

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Graham Merrett
U.S. Patent No.: 11,991,600 Attorney Docket No. 50095-0263IP1
Issue Date: May 21, 2024
Appl. Serial No.: 18/143,387
Filing Date: May 4, 2023
Title: METHODS FOR BEARER SELECTION PERFORMED BY A
SENDING MOBILE DEVICE

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: 31 October 2025

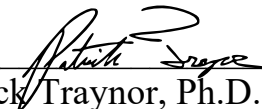
By: 
Patrick Traynor, Ph.D.

Table of Contents

I.	QUALIFICATIONS AND BACKGROUND INFORMATION.....	3
II.	LEGAL PRINCIPLES.....	9
	A. Anticipation	9
	B. Obviousness.....	10
III.	OVERVIEW OF CONCLUSIONS FORMED	11
IV.	BACKGROUND KNOWLEDGE ONE OF SKILL IN THE ART WOULD HAVE HAD PRIOR TO THE PRIORITY DATE OF THE '600 PATENT	12
V.	INTERPRETATIONS OF THE '600 PATENT CLAIMS AT ISSUE.....	12
VI.	THE '600 PATENT AND ANALOGOUS ART	13
	A. Overview of the '600 Patent.....	13
	B. Prosecution History of the '600 Patent.....	15
	C. Analogous Art.....	15
VII.	GROUND 1A: OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES	16
	A. Overview of Horvath	16
	B. Overview of Tsampalis.....	20
	C. Overview of Kansal	25
	D. Combination of Horvath, Tsampalis and Kansal.....	27
VIII.	GROUND 1A: MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '600 CLAIMS UNPATENTABLE	33
	A. The Horvath-Tsampalis-Kansal Combination Renders Claims 1, 3-25, 27-30 Obvious	33
IX.	GROUND 1B: OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES	100
	A. Overview of Dorenbosch.....	100
	B. Combination of Horvath, Tsampalis, Kansal and Dorenbosch	102
X.	GROUND 1B: MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '600 CLAIMS UNPATENTABLE	105
	A. The Horvath-Tsampalis-Kansal-Dorenbosch Combination Renders Claims 2, 26 Obvious	105
XI.	CONCLUSION	110

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, 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 Interim Chair of 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 served 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 also previously served as 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, blocking ransomware from encrypting data, and more.

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. 11,991,600 (“the ’600 Patent”)
- APPLE-1002 File History of U.S. Patent No. 11,991,600
- APPLE-1004 U.S. Pub. No. 2007/0254681 (“Horvath”)
- APPLE-1005 U.S. Pub. No. 2004/0203956 (“Tsampalis”)
- APPLE-1006 U.S. Pub. No. 2002/0173308 (“Dorenbosch”)
- 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-1011 U.S. Patent No. 6,940,844 (“Purkayastha”)
- APPLE-1012 U.S. Patent No. 7,702,342 (“Duan”)
- APPLE-1014 U.S. Pub. No. US 2006/0286984 (“Bonner”)
- APPLE-1020 U.S. Patent No. US 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-1032 U.S. Pub. No. US 2008/0261577 (claiming priority to Provisional App. No. 60/913,187) (“Celik”)
- 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-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-1050 U.S. Pub. No. 2005/0233737 (“Lin”)
- APPLE-1051 U.S. Pub. No. 2008/0176538 (“Terrill”)
- APPLE-1052 U.S. Patent No. 9,036,620 (“Procopio”)
- APPLE-1053 U.S. Patent. No. 9,467,530 (“Belimpasakis”)
- APPLE-1054 U.S. Patent No. 7,069,008 (“Hill”)
- APPLE-1055 U.S. Pub. No. 2005/0125547 (“Ahonen”)
- APPLE-1056 U.S. Pub. No. 2005/0002407 (“Shaheen”)
- APPLE-1058 WO 01/41477 (“Lee”)
- APPLE-1061 U.S. Pub. No. 2007/0290787 (“Fiatal”)
- APPLE-1063 U.S. Pub. No. 2009/0325609 (“Rosen”)
- APPLE-1064 U.S. Patent No. 7,117,445 (“Berger”)
- APPLE-1065 RFC 3680: A Session Initiation Protocol (SIP) Event Package for Registrations (March 2004)
- APPLE-1066 IMS Share Technote, *available at* https://www.sharetechnote.com/html/Handbook_IMS_SIP_Header_Experience.html
- APPLE-1067 U.S. Pub. No. 2006/0036857 (“Hwang”)
- APPLE-1068 U.S. Pub. No. 2002/0006793 (“Kun-Szabo”)
- APPLE-1069 U.S. Patent No. 6,678,524 (“Hansson”)

- APPLE-1070 U.S. Pub. No. 2007/0004461 (“Bathina”)
- APPLE-1071 U.S. Pub. No 2008/0307487 (“Choyi”)
- APPLE-1072 U.S. Pub. No. 2008/0310425 (“Nath”)
- APPLE-1073 U.S. Pub. No. 2004/0005875 (“Ko”)
- APPLE-1074 U.S. Pub. No. 2008/0263137 (“Pattison”)
- APPLE-1075 U.S. Pub. No. 2014/0258423 (“Schaedler”)
- APPLE-1076 U.S. Pub. No. 2008/0311888 (“Ku”)
- APPLE-1077 U.S. Pub. No. 2008/0192770 (“Burrows”)
- APPLE-1078 U.S. Pub. No. 2006/0264213 (“Thompson”)
- APPLE-1084 U.S. Pub. No. 2009/0280779 (“Torres”)
- APPLE-1085 U.S. Pub. No. 2009/0220091 (“Howard”)
- APPLE-1086 U.S. Pub. No. 2008/0039081 (“Ma”)
- APPLE-1087 U.S. Pub. No. 2008/0045214 (“Wen”)
- APPLE-1088 U.S. Pub. No. 2006/0185003 (“Laitinen”)
- 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 ’600 Patent

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 '600 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 '600 Patent are obvious over Horvath in view of Tsampalis, Kansal and Dorenbosch.

IV. BACKGROUND KNOWLEDGE ONE OF SKILL IN THE ART WOULD HAVE HAD PRIOR TO THE PRIORITY DATE OF THE '600 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 '600 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 '600 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 '600 PATENT AND ANALOGOUS ART

A. Overview of the '600 Patent

24. The '600 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, 3:6-44, 8:4-10:7. The Abstract summarizes the disclosed techniques as follows, for example:

A method performed by a sending mobile phone that transmits SMS messages and packet switched messages may comprise: (a) retrieving a destination address of a message from the message; (b) sending information representing a phone number of a

receiving mobile phone; (c) receiving a response to the sending of the information; and (d) based at least in part on the response, automatically selecting a bearer for the message. The bearer may be selected from a group including: an SMS bearer; a packet-switched message bearer supported by a cellular connection between the sending mobile phone and a cellular base station; and a packet-switched message bearer supported by a wireless local area network (WLAN) connection between the sending mobile phone and a WLAN base station.

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:

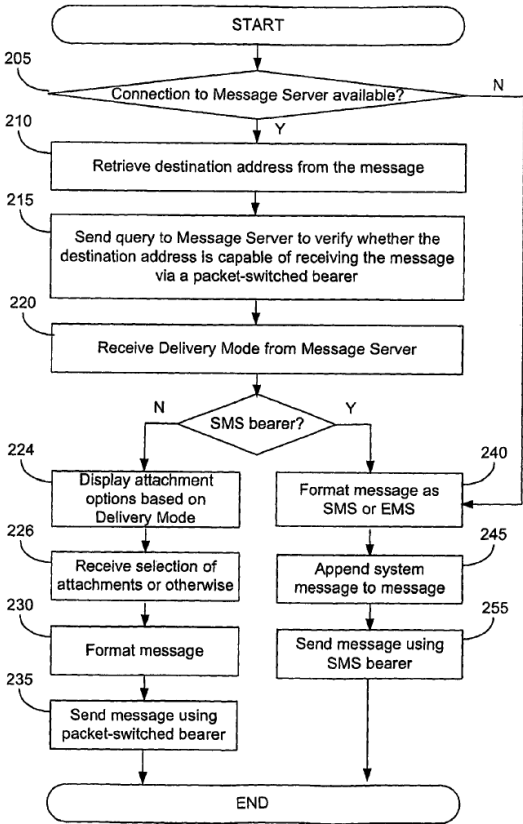


FIG. 3

APPLE-1001, FIG. 3

B. Prosecution History of the '600 Patent

26. In the only Office Action issued during prosecution, the Examiner identified claims 18-27 as allowable because the prior art of record allegedly “fails to teach wherein based at least in part on the third response, automatically selecting a packet-switched bearer for the third message; formatting the third message for transmission via the packet-switched bearer and a wireless local area network (WLAN) connection.” APPLE-1002, 155-156, 161-165.

C. Analogous Art

27. Horvath, Tsampalis, Kansal, and Dorenbosch are all analogous art, each being in the same field of endeavor (mobile messaging over wireless networks) and reasonably pertinent to the problems said to be addressed by the '600 Patent. APPLE-1001, Title, Abstract; APPLE-1004, Title, Abstract; APPLE-1005, Title, Abstract; APPLE-1042, Abstract; APPLE-1006, Abstract; *infra*, §§VII-VIII. Like the '600 Patent, the Horvath, Tsampalis, Kansal and Dorenbosch each seek to provide users with a wider range of messaging options. *See* APPLE-1001, 3:18-25; APPLE-1004, [0009] (ability to select wider range of message delivery networks); APPLE-1005, [0065] (“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-1042, [0009] (“a mobile computing device may send and receive messages

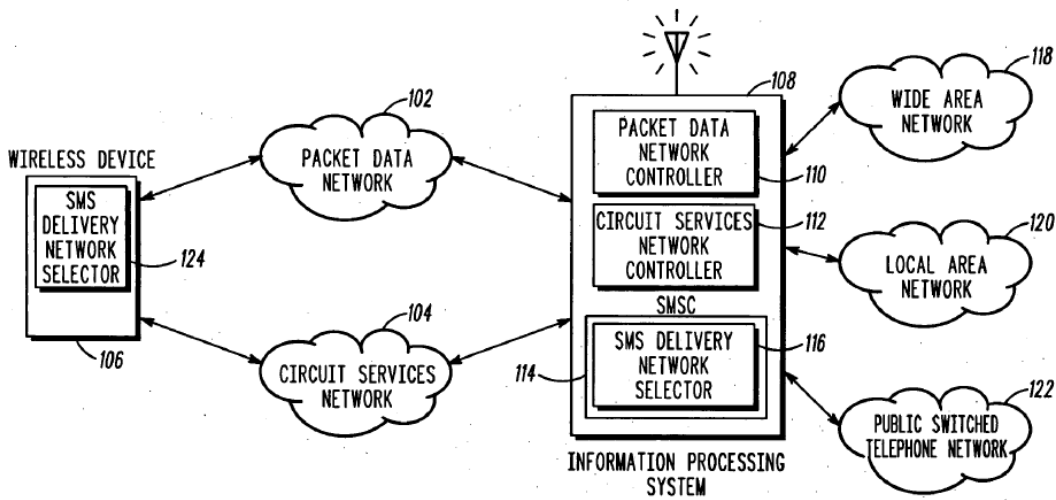
of different types”); APPLE-1006, [0002] (improving use of instant messaging on mobile devices).

VII. GROUND 1A: OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES

A. Overview of Horvath¹

28. Horvath discloses “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, 6, 7. That is, if a wireless device is registered on a packet-data network, it will send and receive messages via an information processing system over the packet-data network, and otherwise will send and receive messages via the information processing system over the circuit-services network. *Id.*

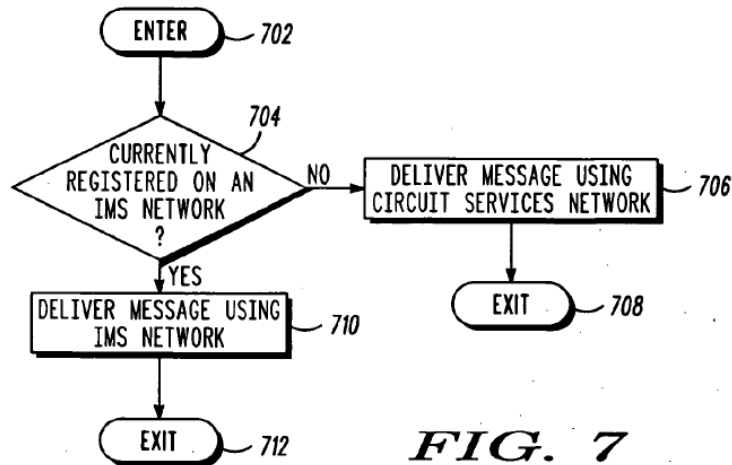
¹ General prior art and combination descriptions are incorporated into forthcoming subsections. Emphasis and annotations are each added unless otherwise indicated.



100
FIG. 1

APPLE-1004, FIG. 1

29. As shown in FIG. 1, wireless device 106 exchanges messages with remote recipient devices, as sender or receiver, via information processing system 108. See APPLE-1004, [0024], [0028]-[0029], [0074]-[0078], FIGS. 1, 6-7. When instructed to send an SMS message (*i.e.*, 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], [0078], FIGS. 1, 4, 7.



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

30. Although Horvath focuses on the selective use of packet-data or circuit-services bearers for delivery of SMS messages, Horvath notes that wireless device 106 can transmit other types of messages as well, including instant messages (“IM”). APPLE-1004, [0025], [0033] (“The SIP network is used for establishing instant messaging, ... and other real-time communications over the Internet”), [0038]-[0039]. With this, Horvath encourages operation of a session initiation protocol (“SIP”) network atop the packet-data network 102 to establish communication sessions and carry messages between wireless devices when the circuit-services network 104 is not used. *Id.*, [0041], [0050], FIG. 5.

31. Per Horvath, message requests are 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, utilizing its “SMS delivery network selector 116,” “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 with the packet-data network 102.² *Id.*, Abstract, [0002], [0006], [0008], [0028], [0033]-[0038], [0045]-[0047], [0053], [0075]-[0076], FIGS. 1, 2, 3, 6. When available, Horvath delivers messages to wireless devices over a packet-data network rather than a circuit-services network to reduce the amount of traffic transmitted over the circuit-services network, thereby freeing bandwidth for voice calls or other services on the circuit-services network. APPLE-1004, [0009], [0021], [0039], [0050]. An example of this network selection process is further described at [0016] and illustrated by the following FIG. 6 flowchart.

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).

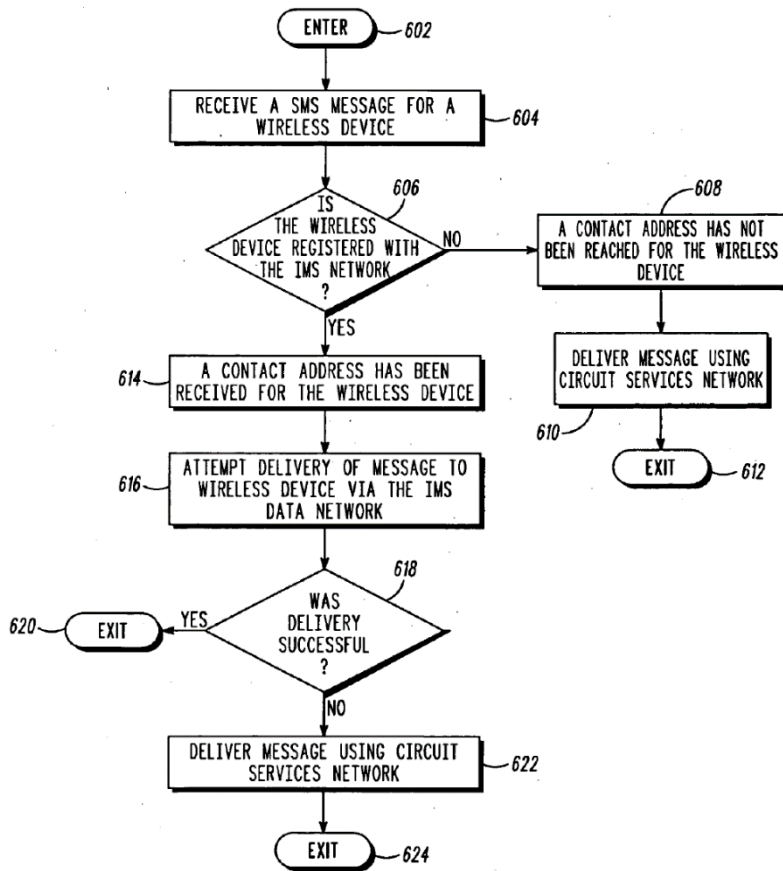


FIG. 6

APPLE-1004, FIG. 6 (Server Perspective)

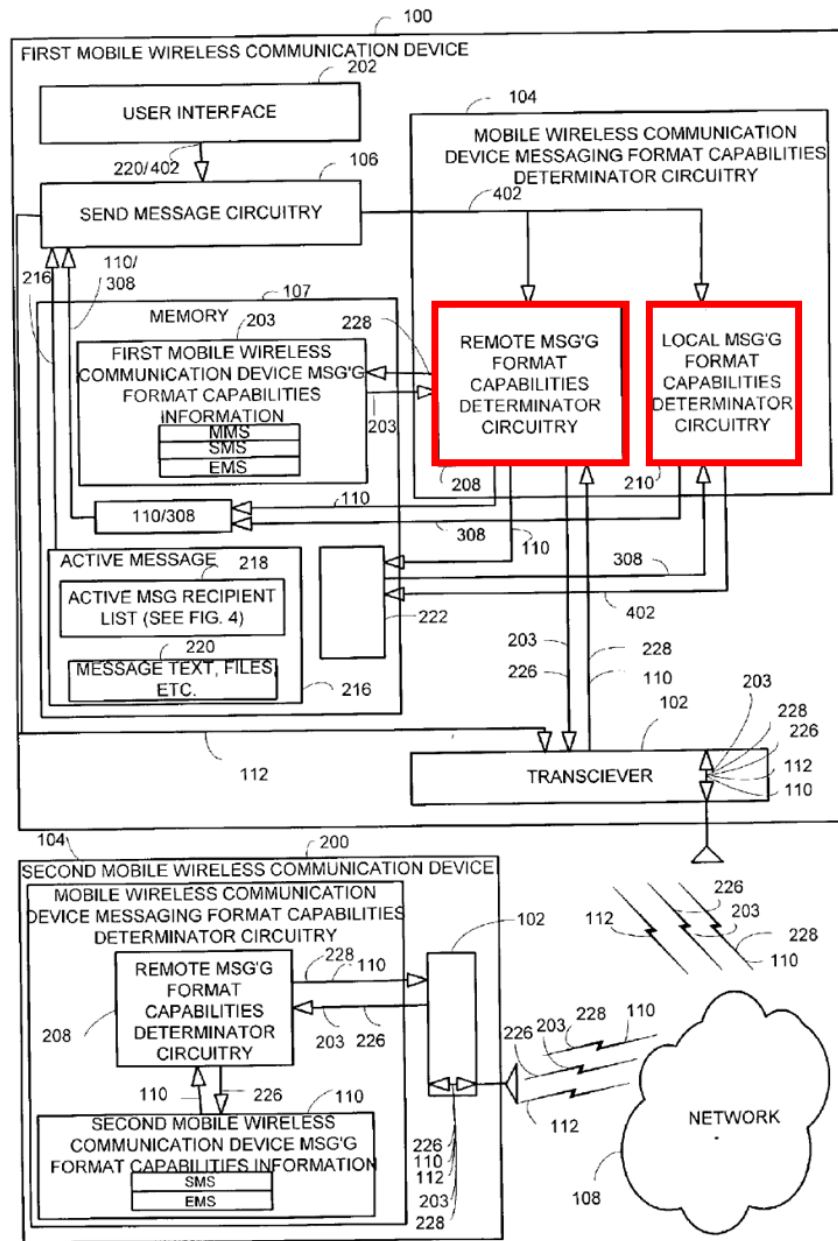
B. Overview of Tsampalis

32. Without regard for wireless network registration (*e.g.*, among packet-data network or circuit-services network) of either the sending or receiving wireless device, Tsampalis teaches the sending wireless device querying the receiving wireless device’s messaging format capabilities to inform the type of messages (SMS, MMS, etc.) it is able to effectively process and display. APPLE-1005,

Abstract, [0002]-[0004], [0022], [0025]. In this way, Tsampalis complements Horvath.

33. Specifically, Tsampalis describes a sender (*e.g.*, first mobile wireless communication device 100) obtaining, either locally or via “a web server” or other “network element,” the “messaging format capabilities information [MFCI] 110” of a recipient (*e.g.*, a second mobile wireless communication device 200), to inform delivery of messages from the sender to the recipient. *See e.g.*, APPLE-1005, Title, Abstract, [0029]-[0039], FIG. 1, FIG. 2 (below, highlighting the local and remote messaging format capabilities determinator circuitries residing on the first wireless device), FIGS. 5-7. Among the MFCI 110 are the types of messages (*e.g.*, SMS, MMS, EMS) that the intended recipient device is capable of processing. APPLE-1005, [0022]-[0024].

FIG. 2



APPLE-1005, FIG. 2 (Annotated)

34. By way of example, the sender device 100 generates and sends a “mobile wireless communication device [MFCI] request” to a remote web server when recipient device 200’s MFCI 110 “must be retrieved remotely,” and the sender

device “receiv[es] a **response** [e.g., from the web server] to the request where the response contains the second mobile wireless communication device [MFCI] 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 [MFCI] 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 [MFCI] 110”), FIGS. 6 (below), 13 (below). Exchanged MFCI 110 can be stored, according to Tsampalis, in “a network element within the network 108” (e.g., “a web server,”) or elsewhere (e.g., at the remote relay/server 1304). *Id.*, [0039], [0057]. When stored within network 108, the sender device can retrieve the recipient device’s MFCI 110 from a remote server using the process described by Tsampalis’ FIG. 13 (below). *Id.*; *see also id.*, [0056]-[0060], FIGS. 13-15.

