

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Graham Merrett
U.S. Patent No.: 11,991,601 Attorney Docket No. 50095-0265IP1
Issue Date: May 21, 2024
Appl. Serial No.: 18/224,817
Filing Date: July 21, 2023
Title: WIRELESS MESSAGING METHOD AND SERVER

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

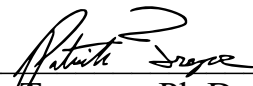
By: 
Patrick Traynor, Ph.D.

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 '601 PATENT	11
V.	INTERPRETATIONS OF THE '601 PATENT CLAIMS AT ISSUE.....	12
VI.	THE '601 PATENT.....	13
	A. Overview of the '601 Patent.....	13
	B. Prosecution History of the '601 Patent.....	14
VII.	OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES .	15
	A. Overview of Horvath	16
	B. Overview of Tsampalis.....	20
	C. Overview of Kansal	25
	D. Overview of Quon	27
	E. Combination of Horvath, Tsampalis, Kansal, and Quon.....	29
VIII.	MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '601 CLAIMS UNPATENTABLE	39
	A. The Horvath-Tsampalis-Kansal-Quon Combination Renders Claims 1- 30 Obvious.....	40
IX.	CONCLUSION	113

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 serve as an Associate Editor for IEEE Security and Privacy Magazine, have been the Program Chair for eight conferences and workshops, and have served as a member of the Program Committee for over 50 different conferences and workshops. I 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. 11,991,601 (“the ’601 Patent”)
- APPLE-1002 File History of U.S. Patent No. 11,991,601
- 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. 2006/0286984 (“Bonner”)
- APPLE-1016 U.S. Pub. No. 2005/0037762 (“Gurbani”)
- APPLE-1024 U.S. Patent No. 7,171,190 (“Ye”)
- 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-1029 U.S. Pub. No. 2008/0292080 (“Quon”)
- APPLE-1030 U.S. Provisional Application No. 60/814,150 (“Quon-Prov”)
- APPLE-1032 U.S. Pub. No. 2008/0261577 (claiming priority to Provisional App. No. 60/913,187) (“Celik”)

- APPLE-1033 U.S. Provisional App. No. 60/913,187
- APPLE-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-1050 U.S. Pub. No. 2005/0233737 (“Lin”)
- 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-1059 U.S. Pub. No. 2006/0129643 (“Nielson”)
- APPLE-1061 U.S. Pub. No. 2007/0290787 (“Fiatal”)
- APPLE-1062 U.S. Pub. No. 2005/0149620 (“Kirkland”)
- APPLE-1063 U.S. Pub. No. 2009/0325609 (“Rosen”)
- APPLE-1064 U.S. Patent No. 7,117,445 (“Berger”)
- APPLE-1068 U.S. Pub. No. 2002/0006793 (“Kun-Szabo”)
- APPLE-1069 U.S. Patent No. 6,678,524 (“Hansson”)
- APPLE-1072 U.S. Pub. No. 2008/0310425 (“Nath”)
- 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-1079 U.S. Pub. No. 2005/0102328 (“Ring”)
- APPLE-1080 U.S. Pub. No. 2007/0061405 (“Keohane”)
- APPLE-1081 U.S. Pub. No. 2005/0037762 (“Gurbani”)
- APPLE-1082 European Application Publication EP 1744527
 (“Satzke”)
- APPLE-1083 U.S. Patent No. 7,254,614 (“Mulligan”)
- 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 ’601 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 '601 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 '601 Patent are obvious over Horvath in view of Tsampalis, Kansal and Quon.

IV. BACKGROUND KNOWLEDGE ONE OF SKILL IN THE ART WOULD HAVE HAD PRIOR TO THE PRIORITY DATE OF THE '601 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 ’601 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 ’601 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 '601 PATENT

A. Overview of the '601 Patent

24. The '601 Patent describes wireless messaging techniques that allow a sending wireless device to selectively transmit an outgoing message via either a packet switched bearer or a circuit switched bearer based on whether the recipient is determined to be a subscriber of a service for receiving messages via the packet switched bearer. APPLE-1001, 3:8-48, Abstract. The Abstract of the '601 Patent, for example, discloses:

A method performed by a mobile wireless device may comprise receiving an SMS message or an EMS message indicating a client program, when a phone number associated with the mobile wireless device is not associated with a subscriber of a service associated with the client program at the time of receiving the SMS message. The method may further comprise downloading the client program on the mobile wireless device and authenticating, via the client program, the phone number associated with the mobile wireless device to the service via SMS protocol. After the authenticating, the client program may cause transmission of first information comprising a first phone number. The client program may receive a first response to the transmission of the first information indicating that the first phone number is associated with a subscriber of the service.

APPLE-1001, Abstract.

25. FIG. 1 is a diagram of the messaging system:

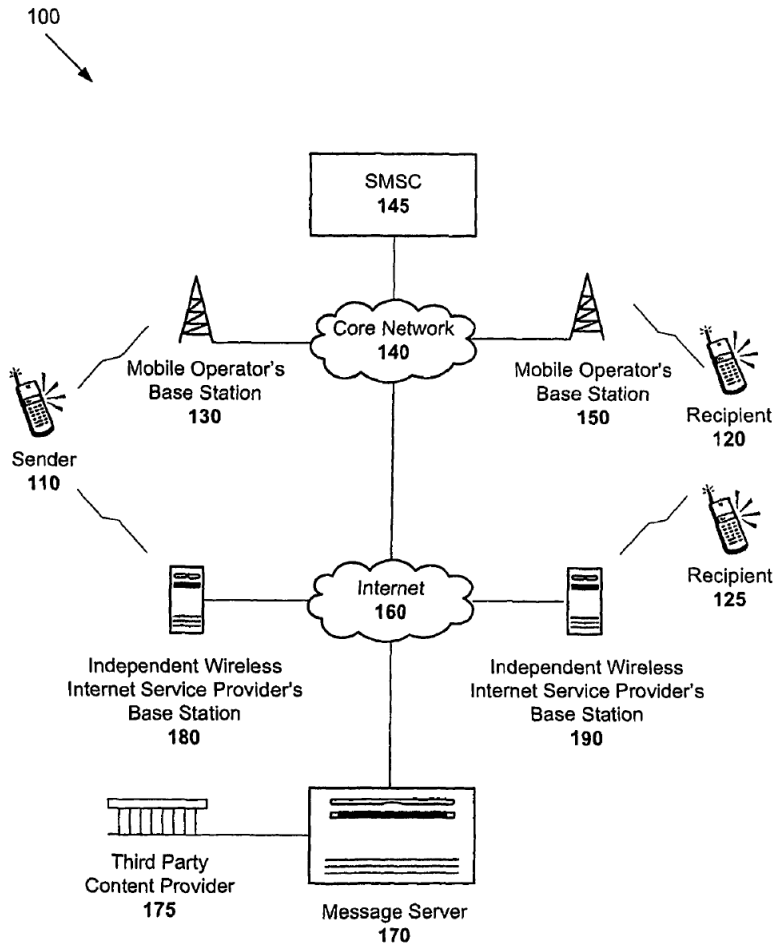


FIG. 1

APPLE-1001, FIG. 1

B. Prosecution History of the '601 Patent

26. In the only Office Action issued during prosecution, the Examiner rejected application claims 18-30 under §112 as being indefinite, for which the Applicant filed an amendment, and the Examiner identified a collection of limitations in claims 1-17 as allowable. APPLE-1002, 10-18, 170-182, 185-188.

However, as discussed in §IV, the application never should have been allowed. All features recited in the Challenged Claims are disclosed in one or more of Horvath, Tsampalis, Kansal, and Quon, and the claimed combinations of these features would have been obvious before the Critical Date.

VII. OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES

27. Horvath, Tsampalis, Kansal, and Quon are all analogous art, each being in the field of endeavor (mobile messaging over wireless networks) and reasonably pertinent to the problems said to be addressed by the '601 Patent. APPLE-1001, Title, Abstract; APPLE-1004, Title, Abstract; APPLE-1005, Title, Abstract; APPLE-1042, Abstract; APPLE-1029, [0006]; *infra*, §VIII.A. Like the '601 Patent, Horvath, Tsampalis, Kansal, and Quon each seek to provide users with a wider range of messaging options. APPLE-1001, 3:21-28; *See* 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-1029, [0006] (“enables users to make global calls at some of the lowest international rates available, send global text messages, and chat using all the major Instant Messaging clients such as MSN Messenger, GoogleTalk, Yahoo, AIM, and ICQ”), [0027].

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.

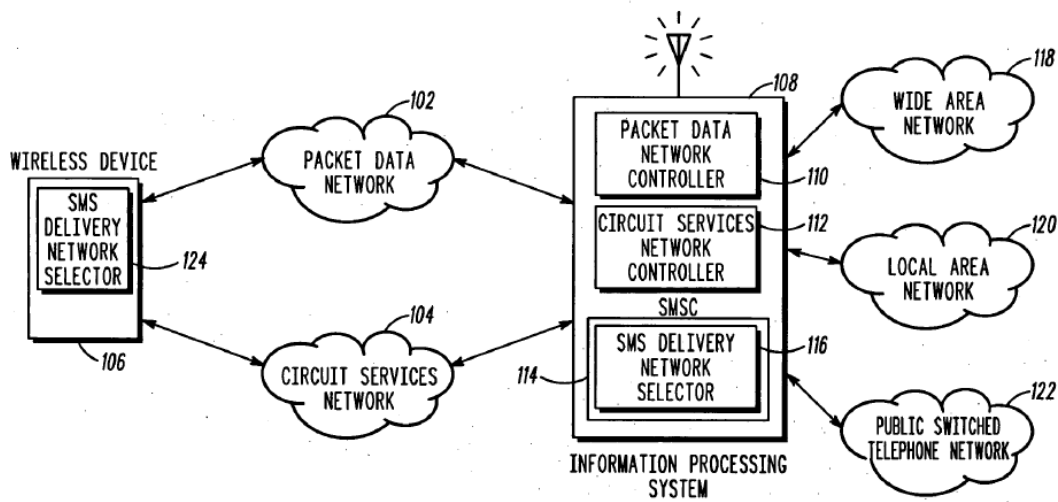
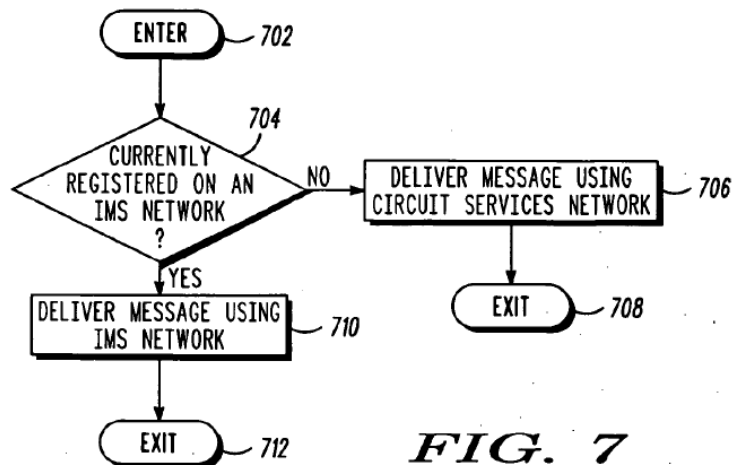


FIG. 1

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 and a server 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, using 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).

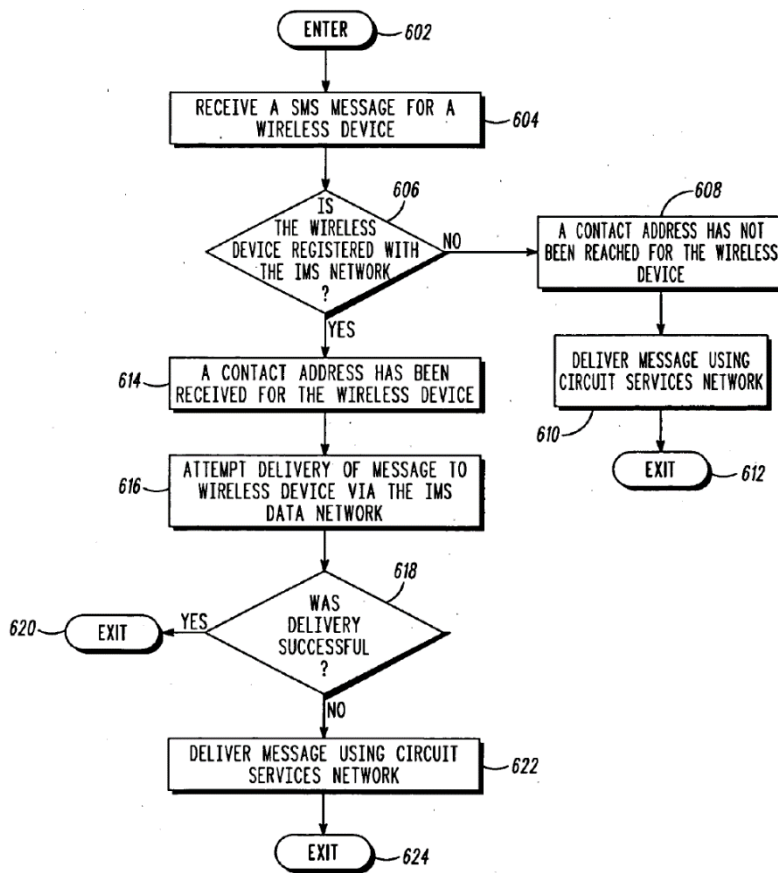


FIG. 6

APPLE-1004, FIG. 6 (Server Perspective)

