement (via Fish & Richardson, LLP). Status: Dismissed with Prejudice. *July 2023 - September 2023.*
6. *Epic Games, Inc. & Anor v Google LLC & Ors - Federal Court of Australia Proceeding NSD 190 of 2021:* Expert witness for the Defendant (via Corrs Chambers Westgarth). Status: Ongoing. *January 2023 - June 2024.*
7. *Rubin vs KAHOOT! ASA and KAHOOT! EDU:* Expert witness for the Defendant for Inter Partes Review (via Vasquez Benisek & Lindgren, LLP). Status: Ongoing. *December 2022 - June 2024.*
8. *Telefonaktiebolaget LM Ericsson vs Apple, Inc:* Expert witness for the Defendant, Non-Infringement and Invalidity (via WilmerHale LLP). Status: Settled. *February 2022 - December 2022.*
9. *Wepay Global Payments, LLC v. Bank of America N. A.:* Expert Witness for the Defendant (via WilmerHale LLP) Status: Dismissed. *September 2022 - November 2022.*
10. *Apple vs. R.N Nehushtan Trust Ltd.:* Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Status: Petition Denied. *August 2022 - June 2023.*
11. *Apple/Microsoft vs. Zipit Wireless:* Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Status: Settled. *May 2021 - November 2022.*
12. *Blackberry Inc v MobileIron, Inc:* Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Verdict: Settled. *January 2021 - March 2021.*

13. *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*.
14. *mSIGNIA, Inc. v. InAuth, Inc.*: Expert Witness for the Defendant for Inter Partes Review, Non-Infringement and Invalidity, Trade Secrets (via Quinn Emanuel Urquhart and Sullivan, LLP). Verdict: Dismissed with prejudice. *October 2017 - December 2018*.
15. *Huawei v. T-Mobile*: Expert Witness for the Defendant for Non-Infringement (via WilmerHale LLP, Alston & Bird LLP) Verdict: Settled *June 2016 - December 2017*.
16. *Telefonaktiebolaget LM Ericsson v Apple*: Expert Witness for the Defendant for Non-Infringement, Invalidity (via WilmerHale LLP). Verdict: Settled *June 2015 - December 2015*.
17. *Mayfonk v Nike*: Expert Witness for the Plaintiff for Infringement/Trade Secrets (via Paul Hastings). Verdict: Settled. *June 2015 - November 2015*.
18. *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*.
19. *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*.
20. *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*.
21. *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*.
22. *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*.
23. *Intellectual Ventures LLC vs. Check Point; et al.*: Expert Consultant for the Plaintiff 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 in Computer Security Research. Learning from Authoritative Security Experiment Results (LASER) Workshop, December 2024. École Polytechnique Fédérale de Lausanne (EPFL, Switzerland).
2. Social Engineering and Two-Factor Authentication. Cyber Security Training Eastern Indonesia, August 2024. Financial Innovation Lab (EIFIL) (Denpasar, Bali, Indonesia).
3. DFS Security and Mobile Money Analysis. Cyber Security Training Eastern Indonesia, August 2024. Financial Innovation Lab (EIFIL) (Denpasar, Bali, Indonesia).
4. Keynote: Well, It Worked on My Computer: Reproducibility in Computer Security Research. EPFL Summer Research Institute (SURI), July 2024. École Polytechnique Fédérale de Lausanne (EPFL, Switzerland).
5. Humans vs The Computer Interfaces: The Challenge of Separating Deepfakes/Bots from People. North Central Florida Institute of Internal Auditors (IIA), May 2024.
6. Humans vs The Computer Interfaces: The Challenge of Separating Deepfakes/Bots from People. UF Quest 2: Siri is my Superpower: Communicating with AI, March 2024. University of Florida.
7. Humans vs The Computer Interfaces: The Challenge of Separating Deepfakes/Bots from People. Federal Information Integrity Research and Development (FIIRD) Interworking Group (IWG), March 2024. via NITRD, OSTP.
8. AI driven voice cloning scams. Discussion at the White House with Anne Neuberger (Deputy National Security Advisor for Cyber and Emerging Technologies), Jessica Rosenworcel (Chair of the Federal Communications Commission) and Lina Khan (Chair of the Federal Trade Commission), January 2024. Lead Academic facilitator.
9. 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.
10. 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.
11. 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.
12. The State of Voice Cloning Technology. Federal Trade Commission (FTC) Workshop on Voice Cloning Technologies, January 2020. Washington, DC.
13. 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.
14. 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.
15. 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.

16. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. Bank of America - Colloquium Series, March 2019. Charlotte, NC.
17. 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.
18. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. University of Maryland - Distinguished Colloquium, February 2019. College Park, MD.
19. Responsible Finance for the Digital Client. Foromic Conference, October 2018. Barranquilla, Colombia.
20. Panel: Authentication Challenges for New Interfaces, Devices, and Wireless Networks. ACM Conference on Security and Privacy in Wireless and Mobile Networks, June 2018. Stockholm, Sweden.
21. Sonar: Detecting SS7 Redirection Attacks Via Call Audio-Based Distance Bounding. CyberSecurity@KAIST Workshop - KAIST, June 2018. Daejeon, South Korea.
22. 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.
23. Panel: The Future of Cybersecurity. SEC Academic Conference - Auburn University, May 2018. Auburn, AL.
24. Sound Principles: Verifying Voice Commands in an IoT World. IoT Security Workshop - Aalto University, September 2017. Helsinki, Finland.
25. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Eurecom Institute, September 2017. Sophia Antipolis, France.
26. Panel: Infrastructure Stability. ITU-T Focus Group Digital Financial Services, December 2016. Geneva, Switzerland.
27. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. ETH Zurich, December 2016. Zurich, Switzerland.
28. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. University of Richmond, October 2016. Richmond, Virginia.
29. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Indiana University, September 2016. Bloomington, Indiana.
30. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Aalto University Computer Science Department Forum, August 2016. Helsinki, Finland.
31. 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.
32. Updated Mobile Money Vulnerability Report. International Telecommunications Union Digital Financial Services Working Group Workshop, May 2016. Washington, DC.
33. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. UF Eye Opener Discovery Breakfast - University of Florida, May 2016. Gainesville, FL.

34. 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.
35. 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.
36. 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.
37. Chasing Telephony Security: Where the Wild Things... Are? University of Florida - Department Colloquium, January 2014. Gainesville, FL.
38. Chasing Telephony Security: Where the Wild Things... Are? Verizon Wireless RNC/Data Center, October 2013. Alpharetta, GA.
39. Chasing Telephony Security: Where the Wild Things... Are? University of Waterloo - CrySP Speaker Series on Privacy, October 2013. Waterloo, ON, Canada.
40. Analyzing Malicious Traffic in Cellular Networks. GSM Association's (GSMA) Mobile Malware Community Workshop, July 2013. Mountain View, CA.
41. Threats to Mobile Devices. US Federal Trade Commission (FTC) Public Forum - Invited Speaker, June 2013. Washington, D.C.
42. Chasing Telephony Security: Where the Wild Things... Are? University of Wisconsin - Madison, Security Seminar, March 2013. Madison, WI.
43. 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.
44. Chasing Telephony Security: Where the Wild Things... Are? Stanford Security Seminar, March 2013. Stanford, CA.
45. Chasing Telephony Security: Where the Wild Things... Are? University of California, Berkeley, Security Group, March 2013. Berkeley, CA.
46. Chasing Telephony Security: Where the Wild Things... Are? Carnegie Mellon University CyLab Seminar, February 2013. Pittsburgh, PA.
47. Chasing Telephony Security: Where the Wild Things... Are? University of Oregon Department of Computer Science Colloquium, November 2012. Eugene, OR.
48. 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.
49. Needles and Haystacks: Digging for Ground Truth on Mobile Malware. ZISC Workshop on Secure Mobile and Cloud Computing, ETH Zurich, June 2012. Zurich, Switzerland.
50. Panel: Advice for Early Career Faculty. CRA Career Mentoring Workshop, February 2012. Washington, D.C.
51. Research Challenges in Cellular and Mobile Network Security. US-China Software Workshop (Co-Sponsored by NSF and NSFC), September 2011. Beijing, China.