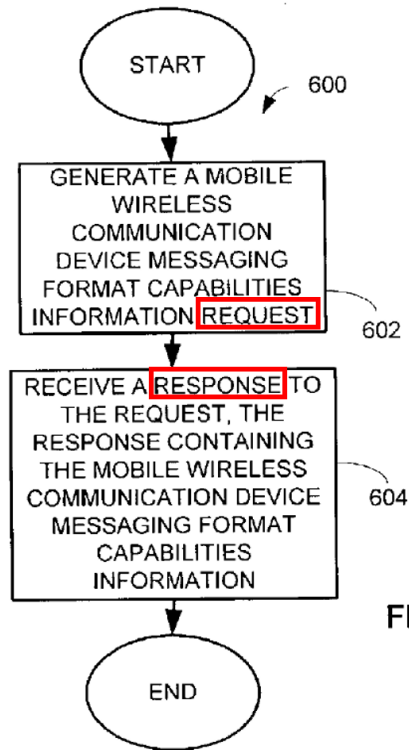
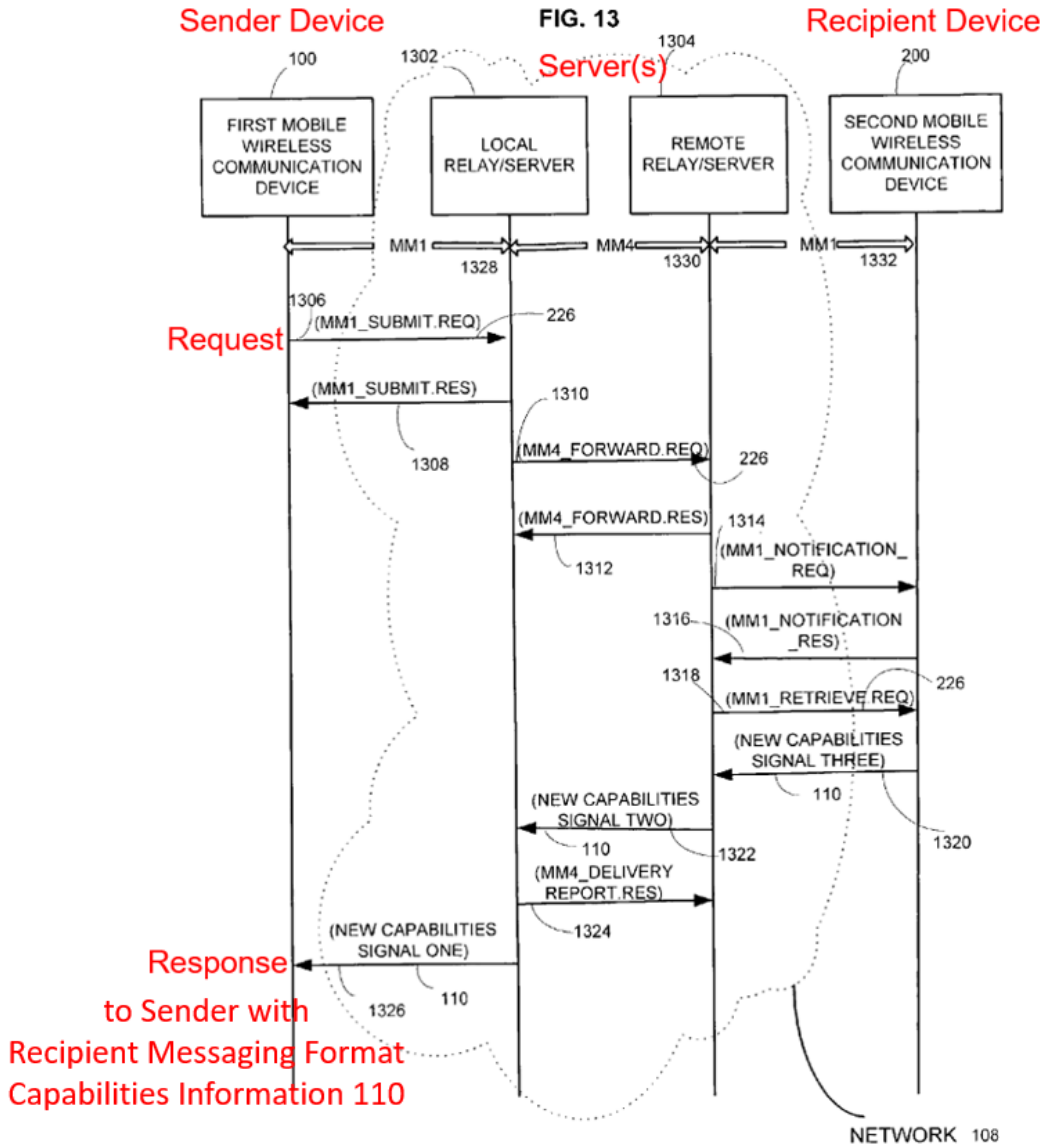


FIG. 6

APPLE-1005, FIG. 6 (Annotated)

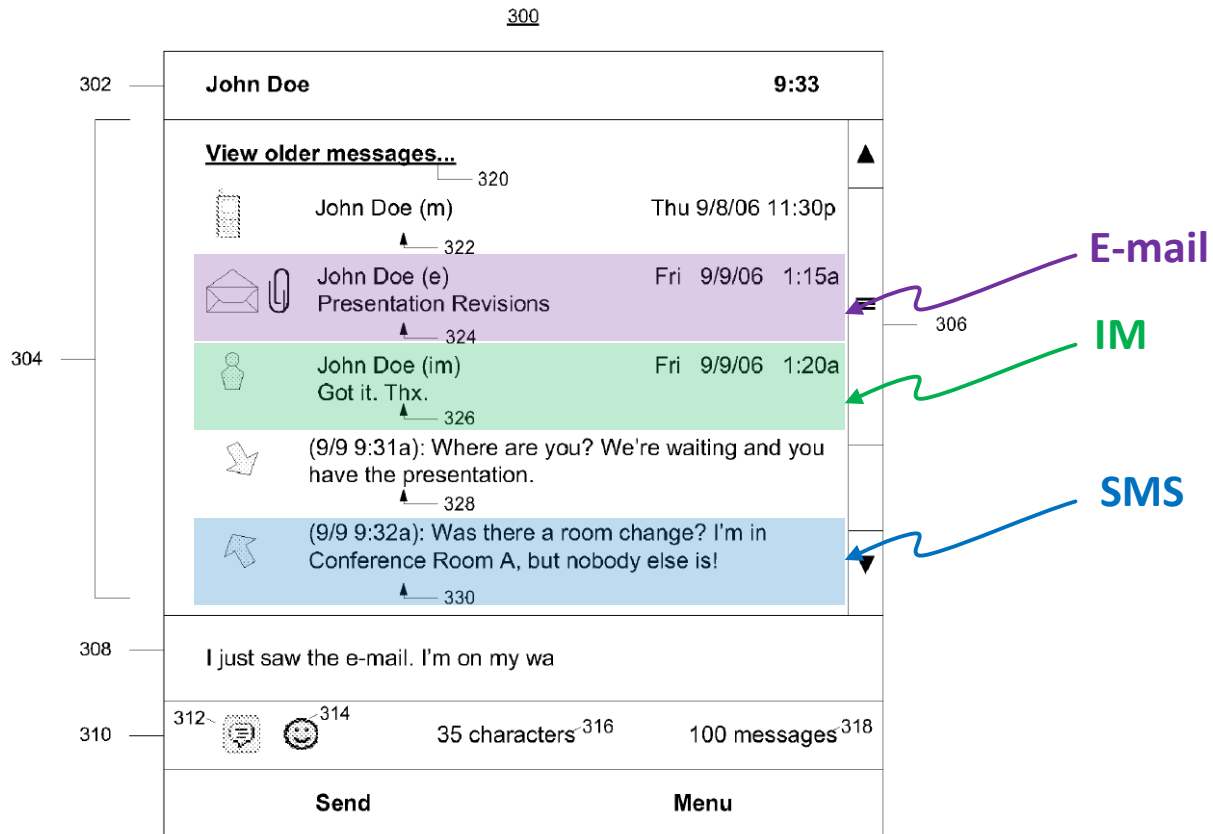


APPLE-1005, FIG. 13 (Annotated)

C. Overview of Kansal

35. (a) Like Horvath and Tsampalis, Kansal describes 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 presents a tool for correlating and aggregating for display all

messages received by a “particular recipient,” including each of several message types/formats (e.g., SMS, IM, MMS), without regard for the network over which the messages are received. APPLE-1042, [0009]; [0040]-[0043]; [0066]-[0069].



APPLE-1042, FIG. 3 (Annotated)

36. As shown above, Kansal describes a “unified messaging UI” from which a user may view received messages of various messaging types and may select from a variety of types when composing and sending a response, demonstrating the utility and viability of integration. APPLE-1042, [0062], [0077]-[0078]. In particular, the unified messaging UI “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 (above).

D. Combination of Horvath, Tsampalis and Kansal

37. Like the '600 Patent, Horvath describes techniques for 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, 3:6-35; APPLE-1004, [0001], [0007], [0024]-[0026], [0050], [0061]-[0062], FIGS. 1, 4, 7; *supra*, §VII.A (Horvath Overview). In seeking to keep the circuit-services network from being “unnecessarily burdened with SMS traffic,” Horvath proposes to default to a packet-data network for transmitting messages whenever the sending and receiving devices are registered with the packet-data 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”). With this approach, Horvath diverts some of the load otherwise carried by and burdening the circuit-services network. APPLE-1004, [0004], [0009]. Still, a POSITA would have recognized that Horvath’s system was ripe for improvement. For example, although Horvath describes messaging services

apart from SMS (*e.g.*, MMS, EMS, IM), Horvath leaves implementation details relating to these services to the discretion of a POSITA. APPLE-1005, [0025], [0039]. Additionally, a POSITA would have appreciated from Horvath that different users did not all subscribe to the same messaging services, leaving some users with relatively limited messaging capabilities that precluded them from receiving or processing richer media formats beyond SMS (*e.g.*, MMS, EMS, IM), despite other users sending messages in those richer media formats. Without more, this leaves a Horvath sender device vulnerable to sending a message in a format that a Horvath recipient device would be incapable of processing or presenting to a user.

(i) Tsampalis's Message-Format Determination

38. In a multi-modal messaging environment like Horvath's, in which different mobile-device users subscribed to different messaging services (*e.g.*, SMS, MMS, EMS, IM), a POSITA would have been led by Tsampalis to improve the user experience and better manage and coordinate messaging formats. *Supra*, §VII.A (Horvath Overview); §VII.B (Tsampalis Overview). In particular, Tsampalis describes an effective solution for improving messaging in such an environment by sharing the recipient's MFCI with the sender. *Supra*, §VII.B. For various reasons, 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 MFCI of a recipient device to determine how to format and transmit an outgoing message to the recipient.

39. First, a POSITA would have combined Horvath and Tsampalis such that the sender would obtain and use a recipient's MFCI 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 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).

40. Second, a POSITA would have sought to leverage Tsampalis-like MFCI 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; APPLE-1025, Introduction. Tsampalis's proposal to share the recipients' MFCI 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.

41. Third, a POSITA would have been motivated to apply Tsampalis-like MFCI 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].

42. Fourth, 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. Here, Tsampalis recognized a known problem with dynamic messaging environments like Horvath's, and Tsampalis's teachings would help address this problem in a straightforward manner that was well within the skill of a POSITA.

43. Likewise, a POSITA would have reasonably expected success implementing the combination, especially since the resulting system would 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 '600 Patent. Further, the techniques 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-services network.

(ii) **Kansal's Unified Interface for Selection of Appropriate Messaging Format**

44. The combination provides a wireless mobile device capable of messaging using different messaging services including, SMS, MMS, and IM. *Supra* §VII.D(i). Kansal suggests using a unified messaging UI for precisely this kind of environment, with variously formatted messages unified within a single application interface. APPLE-1042, [0077]-[0078], [0086]. Multiple reasons would have prompted a POSITA to implement this combination.

45. First, a POSITA would have been motivated to apply Kansal's suggested unified-messaging user interface to the wireless device in the 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 involving a particular user in a single thread would advantageously mitigate the need to navigate to different messaging applications or interfaces for each different message type. APPLE-1045, 1-2 (a multi-protocol messaging application, Trillian, providing "a powerful and efficient user experience."); APPLE-1042, [0009], [0045]-[0046], [0054]-[0056], [0062]-[0064], [0070], [0077]-[0078], FIGs. 2-3.

46. 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 unified UI 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. A POSITA would have

sought to implement Kansal's user interface to provide this additional contextual information to a user.

47. Third, Kansal's techniques are fully compatible with the types of messaging formats disclosed in each of Horvath and Tsampalis (*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. 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. 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. And the combination with Kansal described above would not fundamentally change any of the other operations of the combination.

VIII. GROUND 1A: MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '600 CLAIMS UNPATENTABLE

A. The Horvath-Tsampalis-Kansal Combination Renders Claims 1, 3-25, 27-30 Obvious

Element [1pre1]: A method performed by

48. To the extent the preamble is limiting, Horvath-Tsampalis-Kansal renders [1pre1] obvious. For example, Horvath discloses 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”), [0011];
see also APPLE-1005, [0001], [0006].

Element [1pre2]: a sending mobile phone that transmits short message service (SMS) messages and non-SMS based packet switched messages, the method comprising:

49. To the extent the preamble is limiting, Horvath-Tsampalis-Kansal renders [1pre1] obvious. For example, Horvath’s FIG. 4 (below) shows an example “wireless device 106” (***a sending mobile phone***³) that transmits messages on “either the packet data network 102 or the circuit services network 104.” APPLE-1004, [0014], [0060]-[0070]; *see also* APPLE-1042, [0028]. “The SMS delivery network selector 124 selects a network 102, 104 for the wireless device 106 to transmit a SMS message on” (***transmits short message service (SMS) messages***). APPLE-1004, [0062].

³ Bold and italicized text corresponds to claim language.

Selects network 102 or 104 for transmission

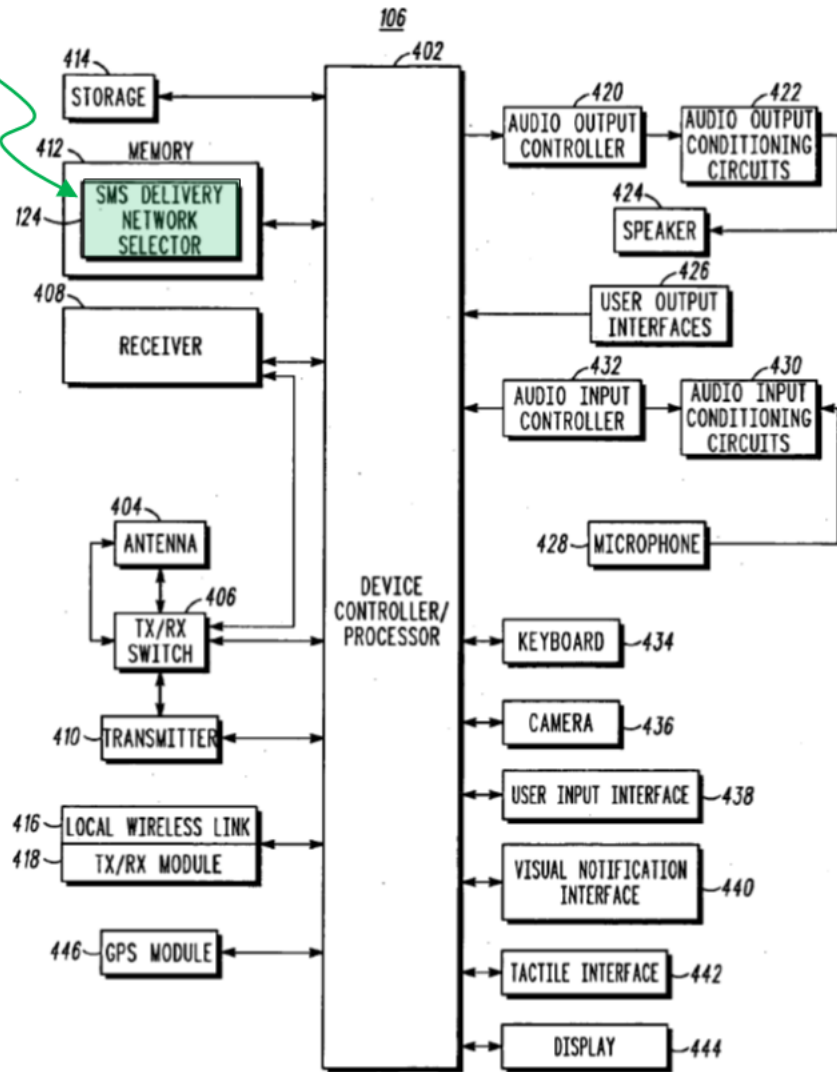
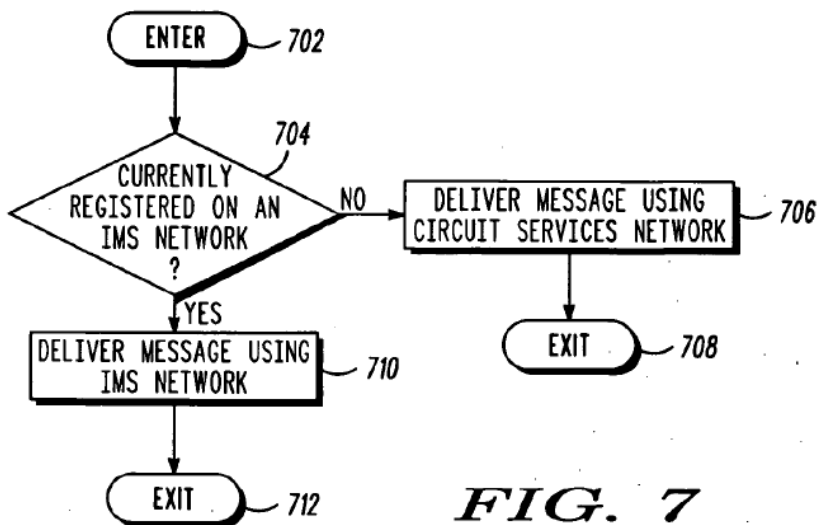


FIG. 4

APPLE-1004, FIG. 4 (Annotated)

50. As shown in Horvath's FIG. 7 (below), the sending mobile phone "select[s] a network for transmitting a [] message based on what network the wireless device is registered with." APPLE-1004, [0078].



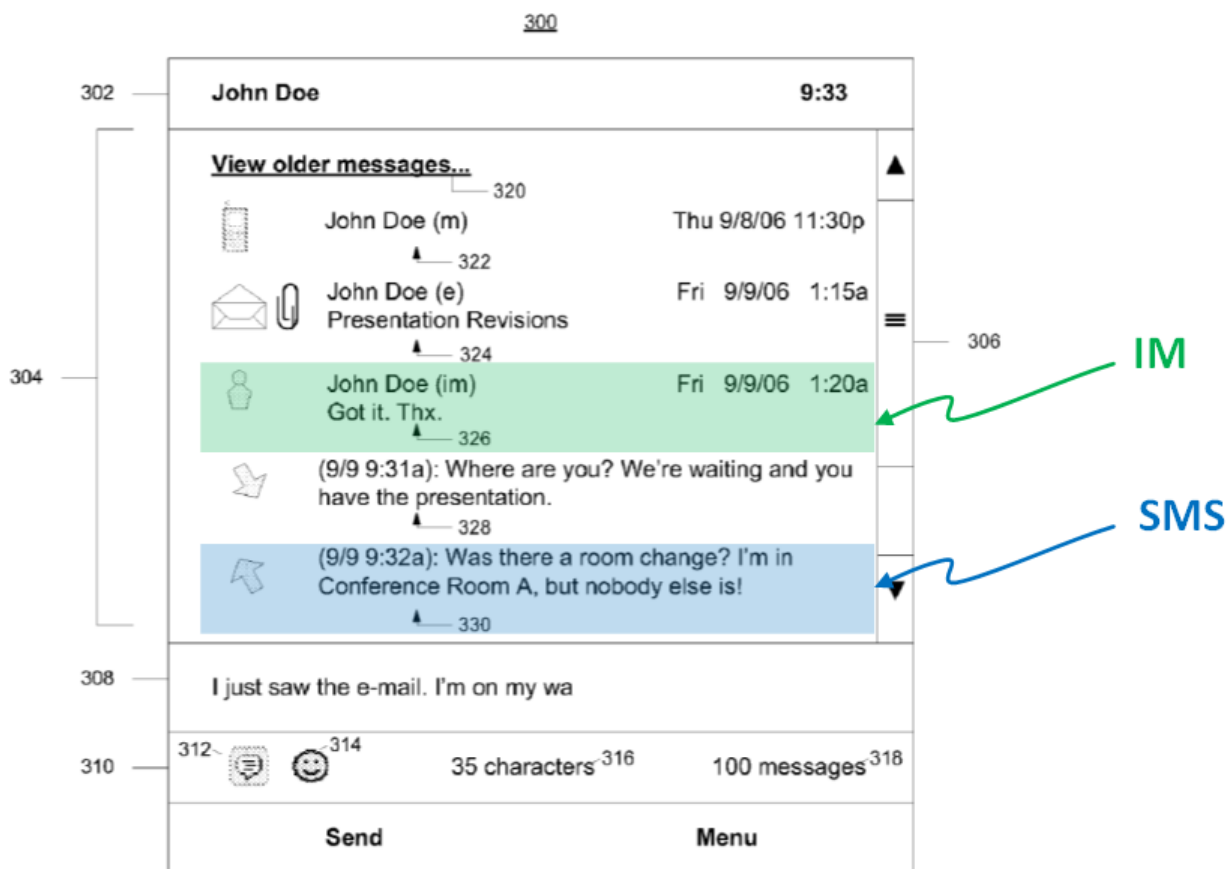
APPLE-1004, FIG. 7 (Sender Device Perspective)

51. Wireless device 106 sends messages, e.g., short message service (SMS) messages, “through a circuit services 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].