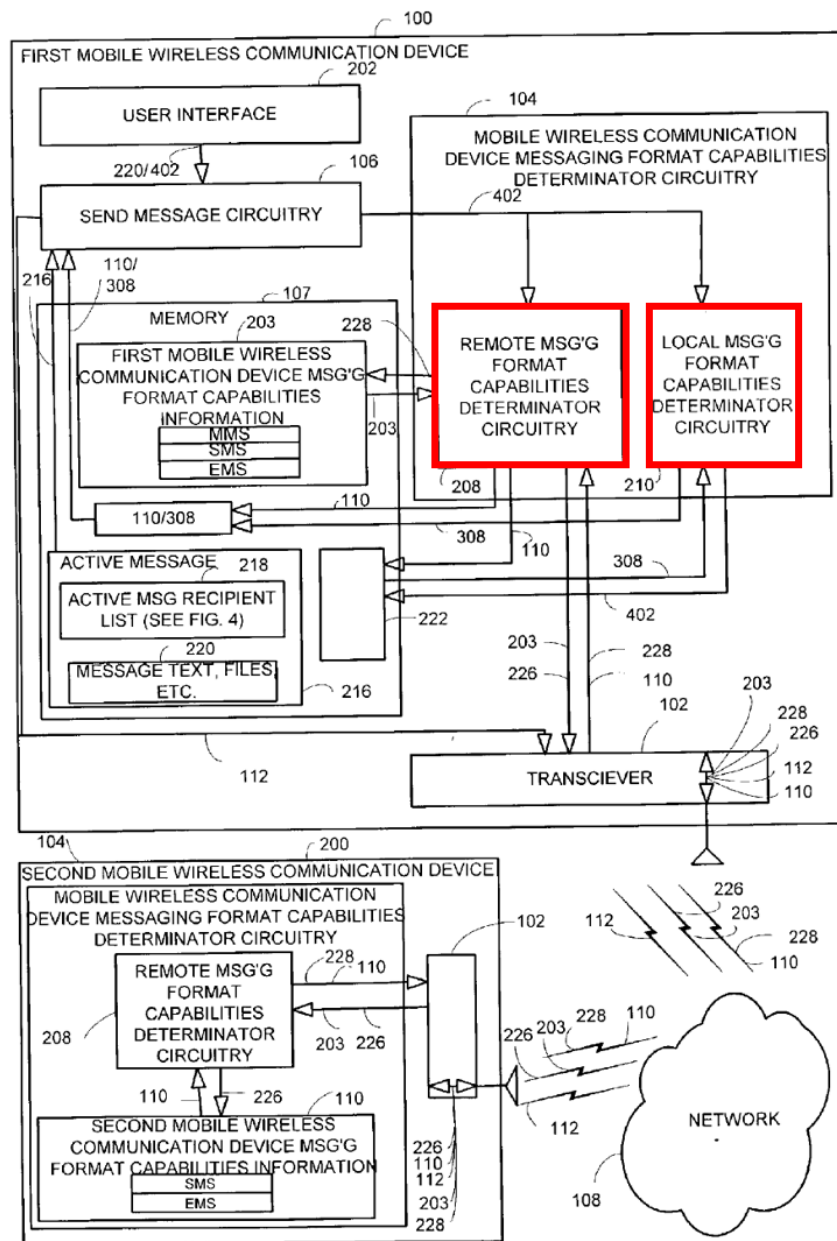
B. Overview of Tsampalis

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 be 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.

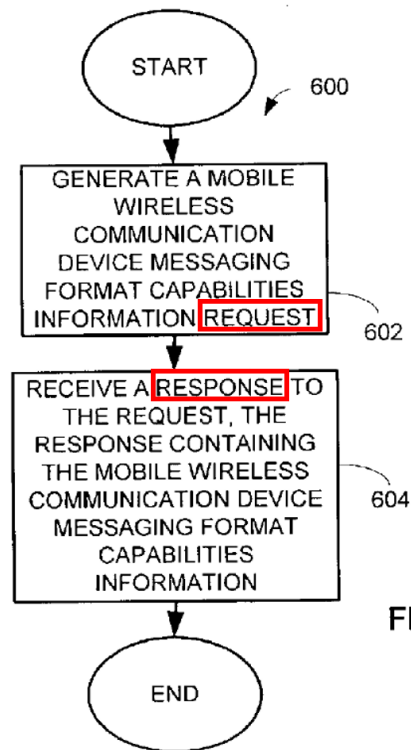
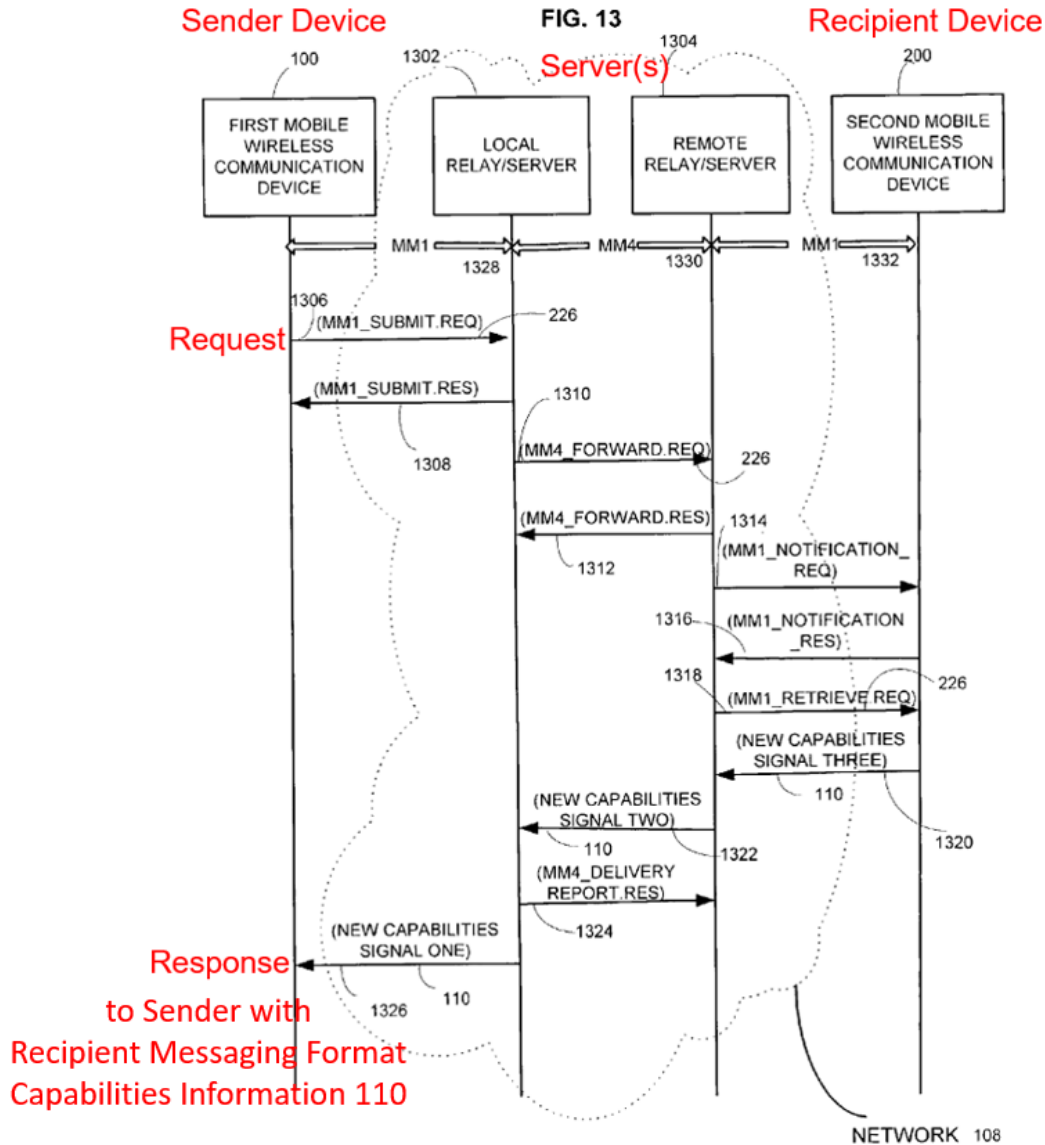


FIG. 6

APPLE-1005, FIG. 6 (Annotated)

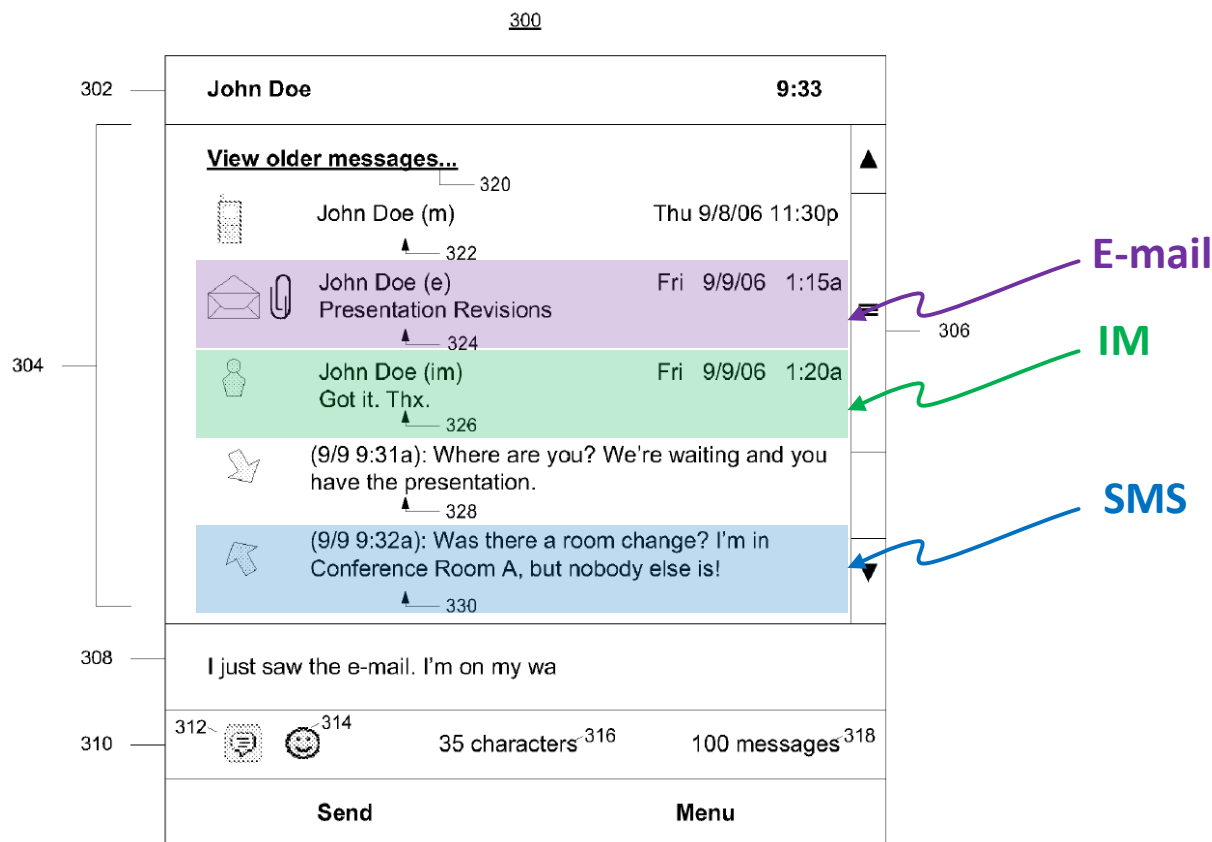


APPLE-1005, FIG. 13 (Annotated)

C. Overview of Kansal

35. 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].



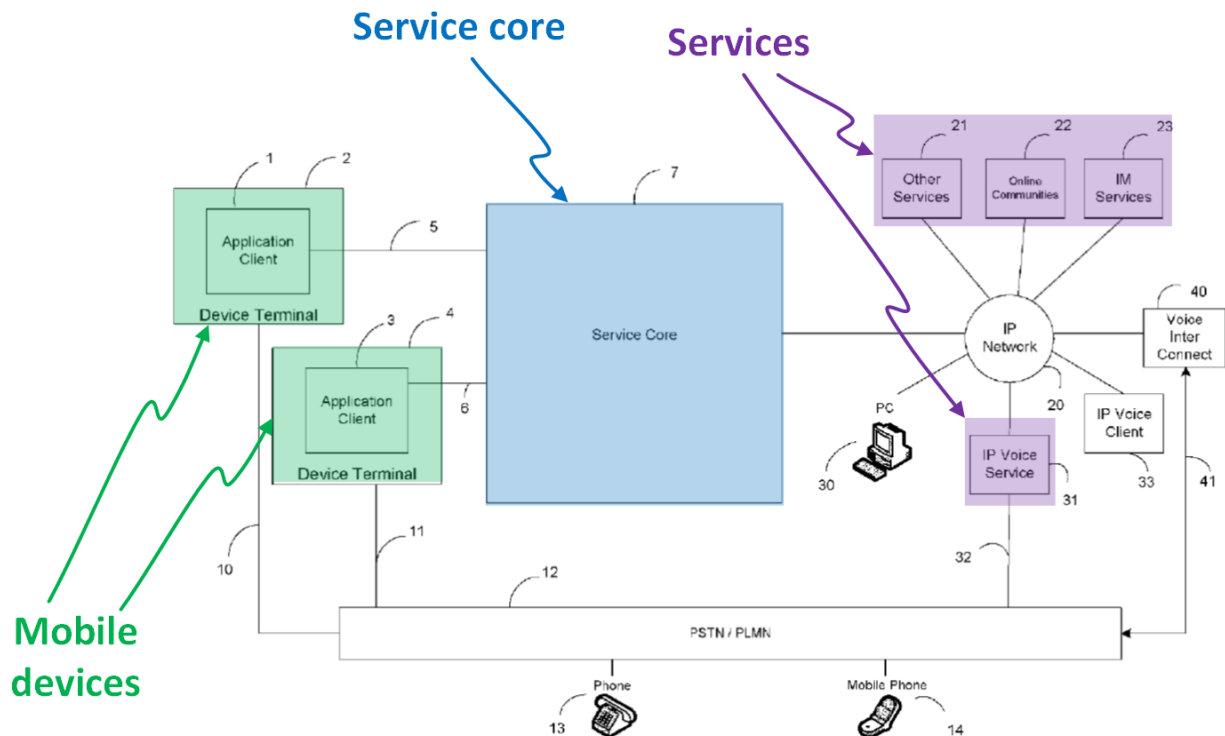
APPLE-1042, FIG. 3 (Annotated)

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 (shown below).