52. Mobile Security: Understanding Risks to Critical Infrastructure. Invited Talk: US Department of State East African Workshop on Cyberspace Security, July 2011. Nairobi, Kenya.
53. Tomorrow's Issues: Solving the Mobile Security Threat. Invited Talk: Centre for Secure Information Technologies (CSIT) Queen's University, March 2011. Belfast, Northern Ireland.
54. PinDr0p: Using Single-Ended Audio Features to Determine Call Provenance. Invited Talk: MITRE Corporation, March 2011. Burlington, MA.
55. Defeating Session Hijacking Attacks with Disposable Web Credentials. Invited Talk: Facebook, February 2011. Palo Alto, CA.
56. Understanding the Disruptive Potential of Malware in Cellular Networks. Invited Talk: RSA Conference, February 2011. San Francisco, CA.
57. Panel: Voice Security – Now Just a False Sense of Security and Privacy. Invited Panelist: Mobile Security Symposium, February 2011. San Francisco, CA.
58. Understanding the Disruptive Potential of Malware in Cellular Networks. Invited Talk: Concordia University, May 2010. Montreal, QC, Canada.
59. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Qualcomm Research, March 2010. San Diego, CA.
60. 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.
61. Considerations for EAS Over Cellular Text Messaging Services. 3G Americas Webinar, July 2009.
62. University Telephony Research Panel. Conference on Principles, Systems and Applications of IP Telecommunications (IPTCOMM), July 2009.
63. The Evolving Mobile Landscape: Emerging Security Threats. Mobile Security eConference, SC Magazine, June 2008.
64. Characterizing the Impact of Rigidity on the Security of Cellular Networks. University of Washington, February 2009. Seattle, WA.
65. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Microsoft Research, February 2009. Redmond, WA.
66. Next Year's Problems. Secure Computing (SC) Magazine Webinar, November 2008.
67. Panel: Embedded Systems and their Increasing Impact on Infrastructure Security. Workshop on Embedded Systems Security (WESS), October 2008.
68. Can you DoS me now? Security Issues in Cellular Networks. Georgia Institute of Technology, September 2008. Atlanta, GA.
69. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Georgia Institute of Technology, April 2008. Atlanta, GA.
70. Characterizing the Impact of Rigidity on the Security of Cellular Networks. AT&T Research Labs, April 2008. Florham Park, NJ.
71. Characterizing the Impact of Rigidity on the Security of Cellular Networks. University of Arizona, March 2008. Tucson, AZ.

72. Cellular Networks Security Panel. USENIX Security Symposium, August 2007. Boston, MA.
73. malnets:Large-Scale Malicious Networks via Compromised Access Points. The Pennsylvania State University - ACM Club Invited Speaker, October 2006. State College, PA.
74. malnets:Large-Scale Malicious Networks via Compromised Access Points. The University of Michigan, October 2006. Ann Arbor, MI.
75. Exploiting Open Functionality in SMS-Capable Cellular Networks. The University of Michigan, October 2006. Ann Arbor, MI.
76. Exploiting Open Functionality in SMS-Capable Cellular Networks. High Technology Crime Investigation Association (HTCIA), September 2006. Pittsburgh, PA.
77. Trends in Security: Critical Engineering in the Large. Schlumberger Innovate IT! Workshop, May 2006. Cambridge, MA.
78. Exploiting Open Functionality in SMS-Capable Cellular Networks. InfraGard Pittsburgh Chapter General Meeting, September 2006. Pittsburgh, PA.
79. 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-ransomware-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/#ixzz2EGtQsuId, 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 - http://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.