52. On the other hand, when device 106 “[is] registered with the [SIP] registrar,” device 106 sends “SIP message[s]” in “SIP packets” (*non-SMS based packet switched messages*) “through the [SIP] network communicating over the packet data network.” APPLE-1004, [0002], [0006]-[0007], [0017], [0024], [0034], [0037] (messages are sent over the SIP network in “SIP packets”), [0038], [0039], [0041], [0078], FIG. 7. One type of message service provided over the SIP network is an “instant messaging” service. APPLE-1004, [0033] (“The SIP network is used

for establishing instant messaging...and other real-time communications over the Internet.”).

53. Moreover, as I previously explained in §VII.D, the combination includes a “messaging UI 500 [that] enable[s] a user to compose messages of different types of formats,” including “SMS..., MMS, e-mail, IM [*non-SMS based packet switched messages*], etc.” APPLE-1042, [0077]-[0078]; *see also id.*, [0002], [0062]-[0063].



APPLE-1042, FIG. 3 (Annotated)

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

54. Horvath-Tsampalis-Kansal renders Element [1a] obvious. 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-services networks 104. APPLE-1004, [0050], [0078], FIG. 7. 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] (“A tel-URI, for example is the telephone number assigned to the wireless device 106.”), [0045], [0050], [0073] (“the contact address (for example, tel-URI) of the wireless device 106”), [0076].

55. 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 sending device receives phone numbers of intended messaging recipients while composing an active message. APPLE-1005, [0033]-[0034], [0061]. 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 in the form of a MSISDN. *See* APPLE-1005, FIG. 4 (below, showing “recipient ID” 402 list in the form of telephone numbers), [0032]-[0033], [0046], [0061], [0064], FIGS. 3-4, 7, 10;

APPLE-1052, 12:53-60; *see also* APPLE-1042, [0037]-[0038], [0066], [0072] (“the address bar 504 may comprise a ‘To’ field which may display the contact name...through reverse look up in the contact records or the telephone number of the recipient”).

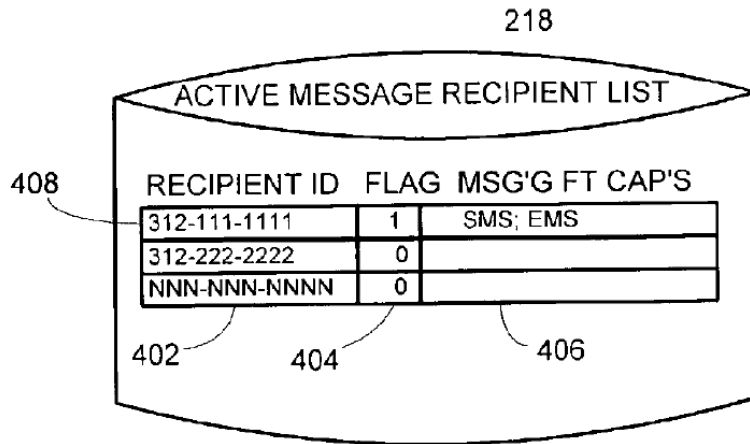


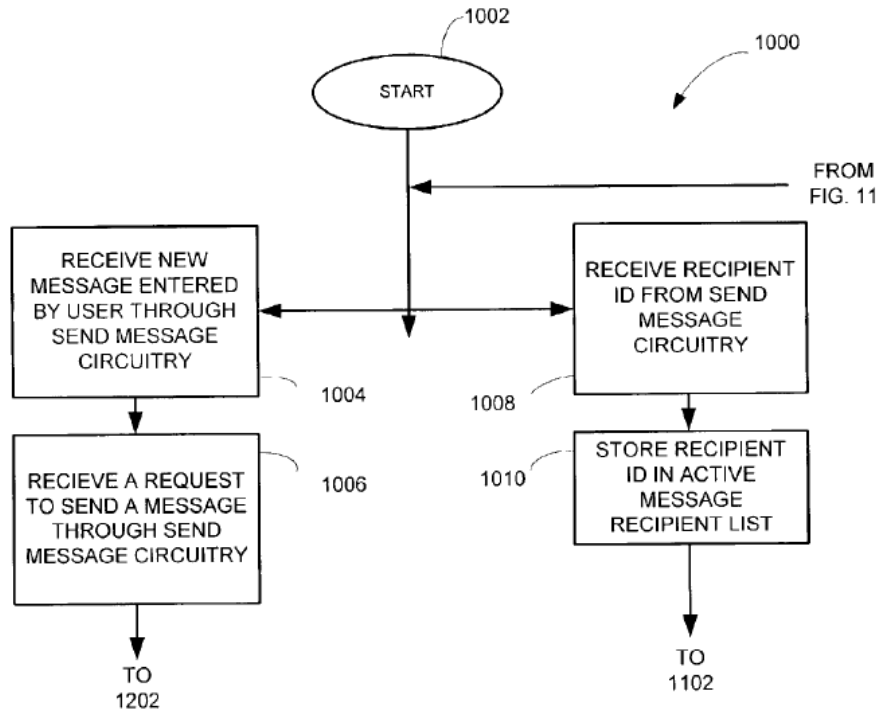
FIG. 4

APPLE-1005, FIG. 4

56. Referring to FIG. 10 (below), Tsampalis explains, “[a]s shown in Block 1004, the method includes [] receiving a new unformatted message 110 entered by a user” and “[b]lock 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. Tsampalis describes that as a user enters message text and an active message recipient list into the sending mobile phone’s user interface, “the mobile wireless communication device messaging format capabilities

determinator circuitry 104...retrieve[s] the [receiving] mobile wireless communication device [MFCI] 110 associated with the” recipient ID of a receiving mobile phone entered into the active message recipient list. APPLE-1005, [0033]; *see also id.*, [0046].

FIG. 10



APPLE-1005, FIG. 10

57. Accordingly, Horvath-Tsampalis-Kansal’s sending mobile phone (e.g., wireless device 106) *retriev[es] a destination address of a message from the message* (e.g., the send message circuitry 106 retrieving a “destination address” or “recipient ID” from an active message being composed by the user of the sending

mobile phone), *wherein the destination address is a phone number of a receiving mobile phone* (e.g., the “recipient ID” is a telephone number, in the form of a tel-URI or MSISDN).

Element [1b]: sending information representing at least the phone number of the receiving mobile phone;

58. Horvath-Tsampalis-Kansal renders Element [1b] obvious. As I previously discussed for Element [1a], the combination’s sending mobile phone “retrieve[s] the [receiving] mobile wireless communication device [MFCI] 110 associated with the” recipient ID of a receiving mobile phone entered into the active message recipient list. APPLE-1005, [0033]; *see also id.*, [0046]. As I previously discussed for Element [1a], Tsampalis describes that the recipient ID may be the phone’s MSISDN, which was known to be “the standard international telephone number used to identify a given subscriber.” *See* APPLE-1005, [0061], FIGS. 3, 4 (illustrating that the recipient ID may be a telephone number); APPLE-1052, 12:53-60. If the MFCI is not available in the sending mobile phone’s local phonebook, “the remote message format capabilities determinator circuitry 208 [of the sending mobile phone] is then invoked and generates a second mobile wireless communication device messaging format capabilities information request 226.” APPLE-1005, [0033]-[0034].

59. The requested MFCI 110 for the receiving mobile phone may be “stored in a location other than within the second mobile wireless communication device

200, for example, such as a network element within the network 108” (e.g., a “web server”), and the sending mobile phone directs the request to the network element. APPLE-1005, [0039], [0056]-[0057]. For example, Tsampalis teaches that, “while inputting the active message 216, the first mobile wireless communication device 100 will transparently contact the network talking to the address(es), (e.g., the MSISDN(s)), of the recipients(s), and try to talk with their home location register (HLR) to find out if they are capable of receiving” certain types of messages. APPLE-1005, [0061].

60. As noted above, Horvath and Tsampalis teach that the HLR and HSS “include[] information to identify each registered wireless device 106 such as...the telephone number assigned to the wireless device.” See APPLE-1004, [0031], [0035], [0047]; APPLE-1005, [0061]. Thus, to obtain the MFCI, it would have been obvious for the combination’s sending mobile phone to send a request that included the telephone number of the receiving mobile phone to the “network element within the network” (e.g., HLR 202 and/or HSS 210), so that the network element was able to look up the profile of the receiving phone. See APPLE-1004, [0035], [0044]; APPLE-1005, [0033], [0039], [0046], [0056]-[0057], [0061]; see also APPLE-1042, [0068] (“a telephone number may be used to correlate and thread together different types of messages such as telephone messages, voicemail messages, fax messages, SMS messages, and MMS messages”).

61. Thus, Horvath-Tsampalis-Kansal's sending mobile phone *send[s] information representing at least the phone number of the receiving mobile phone* (e.g., sending a request to the HLR and/or HSS including the receiving mobile phone's telephone number to determine the receiving mobile phone's MFCI).

Element [1c]: receiving a response to the sending of the information;

62. Horvath-Tsampalis-Kansal renders obvious Element [1c]. As I previously explained for Element [1b], to obtain the MFCI, the combination's sending mobile phone sends a request to a network element within the network (e.g., HLR 202 and/or HSS 210) to look up the profile of the receiving mobile phone based on the telephone number of the receiving phone. Tsampalis goes on to teach that "the method includes receiving a response to the request where the response contains the second mobile wireless communication device [MFCI] 110, as shown in step 604." APPLE-1005, [0042]; *see also id.*, [0057].

63. In Horvath-Tsampalis-Kansal, the response from the network element (e.g., HLR and/or HSS) with the MFCI would also include information about the services to which the wireless device 106 is subscribed (e.g., an IM service hosted on the IMS network, which together is a *PSMS*). Horvath's HSS "comprises a database including profiles associated with each wireless device 106 registered with

the IMS,” and these profiles “include[] subscription⁴ related information,” as well as capability information indicating whether each wireless phone is configured to receive messages through the packet-data network. APPLE-1004, [0035], [0044]. And Tsampalis describes that one problem its system seeks to overcome is “[b]eing unable to process the message due to the incompatibility of its messaging service capabilities with that of the format of the received message.” APPLE-1005, [0003]. In other words, Tsampalis recognizes that MFCI is related to the messaging services to which a mobile phone is subscribed, and therefore at least suggests that the MFCI itself indicates subscription information. *Id.*

64. Providing such subscription information along with format information to a sending mobile phone was well known. *See, e.g.*, APPLE-1053, 1:24-50 (“there are many different protocols or services that can be used for exchanging content,” including MMS and e-mail), 5:29-33, 7:28-8:45 (describing one service provided by

⁴ In the context of IMS networks, a “subscription” is a persistent characteristic of a user indicating service capability (*e.g.*, whether a user has signed up for and/or is paying for a service), whereas “registration” is a session specific “sign-in” through which a wireless device provides its location to the network and is assigned a corresponding S-CSCF that provides it with services. *See, e.g.*, APPLE-1051, [0002]-[0026].

cellular operators is “Instant Messaging (IMing),” and describing a sending mobile phone requesting and receiving from a presence server a “resource file,” which includes “information, such as the protocols and connectivity bearers supported by, the capabilities of, and/or the security associations relating to respective devices operated by, or otherwise associated with, the” receiving mobile phone), 12:25-36; APPLE-1063, [0103] (“information related to the subscriber...and settings related to the purchased/subscribed service(s)”), [0107], [0115] (“delivery decision comprises delivery instructions with regard to destination device(s) and/or content and/or format and/or layout of the message to be delivered”), [0122] (describing a sending device receiving information about the destination device of a message to make a “delivery decision”), [0127]. Thus, for similar reasons to those described in §VII.D(i), *supra*, providing a sending mobile phone with more detailed information about the recipient, including their subscriber information, would help the sending user determine how and where to send a message and what content should be included. *See supra* §VII.D(i) (providing similar motivations for the Tsampalis combination).

65. Thus, Horvath-Tsampalis-Kansal’s sending mobile phone *receiv[es] a response to the sending of the information* (e.g., the response with the MFCI).

Element [1d1]: based at least in part on the response, automatically selecting a bearer for the message, wherein the bearer is selected from a group including:

66. For context, it was well known that “various bearers in the mobile network technology” include, for example, “SMS, USSD (Unstructured Supplementary Services Data), CSD (Circuit Switched Data) and packet-switched bearers, such as e.g., GPRS (General Packet Radio Service) etc.” *See* APPLE-1055, [0014]; *see also* APPLE-1054, 4:42-46. The ’600 Patent describes that a “conventional SMS bearer” may be used on a circuit-switched network (*e.g.*, GSM), whereas a “packet-switched bearer may be a HSDPA, WCDMA, CDMA2000, GPRS or similar data bearer.” APPLE-1001, 3:26-35. In general, messages sent over a circuit-switched network are sent via a circuit-switched bearer and messages sent over a packet-switched network are sent via a packet-switched bearer. Thus, when an SMS message is sent over a circuit-switched network⁵, it is utilizing an SMS bearer, which is a type of circuit-switched bearer. *See* APPLE-1001, 3:26-35,

⁵ Some packet-switched networks support SMS messages, and in those cases, an SMS bearer would also be a packet-switched bearer. *See, e.g.*, APPLE-1056, [0091]. However, in other cases, SMS sent over a packet-switched network is encapsulated in a packet-switched bearer. *See, e.g.*, APPLE-1004, [0050] (describing encoding SMS content as the payload of an SIP message); APPLE-1056, [0166] (describing encapsulating SMS data “in IP format before delivery to the WLAN”).

APPLE-1054, 4:42-46. On the other hand, for messages sent over the packet-switched network, such as the SIP messages taught by Horvath, the bearer (*e.g.*, GPRS) is a packet-switched bearer. *See* APPLE-1004, [0024] (identifying GPRS as an example of its packet-switched network 102), [0040]-[0041], [0050] (describing the delivery of an SIP message over a packet-switched network).

67. Horvath-Tsampalis-Kansal renders obvious Element [1d1]. As I previously discussed in §VII.A, Horvath describes that the sending mobile phone will send its message over the packet-switched network whenever it (the sending mobile device) is registered on the packet-switched network. *See* APPLE-1004, [0021], [0039]-[0042], [0078]. Only when “delivery of the SMS message is not possible on the packet data network” (*e.g.*, the sending mobile phone is not registered) will the sending mobile phone “select the circuit services network for SMS delivery.” *Id.*

68. Tsampalis describes “sending of a message in a message format compatible with at least one of the messaging formats identified in the second mobile wireless communication device [MFCI].” APPLE-1005, [0041]. That is, after the network element (*e.g.*, HLR and/or HSS) sends the receiving mobile phone’s MFCI to the sending mobile phone, the sending mobile phone utilizes the information to determine how to send the message to the receiving mobile phone. *See id.*

69. Taken together and as I previously described in §VII.D, Horvath-Tsampalis-Kansal’s sending mobile phone utilizes both sets of information when determining how to format and deliver a message to a receiving mobile phone. First, the sending mobile phone checks if it is registered on the packet-data network. *See* APPLE-1004, [0021], [0039]-[0042], [0078]. If it is, it will utilize the packet-data network, and otherwise it will utilize the circuit-services network. *Id.* Second, the sending mobile phone will check the receiving mobile phone’s MFCI and service-subscription information to determine the best way to send a message that is compatible with the capabilities and subscriptions of the receiving mobile phone. APPLE-1005, [0041], [0049], [0052]-[0054], [0062].

70. Tsampalis describes that, where “the default messaging format” of the sending mobile phone “is not found in the” receiving mobile phone’s “messaging format capabilities list,” the sender mobile phone performs a “transformation of the message into a compatible format as found in the recipient list messaging format capabilities.” APPLE-1005, [0049], [0052]-[0054]. While Tsampalis describes some embodiments where a user is “prompted” to select a “compatible format” into which the message may be transformed, Tsampalis also describes “yet other embodiments [that] include no user prompts whatsoever.” APPLE-1005, [0052]-[0055]. Indeed, Kansal describes that its unified messaging UI is configured to automatically select a bearer for the message. *See* APPLE-1042, [0077]-[0078]. For

example, “after a media object has been added to the message, the messaging UI 500 may undergo an automatic or seamless conversion...from an SMS messaging UI to an MMS messaging UI, and the message will be sent as an MMS message.” APPLE-1042, [0077]. “In some cases, the conversion of a message from one format to a particular sending format may be based on programmed and/or detected preferences, constraints, and/or availability of a recipient to receive messages of a certain format.” APPLE-1042, [0078].

71. Accordingly, Horvath-Tsampalis-Kansal’s sending mobile phone, *based at least in part on the response, automatically select[s] a bearer for the message* (e.g., the sending mobile phone selects between the circuit-services network and the packet-data network based on its own registration status, and selects the format of the message, such as SMS, MMS, or IM, based on the received MFCI). *Element [1d2]: an SMS bearer;*

72. Horvath-Tsampalis-Kansal renders obvious Element [1d2]. As I previously discussed for Element [1d1], Horvath-Tsampalis-Kansal’s sending mobile phone utilizes both (1) its own registration status with the packet-data network and (2) the MFCI and service-subscription information received from the network element (e.g., HLR and/or HSS) when determining how to format and deliver a message to a receiving mobile phone. Where, for example, both the sending mobile phone is not currently registered with the packet-switched network

and the receiving mobile phone's MFCI indicates that the receiving mobile phone can only receive SMS messages (*e.g.*, because one or both lost their connection "due to roaming or the like"), Horvath-Tsampalis-Kansal's sending mobile phone will send an SMS over the circuit-switched network and it will be received as an SMS at the receiving mobile phone.⁶ *See* APPLE-1006, [0020] (describing a wireless device losing connection), [0028], [0030]. Even where the sending mobile phone is registered with the packet-data network, the receiving mobile phone's MFCI may indicate it is only capable of receiving SMS, so the sending mobile phone would send an SMS message to the receiving mobile phone, given its limited capabilities. *See* APPLE-1005, [0062]; APPLE-1056, [0091]. This is consistent with the unified messaging UI described by Kansal, which determines sending format "based on programmed and/or detected preferences, constraints [*e.g.*, the sending mobile phone's registration or connection status with the circuit-switch and packet-switched

⁶ The sending mobile phone could lose connection at any time, including between when it requested the receiving mobile phone's MFCI and service-subscription information and when it sends a message, which would limit how the sending mobile phone would be able to communicate. *See* APPLE-1006, [0020], [0028], [0030].

networks], and/or availability of a recipient to receive messages of a certain format.”
APPLE-1042, [0078].

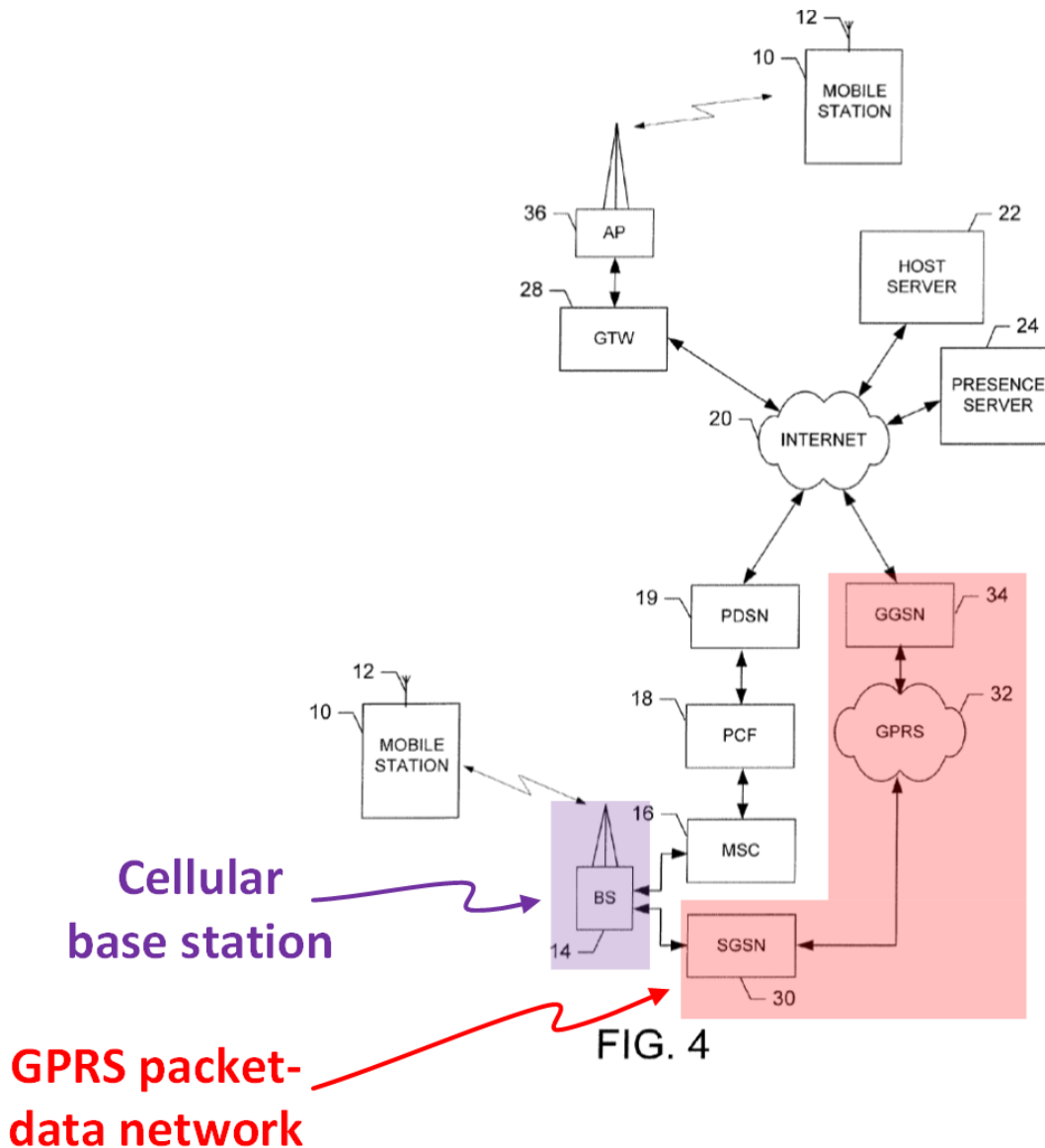
73. Accordingly, in Horvath-Tsampalis-Kansal, *the bearer is selected from a group including an SMS bearer* (e.g., when either the sending mobile phone is not registered with the packet-data network or the receiving mobile phone’s MFICI indicates it has “limited messaging capabilities,” an SMS bearer would be selected).