D. Overview of Quon

37. Quon relates to “a mobile phone service...that enables users to make global calls at some of the lowest international rates available, send global text messages, and chat using all the major Instant Messaging clients such as MSN Messenger, GoogleTalk, Yahoo, AIM, and ICQ.” APPLE-1029, [0002]. As shown in FIG. 1 (below), Quon’s system “comprises multiple application clients 1, 3 hosted on any of a variety of respective device terminals 2, 4,” which, like the mobile devices of Horvath, are configured to communicate over “converged voice and data service networks including GSM/GPRS/EDGE, UMTS, CDMA, WiFi, and WiMAX.” APPLE-1029, [0025]. The application clients interface over the networks with a service core 7 that “includes service gateway functionality for bridging core services extended to the application clients 1, 3.” APPLE-1029, [0027]. These services include access to IM (*e.g.*, connection to MSN, Yahoo, and/or AIM), online social network communities (*e.g.*, Myspace or Facebook), SMS service, and/or voice services (*e.g.*, connection to PSTN or VoIP services). *See* APPLE-1029, [0027]-[0028].



APPLE-1029, FIG. 1 (Annotated)

38. “The application clients 1, 3 preferably provide user interfaces to content such as a contact list, message list, instant messaging, and/or events such as call requests, presence status indicators, messaging, and contact synchronization based on digital signals received over the respective interfaces 5, 6.” APPLE-1029, [0026]. In other words, like Kansal, Quon provides a unified message client that allows a user to communicate with other mobile devices via various communication methods (e.g., SMS, IM, VoIP) over various different wireless networks. *See* APPLE-1029, [0025]-[0029]; *supra* §VII.C. Indeed, Quon incorporates U.S. Provisional Application No. 60/814,150 (Quon-Prov) by reference in its entirety, and Quon-Prov confirms that “a user ‘A’ with one or more service identities, such

as ‘a’, can publish or send communications session invites called ‘EQO Me’ to user ‘B’ with service identity ‘b’ which can progress through various session permissions stages and then communicate through a number modes comprising message, SMS, IM chat, and voice.” APPLE-1030, 5; APPLE-1029, [0024], [0052].

39. Importantly, Quon provides a specific method for users to obtain the application client of the unified communication system. *See* APPLE-1029, [0031]-[0034]. Specifically, Quon allows existing users who already have the application client and are registered with the unified messaging service to invite other users through a common messaging service (*e.g.*, SMS or email). *See* APPLE-1029, [0031]-[0034], [0036]. For example, Quon describes, “where the service user may decide to invite non-user contacts manually[,]...[a] service invitation message may preferably be delivered to the invitee as an SMS message.” APPLE-1029, [0031]. “This invitation message may contain a link to a web page where an invitee can sign up and download an application client 1, 3 to his or her own phone.” APPLE-1029, [0032].

E. Combination of Horvath, Tsampalis, Kansal, and Quon

40. Like the ’601 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, 3:8-39; 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-1004, [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**

41. 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.

42. 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).

43. 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.

44. 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].

45. 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.

46. 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 ’601 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-switched network.

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

47. The combination provides a wireless mobile device capable of messaging using different messaging services including, SMS, MMS, and IM. *Supra* §VII.E(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.

48. 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 at a glance in a single thread would advantageously allow a user to see all messages received from particular senders within a single interface without needing to navigate to different messaging applications or interfaces for each different message type. APPLE-1045, 1-2 (a multi-protocol messaging application providing "a powerful and efficient user experience."); APPLE-1042, [0009], [0045]-[0046], [0054]-[0056], [0062]-[0064], [0070], [0077]-[0078], FIGs. 2-3.

49. 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.

50. 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.A-C. 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.

51. 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. Further, the techniques integrated from Kansal in the Horvath-Tsampalis-Kansal combination are fully compatible with Horvath's and Tsampalis's teachings and would not disturb the ability of Horvath's system to transmit or deliver messages over either a packet-based or circuit-switched network or the use of MFCI-based messaging techniques taught by Tsampalis.

(iii) Quon's Application Distribution

52. Tsampalis describes that the "send message circuitry 106 operates to send a message in a message format compatible with at least one of the formats identified in the second mobile wireless communication device [MFCI] 110." APPLE-1005, [0025]. Tsampalis explains that the send message circuitry 106 is preferably a software module "stored as computer code on a variety of computer readable mediums." APPLE-1005, [0027]; *see also id.*, [0024]. However, Tsampalis does not describe how the send message circuitry software module is received by the wireless communication device in the first place. *See* APPLE-1005, [0024], [0025], [0027].

53. Similarly, Kansal describes "application programs" that "allow a user to accomplish one or more specific tasks." APPLE-1042, [0034]. Kansal describes that these application programs are "software programs" that are executed by the

host processor of the mobile computing device 100. APPLE-1042, [0032]. However, Kansal does not describe how the software programs are received by and/or stored in the mobile computing device 100 in the first place. *See* APPLE-1042, [0032]-[0034], [0082]-[0090].

54. A POSITA would have found that Quon provides at least one method for providing the software described by Tsampalis and Kansal to at least some of the combination's mobile devices. Specifically, a POSITA would have found it obvious to use Quon's SMS invitation messages to sign-up and distribute to new users, for example, Tsampalis's mobile wireless communication device messaging format capabilities determinator circuitry 104 and send message circuitry 106 and Kansal's associated unified messaging UI, similar to the application client taught by Quon. *See* APPLE-1029, [0026] (describing that the "application clients 1, 3 preferably provide user interfaces to content such as a contact list, message list, instant messaging, and/or events such as call requests, presence status indicators, messaging, and contact synchronization," and "transmit client and user event information" over the network interfaces 5, 6), [0031]-[0032]. Multiple reasons would have prompted a POSITA to implement this combination.

55. First, Quon recognized that existing communication systems relied only allowed current users to invite new users to a given communication service through the use of "online identities, such as email addresses" to "invite and

associate users.” APPLE-1029, [0004]-[0005]. Quon’s “inventive design allows the user to add and invite contacts from multiple interface points in the service such as during ad-hoc calling to any mobile telephone number.” APPLE-1029, [0007]. This “allows a service’s user to import contacts from the user’s pre-existing mobile phone book and send invitations to the contacts based on the contact telephone numbers to join.” *Id.* In the context of the combination, this would have permitted an existing user that uses Tsampalis’s determinator and send message circuitry and Kansal’s associated unified UI to invite friends to download the same software (implemented, *e.g.*, as a messaging client like the one described by Quon) and similarly participate in and use the MFCI capabilities functionality taught by Tsampalis based on the phone numbers that the existing user already stores in their phone. *See id.* Advantageously, this ameliorates the need for existing user’s of the combination system from having to cumbersome ask their friends to join and explain how to do so through other communication means (*e.g.*, through an in-person conversation).

56. Second, a POSITA would have recognized that providing Quon’s easy and intuitive mechanism by which existing users may invite their friends and other contacts to participate in and use the MFCI capabilities functionality taught by Tsampalis would have advantageously increased adoption and use of the system of the combination by more users. *See* APPLE-1029, [0006] (identifying an “easy to

install” application as advantageous); APPLE-1030, 6 (explaining how “extending service reach” to “a much broader audience of circle of friends” as advantageous).

57. Third, Quon’s techniques are fully compatible with the mobile devices, networks (*e.g.*, GSM/GPRS/EDGE, UMTS, CDMA, WiFi, and WiMAX), and types of messaging formats (*e.g.*, SMS, MMS, IM) disclosed in each of Horvath, Tsampalis, and Kansal, and these networks and formats are expressly identified in Quon as being used by its system to distribute the application client to new mobile devices. *See supra* §§VII.A-E. Applying Quon’s sign-up and software distribution system and methods in the similar communication context of Horvath, Tsampalis, and Kansal with the same services to obtain a substantially similar result would have been obvious.

58. A POSITA would have reasonably expected success implementing the combination as the messaging and communication protocols and techniques involved were all well-known before the Critical Date. Further, the techniques integrated from Quon in the Horvath-Tsampalis-Kansal-Quon combination are fully compatible with Horvath’s, Tsampalis’s, and Kansal’s teachings and would not disturb the ability of Horvath’s system to transmit or deliver messages over either a packet-based or circuit-switched network, the use of MFCI-based messaging techniques taught by Tsampalis, or the unified UI taught by Kansal.

VIII. MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE ’601 CLAIMS UNPATENTABLE

A. The Horvath-Tsampalis-Kansal-Quon Combination Renders Claims 1-30 Obvious

Element [1pre]: A method performed by a mobile wireless device, the method comprising:

59. For example, Horvath discloses methods and systems for wireless communication, such as wireless messaging, by mobile wireless devices. *See e.g.*, APPLE-1004, Title (“Method And System For Delivery Of Short Message Service Messages”), [0011]; *see also* APPLE-1005, [0001], [0006].

Element [1a]: receiving a short message service (SMS) message indicating a client program or an enhanced message service (EMS) message indicating the client program, when a phone number associated with the mobile wireless device is not associated with a subscriber of a service associated with the client program at the time of receiving the SMS message or the EMS message;

60. Horvath-Tsampalis-Kansal-Quon renders Element [1a] obvious. As I previously discussed in §§VII.D-E, it would have been obvious to use Quon’s SMS invitation messages to sign-up and distribute to new users, for example, Tsampalis’s mobile wireless communication device messaging format capabilities determinator circuitry 104 and send message circuitry 106 and Kansal’s associated unified UI (implemented, *e.g.*, as a messaging client like the one described by Quon). *See* APPLE-1029, [0026], [0031]-[0032].

61. Quon describes an application client that “provide[s] user interfaces to content such as a contact list, message list, instant messaging, and/or events such as call requests, presence status indicators, messaging, and contact synchronization” and “transmit[s] client and user event information over” an interface to a “converged

voice and data service networks including GSM/GPRS/EDGE, UMTS, CDMA, WiFi, and WiMAX.” APPLE-1029, [0026]. This is similar to the “software modules” that implement Tsampalis’s messaging format capabilities determinator circuitry 104, and send messaging circuitry 106, and “software programs” that implement Kansal’s unified messaging UI. *See* APPLE-1005, [0024] (describing that, in one embodiment, the functionality of the mobile device is carried out by “one or more processing devices executing software stored in memory”), [0025] (“send message circuitry 106 operates to send a message in a message format compatible with at least one of the formats identified in the second mobile wireless communication device messaging format capabilities information 110”), [0033]; APPLE-1042, [0032]-[0034], [0077]-[0078]. A POSITA would have found it obvious to package the software modules needed to implement Tsampalis’s MFCI elements and Kansal’s unified messaging UI as a single application client, like the one taught by Quon, because this would have made software distribution easier for both the provider and the user. *See* APPLE-1029, [0004]-[0007]; *supra* §VII.E.

62. Quon describes that this application client would have been distributed to new users through SMS invites. *See* APPLE-1029, [0031]-[0034]. Specifically, Quon describes, “where the service user may decide to invite non-user contacts manually[,]...[a] service invitation message may preferably be delivered to the invitee as an SMS message.” APPLE-1029, [0031]. “This invitation message may

contain a link to a web page where an invitee can sign up and download an application client 1, 3 to his or her own phone.” APPLE-1029, [0032]. Accordingly, a POSITA would have found obvious that, in Horvath-Tsampalis-Kansal-Quon, an invited user’s mobile device would *receiv[e] a short message service (SMS) message indicating a client program or an enhanced message service (EMS) message indicating the client program* (e.g., receive an SMS text from an existing user that includes a link to sign up and download the combination’s application client).

63. Quon teaches that new and existing users may or may not be subscribers of various messaging services with which the application client interfaces. *See* APPLE-1029, [0029], [0049]-[0051].

For example, a service user’s service phonebook may contain entries for contacts A, B, C, and D. Contacts A and B may have associated mobile phone numbers, whereas contact C has a telephone number, a VoIP account, and an instant messaging screen name. Contact D may only have an instant messaging screen name. Contact B and C may also be users of the service. At any given time, in an embodiment, the user may see that contact B is signed on to the service and available; contact C may be available only through the VoIP account; and contact D is signed on to his IM service.

APPLE-1029, [0029]. In other words, different contacts—both those using the application client and those who are not—may be subscribed to different messaging services (e.g., IM, email, VoIP, cellular telephony, and/or PSTN telephony). *See* APPLE-1029, [0029]; *see also id.*, [0024] (referring to Quon-Prov regarding

supported services); APPLE-1030, 17 (listing various voice services, video, email, various IM services, and SMS as examples of supported services). Further, each of Tsampalis, Kansal, and Quon confirm that information regarding the services to which a user of a given mobile device is subscribed may be determined based on a telephone number of the user's mobile device. See APPLE-1005, [0033], [0035], [0061]; APPLE-1042, [0037]-[0038], [0041]-[0042], [0066] (“[t]he sender or the recipient may be determined using various types of identifying information associated with a particular message such as a telephone number, e-mail address, IM screen name, SMS identifier, MMS identifier, and so forth”); APPLE-1029, [0007], [0030] (“application client 1 may communicate with service core 7 to determine which contacts are also service users, such as by a comparison of mobile number or service ID”), [0037] (“[i]f service user B is added based on user B mobile number by service user A, service user B is added to service user's service phonebook, and service user A will see the presence of service user B, and service user A can initiate communications with service user B via the service”).

64. Accordingly, a POSITA would have found obvious that, in at least some cases, an SMS invitation message would have been received *when a phone number associated with the mobile wireless device is not associated with a subscriber of a service associated with the client program at the time of receiving the SMS message or the EMS message* (e.g., a mobile device that receives an SMS

to sign up and download the combination's application client is not associated with a subscriber of a service, such as an IM service, at the time of receiving the SMS).