Element [1d3]: a packet-switched message bearer supported by a cellular connection between the sending mobile phone and a cellular base station; and

74. Horvath-Tsampalis-Kansal renders obvious Element [1d3]. As I previously discussed for Element [1d1], “various bearers in the mobile network technology” include, for example, “packet-switched bearers, such as e.g., GPRS (General Packet Radio Service) etc.” See APPLE-1055, [0014]; see also APPLE-1054, 4:42-46. Similarly, the ’600 Patent describes a “packet-switched bearer may be a HSDPA, WCDMA, CDMA2000, GPRS or similar data bearer.” APPLE-1001, 3:26-35. In general, messages sent over a circuit-switched network are sent via a circuit-switched bearer and messages sent over a packet-switched network are sent via a packet-switched bearer.

75. Horvath explains that the “packet data network 102, in one embodiment, comprises an Evolution Data Only (‘EV-DO’) network, a General Packet Radio Service (‘GPRS’) network, a Universal Mobile Telecommunications System (‘UMTS’) network, an 802.11 network, an 802.16 (WiMax) network, Ethernet

connectivity, dial-up modem connectivity, or the like.” *See e.g.*, APPLE-1004, [0024]. As shown in the following diagram, a mobile device communicating via GPRS communicates with a base station of a cellular network. APPLE-1053, FIG. 4, 12:54-13:60 (“an antenna 12 for transmitting signals to and for receiving signals from one or more base stations (BS’s),” which are “part of one or more cellular or mobile networks that each includes elements required to operate the network” and may “be coupled to a signaling GPRS (General Packet Radio Service) support node (SGSN) 30”).



APPLE-1053, FIG. 4 (Annotated)

76. As I previously discussed for Element [1d1], Horvath-Tsampalis-Kansal's sending mobile phone utilizes both (1) its own registration status with the packet-data network and (2) the MFCI and service-subscription information received from the network element (*e.g.*, HLR and/or HSS) when determining how to format and deliver a message to a receiving mobile phone. Where, for example,

the sending mobile phone is registered with the packet-switched network and the packet-switched network to which the sending mobile phone is registered is a GPRS network, Horvath-Tsampalis-Kansal's sending mobile phone will send a message via a GPRS bearer. See APPLE-1004, [0024] (packet-data network comprises a GPRS network), [0050] ("If the wireless device 106 is registered on the packet data network 102," it transmits the message through the packet-data network 102).

77. GPRS is *a packet-switched message bearer supported by a cellular connection between the sending mobile phone and a cellular base station*. See APPLE-1055, [0014]; APPLE-1054, 4:42-46.

Element [1d4]: a packet-switched message bearer supported by a wireless local area network (WLAN) connection between the sending mobile phone and a WLAN base station;

78. Horvath-Tsampalis-Kansal renders obvious Element [1d4]. As I previously discussed for Element [1d3], in general, messages sent over a circuit-switched network are sent via a circuit-switched bearer and messages sent over a packet-switched network are sent via a packet-switched bearer.

79. Horvath explains that the "packet data network 102, in one embodiment, comprises an Evolution Data Only ('EV-DO') network, a General Packet Radio Service ('GPRS') network, a Universal Mobile Telecommunications System ('UMTS') network, an 802.11 network, an 802.16 (WiMax) network, Ethernet connectivity, dial-up modem connectivity, or the like." See e.g., APPLE-1004,

[0024]. As shown in the following diagram, a mobile device communicating via an 802.11 network communicates with a WLAN access point, which is a type of base station. APPLE-1053, FIG. 4, 13:61-14:19 (mobile station “coupled to one or more wireless access points...configured to communicate with the mobile station in accordance with techniques such as...WLAN techniques”); 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, 3, 4; APPLE-1037.

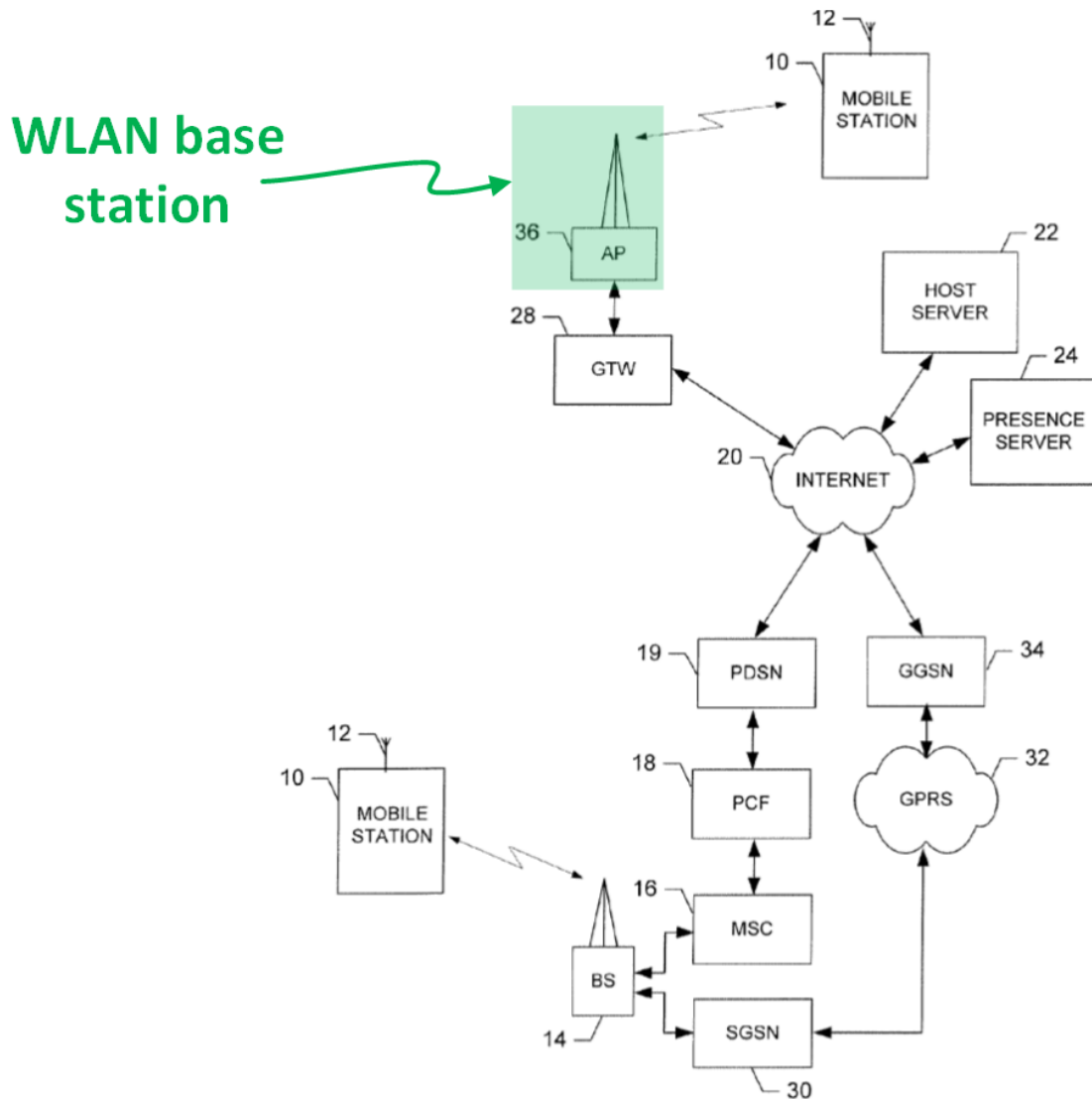


FIG. 4

APPLE-1053, FIG. 4 (Annotated)

80. As I previously discussed for Element [1d1], Horvath-Tsampalis-Kansal's sending mobile phone utilizes both (1) its own registration status with the packet-data network and (2) the MFCI and service-subscription information received from the network element (*e.g.*, HLR and/or HSS) when determining how to format and deliver a message to a receiving mobile phone. Where, for example,

the sending mobile phone is registered with the packet-switched network and the packet-switched network to which the sending mobile phone is registered is an 802.11 network, Horvath-Tsampalis-Kansal's sending mobile phone will send a message via an 802.11 bearer. See APPLE-1004, [0024] (packet-data network comprises "an 802.11 network"), [0050] ("If the wireless device 106 is registered on the packet data network 102," it transmits the message through the packet-data network 102).

81. An 802.11 network provides *a wireless local area network (WLAN) connection between the sending mobile phone and a WLAN base station*, and that in order to utilize the 802.11 network, the message would have to be formatted consistent with *a packet-switched message bearer supported by* the 802.11 network. See APPLE-1055, [0014]; APPLE-1054, 4:42-46.

Element [1e]: after the automatically selecting, formatting the message for transmission via the selected bearer;

82. Horvath-Tsampalis-Kansal renders obvious Element [1e]. As I previously discussed for Element [1d1], Tsampalis describes "sending of a message in a message format compatible with at least one of the messaging formats identified in the second mobile wireless communication device [MFCI]." APPLE-1005, [0041]. That is, after the network element (e.g., HLR and/or HSS) sends the receiving mobile phone's MFCI to the sending mobile phone, the sending mobile

phone utilizes the information to determine how to send the message to the receiving mobile phone. *See id.*

83. Tsampalis describes that, where “the default messaging format” of the sending mobile phone “is not found in the” receiving mobile phone’s “messaging format capabilities list,” the sender mobile phone performs a “transformation of the message into a compatible format as found in the recipient list messaging format capabilities.” APPLE-1005, [0049], [0052]-[0054]. Furthermore, Kansal describes that its unified messaging UI is configured to automatically select a bearer for the message. *See* APPLE-1042, [0077]-[0078]. For example, “after a media object has been added to the message, the messaging UI 500 may undergo an automatic or seamless conversion...from an SMS messaging UI to an MMS messaging UI, and the message will be sent as an MMS message.” APPLE-1042, [0077]. “In some cases, the conversion of a message from one format to a particular sending format may be based on programmed and/or detected preferences, constraints, and/or availability of a recipient to receive messages of a certain format.” APPLE-1042, [0078].

84. Accordingly, Horvath-Tsampalis-Kansal’s sending mobile phone, *after the automatically selecting, format[s] the message for transmission via the selected bearer* (e.g., converting a message “to a particular sending format” based on the MFCI of the receiving mobile phone).

Element [1f]: after the formatting, transmitting, by the sending mobile phone using the selected bearer, the message, to the receiving mobile phone; and

85. Horvath-Tsampalis-Kansal renders obvious Element [1f]. As I previously discussed for Element [1d1], Tsampalis describes “sending of a message in a message format compatible with at least one of the messaging formats identified in the second mobile wireless communication device [MFCI].” APPLE-1005, [0041]; *see also id.* [0025]. Specifically, “[w]hen the user interface 202 detects a request to send the active message 216 (unformatted), the user interface 202 communicates this information to the send message circuitry 106. 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.” APPLE-1005, [0036]. The “send message circuitry 106 formats the message prior to sending the message.” APPLE-1005, [0037].

86. Accordingly, Horvath-Tsampalis-Kansal’s sending mobile phone, ***after the formatting, transmit[s], by the sending mobile phone using the selected bearer, the message, to the receiving mobile phone.***

Element [1g1]: performing the retrieving, the sending, the receiving, the automatically selecting, the formatting and the transmitting for at least first, second and third iterations, wherein:

87. Horvath-Tsampalis-Kansal renders obvious Element [1g1]. The Horvath-Tsampalis-Kansal sending mobile phone would follow the procedures

described with respect to Elements [1a] through [1f], *supra*, every time that a user creates a new message, enters a corresponding recipient ID for the message, and requests to send the active message. *See* APPLE-1005, [0033], [0036], [0046]. In fact, Tsampalis describes an example where a user enters multiple recipients for a single message, and “for each recipient 402 entered in the active message recipient list 218, the same remote message format capabilities determinator circuitry 208 is then invoked to generate a second mobile wireless communication device messaging format capabilities information request 226.” APPLE-1005, [0034]. This process would be followed for each “new unformatted message 110 entered by a user through the send message circuitry 106.” *See* APPLE-1005, [0046].

88. Accordingly, Horvath-Tsampalis-Kansal’s sending mobile phone *perform[s] the retrieving, the sending, the receiving, the automatically selecting, the formatting and the transmitting for at least first, second and third iterations.*

Element [1g2]: during the first iteration, a first message is sent to a first receiving mobile phone using the SMS bearer;

89. Horvath-Tsampalis-Kansal renders obvious Element [1g2]. From the teachings of Horvath, Tsampalis, and Kansal, a first scenario (*first iteration*), when the first receiving phone MFCI contained in the first response indicates that the first receiving phone is not capable of either MMS or IM (*e.g.*, because the first receiving phone is not subscribed or not currently signed into the associated messaging service) and is only capable of SMS, is obvious. *Supra*, §VIII.A, Analyses of Elements [1b]-

[1d2]; APPLE-1042, [0077]-[0078] (describing a unified messaging UI configured to automatically convert between different message formats, including SMS, MMS, e-mail, and IM, based on availability of a recipient to receive messages of a certain format). In this first scenario, the sending mobile phone formats and sends a first message to the first receiving mobile phone as an SMS message (an *SMS bearer*) over the packet-data network by default or over the circuit-services network if it is not possible to send over the packet-data network.

Element [1g3]: during the second iteration, a second message is sent to a second receiving mobile phone using the packet switched message bearer supported by the cellular connection; and

90. Horvath-Tsampalis-Kansal renders obvious Element [1g3]. From the teachings of Horvath, Tsampalis, and Kansal, a second scenario (*second iteration*), where the available packet-data network to which the sending mobile phone is registered is, for example, a GPRS packet-data network, and when the second receiving phone is capable of MMS (and/or IM), is obvious. *Supra*, §VIII.A, Analyses of Elements [1b]-[1d2]; APPLE-1042, [0077]-[0078] (describing a unified messaging UI configured to automatically convert between different message formats, including SMS, MMS, e-mail, and IM, based on availability of a recipient to receive messages of a certain format). In the second scenario, the sending phone obtains this MFCI about the second receiving phone through a second request to and a second response from the remote server(s), then formats and sends the second

message as MMS (or IM) using the GPRS packet-data network (*packet switched message bearer supported by the cellular connection*).

Element [1g4]: during the third iteration, a third message is sent to a third receiving mobile phone using the packet-switched message bearer supported by the WLAN connection;

91. Horvath-Tsampalis-Kansal renders obvious Element [1g4]. From the teachings of Horvath, Tsampalis, and Kansal, a third scenario (*third iteration*), where the available packet-data network to which the sending mobile phone is registered is “an 802.11 network” as discussed above, and when the third receiving phone is capable of MMS (and/or IM), is obvious. *Supra*, §VIII.A, Analyses of Elements [1b]-[1d4]. In the third scenario, the sending phone obtains this MFCI about the third receiving phone through a third request to and a third response from the remote server(s), then formats and sends the third message as MMS (or IM) using the 802.11 network (*packet-switched message bearer supported by the WLAN connection*). *Id.*

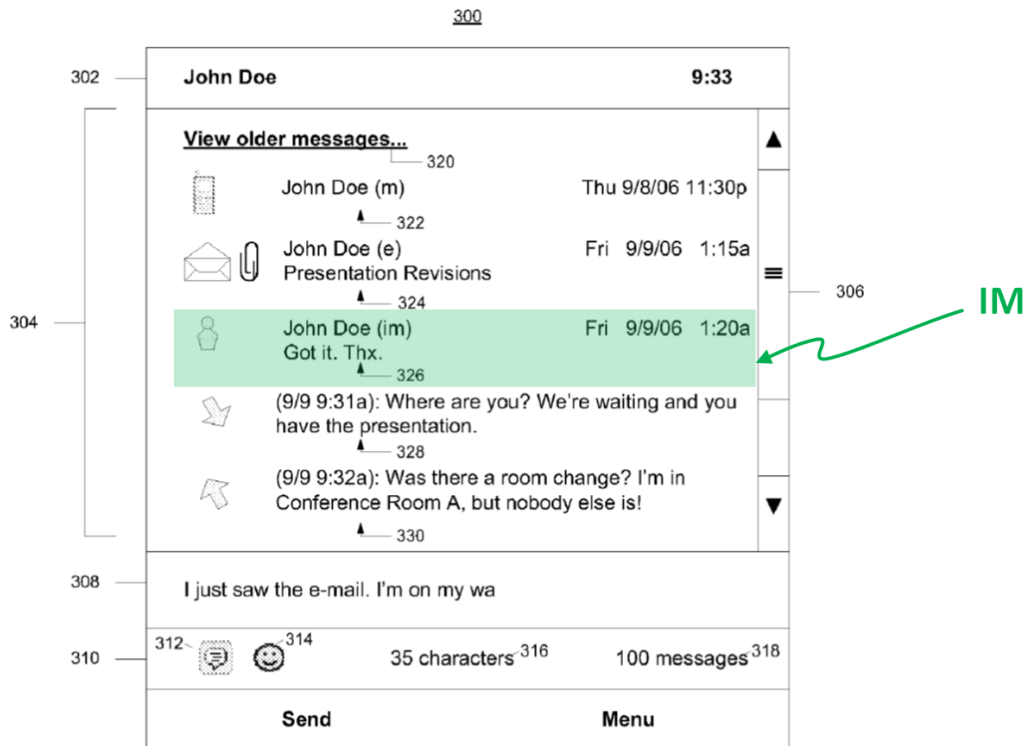
Element [1h]: wherein a packet switched message service (PSMS) is used to send the third message to the third receiving mobile phone;

92. Horvath-Tsampalis-Kansal renders obvious Element [1h]. Horvath describes that when device 106 “[is] registered with the [SIP] registrar,” device 106 sends SIP messages in SIP packets “through the [SIP] network communicating over the packet data network.” APPLE-1004, Abstract, [0002], [0006]-[0007], [0017], [0024], [0034], [0037], [0038], [0039], [0041], [0078], FIG. 7. One type of message

service provided by the SIP/IMS network is an “instant messaging” service, such that the IMS network and its IM service are a *PSMS*. APPLE-1004, [0033]. And Kansal describes an example in which one of the conversations displayed in the unified messaging UI is an instant messaging conversation. *See* APPLE-1042, [0062] (“The message thread 304 includes a message 326 comprising a sent IM message that displays linked IM screen name information of the contact, the text of the IM message, and the date sent”), FIG. 3.

93. Based on these teachings, when a receiving mobile phone is registered with the IM service and is thus capable of communicating via IM, an MFCI response communicates to the sending mobile phone that the receiving mobile phone is subscribed to an IM service and has IM capabilities. *See* APPLE-1004, [0033]; APPLE-1042, [0034], [0042], [0062], [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.)”). In that case, the send message circuitry of the sending mobile device would have formatted the message for delivery by an IM service over the 802.11 network where: (1) the available packet-data network to which the sending mobile phone is registered is an 802.11 network; (2) the sending mobile phone is a subscriber of the IM service; and (3) the receiving mobile phone’s MFCI indicates it is also a subscriber of the IM service and capable of receiving IMs. *Id.* Indeed, Kansal illustrates and describes a “message thread 304 includes a message

326 comprising a sent IM message that displays linked IM screen name information of the contact, the text of the IM message, and the date sent (e.g., Fri Sep. 9, 2006 1:20 a.m.).” APPLE-1042, [0062].



APPLE-1042, FIG. 3 (Annotated)

94. Accordingly, in Horvath-Tsampalis-Kansal, *a packet switched message service (PSMS) is used to send the third message to the third receiving mobile phone* (e.g., where the sending mobile phone subscribes to an IM service and the MFCI indicates that the receiving mobile phone subscribes to an IM service, and both the sending mobile phone and the receiving mobile phone are connected to a packet-data network such as an 802.11 network, the send message circuitry of the

sending mobile phone would have selected the IM service of the IMS network for delivery of a message to the receiving mobile phone).

Element [1i]: 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;

95. Horvath-Tsampalis-Kansal renders obvious Element [1i]. As I previously discussed for Element [1h], Horvath-Tsampalis-Kansal's IM service provided by the IMS network 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 802.11 network). APPLE-1004, [0033] ("The SIP network is used for establishing instant messaging..."). It was well known that IM messages were formatted using, 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, Horvath's IM service and IMS network (*PSMS*) would have been *for sending and receiving packet switched messages other than SMS, enhanced message service (EMS) and multimedia message service (MMS) messages.*

Element [1j]: wherein a same messaging client on the sending mobile phone performs at least the retrieving, the sending, the receiving, the automatically selecting, the formatting and the transmitting for each of the first, second and third iterations.

96. Horvath-Tsampalis-Kansal renders obvious Element [1j]. As I previously discussed for Elements [1a] through [1g4], the sending mobile phone *performs at least the retrieving, the sending, the receiving, the automatically selecting, the formatting and the transmitting for each of the first, second and third iterations*. In Horvath-Tsampalis-Kansal, these functions would have been performed by *a same messaging client* on the sending mobile phone.

97. For example, Horvath teaches that “[t]he wireless device 106 operates under the control of a device controller/processor 402, that controls the sending and receiving of wireless communication signals.” APPLE-1004, [0061]. “The wireless device 106 also includes non-volatile storage memory 414 for storing, for example, an application waiting to be executed (not shown) on the wireless device 106.” APPLE-1004, [0064]. In at least some implementations, the “application” would have performed any one or all of the functions of [1a] through [1g4].

98. As I previously discussed in §VII.C and analyses for Elements [1pre2] and [1h], Kansal describes a “messaging UI 500 [that] may enable a user to compose messages of different types of formats [e.g., SMS, MMS, IM] using the same unified messaging UI.” APPLE-1042, [0077]-[0078]. Underlying the unified messaging UI, Kansal describes “several messaging applications 130 arranged to communicate [the] various types of messages in a variety of formats.” APPLE-1042, [0035]. However, Kansal further teaches that the “components and modules [described

throughout its disclosure] may be combined,” which would have at least suggested to a POSITA that a single application could be used for the same purpose. *See* APPLE-1042, [0086]. And it was well known that a unified messaging client would have been configured to retrieve, send, receive, automatically select, format and transmit of [1a] through [1g4]. *See, e.g.*, 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”), 1-2 (a multi-protocol messaging application providing “a powerful and efficient user experience.”)); APPLE-1061, FIG. 4, [0048]-[0054] (describing an “extensible communication application 160” through which “a message is input, addressed to a group of contacts, and sent to each contact using the contact's preferred or optimal communication medium,” including e-mail, instant messaging, and text messaging).

Claim [3]: The method of claim 1, wherein at the time the first message is sent to the first receiving mobile phone: no phone number corresponding to the first receiving phone is associated with a subscriber of the PSMS.

99. Horvath-Tsampalis-Kansal renders Claim [3] obvious. As I previously discussed for Element [1g2], the sending phone learns from the first response that the first receiving phone is not capable of IM (*e.g.*, because the first receiving phone is not subscribed to the IM service), the sending phone then formats and sends the first message as an SMS. When the MFCI indicates that the first receiving phone is

not capable of IM, *no phone number corresponding to the first receiving phone is associated with a subscriber of the IM service of the IMS network (the PSMS).*

APPLE-1004, [0038] (“services subscribed to by the device 106”); *see also id.*, [0031], [0033], [0039], [0041], [0050], [0071]-[0073], FIG. 5.

Claim [4]: The method of claim 1, wherein the messaging client provides an option to modify the third message, wherein the option is not available to modify the first message.

100. Horvath-Tsampalis-Kansal renders Claim [4] obvious. For example, Tsampalis teaches that an MMS may include “attached/inserted multimedia files,” which would be lost in the event that the MMS is transformed into an SMS. APPLE-1005, [0062]. Similarly, Kansal describes that, “after a media object has been added to the message, the [unified] messaging UI 500 may undergo an automatic or seamless conversion” from SMS to MMS. APPLE-1042, [0077]. “In the event that the user adds a media object and then removes the media object, the messaging UI 500 may automatically or seamlessly convert back from an MMS messaging UI to an SMS messaging UI.” *Id.*

101. It was well known that IM (*the third message*) supported the addition (*e.g.*, attachment) of media objects (*see, e.g.*, APPLE-1007, 7 (describing IM support for “file transfer”); APPLE-1008, [0046]-[0047] (describing transmission of multimedia content via an IM client)), and that SMS (*the first message*) does not support attachment of media objects (*see e.g.*, APPLE-1005, [0062] (describing that

“attached/inserted multimedia files will be lost” for SMS); APPLE-1042, [0075]-[0077] (describing need to convert SMS to another message type in order to add “media objects such as pictures, video, and/or sounds to a message”). The attachment of a media object is type of modification to a message.

102. When Kansal describes “automatically or seamless[ly] convert[ing] back from an SMS messaging UI to an MMS messaging UI” when, for example, a user adds a media object to the composed message, Kansal’s unified message UI is necessarily making the sending of the media object and thus the associated modification to the message *not available* for SMS and *available* for other message types (e.g., MMS). See APPLE-1042, [0075]-[0077]. Indeed, it was well known to “grey out” options that are not available to the user, which is a visual indication to a user of options that are available and unavailable. See, e.g., APPLE-1070, [0060] (“the SMS option is greyed out since the message includes media items which are unable to be transmitted by SMS”).

103. Accordingly, Horvath-Tsampalis-Kansal’s *messaging client provides an option to modify the third message* (e.g., providing the user an option to attach a media object to an IM), *wherein the option is not available to modify the first message* (e.g., not providing the user an option to attach a media object to an SMS by, for example, greying out the option).

Claim [5]: The method of claim 1, wherein the response originates from a server which is located outside of a cellular core network, wherein the sending mobile

phone is authenticated to the PSMS via SMS and the sending mobile phone is authenticated to the PSMS via a hardware identifier of the sending mobile phone.

104. Horvath-Tsampalis-Kansal renders obvious Claim [5].

105. For example, as I previously discussed for Element [1b], *supra*, the HSS is a network element that would have stored MFCI. *See* APPLE-1004, [0035]; APPLE-1005, [0039]. The HSS is “part of an Internet Protocol multimedia subsystem (‘IMS’) core that supports the SIP network.” *See* APPLE-1004, [0033]. The IMS core is distinct from the cellular core network, and therefore the HSS ***is located outside of a cellular core network***. *See* APPLE-1004, [0033]; APPLE-1072, FIG. 3 (illustrating the HSS 330 outside of the core network 310), [0059]-[0061] (HSS 330 “interface[s] to one or more CSCF servers 320 of the core network 310”); APPLE-1071, [0006] (“Independent ‘Mobile Core’ and ‘Fixed Core’ networks will be replaced with what is referred to as a converged network which has a common core connecting to different access technologies”); APPLE-1014, [0006] (describing the circuit-services GSM network as a “cellular network”), [0047]. Accordingly, in Horvath-Tsampalis-Kansal, ***the response originates from a server which is located outside of a cellular core network*** (e.g., the response with the MFCI originates from the HSS, which stores the MFCI and is located outside of the cellular core network).

106. Furthermore, Horvath describes authenticating its sending wireless device (wireless devices 106) both during registration with the SIP/IMS network and

for transmitting subsequent messages, through the S-CSCF and HSS. APPLE-1004, FIG. 5 (“S-CSCF authenticates and registers the wireless device” at step 508), [0035] (“The HSS 210 also performs authentication and authorization of the wireless device 106”), [0036], [0040]. Horvath details 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 is performed using “profiles associated with each wireless device 106” stored on the HSS 210. APPLE-1004, [0035]-[0036], [0038], [0040] (“[w]hen 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”), [0041], [0072]-[0073], [0076], FIGS. 2, 5. Once registration is complete, the P-CSCF “authenticate[s] subsequent messages allowing the other network entities such as the I, S-CSCF 208 to trust the messages.” APPLE-1004, [0036].

107. As part of authentication through a S-CSCF and HSS, the mobile phone would provide its International Mobile Equipment Identity (IMEI) for verification. *See, e.g.*, APPLE-1073, [0005]-[0017] (“Existing mobile networks provide a security service according to a three-step process” including “checking whether mobile equipment of the user is illegal mobile equipment through an Equipment Identity Register (EIR)” based on whether the mobile equipment’s IMEI is “include[d on] a white list, a black list, and a gray list”). Accordingly, part of

authentication through a S-CSCF and HSS included *the sending mobile phone being authenticated via a hardware identifier of the sending mobile phone*. See *id.*

108. Through authentication with the S-CSCF and HSS, wireless device 106 is also authenticated to the IM service provided by the IMS network (*authenticated to the PSMS*). APPLE-1004, [0033], [0038]-[0039] (“[a]n application server [providing, e.g., 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. ... The SMSC 114 does not have to authenticate the wireless device 106 because the S-CSCF 206 has already done so.”), [0073].

109. As noted above, the mobile phone is authenticated whenever transmitting subsequent messages. Specifically, Horvath describes that, “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.” APPLE-1004, [0036]. “The P-CSCF 206 can authenticate subsequent messages allowing the other network entities such as the I,S-CSCF 208 to trust the messages.” *Id.* That is, after registration, the mobile phone utilizes the security keys (e.g., session keys CK and IK) to encrypt and/or integrity protect all subsequent messages, including SMS messages. *Id.*; see

also APPLE-1087, [0007]-[0014]; APPLE-1088, [0019], [0035]; APPLE-1072, [0055]. An element of the IMS network (e.g., the P-CSCF) will utilize the security key(s) provided during registration to verify the authenticity of, e.g., a sent SMS message (*the sending mobile phone is authenticated to the PSMS via SMS*). *Id.* Where authentication is successful, the message is sent further into the IMS network implemented by Horvath's IMS network that includes the IM service (*PSMS*) and the identity of the source of the message is believed due to this authentication process.

110. Accordingly, in Horvath-Tsampalis-Kansal, *the sending mobile phone is authenticated to the PSMS via SMS* (e.g., authenticating the sending mobile phone with the IMS network—which includes the IM application server—by authenticating all messages sent by the sending mobile phone, including SMS messages, utilizing session keys) *and the sending mobile phone is authenticated to the PSMS via a hardware identifier of the sending mobile phone* (e.g., authenticating a mobile phone with the S-CSCF and the EIR based on the IMEI of the mobile phone).

Claim [6]: The method of claim 1, wherein the response is correlated with a status of the receiving mobile phone when the receiving mobile phone is associated with a subscriber of the PSMS.

111. Horvath-Tsampalis-Kansal renders obvious Claim [6]. Horvath describes that the “SMS delivery network selector 116, based on the registration status of the wireless device 106, selects either the packet data network 102 or the

circuit services network 104 for delivery of a SMS message.” APPLE-1004, [0053]. The registration status of the wireless device 106 is stored in the profiles included in the HSS’s database. APPLE-1004, [0035]. As discussed for Element [1b] and Claim [5], *supra*, the HSS is one network element that would store MFCI. *See* APPLE-1004, [0035]. Accordingly, in Horvath-Tsampalis-Kansal, the MFCI *response* from the HSS would include (and therefore be *correlated with*) registration status of the receiving mobile device with a packet-data network (*a status of the receiving mobile phone*), at least because access to certain messaging services including the IM service of the IMS network (*PSMS*) is available through a packet-data network, and even when the user of the receiving mobile device is a subscriber to the IM service (*the receiving mobile phone is associated with a subscriber of the PSMS*), the receiving mobile device would need to be registered with a packet-data network in order to access the IM service. Indeed, Kansal teaches that “the conversion of a message from one format to a particular sending format may be based on programmed and/or detected preferences, constraints, and/or availability of a recipient to receive messages of a certain format,” which would have included *a status of the receiving mobile phone*, such as whether the receiving mobile device is connected to the IM service. *See* APPLE-1042, [0078].

Claim [7]: The method of claim 1, wherein the sending mobile phone is authenticated to the PSMS via SMS and the sending mobile phone is authenticated to the PSMS via a randomly generated authentication identifier.

112. Horvath-Tsampalis-Kansal renders obvious Claim [7]. As I previously discussed for Claim [5], in Horvath-Tsampalis-Kansal, *the sending mobile phone is authenticated to the PSMS via SMS*.

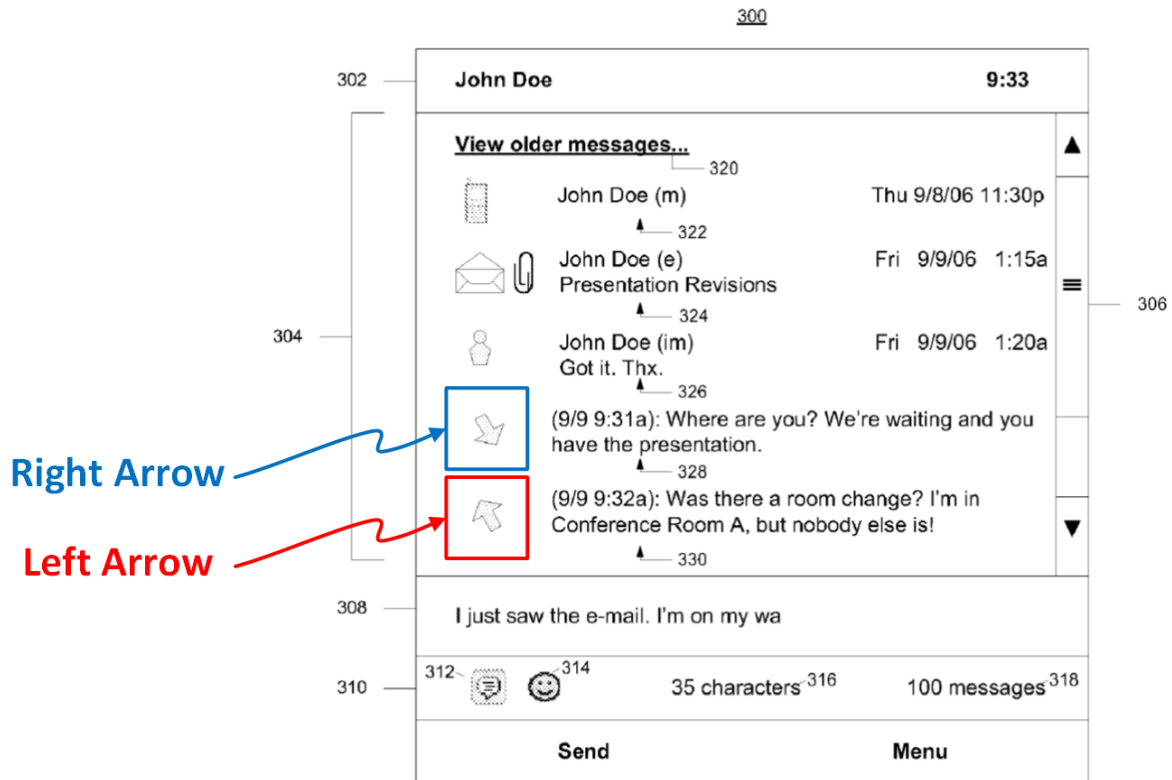
113. According to the signaling procedures set forth in 3GPP TS33.203, a mobile phone authenticating with an S-CSCF receives a RAND parameter used as part of an authentication vector and is stored in the S-CSCF for use in future re-authentication. See, e.g., APPLE-1085, [0064]; APPLE-1086, [0013]-[0018]. Because the RAND parameter is associated with the mobile phone in the HSS, it is a *randomly generated authentication identifier*.

114. Additionally or alternatively, Horvath-Tsampalis-Kansal's IM service of the IMS network (*PSMS*) would authenticate users with a password, which in at least some cases would have been a *randomly generated authentication identifier*. See, e.g., APPLE-1028, 1 (describing that a user provides a password to log into an IM service); APPLE-1058, 12:15-13:8 ("if the user does not know the password, the login processor 222a transmits the password generated at random to the user using the cellular phone number input by the user and authenticates the user by receiving the phone number and the transmitted password"); APPLE-1067, [0016] (describing the use of a random number generator when logging into a system), [0032], [0044]; APPLE-1048, [0043] ("[A] User 100 may employ a Telephone 102 to communicate an IM message to a second IM User 104 via IM protocols. The User 100 may provide

login information such as a username and password or a session ID, obtained from a previous session, via the Telephone 102 to an IVR 106.”); APPLE-1032, [0021], [0028].

Claim [8]: The method of claim 1, wherein the sending mobile phone simultaneously displays a left arrow and a right arrow in an interface which displays message content corresponding to a plurality of messages exchanged between the sending mobile phone and the third receiving mobile phone.

115. Horvath-Tsampalis-Kansal renders Claim [8] obvious. For example, in FIG. 3, Kansal illustrates a “message thread 304 includes a message 328 comprising a received and read SMS message that displays the date of receipt (e.g., Sep. 9, 2006 9:31 a.m.) and the text of the SMS message.” APPLE-1042, [0063]. The message thread 304 also includes “a message 330 comprising a sent SMS message that displays the date sent (e.g., Sep. 9, 2006 9:32 a.m.) and the text of the SMS message.” APPLE-1042, [0063]. As shown in FIG. 3 (below), the received and read SMS message 328 is illustrated with an arrow pointing to the right and down (***a right arrow***) and the sent SMS message 330 is illustrated with an arrow pointing to the left and up (***a left arrow***). *See* APPLE-1042, FIG. 3. Accordingly, in Horvath-Tsampalis-Kansal, the unified messaging UI would have utilized similar arrows to illustrate IM messages sent to and received from ***the third receiving mobile phone***. *See id.*



APPLE-1042, FIG. 3 (Annotated)

Claim [9]: The method of claim 1, wherein the first receiving mobile phone, the second receiving mobile phone and the third receiving mobile phone are different mobile phones.

116. Horvath-Tsampalis-Kansal renders obvious Claim [9]. Both Horvath and Tsampalis describe messaging among a plurality of mobile phones. *See e.g.*, APPLE-1004, [0002] (“a wireless device such as a mobile phone to send and receive short messages from other wireless devices”), [0027] (“The packet data network 102 and the circuit services network 104 support any number of wireless devices 106.”); APPLE-1005, [0032], [0036] (“sends the message...to the corresponding mobile wireless communication devices associated with the particular recipient IDs”), [0055]

(“groups of recipients”), [0062] (“multiple remote recipients”). Thus, in at least some circumstances, the first, second, and third receiving mobile phones are different mobile phones.

Claim [10]: The method of claim 1, wherein the first receiving mobile phone, the second receiving mobile phone and the third receiving mobile phone are the same mobile phone.

117. Horvath-Tsampalis-Kansal renders obvious Claim [10]. As I previously discussed for Element [1b], the response from the network element (HLR and/or HSS) with the MFCI would also include information about the services to which the wireless device 106 is subscribed. In at least some cases, the first, second and third receiving phones are the same phone that varies over time in its registration and/or subscription status with respect to the various messaging services (*e.g.*, SMS, MMS, and IM), such that the same mobile phone has an unregistered/unsubscribed status with the MMS and/or IM services in the first iteration, and an registered/subscribed status with IM in both the second and the third iterations.

Claim [11]: The method of claim 1, wherein: between the automatically selecting and the formatting of the third iteration, an attachment option is presented; and during the entirety of the first iteration, the attachment option is not presented.

118. *Supra*, §VIII.A, Analysis of Claim [4] (describing the availability of attaching multimedia objects to an IM and not to an SMS in Horvath-Tsampalis-Kansal).

Claim [12]: The method of claim 11, wherein the attachment option is a voice message attachment option.

119. Horvath-Tsampalis-Kansal renders obvious Claim [12]. For example, both Horvath and Tsampalis disclose messaging text as well as multimedia messages, which were well known to include images, audio (*e.g.*, **voice**) and video messages. APPLE-1004, [0025], [0029], [0033]-[0034], [0068]-[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, [0062]; APPLE-1042, [0075]-[0077] (describing need to convert SMS to another message type in order to add “media objects such as pictures, video, and/or sounds to a message”); APPLE-1007, page 8 (“By using IM&P, we can deliver voice, video, and data together to various endpoints”), page 11 (“integrated voice, video, and data services in IM systems”); *supra*, §VIII.A, Analysis of Claim [4].

Element [13pre]: A system comprising:

120. *Supra*, §VIII.A, Analysis of Element [1pre1].

Element [13a]: a sending mobile phone comprising a message client, wherein the sending mobile phone retrieves a destination address of a message from the message, wherein the destination address is a phone number of a receiving mobile phone; and

121. *Supra*, §VIII.A, Analyses of Elements [1a], [1j].

Element [13b1]: a server of a packet switched message service (PSMS)

122. Horvath-Tsampalis-Kansal renders Element [13b1] obvious. As I previously discussed for Element [1h], Horvath describes that when device 106 “[is] registered with the [SIP] registrar,” device 106 sends SIP messages in SIP packets

“through the [SIP] network communicating over the packet data network.” APPLE-1004, Abstract, [0002], [0006]-[0007], [0017], [0024], [0034], [0037], [0038], [0039], [0041], [0078], FIG. 7. One type of message service provided over the SIP network is an IM service (*PSMS*). APPLE-1004, [0033]. In an IMS network like the one taught by Horvath, the IM service would be administered by an application server within the IMS domain of the SIP network, as was well known. *See, e.g.*, APPLE-1074, [0069] (“The IMS domain includes standard network elements such as HSS (Home Subscriber Server) 608, BGCF (Break out Gateway Control Function) 610, S-CSCF (Serving Call Session Control Function) 612, I-CSCF 614,...IMM (Instant Multimedia Messaging) application server 626, and Presence application server 628.”); APPLE-1075, [0005]-[0010] (“FIG. 1 is...a conventional IMS system” includes an “application server” that “enables different services in the IMS network, such as call-forwarding, call waiting, presence and instant messaging”); APPLE-1004, [0039] (“An IMS system also includes application servers that host and execute services for the wireless device 106.”).

123. Horvath teaches that, “[a]lthough only the SMSC 114 is shown as residing in the main memory 306 [of the information processing system 108], any combination of IMS components...can also reside in the main memory 306.” APPLE-1004, [0052]. In other words, the IM application server—a part of the IMS system, as described above—may be part of the same information processing system

108 as the P-CSCF 206, I,S-CSCF 208, and HSS 210. *See* APPLE-1004, [0039], [0052]. And Horvath teaches that “[a]ny suitably configured processing system is similarly able to be used as the information processing system 108,” including, for example, “a personal computer, workstation, or the like.” APPLE-1004, [0052]. Accordingly, Horvath teaches that the IM application service of the IMS network (*PSMS*) and HSS may be part of the same *server*.

124. Accordingly, Horvath-Tsampalis-Kansal includes *a server of a packet switched message service (PSMS)* (e.g., information processing system 108 that hosts any combination of IMS components, including, for example, the IM service and the HSS).