Element [1b]: downloading the client program on the mobile wireless device;

65. Horvath-Tsampalis-Kansal-Quon renders Element [1b] obvious. As discussed for [1b] and in §§VII.D-E, *supra*, a user who has already downloaded the combination's application client to their mobile device is able to invite another user who has not signed up and downloaded the combination's application client through an SMS message. *See* APPLE-1029, [0007], [0031]-[0034]. "This invitation message may contain a link to a web page where an invitee can sign up and download an application client 1, 3 to his or her own phone." APPLE-1029, [0032]. "From the mobile browser, the invitee can signup for the service (which may include steps such as creating a Service ID and password, specifying an email address, and the like) and then download the appropriate application client 1, 3 to the invitee terminal device 2, 4, such as their phone." *Id.*

66. Accordingly, a POSITA would have found obvious, in Horvath-Tsampalis-Kansal-Quon, that an invited user's mobile device would ***download[] the client program on the mobile wireless device.***

Element [1c]: authenticating, via the client program, the phone number associated with the mobile wireless device to the service via SMS protocol;

67. Horvath-Tsampalis-Kansal-Quon renders Element [1c] obvious. For example, Horvath describes that 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]. On the other hand, when device 106 “[is] registered with the [SIP] registrar,” device 106 sends “SIP message[s]” in “SIP packets” “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.”).

68. Horvath further describes authenticating its sending wireless device (wireless devices 106) both during registration with the SIP/IMS network and for transmitting subsequent messages, through an S-CSCF and HSS of the SIP/IMS network. 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 describes the SIP registration process for the wireless device 106 with the S-CSCF component of the SIP/IMS network, 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. The profiles stored on the HSS 210 are accessed based on the mobile devices tel-URI, which “for example is the telephone number assigned to the wireless device 106.” APPLE-1004, [0035]; *see also id.*, [0043] (“the registration event package is an XML document that includes a list of explicitly and implicitly registered public URIs such as a tel-URI”), [0073].

69. Through authentication with the S-CSCF and HSS, wireless device 106 is also authenticated to the IM service (*authenticating...to the service*). 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]. 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.*, the SMS message (*authenticating...the mobile wireless device to the service via SMS protocol*). *Id.* Where authentication is successful, the message is sent further into the IMS network implemented by Horvath’s IMS network that provides the IM service (*the service*) and the identity of the source of the message is believed due to this authentication process. Where the decryption is unsuccessful, the SMS message is not forwarded on.

70. A POSITA would have found it obvious that the above-described authentication would have happened *via the client program*. For example, Quon-Prov describes that its application client (referred to here as the “Personal Network Service Convergence Application (PNSCA)”) “uses industry open standards such as Session Initiation Protocol (SIP) for signaling,” like the mobile device described in Horvath. APPLE-1030, 30, 38. A “user agent” portion of the application client

“provides an integrated user agent and back-to-back user agent allowing the PNSCA software (100) to register into the core network such as IMS or a centralized SIP server.” APPLE-1030, 40. And, “[a]t the network service access layer, the PNSCA software (100) implements the transport broker (240) for...client authentication (244) for access control to the services network.” APPLE-1030, 39. Accordingly, it would have been obvious for the application client of the combination to similarly perform the registration and authentication described by Horvath.

71. [RESERVED]

72. Accordingly, a POSITA would have found it obvious, in Horvath-Tsampalis-Kansal-Quon, that the mobile devices would *authenticate[e], via the client program, the phone number associated with the mobile wireless device to the service via SMS protocol* (e.g., using the telephone number and session keys to authenticate all messages sent with the client program of the sending mobile device via the IMS network, including SMS messages).

Element [1d]: after the authenticating: transmitting, via the client program, first information comprising a first phone number;

73. Horvath-Tsampalis-Kansal-Quon renders Element [1d] obvious. Horvath explains that the sending mobile device, 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].

74. 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 device 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”).

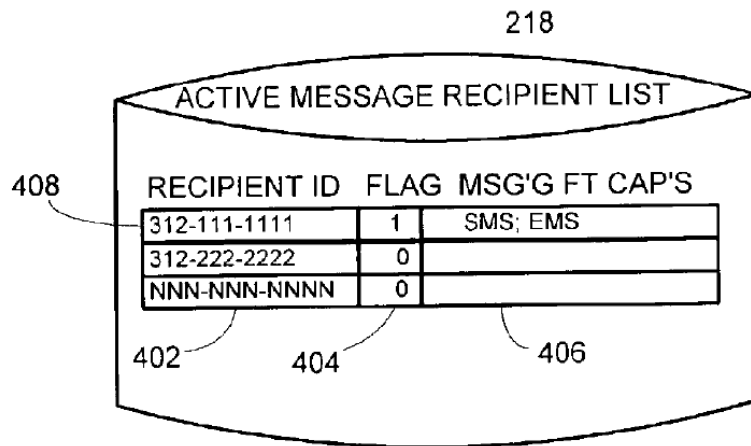
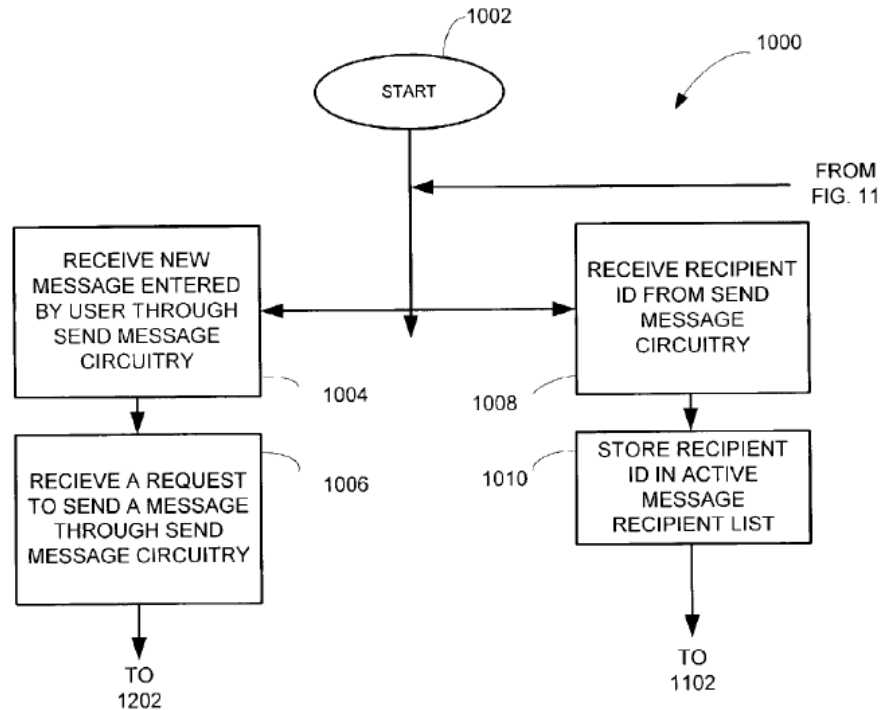


FIG. 4

APPLE-1005, FIG. 4

75. 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 device’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 device entered into the active message recipient list. APPLE-1005, [0033]; *see also id.*, [0046].

FIG. 10



APPLE-1005, FIG. 10

76. If the MFCI is not available in the sending mobile device's local phonebook or the phonebook's information has not been updated within a certain period of time, "the remote message format capabilities determinator circuitry 208 [of the sending mobile device] is then invoked and generates a second mobile wireless communication device messaging format capabilities information request 226." APPLE-1005, [0033]-[0034].

77. The requested MFCI 110 for the receiving mobile device 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 device 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].

78. 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 device to send a request that included the telephone number of the receiving mobile device 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 device. 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”).

79. Thus, a POSITA would have found obvious that, in Horvath-Tsampalis-Kansal-Quon, a sending mobile device would *transmit[]*, *via the client program* (e.g., the combination's application client, which implements Tsampalis's MFCI functionality), *first information comprising a first phone number* (e.g., sending a request to the HLR and/or HSS including the receiving mobile device's telephone number to determine a first receiving mobile device's MFCI).

Element [1e1]: receiving, via the client program, a first response to the transmitting of the first information,

80. Horvath-Tsampalis-Kansal-Quon renders Element [1e1] obvious. As I previously explained for Element [1d], to obtain the MFCI, it would have been obvious for the combination's sending mobile device to send 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 device 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].

81. Thus, a POSITA would have found obvious that, in Horvath-Tsampalis-Kansal-Quon, a sending mobile device would *receiv[e]*, *via the client program* (e.g., the combination's application client, which implements Tsampalis's

MFCI functionality), *a first response to the transmitting of the first information* (e.g., the response with the MFCI).

Element [1e2]: wherein the first response indicates that the first phone number is associated with a subscriber of the service;

82. Horvath-Tsampalis-Kansal-Quon renders Element [1e2] obvious. A POSITA would have found obvious that 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). 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.*

83. And providing such subscription information along with format information to a sending mobile device 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 cellular operators is “Instant Messaging (IMing),” and describing a sending mobile device 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 device), 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, a POSITA would have found obvious, for similar reasons to those described in §VII.E(i), *supra*, providing a sending mobile device with more detailed information about the recipient, including their subscriber information, will help the sending user determine how and where to send a message and what content should be included. *See supra* §VII.E(i) (providing similar motivations for the Tsampalis combination).

84. Thus, a POSITA would have found obvious that, in Horvath-Tsampalis-Kansal-Quon, ***the first response indicates that the first phone number is associated with a subscriber of the service*** (e.g., the response from the HLR/HSS includes both MFCI and subscription information).

Element [1f]: transmitting, via the client program and a wireless local area network (WLAN), based on the first response, first message content, to a mobile wireless device associated with the first phone number;

85. Horvath-Tsampalis-Kansal-Quon renders Element [1f] obvious. 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]; 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.

86. As I previously discussed in §VII.A, Horvath describes that the sending mobile device 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 device is not registered) will the sending mobile device “select the circuit-services network for SMS delivery.” *Id.*

87. 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 device’s MFCI

to the sending mobile device, the sending mobile device uses the information to determine how to send the message to the receiving mobile device. *See id.*

88. Taken together and as I previously described in §VII.E, Horvath-Tsampalis-Kansal-Quon’s sending mobile device uses both sets of information when determining how to format and deliver a message to a receiving mobile device. First, the sending mobile device checks if it is registered on the packet-switched network. *See* APPLE-1004, [0021], [0039]-[0042], [0078]. If it is, it will use the packet-switched network, and otherwise it will use the circuit-switched network. *Id.* Second, the sending mobile device will check the receiving mobile device’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 device. APPLE-1005, [0041], [0049], [0052]-[0054], [0062].

89. Where, for example, the sending mobile device is registered with the packet-switched network and the packet-switched network to which the sending mobile device is registered is an 802.11 network, Horvath-Tsampalis-Kansal-Quon’s sending mobile device 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).

90. Accordingly, a POSITA would have found obvious that Horvath-Tsampalis-Kansal-Quon's sending mobile device *transmitting, via the client program* (e.g., the combination's application client, which implements Tsampalis's send message circuitry) *and a wireless local area network (WLAN)* (e.g., the packet-data network 102 is an 802.11 network), *based on the first response, first message content, to a mobile wireless device associated with the first phone number* (e.g., the sending phone sends a message to the first receiving mobile device via the 802.11 network).

Element [1g]: transmitting, via the client program, second information comprising a second phone number,

91. Horvath-Tsampalis-Kansal-Quon renders Element [1g] obvious. A POSITA would have understood and found obvious that the Horvath-Tsampalis-Kansal-Quon sending mobile device would follow the procedures that I previously described with respect to Element [1d], every time that a user creates a new message and/or enters a new recipient ID for a message. *See* APPLE-1005, [0033], [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].

92. Accordingly, a POSITA would have understood and found obvious that, in Horvath-Tsampalis-Kansal-Quon, the sending mobile device *transmitting, via the client program* (e.g., the combination’s application client, which implements Tsampalis’s MFCI functionality), *second information comprising a second phone number* (e.g., sending a request to the HLR and/or HSS including the receiving mobile device’s telephone number to determine a second receiving mobile device’s MFCI).

Element [1h]: wherein the second phone number is not associated with a subscriber of the service; and

93. Horvath-Tsampalis-Kansal-Quon renders Element [1h] obvious. As I previously discussed for Element [1e2], a POSITA would have found obvious that 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). A POSITA would have understood that the HLR 202 and/or HSS 210 would provide a response to every request for format capabilities and service subscription information, regardless of the formats or services stored in the profile associated with the receiving mobile device. *See, e.g.,* APPLE-1005, [0035], [0042], [0057]-[0060] (not conditioning a response to a format capabilities request on the information contained therein). And it was known

that some wireless devices (*e.g.*, mobile phones) had limited messaging capabilities. *See, e.g.*, APPLE-1005, [0003] (describing receiving mobile devices “capable of only receiving messages in” SMS), [0034] (describing a receiving mobile devices as having “limited messaging capabilities”), [0061]-[0062]; APPLE-1029, [0029] (describing that some users are subscribed an IM service and others are not); APPLE-1042, [0078] (describing messaging decision based on “availability of a recipient to receive messages of a certain format”); APPLE-1053, 2:9-17 (“each device may have a different range of connectivity...and different capabilities for handing different types and sizes of content”). Accordingly, a POSITA would have understood and found obvious that, for certain receiving mobile devices, the HLR 202 and/or HSS 210 would provide a response when the phone number of the receiving mobile device is not associated with a subscriber of an IM service. *See, e.g.*, APPLE-1004, [0047] (describing a case where “the recipient device is not registered on the packet data network 102”), [0053].

94. Accordingly, a POSITA would have understood and found obvious that, in Horvath-Tsampalis-Kansal-Quon, *the second phone number is not associated with a subscriber of the service.*

Element [1i]: inserting, via the client program, second message content into a message for delivery to a mobile wireless device associated with the second phone number,

95. Horvath-Tsampalis-Kansal-Quon renders Element [1i] obvious. As I previously discussed for Element [1a], Quon teaches that “[a]n application client 1 may communicate with service core 7 to determine which contacts are also service users, such as by a comparison of mobile number or service ID.” APPLE-1029, [0030]. In the combination, a POSITA would have found it obvious that some contacts of a sending mobile device will not already be using the application client and Tsampalis’s associated MFCI service, as taught by Quon. *See id.* Like in Quon’s application client, the combination’s application client would have indicated to the user of a sending mobile device whether or not their contacts (*e.g.*, the recipient IDs of receiving mobile devices being entered into the active message) also have an application client and are participating in the associated exchange of MFCI. *See id.* Where they are not, the sending mobile would not be able to gather the same amount of information about the contacts. *See id.* Thus, in order to gain access to the information provided through the combination’s application client and associated service, a user would have needed to invite their non-participating contacts to join, as described by Quon. *Id.*

96. Specifically, Quon describes, “where the service user may decide to invite non-user contacts manually[,]. . . [a] service invitation message may preferably be delivered to the invitee as an SMS message.” APPLE-1029, [0031]. “This invitation message may contain a link to a web page where an invitee can sign up

and download an application client 1, 3 to his or her own phone.” APPLE-1029, [0032]. Thus, a POSITA would have found obvious that, where the mobile device associated with the second phone number (*e.g.*, the second receiving mobile device) is not using combination’s application client and associated services, the user of the sending mobile device would invite the second receiving mobile device by sending an invitation SMS message. *See* APPLE-1029, [0031]-[0032].

97. A POSITA would have found obvious that the combination’s application client would have composed and sent the invitation message in response to the user of the sending mobile device requesting that an invite be sent. Quon discloses that “the service [*i.e.*, the service core 7] can spoof the originating mobile number of the SMS message that originates from the service to be that of the mobile MS ISDN of the user's device terminal 2.” APPLE-1029, [0031]. However, Quon describes that the service core 7 acts as a gateway “for bridging core services extended to the application clients.” APPLE-1029, [0027]. In this regard, the service core 7 acts as a proxy for the various communication services (*e.g.*, voice, video, IM, email, SMS). *See* APPLE-1029, [0026]-[0028].

98. Unlike in Quon, it would have been obvious that the combination’s application client has the interface software necessary to directly communicate with the services, as taught by Tsampalis (*e.g.*, the send message circuitry 106) and Kansal (*e.g.*, messaging applications 130). *See* APPLE-1005, [0025] (“send

message circuitry 106 operates to send a message in a message format compatible with at least one of the formats identified in the” MFCI); APPLE-1029, [0035] (mobile device “implement[s] several messaging applications 130 arranged to communicate various types of messages in a variety of formats,” and each “may be representative of a particular kind of transport, enabling handling of messages of particular types and formats”). Thus, the combination’s application client would be able to directly send the SMS invitation to receiving mobile device being invited. *Id.*

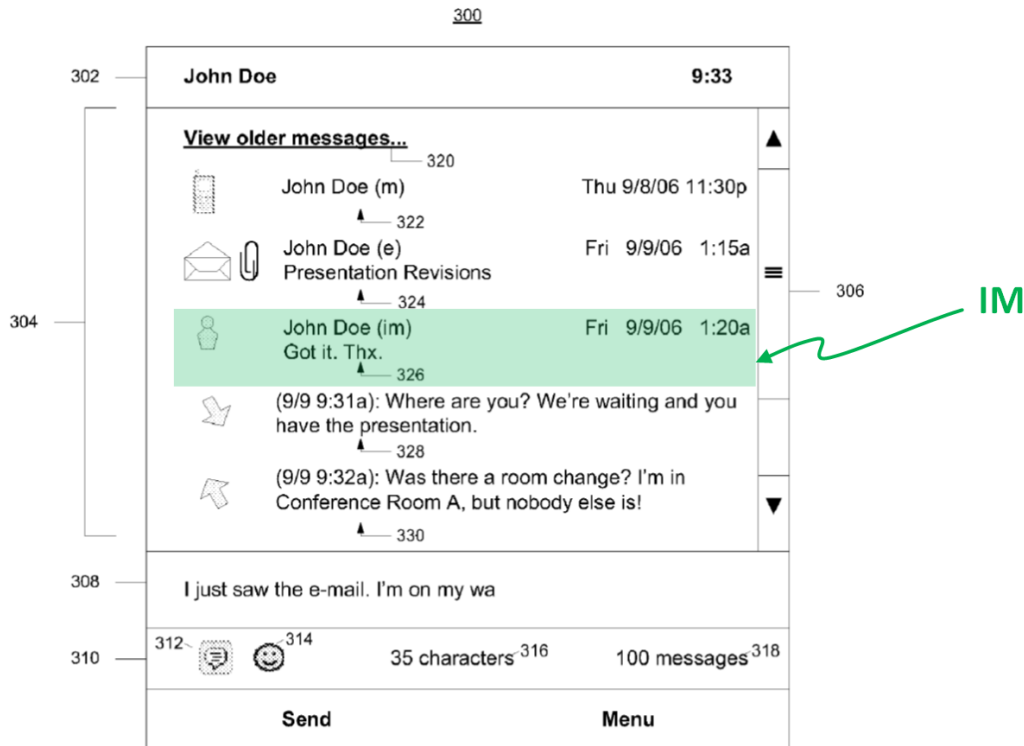
99. Indeed, POSITAs would have known of other systems in which a mobile device directly sends invitation messages to “non-members” of a communication service. *See, e.g.*, APPLE-1079, [0080] (“the communication may be an update request bearing an invitation to join the private network, a download of client software, or the like”), [0085]-[0086] (describing FIG. 4a as showing a member M0 who sends “communications that expose the non-members U to the private network, for example, service requests with invitations to join, e-mails or other messages mentioning the private network service, or the like”); APPLE-1050, [0006] (“initiating mobile device then sends to a target mobile device an invitation message containing the server’s network address and the session identifying information...through a page-mode messaging service (e.g., SMS)”), [0014]-[0015].

100. Accordingly, a POSITA would have found obvious, in Horvath-Tsampalis-Kansal-Quon, that the sending mobile device would *insert[]*, *via the*

client program, second message content into a message for delivery to a mobile wireless device associated with the second phone number (e.g., the application client of the sending mobile device composing an invitation message to a non-user and inserting a link to download the application client and sign-up for the services of the combination, including, for example, Tsampalis’s MFCI services), wherein the second message content is received by the mobile wireless device associated with the second phone number via SMS or EMS protocol (e.g., the invitation message is an SMS, per Quon).

Element [1j]: wherein the service is a service for exchanging message content between subscribers;

101. Horvath-Tsampalis-Kansal-Quon renders obvious Element [1j]. As I previously discussed for Element [1c], one type of message service provided over Horvath’s SIP network is an IM service. APPLE-1004, [0033] (“The SIP network is used for establishing instant messaging...and other real-time communications over the Internet.”). 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)

102. Accordingly, a POSITA would have found obvious that, in Horvath-Tsampalis-Kansal-Quon, *the service is a service for exchanging message content between subscribers* (e.g., an IM service through which users send and receive IMs). *Element [1k]: wherein the service restricts third parties from receiving certain subscriber information absent subscriber consent.*

103. Horvath-Tsampalis-Kansal-Quon renders Element [1k] obvious. The Horvath-Tsampalis-Kansal-Quon application client would have requested presence information, either as part of the MFCI information request and response taught by Tsampalis or directly from the application server(s) hosting the messaging services. See APPLE-1004, [0035] (“The HSS 210 comprises a database including profiles

associated with each wireless device 106 registered with the IMS,” and a profile “includes subscription related information”), [0039] (“An IMS system also includes application servers that host and execute services for the wireless device 106.”); 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.”).

104. For example, Kansal illustrates and describes that “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]. “In some embodiments, an IM icon associated with the message 326 may indicate whether the contact is currently online and available to receive an IM message.” *Id.* This type of status was known as “presence information.” *See, e.g.*, APPLE-1006, [0018] (“presence information for informing subscriber buddies of the login presence of the subscriber”); APPLE-1053, 8:3-7 (“Presence refers to the ability and willingness of a user to communicate information regarding the location and availability of his or her device(s) across various sets of services and devices”); APPLE-1061, [0034] (“various communication media require that a message recipient turn on his/her mobile device,

log in, sign in, or the like, in order to access a message. Such presence information may be received by mobile device 110”); APPLE-1064, 8:23-28 (“‘presence’ information refers to any information describing the status of a user with respect to one or more different communication channels”).

105. According to Quon, “the major Instant Messaging clients” around the Critical Date included “MSN Messenger, GoogleTalk, Yahoo, AIM, and ICQ.” APPLE-1029, [0006]. Each of these clients were known to support some form of presence. *See, e.g.*, APPLE-1007, Title (“instant messaging and presence technologies for college campuses”), Abstract (“Presence provides information about users’ reachability and willingness to accept/reject a brief chat session”), Page 4 (“IM systems, with the ability of providing presence information, enables a user to know the availability of other users. By using presence information, an IM system enables us to search for a specific user, check the user’s status, and send short messages. Popular IM applications include AOL™ Instant Messenger (AIM), ICQ™ (“I Seek You”), MSN™ or WindowsXP™ Messenger, and Yahoo™ Messenger....”). Accordingly, it would have been obvious to integrate presence into the combination’s application client in order to support the presence information already available within these common IM services.

106. Quon further describes when one subscribing user (“inviter”) attempts to add another subscribing user (“invitee”) to their service phonebook the “invitee

service user does not show up in the inviter service user service phonebook until the invitee service user accepts the invitation request.” APPLE-1029, [0045]. It would have been obvious that, until the invitee service user shows up in the inviter service user’s service phonebook, various information about the invitee service user (*e.g.*, “whether the contact is also a service user, the availability of another service user, preferred modes of communication for the other service user and the like”) would not be shared with the inviter. *See* APPLE-1029, [0029]. Indeed, Quon-Prov describes that the messaging system is able to provide “an aggregated view of the collected presence information” for a given user to the user’s other contacts, but that the “type of aggregated presence (*e.g.* aggregated person status, aggregated service status *etc.*) which the contact nodes can receive is determined by the policy specified by the user for privacy protection.” APPLE-1030, 47-49. In other words, Quon explains that a messaging system like that of the combination would advantageously set limits on the type and amount of user information (*e.g.*, presence information) shared with other subscribing and non-subscribing users in order to beneficially maintain appropriate privacy levels. *See id.*

107. Accordingly, a POSITA would have found obvious that, in Horvath-Tsampalis-Kansal-Quon, *the service restricts third parties from receiving certain subscriber information absent subscriber consent* (*e.g.*, the IM service—on its own

or in collaboration with the HSS—restricts what user information, such as presence and other status, is shared with other users within the system).

Claim [2]: The method of claim 1, further comprising: receiving an SMS message, including content originated by a subscriber of the service, subsequent to the phone number associated with the mobile wireless device being authenticated to the service.

108. Horvath-Tsampalis-Kansal-Quon renders Claim [2] obvious. Kansal describes that the unified messaging UI 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 networks], and/or availability of a recipient to receive messages of a certain format.” APPLE-1052, [0078]. Quon-Prov provides examples of when determining and accounting for user preferences is particularly advantageous. *See* APPLE-1030, 20-21.

For outbound communications, a typical user is faced with annoying and time-wasting telephone tag trying to reach the callee through a number of communications services and associated devices such as office line or mobile phone. The callee may elect to avoid the call due to various states of availability, would **prefer** to use an alternate service, or simply cannot access the service such as while away from the office. For instance, while the user is driving, it is difficult to engage with the caller in an instant message session. Likewise, while the user is at home or in the office, the user might have preferred the caller to use the land line due to cost or voice quality preferences.

Id.

109. Indeed, it was well known to use users' preferences when determining how and when to communicate with them. *See* APPLE-1068, [0050] ("user may be provided with the ability to select a preferred mode for the connection, i.e. the least expensive in which case the sending terminal might choose to send a URL to the receiving terminal rather than an entire web page which would require much greater resources"), claim 8; APPLE-1063, [0110] ("The contacts manager 222 is configured to manage a list of the Subscriber's contacts (including groups). This list includes one or more communication devices assigned to said contact persons, capabilities of said devices, senders and/or receivers' preferences, if any, related to destination device, message layout and/or format, etc."), [0122] ("The client may be also configured to request the messaging system for information with regard to subscriber B preferences and/or results of preferred destination device calculations, and the messaging system may be configured to provide such information to the client. After the client obtains information with regard to the destination device, it takes 912 delivery decision and provides the appropriate transcoding 913 matching (fully or partly) the message to capabilities of destination device 94 and communication media.").

110. Accordingly, a POSITA would have found it obvious that a user of a mobile device that is using the combination's application client would provide preference information about how they would like to receive messages, including a

preference of communication mode (e.g., SMS, email, IM), regardless of whether they are authenticated and signed into any particular service (e.g., an IM service). The applications client would send this preference information to, e.g., the HSS 210 that stores user profiles include MFCI and subscription information. See APPLE-1004, [0035], [0041]. The application clients of the user's contacts would receive this preference information along with the MFCI and use it in determining how to communicate with the user, as taught by Kansal. See APPLE-1052, [0078]. For example, the user may indicate a preference to receive communications through SMS under certain circumstances, regardless of whether the user is authenticated and signed-into other messaging services (e.g., an IM service). In at least this case, a POSITA would have found obvious that the Horvath-Tsampalis-Kansal-Quon application client would *receiv[e] an SMS message, including content originated by a subscriber of the service, subsequent to the phone number associated with the mobile wireless device being authenticated to the service.*

111. Additionally or alternatively, *a subscriber of the service* may not always be authenticated with and signed into the service to which they subscriber (e.g., an IM service). Quon provides a similar example where a “contact C has a telephone number, a VoIP account, and an instant messaging screen name,” yet “[a]t any given time,...the user may see that...contact C may be available only through the VoIP account....” APPLE-1029, [0029]. That is, contact C is a subscriber of an

instant messaging service, because they have a screen name, but they may not be signed into that service. *See id.* This may be due to the fact that the user's mobile wireless device only has access to Horvath's circuit-services network, and not currently have access to the packet-data network through which it uses the IM service. *See* APPLE-1004, [0062] (“[i]f the wireless device is not registered on the packet data network 102, the SMS delivery network selector 124 selects the circuit services network 104 for transmission of the SMS message”). In this case, the ***subscriber of the service*** would be forced to communicate by sending ***an SMS message***, even after the ***mobile wireless device [was] authenticated to the service***.

Claim [3]: The method of claim 1, wherein the first message content includes one or more images.