Element [13b2]: that receives information, wherein the information indicates the phone number of the receiving mobile phone;

125. *Supra*, §VIII.A, Analysis of Element [1b] (explaining that a network element (e.g., the HLR and/or HSS) stores the MFCI and receives the requests for MFCI from sending mobile phones).

Element [13c]: wherein the server of the PSMS sends a response in response to receipt of the information;

126. *Supra*, § VIII.A, Analyses of Element [1c] (explaining the network element (e.g., the HLR and/or HSS) responds to requests for MFCI), and Element [13b1] (explaining that the HSS may be hosted on the same information processing system 108 as the IM service).

Element [13d1]: wherein, based at least in part on the response, the sending mobile phone automatically selects a bearer for the message, wherein the bearer is selected from a group including:

127. *Supra*, §VIII.A, Analysis of Element [1d1].

Element [13d2]: a short message service (SMS) bearer;

128. *Supra*, §VIII.A, Analysis of Element [1d2].

Element [13d3]: a packet-switched message bearer supported by a cellular connection between the sending mobile phone and a cellular base station; and

129. *Supra*, §VIII.A, Analysis of Element [1d3].

Element [13d4]: a packet-switched message bearer supported by a wireless local area network (WLAN) connection between the sending mobile phone and a WLAN base station;

130. *Supra*, §VIII.A, Analysis of Element [1d4].

Element [13e]: wherein, after the sending mobile phone automatically selects the bearer, the sending mobile phone formats the message for transmission via the selected bearer;

131. *Supra*, §VIII.A, Analysis of Element [1e].

Element [13f]: wherein, after the message is formatted, the sending mobile phone transmits, using the selected bearer, the message to the receiving mobile phone;

132. *Supra*, §VIII.A, Analysis of Element [1f].

Element [13g]: wherein the sending mobile phone sends a first message to a first receiving mobile phone using the SMS bearer;

133. *Supra*, §VIII.A, Analysis of Element [1g2].

Element [13h]: wherein the sending mobile phone sends a second message to a second receiving mobile phone using the packet-switched message bearer supported by the cellular connection; and

134. *Supra*, §VIII.A, Analysis of Element [1g3].

Element [13i]: wherein the sending mobile phone sends a third message to a third receiving mobile phone using the packet-switched message bearer supported by the WLAN connection;

135. *Supra*, §VIII.A, Analysis of Element [1g4].

Element [13j]: wherein the server of the PSMS receives content of the third message and sends the content to the third receiving mobile phone;

136. *Supra*, §VIII.A, Analyses of Elements [1b], [13b1] (explaining that the HSS may be hosted on the same information processing system 108 as the IM service).

Element [13k]: 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;

137. *Supra*, §VIII.A, Analysis of Element [1i].

Element [13l]: wherein the message client retrieves the destination address and formats the message.

138. *Supra*, §VIII.A, Analysis of Element [1j].

Claim [14]: The system of claim 13, further comprising: a subscriber data store; wherein the server of the PSMS receives an indication that a subscriber of the PSMS has become associated with a mobile phone which has capabilities different than those reflected in the subscriber data store; wherein the server updates the subscriber data store to reflect a change of mobile phone.

139. Horvath-Tsampalis-Kansal renders Claim [14] obvious. As I previously discussed for Element [1b], the MFCI is stored in a “network element” (e.g., the HLS and/or HSS). Horvath’s HSS “comprises a database including profiles associated with each wireless device 106 registered with the IMS,” where the

“profile, for example, includes subscription related information.” APPLE-1004, [0035]. As I previously discussed for Element [13b1], the HSS and IM service (*PSMS*) are part of the same information processing system 108 (*server*). Accordingly, the information processing system 108 includes the HSS and its database of profiles (*a subscriber data store*).

140. Horvath explains how a wireless device can “deregister” from the IMS core, which as explained below, occurs when the device transmits a deregistration message, thereby leaving the device unable to receive messages on the packet-data network. APPLE-1004, [0047], [0053], [0075]. For example, one obvious scenario in which a mobile phone would deregister from the IMS core is when a user of the mobile phone changes to a new mobile phone. Users often registered with the IMS core using a phone number, *e.g.*, a phone number associated with the mobile phone, and the user would have deregistered the phone number of an old mobile phone in favor of registration for a new number associated with a new mobile phone when the mobile phone is changed.

141. Specifically, IMS users are assigned IMS Public User Identities (IMPUs) that “are used by any user to request communications to other users,” and an IMPU can use “telecom numbering” in “the form of a SIP URI ... or the ‘tel:’-URI format.” APPLE-1051, [0017]-[0019]; *see also* APPLE-1004, [0035] (“tel-URI, for example is the telephone number assigned to the wireless device 105”);

APPLE-1051, [0006]-[0030], FIG. 2. When a user's IMPU is defined according to his/her phone number ("telecom numbering"), the user would seek to update his/her IMPU upon obtaining a new mobile phone associated with a new phone number so that the IMPU would correspond to the new phone number of the new mobile phone rather than the old phone number of the old mobile phone.

142. Updating an IMPU involved registering the new IMPU defined by the new phone number and deregistering (also referred to as "unregistering") the IMPU defined by the old phone number. APPLE-1004, [0007], [0053]. De/unregistering from an IMS network conventionally involves transmission of an unregister message from the user's device (*e.g.*, the mobile phone) to the IMS core. APPLE-1066 ("If expires header is set to be Zero in REGISTER message, it means 'DeREGISTER'."); APPLE-1065, 9. The transmitted message to de/unregister the phone number of the old mobile phone from the IMS and the transmitted message to register the phone number of the new mobile phone with the IMS represent an indication that a subscriber of the PSMS has become associated with a mobile phone which has capabilities different than those reflected in the subscriber data store. And Horvath teaches that all of this registration information is stored in the profile database of the HSS. APPLE-1005, [0035], [0044].

143. Accordingly, Horvath-Tsampalis-Kansal's *server of the PSMS* (*e.g.*, information processing system 108, hosting the IM service and including the HSS)

receives an indication that a subscriber of the PSMS has become associated with a mobile phone which has capabilities different than those reflected in the subscriber data store (e.g., the information processing system 108 receives an SIP “deregister” message for a subscriber’s old mobile phone and an SIP “register” message for the subscriber’s new mobile phone); *wherein the server updates the subscriber data store to reflect a change of mobile phone* (e.g., the information processing system 108 updates the HSS’s profile database with the new registration information).

Claim [15]: The system of claim 14, wherein the subscriber data store is updated to reflect that the subscriber is no longer associated with a mobile phone which is identified by the subscriber data store.

144. Horvath-Tsampalis-Kansal renders obvious Claim [15]. As I previously discussed for Claim [14], the database HSS 210 (*subscriber data store*) is updated to reflect a deregistration of the IMPU of an old mobile phone, and a registration of the IMPU of a new mobile phone (*is updated to reflect that the subscriber is no longer associated with a mobile phone which is identified by the subscriber data store*).

Claim [16]: The system of claim 15, wherein the subscriber data store is located outside of a cellular core network.

145. *Supra*, §VIII.A, Analysis of Claim [5].

Claim [17]: The system of claim 13, wherein the message client displays at least one of a right arrow and a left arrow simultaneously with the third message.

146. *Supra*, §VIII.A, Analysis of Claim [8].

Claim [18]: The system of claim 13, wherein: a phone number associated with a plurality of receiving mobile wireless devices is received by the server of the PSMS; and the server of the PSMS sends a response in response to receipt of the phone number associated with the plurality of receiving mobile wireless devices indicating that each one of the plurality of receiving mobile wireless devices corresponds to a subscriber of the service.

147. Horvath-Tsampalis-Kansal renders obvious Claim [18]. As I previously discussed for Element [1b], the HSS is a network element that would have stored MFCD. *See* APPLE-1004, [0035]; APPLE-1005, [0039]. The HSS is “part of a session initiation protocol (‘SIP’) network” and more specifically “part of an Internet Protocol multimedia subsystem (‘IMS’) core that supports the SIP network.” *See* APPLE-1004, [0033]. “An IMS network usually implements private and public subscriber identities, known as an IP multimedia private identity (IMPI) and an IP multimedia public identity (IMPU).” APPLE-1076, [0004]. “An IMPI is unique to a subscriber terminal (e.g., a telephone), which may have multiple IMPUs (e.g., a telephone URI and an SIP URI) per IMPI.” *Id.* “An IMPU can be shared between telephones, so both telephones can be reached with the same identity (e.g., a single telephone number for an entire family).” *Id.*; *see also* APPLE-1077, [0015] (describing two different devices that “share a single number” and that the network is able to “deliver[] a notification of an incoming call (e.g., ring tone) to multiple devices”).

148. Because Horvath’s HSS stores subscriber and device profiles, the HSS would have stored information about all of the devices associated with a given IMPU

(e.g., telephone number) along with the capabilities of those devices. *See, e.g.,* APPLE-1084, [0068] (the HSS “comprises information relating to the devices associated with the subscribers and may specifically comprise a list of the devices associated with **each** public identity as well as various data for these devices” including “information of the capabilities of the devices, such as an indication of which services it can support”). Indeed, it was well known to store profiles that identify multiple devices associated with a given subscriber and the addressing information at which those devices can be contacted. *See, e.g.,* APPLE-1053, 5:30-33 (describing a “resource file” that “includes information, such as the protocols and connectivity bearers supported by, the capabilities of, and/or the security associations relating to respective devices operated by, or otherwise associated with, the individual”), 9:34-41 (“the resource file will be directly linked to the telephone number in the contact entry”).

149. When a sending mobile phone requests MFCI associated with a telephone number from the “network element” (*e.g.*, HSS), the profile returned by the HSS would have included information about all of the devices associated with the telephone number, along with their capabilities. *See* APPLE-1005, [0061] (“the 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)...to find out if they are capable of receiving an MMS message”).

150. Accordingly, in Horvath-Tsampalis-Kansal, *a phone number associated with a plurality of receiving mobile wireless devices is received by the server of the PSMS* (e.g., the HSS of the information processing system 108 receives information—through, for example, SIP registrations—about multiple devices associated with the same IMPU and stores the information a profile of the associated subscriber); *and the server of the PSMS sends a response in response to receipt of the phone number associated with the plurality of receiving mobile wireless devices* (e.g., when a sending mobiles phone sends an MFCI request to the HSS for a receiving mobile phone’s telephone number, and the HSS provides a response based on the information contained in the profile associated with the telephone number) *indicating that each one of the plurality of receiving mobile wireless devices corresponds to a subscriber of the service* (e.g., because the profile contains information about multiple devices associated with the telephone number, the response from the HSS would include MFCI for each of the devices, as well as subscriber information).

Claim [19]: The system of claim 13, wherein: a phone number associated with a plurality of receiving mobile wireless devices is received by the server of the PSMS; and the server of the PSMS sends a response in response to receipt of the phone number associated with the plurality of receiving mobile wireless devices indicating that a message to the plurality of receiving mobile wireless devices should not be sent via the service.

151. *Supra*, §VIII.A, Analysis of Claim [18] (the MFCI returned by the HSS would have included capability and subscription, including those services that

should not be used to send a message—because, for example, the user does not subscribe to a particular service).

Claim [20]: The system of claim 19, wherein: prior to the response sent in response to receipt of the phone number associated with the plurality of receiving mobile wireless devices being sent, the server of the PSMS determines that at least one of the plurality of receiving mobile wireless devices has an inactive status with the PSMS.

152. *Supra*, §VIII.A, Analysis of Claim [18].

153. Horvath describes that the HSS stores information about the registration status of wireless devices. *See* APPLE-1004, [0041], [0073]. Specifically, Horvath describes that “[t]he S-CSCF, at step 510, receives filter criteria from the HSS 210 to notify specific application servers that the wireless device 106 has registered with the packet data network 102.” APPLE-1004, [0073]. Accordingly, the profiles stored in the HSS would store information regarding whether certain mobile devices are registered with the packet-data network. *See id.* It was well known that, in IMS networks, a mobile device that has been deregistered is considered “inactive.” *See, e.g.*, APPLE-1078, [0045] (“the IP Multimedia Subsystem, in response to receipt of a de-registration request, at step 803 de-registers mobile subscriber station 100 at the HSS via path 703 and transmits at step 804 an extended mobile station inactive (MSINACT) message via path 7-6 to Home Location Register 111”).

154. Accordingly, in Horvath-Tsampalis-Kansal, *prior to the response sent in response to receipt of the phone number associated with the plurality of receiving mobile wireless devices being sent* (e.g., prior to the HSS responding to a request for MFCI for a telephone number associated with a number of mobile devices), *the server of the PSMS determines that at least one of the plurality of receiving mobile wireless devices has an inactive status with the PSMS* (e.g., to create a response to a request for MFCI, the HSS accesses a profile containing, in part, registration information for the mobile devices associated with the telephone number, including where a mobile device has been deregistered—a type of inactive status—from the packet-data network).

Element [21pre1]: A method performed by

155. *Supra*, §VIII.A, Analysis of Element [1pre1].

Element [21pre2]: a sending mobile device that transmits short message service (SMS) messages and non-SMS based packet switched messages, the method comprising:

156. *Supra*, §VIII.A, Analysis of Element [1pre2].

Element [21a]: sending first information representing a first phone number of a first receiving mobile device to a server;

157. *Supra*, §VIII.A, Analyses of Elements [1a]-[1b], Claim [5].

Element [21b]: receiving a first response to the sending of the first information;

158. *Supra*, §VIII.A, Analysis of Element [1c].

Element [21c]: based at least in part on the first response, automatically selecting an SMS bearer for a first message;

159. *Supra*, §VIII.A, Analyses of Elements [1d1], [1d2], [1g2].

Element [21d]: formatting the first message for transmission via the SMS bearer;

160. *Supra*, §VIII.A, Analyses of Elements [1d2], [1e], [1g2].

Element [21e]: transmitting the first message using the SMS bearer;

161. *Supra*, §VIII.A, Analyses of Elements [1f], [1g2].

Element [21f]: retrieving a destination address of a second message, wherein the destination address of the second message represents at least a second phone number of a second receiving mobile device;

162. *Supra*, §VIII.A, Analyses of Elements [1a], [1g1], [1g3].

Element [21g]: sending the destination address of the second message to the server;

163. *Supra*, §VIII.A, Analyses of Elements [1b], [1g3].

Element [21h]: receiving a second response to the sending of the destination address of the second message;

164. *Supra*, §VIII.A, Analyses of Elements [1c], [1g3].

Element [21i]: based at least in part on the second response, automatically selecting a first packet-switched message bearer for the second message;

165. *Supra*, §VIII.A, Analyses of Elements [1d1], [1d3], [1g3].

Element [21j]: formatting the second message for transmission via a cellular connection between the sending mobile device and a cellular base station;

166. *Supra*, §VIII.A, Analyses of Elements [1d3], [1e], [1g3].

Element [21k]: transmitting, via the cellular connection, the second message to the second receiving mobile device;

167. *Supra*, §VIII.A, Analyses of Elements [1f], [1g3].

Element [21l]: retrieving a destination address of a third message, wherein the destination address of the third message represents at least a third phone number of a third receiving mobile device;

168. *Supra*, §VIII.A, Analyses of Elements [1a], [1g1], [1g4].

Element [21m]: sending the destination address of the third message to the server;

169. *Supra*, §VIII.A, Analyses of Elements [1b], [1g4].

Element [21n]: receiving a third response to the sending of the destination address of the third message, wherein the third response indicates that a plurality of receiving mobile devices corresponding to the destination address of the third message are associated with a packet switched message service (PSMS);

170. *Supra*, §VIII.A, Analyses of Elements [1c], [1g4], and Claim [18].

Element [21o]: based at least in part on the third response, automatically selecting a second packet-switched bearer for the third message;

171. *Supra*, §VIII.A, Analyses of Elements [1d1], [1d4], [1g4], and Claim [18].

Element [21p]: formatting the third message for transmission via the second packet-switched bearer and a wireless local area network (WLAN) connection between the sending mobile device and a WLAN base station; and

172. *Supra*, §VIII.A, Analyses of Elements [1e], [1d4], [1g4].

Element [21q]: transmitting, using the second packet-switched bearer and the WLAN connection, the third message to the plurality of receiving mobile devices;

173. *Supra*, §VIII.A, Analyses of Elements [1f], [1g4], and Claim [18].

Element [21r]: 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.

174. *Supra*, §VIII.A, Analysis of Element [1i].

Claim [22]: *The method of claim 21, wherein each one of the first response, second response and third response originates from a server which is located outside of a cellular network.*

175. *Supra*, §VIII.A, Analyses of Claims [5], [21].

Claim [23]: *The method of claim 22, further comprising: sending a group based message to the third receiving mobile device and to a fourth receiving mobile device, via the PSMS and the WLAN, wherein the group based message comprises video information.*

176. Horvath-Tsampalis-Kansal renders obvious Claim [23]. 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 user composes. *See e.g.*, APPLE-1005, [0004] (“list of delivery recipients” for “a message”), [0009], [0032], [0055] (“groups of recipients”), FIG. 4 (below).

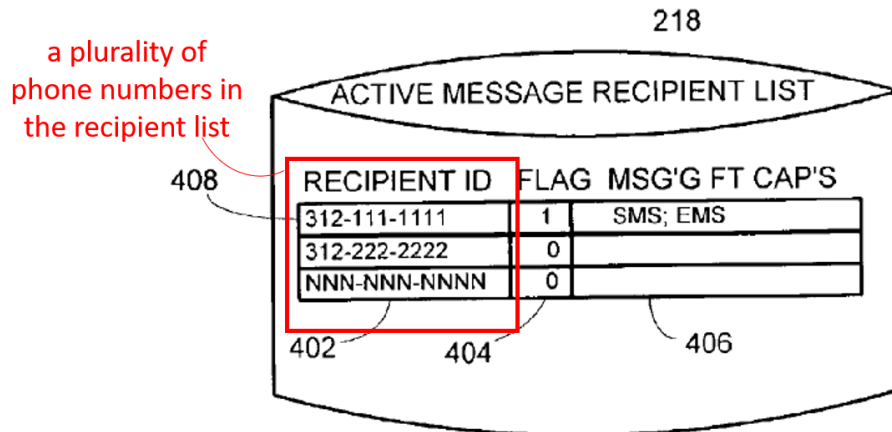


FIG. 4

APPLE-1005, FIG. 4 (Annotated)

177. Horvath-Tsampalis-Kansal’s method would have comprised sending a group based message to the third receiving mobile device and to a fourth receiving mobile device, in accordance with at least Tsampalis; when the third and fourth receiving devices are both subscribers of IM and both have an active status, the group based message is sent to the two receiving mobile devices via IM and the “802.11 network” (*via the PSMS and the WLAN*). *Supra*, §VIII.A, Analyses of Elements [1d4], [1e], [1f], [1g4], and Claim [22].

178. Moreover, as I previously discussed for Claim [4], IM has the option of attaching multimedia files, such as video, such that the group based IM comprises *video information*. See APPLE-1004, [0029], [0033]-[0034], [0068]-[0069] (“multimedia message” such as “a video media component”); 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.”), page 11, (“integrated voice, video, and data services in IM systems.”).

Claim [24]: The method of claim 21, wherein the first phone number is not listed as being associated with a subscriber of the PSMS at the time the first response is received.

179. *Supra*, §VIII.A, Analysis of Claim [3].

Claim [25]: The method of claim 21, wherein the second receiving mobile device is authenticated to the PSMS, via SMS protocol, prior to the transmitting of the second message, wherein the second message is routed via the PSMS; wherein the first receiving mobile device is not authenticated to the PSMS, via SMS

*protocol, prior to receiving at least one SMS message from one of the plurality of receiving mobile devices*⁷.

180. Horvath-Tsampalis-Kansal renders obvious Claim [25]. As I previously discussed for Claim [5], in Horvath-Tsampalis-Kansal, *the sending mobile phone is authenticated to the PSMS via SMS*. In a case where the second receiving mobile device is similarly registered and authenticated with the IMS network and has previously sent an SMS vis the IMS network, the second receiving mobile device would have similarly been *authenticated to the PSMS via SMS*. See APPLE-1004, [0036]; *see also* APPLE-1087, [0007]-[0014]; APPLE-1088, [0019], [0035]; APPLE-1072, [0055]. On the other hand, to the extent that the first receiving mobile device is not registered and authenticated with the IMS network, it would *not [be] authenticated to the PSMS, via SMS protocol, prior to receiving at least one SMS message from one of the plurality of receiving mobile devices*. *Id.*

⁷ The recited “from one of the plurality of receiving mobile devices” is indefinite, as the SMS message received by the first receiving mobile device is received from the sending mobile device, and also because the “plurality of receiving mobile devices” recited in Claim 21 that Claim 26 depends from is “corresponding to the destination address of the third message” which is not the “at least one SMS message” recited in Claim 26.

Claim [27]: The method of claim 21, wherein the destination address of the second message is a sequence of decimal numbers and the destination address of the third message is a sequence of decimal numbers.

181. *Supra*, §VIII.A, Analyses of Claims [1], [21].

182. Horvath describes that 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.” APPLE-1004, [0038]. In other words, when the wireless device is registered with the packet-data network, it has an IP address that identifies its “location” (*destination address*). An IP address is *a sequence of decimal numbers*.

Claim [28]: The method of claim 21, wherein the sending mobile device simultaneously displays a left arrow and a right arrow in an interface which displays message content corresponding to a plurality of messages exchanged between the sending mobile device and a receiving mobile device associated with the PSMS.

183. *Supra*, §VIII.A, Analysis of Claim [8].

Element [29pre1]: A method performed by

184. *Supra*, §VIII.A, Analysis of Element [1pre1].

Element [29pre2]: a sending mobile device that transmits short message service (SMS) messages and non-SMS based packet switched messages, the method comprising:

185. *Supra*, §VIII.A, Analysis of Element [1pre2].

Element [29a]: sending first information representing a first phone number of a first receiving mobile device to a server;

186. *Supra*, §VIII.A, Analyses of Elements [1a]-[1b], and Claim [5].