112. Horvath-Tsampalis-Kansal-Quon renders Claim [3] obvious. For example, both Horvath and Tsampalis disclose messaging text as well as multimedia messages, which a POSITA would have understood and found obvious to include images, audio, 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”); APPLE-1061, [0049] (“[i]nputting a message may include composing various types of content, including text, images, sound, and/or the like”); APPLE-1063, [0083] (“The message formats include formats fitting e-mail, Short Message Service, instant messaging, EMS, MMS, SyncML, or/and other electronic messaging services, communication media and protocols thereof. The message content may include a text and/or one or more media items to be transmitted to the other party, wherein the media items may include text files, image files, moving picture files, sound files, hyperlinks, electronic signatures, etc. in any available formats.”).

Claim [4]: The method of claim 1, wherein the service is adapted to identify a subscriber based on a phone number absent user input of a username and absent user input of an email address.

113. Horvath-Tsampalis-Kansal-Quon renders Claim [4] obvious. As I previously discussed for Element [1a], each of Tsampalis, Kansal, and Quon confirm that information regarding the services to which a user of a given mobile device is subscribed may be determined based on a telephone number of the user’s mobile device. See APPLE-1005, [0033], [0035], [0061]; APPLE-1042, [0037]-[0038], [0041]-[0042], [0066] (“[t]he sender or the recipient may be determined using various types of identifying information associated with a particular message such as a telephone number, e-mail address, IM screen name, SMS identifier, MMS identifier, and so forth”); APPLE-1029, [0007] (the “system allows a service’s user

to import contacts from the user's pre-existing mobile phone book and send invitations to the contacts based on the contact telephone numbers to join and become members of the service”), [0030] (“application client 1 may communicate with service core 7 to determine which contacts are also service users, such as by a comparison of mobile number or service ID”), [0037] (“[i]f service user B is added based on user B mobile number by service user A, service user B is added to service user's service phonebook, and service user A will see the presence of service user B, and service user A can initiate communications with service user B via the service”).

114. In fact, Quon describes an example in which “the service user may decide to invite non-user contacts manually,” in which case “the service user may be presented with a list of the service user's non-user contacts with mobile numbers to invite.” APPLE-1029, [0031]. On the other hand, “[w]hen service user A adds or imports a mobile number belonging to service user B, the service can automatically send an add request to service user B to add service user A to service user B's service phonebook.” APPLE-1029, [0037]. In either case, the system is recognizing a user based only on its telephone number.

115. Accordingly, a POSITA would have found obvious that, in Horvath-Tsampalis-Kansal-Quon, *the service is adapted to identify a subscriber based on a phone number absent user input of a username and absent user input of an email address.*

Claim [5]: The method of claim 1, wherein the client program is adapted to send a message to a subscriber based on each one of a user name, phone number and email address.

116. Horvath-Tsampalis-Kansal-Quon renders Claim [5] obvious. Kansal describes that “identifying information (e.g., telephone number, e-mail address, IM screen name, SMS identifier, MMS identifier, etc.), included in messages received by the messaging applications 130 may be compared against the contacts database 142 to identify the sender of a message.” *See* APPLE-1042, [0038]. “The contacts database 142 also may be used or accessed when composing and/or sending messages.” *Id.*

117. As I previously discussed for Claim [4], “[i]nstant messages may be directed to the instant messaging service to which the user subscribes, with the user being identified with a username,” otherwise known as a “screen name.” APPLE-1016, [0019], [0030]; APPLE-1029, [0024] (“instant messaging service screen names”); *see also* APPLE-1024, 3:28-35 (“each communication type for a user is associated with one or more addresses” such as “a username for an instant message client is used to contact a user through IM”); APPLE-1059, [0025] (“Instant messages can be addresses using a User-ID which is a unique instant messaging address assigned to a user. The User-ID is syntactically equivalent to an e-mail address. It has the format alphanumeric string or alphanumeric string@domain. A user may also be referred to by screen names, nicknames and aliases.”). A POSITA

would have known and found obvious that the “IM screen name” or “username” used to address instant messages to a receiving mobile phone may be an e-mail address of the receiving user. *See, e.g.*, APPLE-1062, [0053]-[0054], [0064] (describing a user being “connected to an instant messaging server” with a work e-mail address); APPLE-1032, [0017] (“virtual communities (e.g., communities hosted on social networking sites such as...Instant Messenger, ICQ...”), [0025] (“the user ID that is associated with the user’s virtual community account (e.g., an e-mail address”), FIGS. 2 (“UserID (e.g., e-mail address) for this account”), 5; APPLE-1033, 3:4-5, 4:2-6.

118. Accordingly, a POSITA would have found obvious that, in Horvath-Tsampalis-Kansal-Quon, *the client program is adapted to send a message to a subscriber based on each one of a user name (e.g., IM screen name), phone number and email address.*

Claim [6]: The method of claim 1, wherein a server of the service which maintains a subscriber list is located outside of a cellular network.

119. Horvath-Tsampalis-Kansal-Quon renders obvious Claim [6]. As I previously discussed for Element [1k], Horvath describes that “[a]n IMS system also includes application servers that host and execute services for the wireless device 106.” APPLE-1004, [0039]. One type of service provided over Horvath’s SIP network is an IM service. APPLE-1004, [0033]. A POSITA would have found it obvious that, in an SIP 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-1004, [0039] (“An IMS system also includes application servers that host and execute services for the wireless device 106.”).

120. A POSITA would have found obvious that the IMS domain is distinct from the cellular core network, and therefore the application server that provides the IM service and is part of the IMS domain *is located outside of a cellular network*. See APPLE-1004, [0039]; APPLE-1072, FIG. 3 (illustrating the application servers 360 outside of the core network 310), [0059]-[0061] (application servers 360 “interface to one or more CSCF servers 320 of the core network 310,” and therefore are outside the cellular network); APPLE-1074, FIGS. 5A-5C (illustrating the application servers, including an instant multimedia messaging application server 626, as distinct from the “Common Access Layer” that includes the cellular networks, such as GSM and CDMA); [0068] (describing a “Common Access Layer [that] includes network infrastructure such as that found in a cellular network, and

which may be common to various types of networks”), [0069]; APPLE-1014, [0006] (describing the circuit-services GSM network as a “cellular network”), [0047].

121. A POSITA would have further found obvious that the application server of the IM service *maintains a subscriber list*. For example, Horvath describes that “[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. APPLE-1004, [0041]. In other words, the application server receives notifications for all of the registered wireless devices to which they are to provide services, and because the provision of these services would have been an ongoing function, the application server would have kept a list of the registered and subscribed wireless devices. *See id.* Indeed, it was well known that application servers providing messaging services maintained lists of information about subscribers, such a presence information. *See, e.g.,* APPLE-1046, [0035] (“...the application server maintains the online status of the user despite the user being temporarily disconnected. Any messages directed to the user during this time may be temporarily stored in a memory and then sent to the second device once the second device has logged in the application server.”); APPLE-1006, [0004] (“Conventional instant message (IM)...typically require that potential IM participants...must register and establish a connection with an IM login server. Participant-specific information, such as presence contact information, is

generated through this registration and is stored in a database associated with the IM login server for the duration of the IM session.”).

122. Accordingly, a POSITA would have found obvious that, in Horvath-Tsampalis-Kansal-Quon, *a server of the service* (e.g., an application server providing the IM service) *which maintains a subscriber list is located outside of a cellular network*.

Claim [7]: The method of claim 1, further comprising: transmitting, via the client program, third information comprising a third phone number; and receiving, via the client program, an indication that a user name associated with the third phone number is associated with a subscriber of the service.

123. Horvath-Tsampalis-Kansal-Quon renders Claim [7] obvious. A POSITA would have understood and found obvious that the Horvath-Tsampalis-Kansal-Quon sending mobile device would follow the procedures that I previously described with respect to Elements [1d], [1e1], and [1e2], every time that a user creates a new message and/or enters a new recipient ID for a message. *See* APPLE-1005, [0033], [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].

124. As I previously discussed for Element [1a], each of Tsampalis, Kansal, and Quon confirm that information regarding the services to which a user of a given mobile device is subscribed may be determined based on a telephone number of the user’s mobile device. *See* APPLE-1005, [0033], [0035], [0061]; APPLE-1042, [0037]-[0038], [0041]-[0042], [0066] (“[t]he sender or the recipient may be determined using various types of identifying information associated with a particular message such as a telephone number, e-mail address, IM screen name, SMS identifier, MMS identifier, and so forth”); APPLE-1029, [0007] (the “system allows a service’s user to import contacts from the user’s pre-existing mobile phone book and send invitations to the contacts based on the contact telephone numbers to join and become members of the service”), [0030] (“application client 1 may communicate with service core 7 to determine which contacts are also service users, such as by a comparison of mobile number or service ID”), [0037] (“[i]f service user B is added based on user B mobile number by service user A, service user B is added to service user’s service phonebook, and service user A will see the presence of service user B, and service user A can initiate communications with service user B via the service”).

125. A POSITA would have found it obvious that the profiles stored by the HLR 202 and/or HSS 210 would include information about all of a user's devices and addresses on the various messaging services, because this would have helped in identifying the best way to send a message to the user and then sending it. For example, Kansal teaches the "contact record for an individual may comprise identifying information such as first name, last name, company/employer name, mailing addresses (e.g., home, work, other), telephone numbers (e.g., home, work, mobile, fax, pager), e-mail address (e.g., home, work, primary, alternative), IM screen names, SMS identifier, MMS identifier, personal information, notes, and so forth." APPLE-1042, [0037]. In other words, it was known that a user would have multiple devices (e.g., multiple telephones) and addresses, and that a profile of that user (e.g., a contact record in a contact database) would include information about each of these multiple devices. *See id.*; *see also* APPLE-1053, 4:34-41 (describing "generation of personal resource files or databases that are associated with respective individuals and include information relating to, for example, the protocols, capabilities, addresses, bearers and security associations relating to each of the individual's personal devices (e.g., his or her cellular telephone, PDA, pager, PC, laptop, home media server, etc.)"), 5:24-43; APPLE-1063, [0110] ("[C]ontacts manager 222 is configured to manage a list of the subscriber's contacts," and includes "one or more communication devices assigned to said contact persons,

capabilities of said devices, senders and/or receivers' preferences, if any, related to destination device, message layout and/or format, etc.” “[S]aid information or parts thereof and/or derivatives thereof may be stored in one or more external databases, and the contact manager may have capabilities to access such information.”), APPLE-1064, 8:20-51, 11:4-7. Thus, a sending mobile wireless device would have transmitted a request for MFCI based on a receiving mobile wireless device's telephone number, and included with the MFCI would be information about all of a user's devices and addresses (e.g., screen names) on the various messaging services.

126. Accordingly, a POSITA would have found obvious that Horvath-Tsampalis-Kansal-Quon's sending mobile wireless device would *transmit[], via the client program, third information comprising a third phone number* (e.g., a request for MFCI based on a receiving mobile wireless device's telephone number); *and receiv[e], via the client program, an indication that a user name associated with the third phone number is associated with a subscriber of the service* (e.g., receiving an MFCI response that includes all of the information about all of a user's devices and addresses, such as screen names).

Claim [8]: The method of claim 1, wherein the client program automatically determines whether a phone number is associated with a subscriber and when a phone number is not associated with a subscriber, the client program is adapted to provide an invitation, via SMS, for a non-subscriber to subscribe to the service.

127. *Supra*, §VIII.A, Analysis of [1i] (describing that the combination’s application client would have determined whether a phone number of a contact is associated with a subscriber, and, if not, sent an SMS invitation to the phone number).

Claim [9]: The method of claim 1, wherein the service distinguishes between active and inactive subscribers.

128. Horvath-Tsampalis-Kansal-Quon renders Claim [9] obvious. As I previously discussed for Element [1k], a POSITA would have found obvious that the Horvath-Tsampalis-Kansal-Quon application client would have requested presence information, either as part of the MFCI information request and response taught by Tsampalis or directly from the application server(s) hosting the messaging services. A POSITA would further have found obvious that “active” and “inactive” were well known types of presence information and would have been determined by the IM service. *See, e.g.*, APPLE-1063, 7:5-15, 7:45-52 (“the client CPE software and is used to determine when the user is inactive for a predetermined period of time, and therefore possibly away from a CPE device which is registered as online. In step 260, the CPE device continuously monitors for user interaction with a user interface of the CPE device and relays changes in state with the server.”), 7:55-59 (“If interaction with a user interface of the CPE device is sensed, and the previous state was inactive, then the CPE device generates an active message and conveys the active message to the CSP via the Instant Message (IM) server”); APPLE-1080, [0070] (“inactive” is a “presence state”), [0086]; APPLE-1081, [0021] (“The

conditions may also include the fact that the user's instant messaging client is active or inactive.”).

129. Accordingly, a POSITA would have found it obvious that, in Horvath-Tsampalis-Kansal-Quon, *the service distinguishes between active and inactive subscribers* (e.g., the IM service tracks presence of the users and presence includes whether subscribers are active or inactive).

Claim [10]: The method of claim 1, wherein the second message content includes an invitation to subscribe to the service.

130. *Supra*, §VIII.A, Analysis of Claim [1i].

Claim [11]: The method of claim 1, wherein the second message content includes a universal resource locator (URL) indicative of the service.

131. *Supra*, §VIII.A, Analysis of Claim [1i].

Claim [12]: The method of claim 1, wherein the client program is adapted to: receive as input, address information consisting of a third phone number; receive as input, address information consisting of a fourth phone number; send a group message, via a packet switched bearer, to a plurality of mobile wireless devices, based on the third phone number and the fourth phone number.

132. Horvath-Tsampalis-Kansal-Quon renders Claim [12] obvious. A POSITA would have understood and found obvious that the Horvath-Tsampalis-Kansal-Quon sending mobile device would follow the procedures that I previously described with respect to Elements [1d], [1e1], and [1e2], every time that a user creates a new message and/or enters a new recipient ID (e.g., a third phone number and a fourth phone number) for a message. See APPLE-1005, [0033], [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].

133. Further, Tsampalis teaches “the use of an active message recipient list” having a plurality of recipients in a single active message, each recipient having a “recipient ID” that the user enters in the form of phone numbers for the same active message that the use composes. See e.g., APPLE-1005, [0004] (“list of delivery recipients” for “a message”), [0009], [0032], [0055] (“groups of recipients”), FIG. 4 (below).

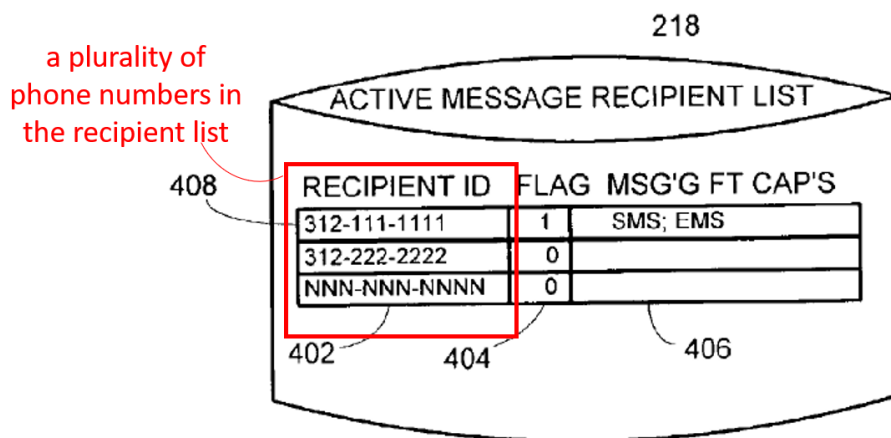


FIG. 4

APPLE-1005, FIG. 4 (Annotated)

134. A POSITA would have found obvious that Horvath-Tsampalis-Kansal-Quon's method comprises sending a group-based message to the third receiving mobile device and to a fourth receiving mobile device, in accordance with at least Tsampalis.

135. Furthermore, the group message would have been sent via a packet switched bearer when the sending, third, and fourth mobile wireless devices are all associated with subscribers to the IM service, and the sending mobile wireless device determines to send the message via the IM service. See, e.g., APPLE-1004, [0024] (“[t]he packet data network 102...comprises...a General Packet Radio Service (‘GPRS’) network”), [0033] (“SIP network is used for establishing instant messaging” and describing the SIP network as being reached via the packet-data network); APPLE-1055, [0014] (describing GPRS as a “packet-switched bearer”); APPLE-1054, 4:42-46 (same).

136. Accordingly, a POSITA would have found it obvious that, in Horvath-Tsampalis-Kansal-Quon, the client program is adapted to: receive as input, address information consisting of a third phone number (e.g., a user enters a third phone number as a recipient ID into an active message recipient list); receive as input, address information consisting of a fourth phone number (e.g., a user also enters a fourth phone number as a recipient ID into the same active message recipient list);

send a group message, via a packet switched bearer (e.g., GPRS), to a plurality of mobile wireless devices, based on the third phone number and the fourth phone number (e.g., Tsampalis's send message circuitry "loop[s] through of the recipient IDs 402 in the active message recipient list 218 to send messages to each designated recipient").

Claim [13]: The method of claim 1, further comprising: receiving, via the client program, at least one message from at least one subscriber, via a push model.

137. Horvath-Tsampalis-Kansal-Quon renders Claim [13] obvious. A POSITA would have known that "some representative push technologies include Short Message Service (SMS), Wireless Application Protocol (WAP) Push, Multimedia Messaging Service (MMS), Session Initiation Protocol (SIP), as well as others" *See* APPLE-1083, 2:11-14; *see also* APPLE-1082, [0033] ("The application server gets messages from the presence handler unit whenever the called party registers/unregisters a device or starts/ends a connection. These are pushed messages with a low rate of many seconds between messages."). Horvath teaches that its system sends and receives SMS, MMS, and IM, which are all operated as a ***push model***. APPLE-1004, [0033], [0039].

Claim [14]: The method of claim 1, wherein the certain subscriber information is comprised of contact information, wherein the contact information is information used to send messages to the client program.

138. As I previously discussed for Element [1k], a POSITA would have found obvious that, until the invitee service user shows up in the inviter service

user's service phonebook, various information about the invitee service user (e.g., "whether the contact is also a service user, the availability of another service user, preferred modes of communication for the other service user and the like") would not be shared with the inviter. *See* APPLE-1029, [0029]. A POSITA would have known that "preferred modes of communication" is a type of ***contact information used to send messages to the client program.***

Claim [15]: The method of claim 1, wherein, based on a second response, the mobile wireless device associated with the second phone number receives an SMS message having content originated via the client program.

139. *Supra*, §VIII.A, Analyses of Elements [1h] (describing that, for certain receiving mobile devices, the HLR 202 and/or HSS 210 would provide a response when the phone number of the receiving mobile device is not associated with a subscriber of an IM service), [1i] (describing invitation is sent from the combination's application client via SMS).

Claim [16]: The method of claim 1, wherein the first message content includes at least one of an image, video or animation.

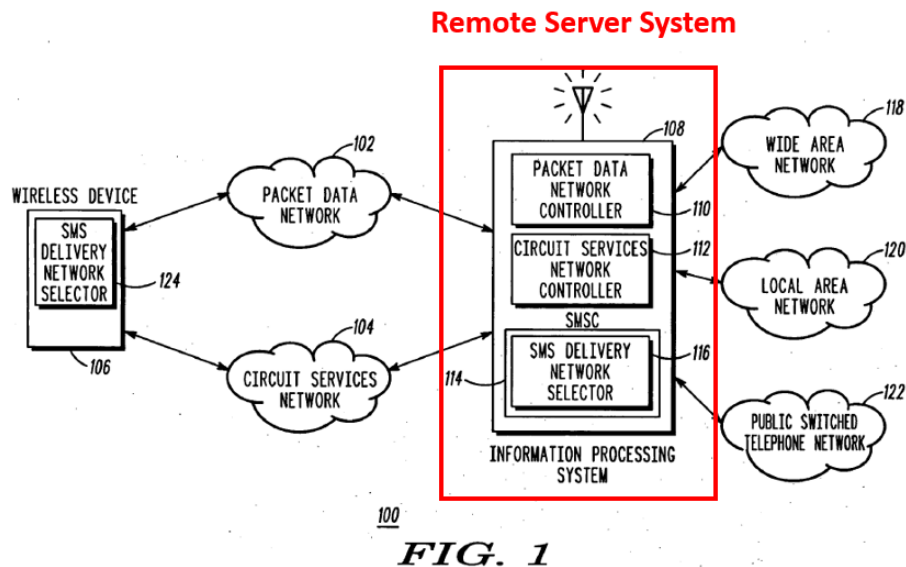
140. *Supra*, §VIII.A, Analysis of Claim [3].

Claim [17]: The method of claim 1, wherein the first phone number is retrieved, by the client program, from a message being composed.

141. *Supra*, §VIII.A, Analysis of Element [1d].

Element [18pre]: A server system for supporting a plurality of client programs, the server system comprising:

142. To the extent the preamble is limiting, Horvath-Tsampalis-Kansal-Quon renders Element [18pre] obvious. Horvath describes an information processing system 108 that “includes, in one embodiment, a packet data network controller 110 and a circuit services network control 112 for maintaining each network 102, 104, respectively.” APPLE-1004, [0028].



APPLE-1004, FIG. 1 (Annotated)

143. Horvath describes that wireless communication system 100 includes a home location register (“HLR”) 202 and a mobile switching center (“MSC”) 204 that are coupled to and control the circuit services network. APPLE-1004, [0002]-[0003], [0031]-[0033] (MSC 204 “controls switching functions” and HLR 202 “achieve[s] connection control in a telephony network”), FIGS. 1, 2. The wireless communication system 100 also includes a “proxy call session control function (‘P-

CSCF') 206," an "interrogating/serving call session control function ('I, S-CSCF') 208," and a "registrar such as a home subscriber server ('HSS')," which are coupled to the packet switched network. See APPLE-1004, [0004], [0006], [0008], [0028], [0033]-[0038], [0075]-[0076], FIGS. 1, 2, 3.

144. Horvath teaches that, "[a]lthough only the SMSC 114 is shown as residing in the main memory 306, any combination of IMS components such as the P-CSCF 206, I,S-CSCF 208, and HSS 210 can also reside in the main memory 306." APPLE-1004, [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," which can run the "Windows Server 2003 operating system." APPLE-1004, [0052], [0057]. Accordingly, Horvath teaches *a server system* (e.g., information processing system 108 including at least P-CSCF 206, I,S-CSCF 208, and HSS 210).

145. Horvath describes that "[t]he packet data network 102 and the circuit services network 104 support any number of wireless devices 106." APPLE-1004, [0027]. As I previously discussed for Element [1a], the combination includes a single application client downloaded to and run on the wireless devices to achieve the benefits identified in §VII.E. Because the information processing system 108 (*server system*) includes controllers for each of the networks 102 and 104—thus supporting the networks—and the networks support any number of wireless devices

106 executing the combination's application client, the information processing system 108 (*server system*) *support[s] a plurality of client programs*.

Element [18a]: a storage device;

146. Horvath-Tsampalis-Kansal-Quon renders Element [18a] obvious. Horvath describes that the information processing system 108 “includes a computer 302” that “has a processor 304...connected to a main memory 306” (*a storage device*).

Element [18b]: and a network interface that supports Internet Protocol (IP): wherein the server system:

147. Horvath-Tsampalis-Kansal-Quon renders Element [18b] obvious. Horvath teaches that the information processing system 108 has a “network adapter hardware 312” that is used to provide “an interface to the packet data network 102 and the circuit services network 104” (*a network interface*), where the packet data network 102 is “an Internet Protocol (‘IP’) connectivity network, which provides data connections at much higher transfer rates than [*sic*] a traditional circuit services network” (*supports Internet Protocol (IP)*). APPLE-1004, [0024], [0058], FIGS. 1-3.

Element [18c]: authenticates a phone number associated with a first mobile wireless device, upon which a client program operates, to a service for sending and receiving packet switched messages, via short message service (SMS) protocol;

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

Element [18d]: adds the phone number to a subscriber list, stored on the storage device, based on the authentication;

149. Horvath-Tsampalis-Kansal-Quon renders Element [18d] obvious. As I previously discussed for Element [1c], the information processing system 108 registers and authenticates the wireless devices 106, through the S-CSCF, P-CSCF 206, and HSS 210. *See* APPLE-1004, [0035]-[0041]. Horvath describes that HSS 210—a part of information processing system 108—“comprises a database including profiles associated with each wireless device 106 registered with the IMS.” APPLE-1004, [0035]. HSS 210 identifies each registered wireless device 106 with a “tel-URI, [which] for example is the telephone number assigned to the wireless device 106.” *Id.*

150. Accordingly, a POSITA would have found it obvious, in Horvath-Tsampalis-Kansal-Quon, that the server system (*e.g.*, information processing system 108) ***adds the phone number to a subscriber list*** (*e.g.*, the addition of a new wireless device 106 profile to the database), ***stored on the storage device*** (*e.g.*, because HSS 210 is part of information processing system 108, at least a portion of the profile database will be stored in main memory 306, particularly where the HSS 210 is performing any functions with respect to the profiles), ***based on the authentication*** (*e.g.*, the creation of a profile results from wireless device 106 registering, which requires authentication).

Element [18e]: receives information, from the client program, comprising a numeric identifier;

151. *Supra*, §VIII.A, Analysis of Element [1d].

Element [18f]: determines that a user name is associated with the numeric identifier;

152. *Supra*, §VIII.A, Analyses of Element [1d] and Claim [7].

Element [18g]: sends a response, to the client program, the response indicating that the user name associated with the numeric identifier is associated with a subscriber of the service;

153. *Supra*, §VIII.A, Analyses of Elements [1e1]-[1e2] and Claim [7].

Element [18h]: receives content originated from the client program, via the network interface, and provides the content to another client program operable on a second mobile wireless device associated with the user name;

154. Horvath-Tsampalis-Kansal-Quon renders obvious Element [18h]. As I previously discussed for Claim [6], a POSITA would have found it obvious that, in an SIP 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. Horvath describes that “application server interfaces with the S-CSCF component of the I,S-CSCF 208 using SIP.” APPLE-1004, [0039]. “The S-CSCF [] determines which application server(s) to forward [an] SIP message associated with the wireless device 106 so that the services subscribed to by the device 106 can be provided.” APPLE-1004, [0038]. In other words, the S-CSCF component of the I,S-CSCF 208 acts as a router for the SIP messages sent between wireless devices 106 and the application server(s). *See* APPLE-1004, [0038]-[0039]. Because the

I,S-CSCF 208 is part of the information processing system 108, the messages routed through the I,S-CSCF 208 would be received via the network adapter hardware 312 (*the network interface*) that is used to provide “an interface to the packet data network 102.” *See* APPLE-1004, [0052].

155. One type of service provided over Horvath’s SIP network is an IM service. APPLE-1004, [0033]. As I previously discussed for Claim [6], a POSITA would have found it obvious that, in an SIP 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. IM servers “facilitat[e] passage of instant messages between subscribers who have registered.” *See, e.g.*, APPLE-1006, [0018]. Thus, IM messages would be sent by a sending mobile device, routed through the information processing system 108 to the IM service application server, and then passed to a receiving mobile device via the information processing system 108 (particularly where the sending and receiving mobile devices shared the same home network). An example of this message flow is illustrated below, where the sending mobile device 701 sends an IM to the IM service application server 704 (shown by green arrows) and the IM service application server 704 passes the IM to the receiving mobile device 703 (shown by blue arrows).