Element [29b]: receiving a first response to the sending of the first information;

187. *Supra*, §VIII.A, Analyses of Elements [1c], [1g1], [1g2].

Element [29c]: based at least in part on the first response, automatically selecting an SMS bearer for a first message;

188. *Supra*, §VIII.A, Analyses of Elements [1d1], [1d2], [1g2].

Element [29d]: formatting the first message for transmission via the SMS bearer; and

189. *Supra*, §VIII.A, Analyses of Elements [1e], [1g2].

Element [29e]: transmitting the first message using the SMS bearer;

190. *Supra*, §VIII.A, Analyses of Elements [1f], [1g2].

Element [29f]: retrieving a destination address of a second message, wherein the destination address of the second message represents at least a second phone number of a second receiving mobile device;

191. *Supra*, §VIII.A, Analyses of Elements [1a], [1g1], [1g3].

Element [29g]: sending the destination address of the second message to the server;

192. *Supra*, §VIII.A, Analyses of Elements [1b], [1g3].

Element [29h]: receiving a second response to the sending of the destination address of the second message indicating that the second message is not to be sent to at least one of a first plurality of receiving mobile devices corresponding to the destination address of the second message via a packet switched message service (PSMS);

193. *Supra*, §VIII.A, Analyses of Element [1c] and Claims [6], [19].

Element [29i]: based at least in part on the second response, automatically selecting the SMS bearer for sending the second message to the at least one of the first plurality of receiving mobile devices;

194. *Supra*, §VIII.A, Analyses of Elements [1d1]-[1d2], [1g2], and Claims [19]-[20].

Element [29j]: formatting the second message for transmission via a cellular connection between the sending mobile device and a cellular base station;

195. Horvath-Tsampalis-Kansal renders obvious Element [29j]. *Supra*, §VIII.A, Analyses of Elements [1d2]-[1d3], [1e], and Claim [5]. Both the traditional CDMA/GSM type of circuit-services network and the EV-DO/GPRS/UMTS type of packet-data network have a cellular connection between the sending mobile device and a cellular base station, and both networks can be SMS bearers used to transmit SMS messages, although the packet-data network is the default bearer to unburden the circuit-services network. *See, e.g.*, APPLE-1053, FIG. 4, 12:54-13:60 (“an antenna 12 for transmitting signals to and for receiving signals from one or more base stations (BS’s),” which are “part of one or more cellular or mobile networks that each includes elements required to operate the network” and may “be coupled to a signaling GPRS (General Packet Radio Service) support node (SGSN) 30” and the MSC of a GSM circuit-services network).

Element [29k]: transmitting, via the cellular connection, the second message to the at least one of the first plurality of receiving devices;

196. *Supra*, §VIII.A, Analysis of Element [1f].

Element [29l]: retrieving a destination address of a third message, wherein the destination address of the third message represents at least a third phone number of a third receiving mobile device;

197. *Supra*, §VIII.A, Analysis of Element [1a].

Element [29m]: sending the destination address of the third message to the server;

198. *Supra*, §VIII.A, Analysis of Element [1b].

Element [29n]: receiving a third response to the sending of the destination address of the third message, wherein the third response indicates that a second plurality of receiving mobile devices corresponding to the destination address of the third message are associated with the PSMS;

199. *Supra*, §VIII.A, Analyses of Element [1c] and Claim [18].

Element [29o]: based at least in part on the third response, automatically selecting a packet-switched bearer for the third message;

200. *Supra*, §VIII.A, Analyses of Element [1d1] and Claim [18].

Element [29p]: formatting the third message for transmission via the packet-switched bearer and a wireless local area network (WLAN) connection between the sending mobile device and a WLAN base station; and

201. *Supra*, §VIII.A, Analyses of Elements [1d4], [1e].

Element [29q]: transmitting, using the packet-switched bearer and the WLAN connection, the third message to the second plurality of receiving mobile devices.

202. *Supra*, §VIII.A, Analyses of Elements [1f], [1g4], and Claim [18].

Claim [30]: The method of claim 29, wherein the sending mobile phone simultaneously displays a left arrow and a right arrow in an interface which displays message content corresponding to a plurality of messages exchanged between the sending mobile device and a receiving mobile device associated with the PSMS.

203. *Supra*, §VIII.A, Analysis of Claim [8].

IX. GROUND 1B: OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES

A. Overview of Dorenbosch

204. Dorenbosch explains that then-conventional “IM systems typically rel[ied] on a best-effort delivery mechanism in which a message intended for a target buddy is delivered if the IM login server determines that the target buddy is available.” APPLE-1006, [0005]. “If the IM login server determine[d] that the target buddy is not available, the message [was] dropped.” *Id.* As illustrated in FIG. 1 (below), Dorenbosch mitigates these issues with “an instant message proxy that is capable of maintaining the availability status of a mobile subscriber when the communicati[on] to the subscriber is temporarily broken.” APPLE-1006, [0002].

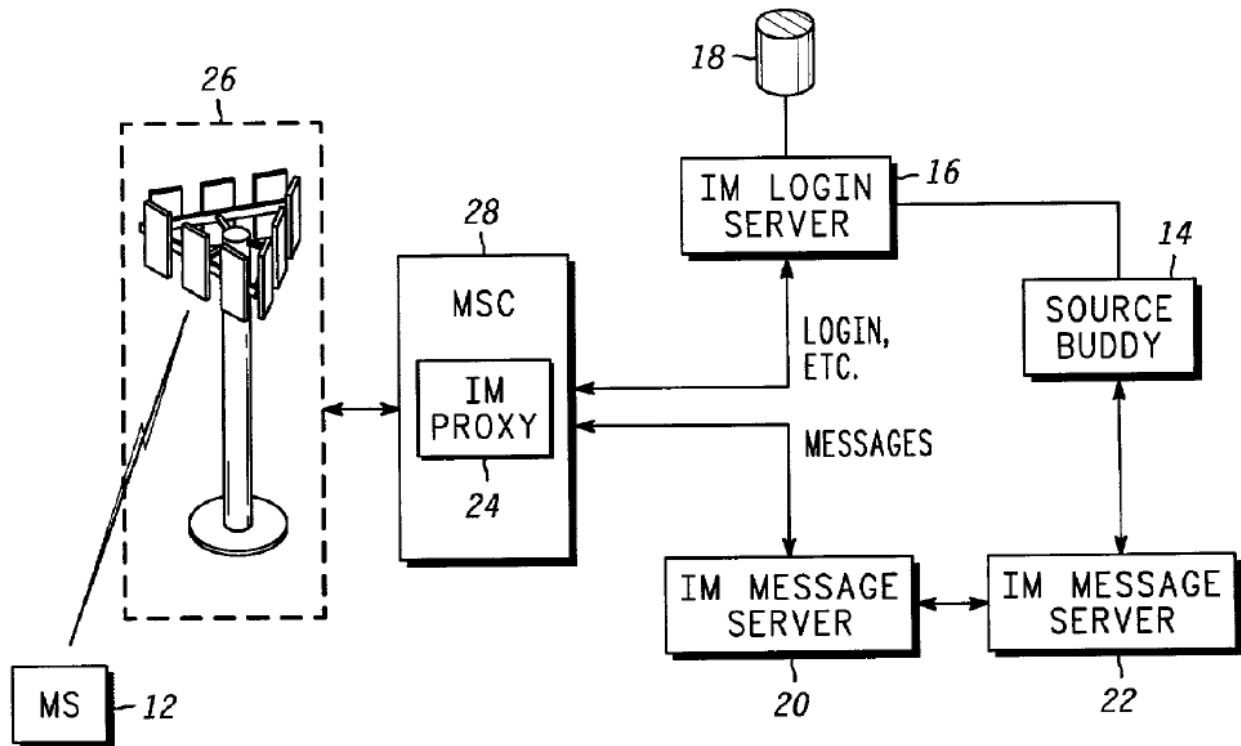


FIG. 1

APPLE-1006, FIG. 1

205. In Dorenbosch, if a mobile IM subscriber temporarily loses network coverage and is therefore unavailable to receive messages, the IM proxy will continue to store messages in the message buffer and retry sending the message(s) (e.g., a predetermined number of times within a predetermined time period) before dropping the message(s) from the buffer. APPLE-1006, [0020], [0024]. Dorenbosch describes a retry counter and timer that “enable the IM proxy 24 to maintain its IP connection with the IM login server 16, and therefore maintain the mobile subscriber’s registered status with the IM login server 16, when the mobile subscriber 12 becomes temporarily unavailable due to roaming or the like.” APPLE-1006, [0020]. In this way, even when a mobile subscriber has poor network coverage, the Dorenbosch interface reflects availability of the mobile subscribers. APPLE-1006, [0024]; *see also id.* [0030]. Only after the mobile subscriber “becomes unavailable for receiving instant messages for a period of time that exceeds the number of retries allotted by and programmed into the retry counter and/or the predetermined time period allotted by the timer” will the IM proxy drop “its connection with the IM login server 16” and “indicat[e] to the IM server 16 that the mobile subscriber 12 is unavailable.” APPLE-1006, [0028]-[0029].

B. Combination of Horvath, Tsampalis, Kansal and Dorenbosch

206. A POSITA would have expected the known problems of wireless network disruption and general unreliability to have been exasperated when

operating real-time IM services using wireless devices, as contemplated by Horvath, Tsampalis and Kansal, and their combination. APPLE-1004, [0033]; APPLE-1047, [0007] (describing that when networks are unreliable “messages sent by real-time messaging clients often fail to get delivered to the recipient”). Dorenbosch provides techniques that mitigate the impact of unreliable wireless networks on IM services. APPLE-1006, [0005] (by moving “in and out of service during an IM session, it may not be possible for the mobile station to maintain a reliable connection with the login server”), [0021].

207. As discussed in §IX.A-B, Dorenbosch teaches an IM proxy caching IM messages for maintaining presence status for IM subscribers, attempting redelivery of messages that are directed to IM subscribers who lose network coverage, and adjusting recipient IM subscriber presence status when the cached messages cannot be delivered after a number of retries. APPLE-1006, [0020], [0024], [0029], [0030], [0039]-[0040]. It would have been obvious to integrate Dorenbosch’s techniques into the combination to enhance Horvath’s IM communications over packet-data networks. Multiple reasons would have prompted a POSITA to implement this combination.

208. First, a POSITA would have been motivated to apply Dorenbosch’s delivery retry techniques to the combination to reduce the number of dropped messages when communicating through IM. APPLE-1006, [0021], [0024], [0026],

[0030]. Dorenbosch's IM proxy maintains a consistent connection with the IM server so that it can cache messages and retry delivering them when a mobile device temporarily loses network connection, which "minimizes the occurrence of instant messages intended for the mobile subscriber being dropped." APPLE-1006, [0021], [0024], [0026], [0030].

209. Second, a POSITA would have found obvious that maintaining a connection to the IM system on behalf of the mobile device, *e.g.*, with an IM proxy, would have allowed the "the mobile subscriber [to] continue[] to appear available to IM buddies when the mobile subscriber is roaming or temporarily out of service even after the IM proxy unsuccessfully attempts to send an instant message to the mobile subscriber." APPLE-1006, [0030]. This would have created a more pleasing experience for users of both the sending and receiving devices. *See* APPLE-1047, [0007].

210. 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) and with known IM protocols. *See* APPLE-1006, [0017]-[0020]. Because the combination interfaces with conventional IM services, as taught by Horvath, the

combination with Dorenbosch described above would not fundamentally change any of the other operations of the combination.

X. GROUND 1B: MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '600 CLAIMS UNPATENTABLE

A. The Horvath-Tsampalis-Kansal-Dorenbosch Combination Renders Claims 2, 26 Obvious

Element [2a]: The method of claim 1, wherein at the time the first message is sent to the first receiving mobile phone: a phone number corresponding to the first receiving mobile phone is on a list of subscribing addresses which is stored on a server of the PSMS; and

211. Horvath-Tsampalis-Kansal-Dorenbosch renders Element [2a] obvious. As I previously discussed for Element [1b], *supra*, the response from the network element (HLR and/or HSS) with the MFCI would also include information about the services to which the wireless device 106 is subscribed (*e.g.*, an IM service, which is a *PSMS*). In Horvath-Tsampalis-Kansal-Dorenbosch, it would have been obvious the response with the MFCI would have further included the user's communication preferences amongst the services identified in the MFCI.

212. For example, Kansal teaches that "the conversion of a message from one format to a particular sending format may be based on programmed and/or detected preferences, constraints, and/or availability of a recipient to receive messages of a certain format." APPLE-1042, [0078]. Kansal leaves to a POSITA the implementation details regarding how the sending mobile phone detects these preferences. *See generally*, APPLE-1042. However, because the preference

information is used to determine the “sending format,” at least one obvious implementation would have been for the preference information to be included with the MFCI.

213. Horvath’s HSS already “comprises a database including profiles associated with each wireless device 106 registered with the IMS,” where the “profile, for example, includes subscription related information.” APPLE-1004, [0035]. And it was known that preference and capability information would have been stored together as part of the same profile. *See, e.g.*, APPLE-1063, [0015], [0083], [0110] (describing a “contacts manager 222 [that] is configured to manage a list of the subscriber’s contacts (including groups),” which “includes one or more communication devices assigned to said contact persons, capabilities of said devices, sender’s and/or receivers’ preferences, if any, related to destination device, message layout and/or format, etc.”), [0112]; APPLE-1069, 3:8-21 (“Each mobile station 16 is associated with a home location register (HLR) 20 in the circuit-switched network 4 that stores subscription, current location, and preference information for the mobile station 16”); APPLE-1068, claim 8 (“the bearer is specified in accordance with a pre-determined user preference”); APPLE-1064, 3:26-32, 4:49-54, 9:41-65.

214. When the MFCI indicates that the first receiving mobile phone prefers communication via SMS, Kansal teaches that the sending mobile phone would be configured to utilize an SMS bearer, even though the first receiving mobile phone is

a subscriber of other services (e.g., MMS and/or IM). See APPLE-1042, [0078]. In these instances in Horvath-Tsampalis-Kansal-Dorenbosch, *at the time the first message is sent to the first receiving mobile phone* (e.g., when the sending mobile phone sends a first message to a first receiving mobile phone using the SMS bearer): *a phone number corresponding to the first receiving mobile phone is on a list of subscribing addresses which is stored on a server of the PSMS* (e.g., the MFCI indicates that the first receiving mobile phone is subscribed to an IM service—which would also store the subscription information—but the MFCI indicates that the first receiving mobile phone currently prefers to receive communications via SMS).

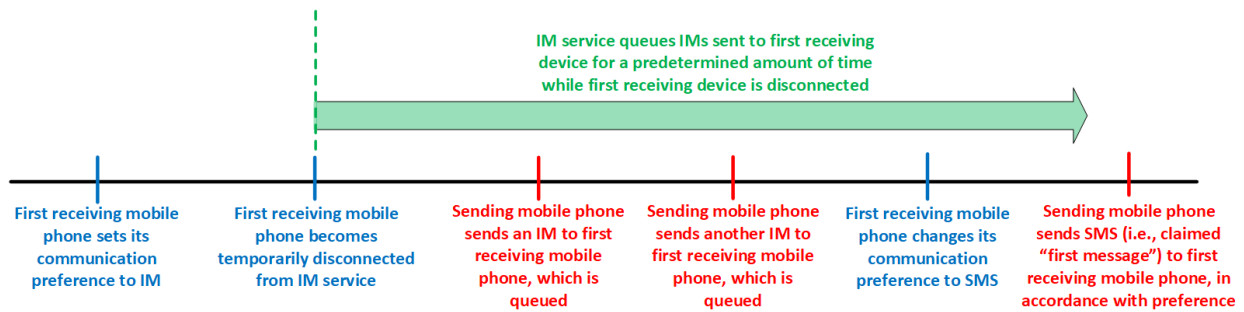
Element [2b]: a plurality of messages sent by the sending mobile phone, to the first receiving mobile phone, via the PSMS, are queued on a server of the PSMS.

215. Horvath-Tsampalis-Kansal-Dorenbosch renders Element [2b] obvious. As I previously discussed in §IX.B, *supra*, Horvath-Tsampalis-Kansal-Dorenbosch includes an IM proxy (*a server of the PSMS*) that queues messages when a receiving mobile phone becomes temporarily disconnected from the network. See APPLE-1006, [0020], [0024], [0028]-[0030].

216. As I previously discussed for Element [2a], *supra*, a POSITA would have further found it obvious that the response with the MFCI would have included the user's communication preferences amongst the services identified in the MFCI. A POSITA would have recognized that this information would have changed at any time a user updated the preference (e.g., when they entered a meeting). See, e.g.,

APPLE-1064, 8:43-9:20 (“For example, during a meeting,...User A may configure the presence management module 700 to indicate to Users B and C that the only communication channels available during the meeting are instant messaging, SMS and/or email.”); APPLE-1070, 11:4-9 (“These are preferences relating to the users activity at a particular time. For example, the user may designate that audio messages are not to be sent while in a meeting, when sleeping, or at any time in which an audio message would be disruptive or otherwise undesirable.”); APPLE-1061, [0024].

217. From the above teachings, one example scenario would have been shown in the below diagram.



218. In this example scenario, a receiving mobile phone would have temporarily lost connection to an IM service, received a plurality of instant messages that were queued by the IM service for a predefined amount of time in case the receiving mobile phone was able to reestablish connection, and during the temporary connection loss, changed its communication preference to SMS (e.g., because the user walked into a meeting). Thus, in this obvious scenario, *a plurality of messages*

sent by the sending mobile phone, to the first receiving mobile phone, via the PSMS, are queued on a server of the PSMS.

Claim [26]: The method of claim 21, wherein the second receiving mobile device is not connected to the PSMS during the entire time between which the destination address of the second message is sent and the second response is received, wherein the second message is routed via the PSMS.

219. Horvath-Tsampalis-Kansal-Dorenbosch renders Claim [26]. As I previously discussed for Element [2b], the IM proxy queues the IMs, in at least one case until the first receiving mobile phone reconnects to the IM proxy.

220. Accordingly, in Horvath-Tsampalis-Kansal-Dorenbosch, ***the second receiving mobile device is not connected to the PSMS during the entire time between which the destination address of the second message is sent and the second response is received*** (e.g., the second receiving mobile device is temporarily disconnected from the IM service as a result of poor network coverage), ***wherein the second message is routed via the PSMS*** (e.g., the IM proxy utilizes a message queue or buffer to accept and store messages while the second receiving mobile device is temporarily disconnected).

XI. CONCLUSION

221. For all the reasons I have noted in the foregoing paragraphs, claims 1-30 of the '600 Patent are obvious in view of the references discussed above.

222. 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)	23
E.3. Conference Presentations without Proceedings	23
F. Other	23
F.1. Submitted Journal Papers	23
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	24
G. Research Proposals and Grants (Principal Investigator)	24
H. Research Proposals and Grants (Contributor)	27
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
Interim Department Chair	University of Florida	July 2025–Present
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 the use of AI in generating non-consensual imagery. Now Research Scientist at ActiveFence.
- Seth Layton** University of Florida
Fall 2020–Summer 2025
Detecting deepfakes in audio samples. Now Research Scientist at PinDrop.
- 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
- Tyler Tucker** University of Florida
Fall 2021–Summer 2025
Evaluating the security of Bluetooth/cellular radios. Now: Associate at the Analysis Group.

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

Kevin Warren University of Florida
Fall 2019–Summer 2025
Detecting deepfake audio through linguistic information. Now: Associate at the Analysis Group.

2. Ph.D. Students Supervised

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

Jordan Greene University of Florida
Fall 2025–Present
Cellular network security.

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.

Aviva Smith University of Florida
Fall 2025–Present
Detecting Deepfakes.

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 malcode through cellular infrastructure.

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

Frank Park Georgia Institute of Technology

Fall 2008–Spring 2010

Research on multi-factor authentication using cellular phones. Left program after failing comprehensive exam to join startup.

Ferdinand Schober Georgia Institute of Technology

Fall 2009–Summer 2010

Developed mechanisms for smart networks and smart mobile devices to fight infection and provide remote remediation. Returned to Microsoft.

4. M.S. Students Supervised

Chaitrali Amrutkar Georgia Institute of Technology

Fall 2008–Spring 2009

Research on improving performance of security critical functions in IMS cellular core. Completed her Ph.D with me at GT.

Logan Blue University of Florida

Fall 2015–Spring 2016

Investigated problems of cellular and network security.

David Dewey Georgia Institute of Technology

Fall 2009–Spring 2010

Research on security issues caused by transitive trust assumptions in the Windows COM infrastructure. Completed his Ph.D. with me at GT.

Christopher Grayson Georgia Institute of Technology

Fall 2012–Fall 2013

Developed continuous authentication mechanisms using the multitude of sensors available on a mobile phone. Now at Bishop Fox Consulting (industry).

Young Seuk Kim Georgia Institute of Technology

Fall 2012–Fall 2013

Performed research that compared the security vulnerabilities found in the traditional and mobile web.

Daniel Komaromy Georgia Institute of Technology

Fall 2008–Summer 2009

Research on building a real-time streaming audio system using attribute-based crypto for broadcast encryption.

Nigel Lawrence Georgia Institute of Technology

Fall 2011–Spring 2012

Discovered hijacking attacks in SNMPv3, a widely used and thought to be secure network management protocol. Now at Solute (industry).

Philip Marquardt Georgia Institute of Technology

Fall 2009–Present

Research on developing an iPhone application to prevent individuals from being profiled by Shopper Loyalty Programs. First with MIT Lincoln Labs, now Raytheon

Rishikesh Naik Georgia Institute of Technology

Fall 2008–Spring 2010

Research on converting expensive cryptographic primitives (e.g., Secure Function Evaluation) into efficient applications for mobile phones. Now with Cisco Systems.

Ashish Nautiyal 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. Daniel Olszewski, Tyler Tucker, Kevin Butler, and Patrick Traynor. SoK: Towards a Unified Approach to Applied Replicability for Computer Security. In *Proceedings of the USENIX Security Symposium (Security)*, 2025.
2. Daniel Olszewski, Allison Lu, Anna Crowder, Nathaniel Bennett, Seth Layton, Sri Hrushikesh Varma Bhupathiraju, Tyler Tucker, Siddhant Kalgutkar, Hunter Ver Helst, Carson Stillman, Kevin Butler, Sara Rampazzi, and Patrick Traynor. "Raise Your Hand If You've Been Personally Victimized By A Lack Of Reproducibility": On Reproducibility in Tier 2 Security Conferences. In *Proceedings of ACM Conference on Reproducibility and Replicability (REP)*.
3. 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.
4. 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%).
5. Anna Crowder, Allison Lu, Kevin Childs, Carson Stillman, Patrick Traynor, and Kevin Butler. Data to Infinity and Beyond: Examining Data Sharing and Reuse Practices in the Computer Security Community. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2025.
6. 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%).
7. 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%).

8. 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%).
9. 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%).
10. 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%).
11. 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).
12. 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%).
13. 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.
14. 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%).
15. 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%).
16. 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%).
17. 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%).
18. 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%).
19. 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.

20. 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%).
21. 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%).
22. 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%).
23. 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%).
24. 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.
25. 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.
26. 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%).
27. 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%).
28. 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.
29. 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%).
30. 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).
31. 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).

32. 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%).
33. 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%).
34. 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%).
35. 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%).
36. Luis 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%).
37. 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%.
38. 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%.
39. 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%.
40. 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.
41. 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.
42. 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%).
43. 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%).

44. 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%).
45. 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%).
46. 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%).
47. 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%).
48. 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%).
49. 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%).
50. 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%).
51. 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%).
52. 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%).
53. 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%).
54. 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%).
55. 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%).
56. 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%).
57. Bradley Reaves, Ethan Shernan, Adam Bates, Henry Carter, and Patrick Traynor. Boxed Out: Blocking Cellular Interconnect Bypass Fraud at the Network Edge. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2015. (Acceptance Rate: 15.7%).

58. 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%).
59. 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%).
60. 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%).
61. 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%).
62. 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%).
63. 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).
64. 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%).
65. 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).
66. 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).
67. 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%).
68. 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%).
69. 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%).
70. 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%).

71. 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%).
72. 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%).
73. 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%).
74. 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%).
75. 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%).
76. 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%).
77. 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%).
78. 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%).
79. 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%).
80. 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%).
81. 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%).
82. 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%).
83. 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%).
84. 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%).

85. 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%).
86. 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).
87. 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%).
88. 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%).
89. 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%).
90. 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%).
91. 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%).
92. 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%).
93. 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%).
94. 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%).
95. 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%).
96. Patrick Traynor. Work in Progress Presentations: Fine-Grained Secure Localization for 802.11 Networks. 15th USENIX Security Symposium (SECURITY), August 2006.
97. 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).
98. 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.

Removed for external version.

E.2. Conference Presentations with Proceedings (Non-Refereed)

None.

E.3. Conference Presentations without Proceedings

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.
3. 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.

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. 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.
2. 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.

F.5. Books in Preparation

None.

F.6. Workshops and External Courses

1. 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.
2. Nigel Lawrence and Patrick Traynor. Under New Management: Practical Attacks on SNMPv3. In *Proceedings of the USENIX Workshop on Offensive Technologies (WOOT)*, 2012.
3. 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.
4. 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.
5. 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.
6. 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).
7. Social Engineering and Two-Factor Authentication. Cyber Security Training Eastern Indonesia, August 2024. Financial Innovation Lab (EIFIL) (Denpasar, Bali, Indonesia).
8. DFS Security and Mobile Money Analysis. Cyber Security Training Eastern Indonesia, August 2024. Financial Innovation Lab (EIFIL) (Denpasar, Bali, Indonesia).

G. Research Proposals and Grants (Principal Investigator)

1. Approved and Funded

1. **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
2. **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
3. **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
4. **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

5. **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
6. **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
7. **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
8. **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, Franz 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. *Natalie Delgado, et al. v. Meta Platforms Inc., Case No.: 23-cv-04181 (N.D. Cal.):* Expert witness for the Defense (via Gibson, Dunn & Crutcher, LLP). *October 2025 - Present.*
2. *Google LLC v Headwater Research LLC:* Expert witness for the Plaintiff for Inter Partes Review (via Wolf, Greenfield & Sacks, P.C.). *August 2025 - Present.*
3. *Amazon v Headwater Research LLC:* Expert witness for the Plaintiff for Inter Partes Review (via Perkins Coie, LLP). *August 2025 - Present.*
4. *HBCU Messaging US LP v. Apple, Inc. et al., Civil No. 1:24-cv-1199,:* Expert witness for the Defense (via Fish & Richardson, LLP). *June 2025 - Present.*
5. *PACid v. Citibank, N.A., 1:24-cv-00272-DAE (W.D. Tex.):* Expert witness for the Defense (via Troutman Pepper Locke LLP). *April 2025 - Present.*
6. *Facebook Inc. Derivative Litigation., Consolidated C.A. No. 2018-0307-JTL (Del. Ch.):* Expert witness for the Defense (via Wachtell, Lipton, Rosen & Katz, LLP) *January 2025 - July 2025.*
7. *Averon US, Inc. vs AT&T Inc., Case No. 1:22-cv-01341-TMH:* Expert witness for the Defense (via O'Melveny & Myers, LLP). *November 2024 - September 2025.*
8. *RightQuestion, LLC v. AT&T Inc. et al.,, Case No. 2-24-cv-00094 -JRG:* Expert witness for the Defense (via Duane Morris, LLP). *September 2024 - Present.*
9. *ByteDance Ltd. vs CellSpin Soft, Inc.:* Expert witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). *February 2024 - October 2024.*
10. *Bank of America, N.A., vs PACid:* Expert witness for the Plaintiff for Inter Partes Review (via McNish PLLC). *December 2023 - March 2024.*
11. *Microsoft vs Proxense, LLC:* Expert witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). *November 2023 - July 2025.*
12. *Samsung vs Headwater Research LLC:* Expert witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). *August 2023 - October 2025.*

13. *Advanced Coding Technologies LLC v. ByteDance PTE. Ltd., and TikTok PTE. Ltd.*: Expert witness for the Defense for Non-Infringement (via Fish & Richardson, LLP). *July 2023 - September 2023.*
14. *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). *January 2023 - Present.*
15. *Rubin vs KAHOOT! ASA and KAHOOT! EDU*: Expert witness for the Defendant for Inter Partes Review (via Vasquez Benisek & Lindgren, LLP). *December 2022 - June 2024.*
16. *Telefonaktiebolaget LM Ericsson vs Apple, Inc.*: Expert witness for the Defendant, Non-Infringement and Invalidity (via WilmerHale LLP). *February 2022 - December 2022.*
17. *Wepay Global Payments, LLC v. Bank of America N. A.*: Expert Witness for the Defendant (via WilmerHale LLP) *September 2022 - November 2022.*
18. *Apple vs. R.N Nehushtan Trust Ltd.*: Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). *August 2022 - June 2023.*
19. *Apple/Microsoft vs. Zipit Wireless*: Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). *May 2021 - November 2022.*
20. *Blackberry Inc v MobileIron, Inc*: Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). *January 2021 - March 2021.*
21. *Apple Inc v Seven Networks, LLC*: Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). *August 2019 - November 2020.*
22. *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). *October 2017 - December 2018.*
23. *Huawei v. T-Mobile*: Expert Witness for the Defendant for Non-Infringement (via WilmerHale LLP, Alston & Bird LLP) *June 2016 - December 2017.*
24. *Telefonaktiebolaget LM Ericsson v Apple*: Expert Witness for the Defendant for Non-Infringement, Invalidity (via WilmerHale LLP). *June 2015 - December 2015.*
25. *Mayfonk v Nike*: Expert Witness for the Plaintiff for Infringement/Trade Secrets (via Paul Hastings). *June 2015 - November 2015.*
26. *Maxim Integrated Products v Bank of the West*: Expert Witness for the Defendant for Non-Infringement (via Paul Hastings LLP). *January 2014 - August 2014.*
27. *Maxim Integrated Products v Comerica Inc, et al*: Expert Witness for the Defendant for Non-Infringement (via McKenna, Long & Aldridge LLP). *June 2014 - August 2014.*
28. *William Grecia v. Apple Inc. et al*: Expert Consultant for the Defendant for Invalidity (via Kirkland & Ellis LLP). *July 2014 - August 2014.*
29. *Intertrust Technologies Corp. v. Apple Inc.*: Expert Consultant for Defendant for Invalidity and Non-Infringement (via Kirkland & Ellis LLP). *October 2013 - February 2014.*
30. *Maxim Integrated Products v KeyCorp Bank*: Expert Witness for the Defendant for Non-Infringement (via Calfee, Halter & Griswold LLP) *April 2013 - June 2013.*
31. *Intellectual Ventures LLC vs. Check Point; et al.*: Expert Consultant for the Plaintiff for Infringement (via Susman Godfrey LLP), *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. EPFL Summer Research Institute (SURI), July 2024. École Polytechnique Fédérale de Lausanne (EPFL, Switzerland).
2. Humans vs The Computer Interfaces: The Challenge of Separating Deepfakes/Bots from People. North Central Florida Institute of Internal Auditors (IIA), May 2024.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. The State of Voice Cloning Technology. Federal Trade Commission (FTC) Workshop on Voice Cloning Technologies, January 2020. Washington, DC.
10. 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.
11. 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.
12. 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.
13. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. Bank of America - Colloquium Series, March 2019. Charlotte, NC.
14. 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.
15. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. University of Maryland - Distinguished Colloquium, February 2019. College Park, MD.

16. Responsible Finance for the Digital Client. Foromic Conference, October 2018. Barranquilla, Colombia.
17. 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.
18. Sonar: Detecting SS7 Redirection Attacks Via Call Audio-Based Distance Bounding. CyberSecurity@KAIST Workshop - KAIST, June 2018. Daejeon, South Korea.
19. 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.
20. Panel: The Future of Cybersecurity. SEC Academic Conference - Auburn University, May 2018. Auburn, AL.
21. Sound Principles: Verifying Voice Commands in an IoT World. IoT Security Workshop - Aalto University, September 2017. Helsinki, Finland.
22. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Eurecom Institute, September 2017. Sophia Antipolis, France.
23. Panel: Infrastructure Stability. ITU-T Focus Group Digital Financial Services, December 2016. Geneva, Switzerland.
24. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. ETH Zurich, December 2016. Zurich, Switzerland.
25. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. University of Richmond, October 2016. Richmond, Virginia.
26. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Indiana University, September 2016. Bloomington, Indiana.
27. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Aalto University Computer Science Department Forum, August 2016. Helsinki, Finland.
28. 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.
29. Updated Mobile Money Vulnerability Report. International Telecommunications Union Digital Financial Services Working Group Workshop, May 2016. Washington, DC.
30. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. UF Eye Opener Discovery Breakfast - University of Florida, May 2016. Gainesville, FL.
31. 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.
32. 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.
33. 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.

34. Chasing Telephony Security: Where the Wild Things... Are? University of Florida - Department Colloquium, January 2014. Gainesville, FL.
35. Chasing Telephony Security: Where the Wild Things... Are? Verizon Wireless RNC/Data Center, October 2013. Alpharetta, GA.
36. Chasing Telephony Security: Where the Wild Things... Are? University of Waterloo - CrySP Speaker Series on Privacy, October 2013. Waterloo, ON, Canada.
37. Analyzing Malicious Traffic in Cellular Networks. GSM Association's (GSMA) Mobile Malware Community Workshop, July 2013. Mountain View, CA.
38. Threats to Mobile Devices. US Federal Trade Commission (FTC) Public Forum - Invited Speaker, June 2013. Washington, D.C.
39. Chasing Telephony Security: Where the Wild Things... Are? University of Wisconsin - Madison, Security Seminar, March 2013. Madison, WI.
40. 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.
41. Chasing Telephony Security: Where the Wild Things... Are? Stanford Security Seminar, March 2013. Stanford, CA.
42. Chasing Telephony Security: Where the Wild Things... Are? University of California, Berkeley, Security Group, March 2013. Berkeley, CA.
43. Chasing Telephony Security: Where the Wild Things... Are? Carnegie Mellon University CyLab Seminar, February 2013. Pittsburgh, PA.
44. Chasing Telephony Security: Where the Wild Things... Are? University of Oregon Department of Computer Science Colloquium, November 2012. Eugene, OR.
45. 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.
46. Needles and Haystacks: Digging for Ground Truth on Mobile Malware. ZISC Workshop on Secure Mobile and Cloud Computing, ETH Zurich, June 2012. Zurich, Switzerland.
47. Panel: Advice for Early Career Faculty. CRA Career Mentoring Workshop, February 2012. Washington, D.C.
48. Research Challenges in Cellular and Mobile Network Security. US-China Software Workshop (Co-Sponsored by NSF and NSFC), September 2011. Beijing, China.
49. Mobile Security: Understanding Risks to Critical Infrastructure. Invited Talk: US Department of State East African Workshop on Cyberspace Security, July 2011. Nairobi, Kenya.
50. Tomorrow's Issues: Solving the Mobile Security Threat. Invited Talk: Centre for Secure Information Technologies (CSIT) Queen's University, March 2011. Belfast, Northern Ireland.
51. PinDr0p: Using Single-Ended Audio Features to Determine Call Provenance. Invited Talk: MITRE Corporation, March 2011. Burlington, MA.
52. Defeating Session Hijacking Attacks with Disposable Web Credentials. Invited Talk: Facebook, February 2011. Palo Alto, CA.

53. Understanding the Disruptive Potential of Malware in Cellular Networks. Invited Talk: RSA Conference, February 2011. San Francisco, CA.
54. Panel: Voice Security – Now Just a False Sense of Security and Privacy. Invited Panelist: Mobile Security Symposium, February 2011. San Francisco, CA.
55. Understanding the Disruptive Potential of Malware in Cellular Networks. Invited Talk: Concordia University, May 2010. Montreal, QC, Canada.
56. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Qualcomm Research, March 2010. San Diego, CA.
57. 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.
58. Considerations for EAS Over Cellular Text Messaging Services. 3G Americas Webinar, July 2009.
59. University Telephony Research Panel. Conference on Principles, Systems and Applications of IP Telecommunications (IPTCOMM), July 2009.
60. The Evolving Mobile Landscape: Emerging Security Threats. Mobile Security eConference, SC Magazine, June 2008.
61. Characterizing the Impact of Rigidity on the Security of Cellular Networks. University of Washington, February 2009. Seattle, WA.
62. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Microsoft Research, February 2009. Redmond, WA.
63. Next Year’s Problems. Secure Computing (SC) Magazine Webinar, November 2008.
64. Panel: Embedded Systems and their Increasing Impact on Infrastructure Security. Workshop on Embedded Systems Security (WESS), October 2008.
65. Can you DoS me now? Security Issues in Cellular Networks. Georgia Institute of Technology, September 2008. Atlanta, GA.
66. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Georgia Institute of Technology, April 2008. Atlanta, GA.
67. Characterizing the Impact of Rigidity on the Security of Cellular Networks. AT&T Research Labs, April 2008. Florham Park, NJ.
68. Characterizing the Impact of Rigidity on the Security of Cellular Networks. University of Arizona, March 2008. Tucson, AZ.
69. Cellular Networks Security Panel. USENIX Security Symposium, August 2007. Boston, MA.
70. malnets:Large-Scale Malicious Networks via Compromised Access Points. The Pennsylvania State University - ACM Club Invited Speaker, October 2006. State College, PA.
71. malnets:Large-Scale Malicious Networks via Compromised Access Points. The University of Michigan, October 2006. Ann Arbor, MI.
72. Exploiting Open Functionality in SMS-Capable Cellular Networks. The University of Michigan, October 2006. Ann Arbor, MI.
73. Exploiting Open Functionality in SMS-Capable Cellular Networks. High Technology Crime Investigation Association (HTCIA), September 2006. Pittsburgh, PA.

74. Trends in Security: Critical Engineering in the Large. Schlumberger Innovate IT! Workshop, May 2006. Cambridge, MA.
75. Exploiting Open Functionality in SMS-Capable Cellular Networks. InfraGard Pittsburgh Chapter General Meeting, September 2006. Pittsburgh, PA.
76. Exploiting Open Functionality in SMS-Capable Cellular Networks. InfraGard Pittsburgh Chapter General Meeting, September 2006. Pittsburgh, PA.
77. 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.
78. 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.
79. 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.

B. Special Activities

Presentations to Lay Media

1. Researchers Unleash Ransomware Annihilation. BankInfoSecurity - <http://www.bankinfosecurity.com/researchers-unleash-ransomware-annihilation-a-9255/>, July 2016.
2. 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.
3. Ransomware 'stopped' by new software. BBC - <http://www.bbc.com/news/technology-36772461>, July 2016.
4. Researchers create effective anti-ransomware solution. Help Net Security - <https://www.helpnetsecurity.com/2016/07/12/anti-ransomware-solution/>, July 2016.
5. Florida U boffins think they've defeated all ransomware. http://www.theregister.co.uk/2016/07/12/ransomware_defeated/, July 2016.
6. 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.
7. 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.
8. Desarrollan una solución para detener el ransomware. ComputerHoy - <http://computerhoy.com/noticias/software/desarrollan-solucion-detener-ransomware-47972>, July 2016.

9. Why your antivirus software can't stop ransomware. Futurity - <http://www.futurity.org/ransomware-computer-files-1198242-2/>, July 2016.
10. 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.
11. 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.
12. Extortion extinction: Researchers develop a way to stop ransomware. Phys.org - <http://phys.org/news/2016-07-extortion-extinction-ransomware.html>, July 2016.
13. 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.
14. 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.
15. 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.
16. 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.
17. Jonathon Cheng. Wall Street Journal - Samsung Phone Studied for Possible Security Gap. <http://online.wsj.com/news/articles/SB10001424052702304244904579276191788427198>, December 2013.
18. 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.
19. 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.
20. Mathew J. Schwartz. InformationWeek - Google: Don't Fear Android Malware. <http://www.informationweek.com/security/mobile/google-dont-fear-android-malware/240162399>, October 2013.
21. 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.
22. 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.

23. 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.
24. 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.
25. 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.
26. 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.
27. United Press International. Study: Most mobile Web browsers unsafe. http://www.upi.com/Science_News/Technology/2012/12/05/Study-Most-mobile-Web-browsers-unsafe/UPI-73431354743353/#ixzz2EGtQsuLd, December 2012.
28. 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.
29. 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.
30. 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.
31. 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.
32. 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.
33. 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.
34. Robert Lemos. Smart Phones Could Hear Your Password. Technology Review - <http://www.technologyreview.com/computing/38913/?p1=A2>, October 2011.
35. 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.
36. PhysOrg. Turning iPhone into spiPhone: Smartphones' accelerometer can track strokes on nearby keyboards. PhysOrg.com - <http://www.physorg.com/news/2011-10-iphone-siphone-smartphones-accelerometer-track.html>, October 2011.

37. 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.
38. Clay Dillow. 'PinDr0p' Tech Uses Unique Noise Fingerprints to Trace Calls. Popular Science - <http://www.popsoci.com/technology/article/2010-10/pindr0p-tech-tags-phone-calls-unique-fingerprints-trace-call-paths-across-networks>, October 2010.
39. Lewis Page. Voice-routing call fingerprint system fights vishing. The Register - http://www.theregister.co.uk/2010/10/06/voice_fingerprints, October 2010.
40. 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.
41. 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.
42. 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.
43. 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.
44. 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.
45. 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.
46. 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.
47. Urvaksh Karkaria. GT researchers work to secure cellphones. Atlanta Business Chronicle - <http://atlanta.bizjournals.com/atlanta/blog/atlantech/2009/11/cellphone.html>, November 2009.
48. Making Carriers Shoulder Smartphone Security. http://mobile.slashdot.org/story/09/11/11_2318247/Making-Carriers-Shoulder-Smartphone-Security?art_pos=31, November 2009.
49. 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.
50. Illena Armstrong. Safeguarding your mobile networks. SC Magazine - <http://www.scmagazineus.com/Safeguarding-your-mobile-networks/article/138289/>, June 2009.
51. 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.

52. Amanda Hoffstrom. Technology's limitations in alerting campus danger. UWire Magazine - <http://www.uwire.com/Article.aspx?id=3738798>, February 2009.
53. Laura Sydell. Compromise Allows Obama To Keep BlackBerry. National Public Radio - <http://www.npr.org/templates/story/story.php?storyId=99790788>, January 2009.
54. 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.
55. 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.
56. Associated Press. Hackers Expected To Start Targeting Cell Phones. <http://cbs5.com/watercooler/Cell.Phones.Hackers.2.840909.html>, 2008.
57. Associated Press. College alert systems unreliable, study says. http://www.ajc.com/search/content/metro/stories/2008/09/25/college_campus_alerts.html, 2008.
58. Lee Shearer. Study: Campus alerts unreliable. Athens Banner Herald http://www.onlineathens.com/stories/092508/uga_336494829.shtml, 2008.
59. Bill Ray. 3G Americas warns against text warning systems. The Register - http://www.theregister.co.uk/2008/09/18/emergency_text/, 2008.
60. 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.
61. Evan Koblentz. Web Exclusive: From Messaging to Management Duty. Wireless Week - <http://www.wirelessweek.com/Messaging-to-Management-Duty.aspx>, 2008.
62. 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.
63. Jamming Cellphones with Text Messages. Slashdot <http://it.slashdot.org/it/05/10/05/1839217.shtml?tid=215&tid=172>, 2005.
64. Cell phone networks at risk? CNN http://money.cnn.com/2005/10/05/technology/hacker_cellphones/, 2005.
65. 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.
- 66.
- 67.
- 68.