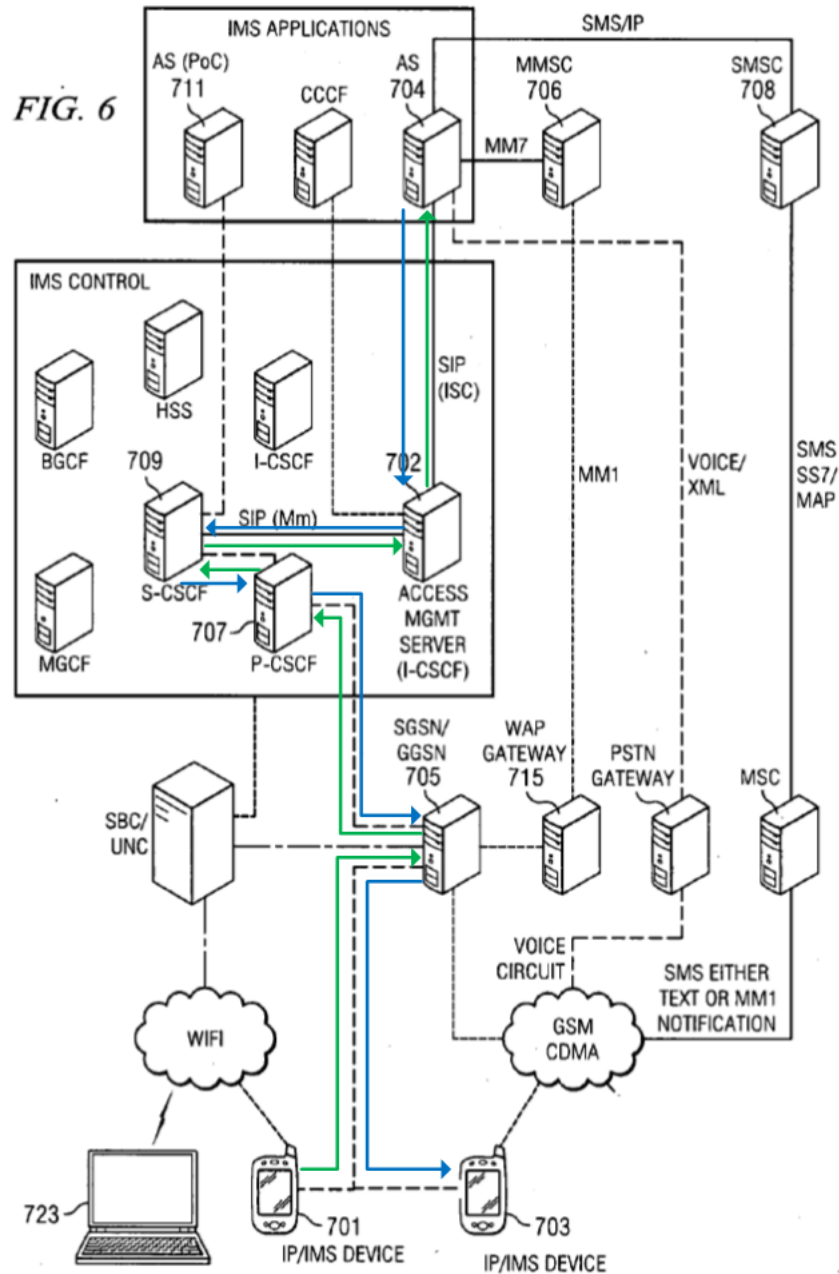


Diagram Based on Modified FIG. 6 of APPLE-1074

156. “Instant messages may be directed to the instant messaging service to which the user subscribes, with the user being identified with a username,” otherwise known as a “screen name.” APPLE-1016, [0019], [0030]; APPLE-1029, [0024]

(“instant messaging service screen names”); *see also* APPLE-1024, 3:28-35 (“each communication type for a user is associated with one or more addresses” such as “a username for an instant message client is used to contact a user through IM”); APPLE-1059, [0025] (“Instant messages can be addresses using a User-ID which is a unique instant messaging address assigned to a user. The User-ID is syntactically equivalent to an e-mail address. It has the format alphanumeric string or alphanumeric string@domain. A user may also be referred to by screen names, nicknames and aliases.”).

157. Accordingly, a POSITA would have found it obvious, in Horvath-Tsampalis-Kansal-Quon, that the server system (*e.g.*, information processing system 108) ***receives content originated from the client program*** (*e.g.*, an IM message composed with the application client through the unified messaging UI), ***via the network interface*** (*e.g.*, via the network adapter hardware 312 of information processing system 108), ***and provides the content to another client program operable on a second mobile wireless device associated with the user name*** (*e.g.*, routing the sending mobile device’s IM to the application server of the IM service and then on to the application client of the receiving mobile device).

Element [18i]: receives a first phone number, from the client program;

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

Element [18j1]: provides a first response to the receipt of the first phone number

159. *Supra*, §VIII.A, Analysis of Element [1e1].

Element [18j2]: indicating that the first phone number corresponds to a subscriber of the service;

160. *Supra*, §VIII.A, Analysis of Element [1e2].

Element [18k1]: receives a second phone number, from the client program and

161. *Supra*, §VIII.A, Analysis of Element [1g].

Element [18k2]: determines that the second phone number does not correspond to a subscriber of the service;

162. *Supra*, §VIII.A, Analysis of Element [1h].

Element [18l]: wherein the client program is adapted to insert message content into a message to be sent to a third mobile wireless device which is not associated with a subscriber of the service, wherein the message to be sent is addressed to a phone number.

163. *Supra*, §VIII.A, Analyses of Elements [1h]-[1i] (the same mechanism for inserting message content into a second message addressed to the second phone number of second receiver mobile wireless device which is not associated with a subscriber of the IM service, as discussed above for Elements [1h]-[1i], applies to inserting message content into a message addressed to a phone number of a third receiver mobile wireless device which is not associated with a subscriber of the IM service).

Claim [19]: The server system of claim 18, wherein the server system routes graphical content between subscribers.

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

Claim [20]: The server system of claim 18, wherein the client program is adapted to send messages based on voice input.

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

Claim [21]: The server system of claim 18, wherein the user name comprises an @ symbol.

166. *Supra*, §VIII.A, Analysis of Element [18h]; APPLE-1059, [0025] (“Instant messages can be addresses using a User-ID which is a unique instant messaging address assigned to a user. The User-ID is syntactically equivalent to an e-mail address. It has the format alphanumeric string or alphanumeric string@domain.”).

Claim [22]: The server system of claim 18, wherein the server system receives another request, from the first mobile wireless device, the another request comprising an email address; wherein the server system determines whether the email address of the another request is on the subscriber list and provides a response to the another request.

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

Claim [23]: The server system of claim 18, wherein the server system does not disclose certain information to third parties absent user consent.

168. *Supra*, §VIII.A, Analysis of Element [1k].

Claim [24]: The server system of claim 18, wherein the numeric identifier is in a format of a phone number.

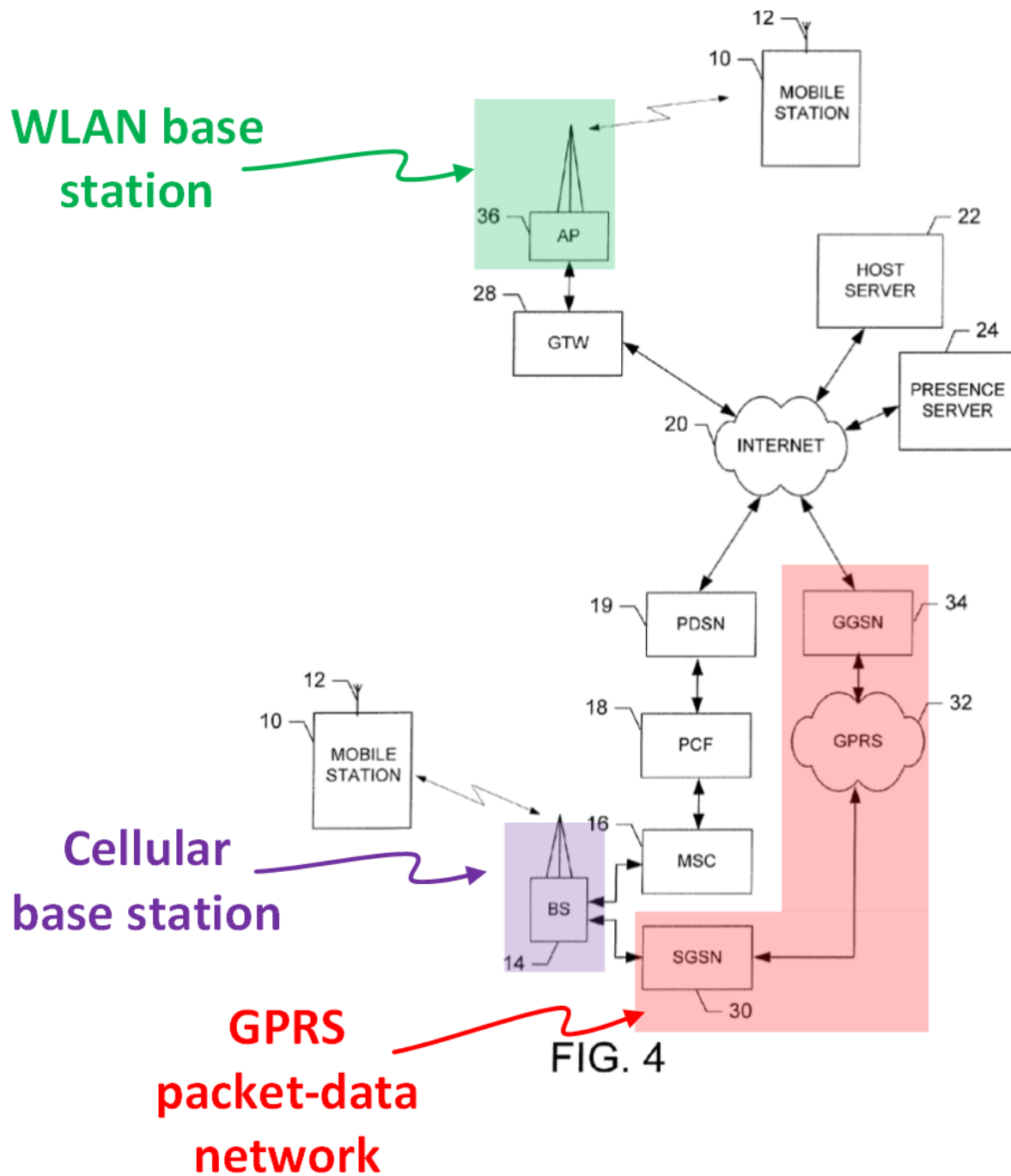
169. *Supra*, §VIII.A, Analyses of Elements [1c]-[1d].

Element [25pre]: A system comprising:

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

Element [25a]: a base station; and

171. Horvath-Tsampalis-Kansal-Quon renders Element [25a] obvious. 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”). And 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: (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.



APPLE-1053, FIG. 4 (Annotated)

Element [25b]: a server system that:

172. *Supra*, §VIII.A, Analysis of Element [18pre].

Element [25c]: receives a subscription message, from a first mobile wireless device having a message client, the subscription message indicating that the first mobile wireless device is subscribing to a service for sending and receiving messages other than Short Message Service (SMS) messages, Enhanced Messaging Service (EMS) messages and Multimedia Messaging Service (MMS) messages;

173. Horvath-Tsampalis-Kansal-Quon renders Element [25c] obvious. As I previously discussed for Claim [6], a POSITA would have found it obvious that, in an SIP 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. “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.” APPLE-1004, [0041]. Horvath describes that these subscriber profiles are stored in the HSS database, which is included in the information processing system 108 (*server system*). APPLE-1004, [0035].

174. At the time a mobile device subscribes to services of an application server, the “subscription updates the subscriber record in the IMS HSS.” *See, e.g.*, APPLE-1014, [0058], [0077]. When a user subscribed to Horvath-Tsampalis-Kansal-Quon’s IM service, a POSITA would have found obvious that the mechanism for updating the subscription information stored in the HSS would have been ***a subscription message indicating that the first mobile wireless device is subscribing to*** the IM service, because the subscription information would have to

be communicated to the HSS in some form of message in order to update the appropriate subscriber profile. *See id.*

175. Horvath-Tsampalis-Kansal-Quon's IM service is a packet-switched message service that is for sending and receiving packet-switched messages other than SMS, EMS, and MMS messages, over the packet data network (*e.g.*, the "SIP network" / "IMS network"). *See* APPLE-1004, [0033] ("The SIP network is used for establishing instant messaging..."). A POSITA would have 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, the IM service implemented by Horvath's SIP network would have been *a service for sending and receiving messages other than Short Message Service (SMS) messages, Enhanced Messaging Service (EMS) messages and Multimedia Messaging Service (MMS) messages.*

Element [25d]: receives a first request, from the first mobile wireless device via the base station, the first request comprising a numeric identifier in the format of a phone number, wherein the numeric identifier is retrieved, by the first mobile wireless device, from a message being composed;

176. As I previously discussed for Element [1d], Tsampalis teaches that an "active message" being composed by a user of the sending mobile device contains a "recipient ID" received from the user, *e.g.*, a phone number in the form of a MSISDN. *See* APPLE-1005, FIG. 4, [0032]-[0033], [0046], [0061], [0064], FIGS. 3-4, 7, 10;

APPLE-1052, 12:53-60; *see also* APPLE-1042, [0037]-[0038], [0066], [0072]. Tsampalis describes that as a user enters message text (*a message being composed*) and an active message recipient list into the sending mobile device'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 device entered into the active message recipient list. APPLE-1005, [0033]; *see also id.*, [0046]. If the MFCI is not available in the sending mobile device's local phonebook or the phonebook's information has not been updated within a certain period of time, "the remote message format capabilities determinator circuitry 208 [of the sending mobile device] is then invoked and generates a second mobile wireless communication device messaging format capabilities information request 226." APPLE-1005, [0033]-[0034].

177. As I previously discussed for Element [1d], to obtain the MFCI, it would have been obvious for the combination's sending mobile device to send a request that included the telephone number of the receiving mobile device 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].

178. As I previously discussed for Element [25a], Horvath explains that the “packet data network 102...comprises...a General Packet Radio Service (‘GPRS’) network...,” and a mobile device communicating, for example, via GPRS communicates with a **base station** of a cellular network. See APPLE-1004, [0024]; APPLE-1053, FIG. 4, 12:54-13:60. That is, all communications with the IMS network, including, e.g., the HSS 210, would have been through the packet-data network and therefore *via the base station*.

179. Accordingly, a POSITA would have found it obvious, in Horvath-Tsampalis-Kansal-Quon, that the server system (e.g., information processing system 108) *receives a first request* (e.g., HSS 210 of the IMS network receives an MFCI request), *from the first mobile wireless device via the base station* (e.g., from a sending mobile wireless device), *the first request comprising a numeric identifier in the format of a phone number* (e.g., the MFCI request includes the recipient ID entered by the user of the sending mobile wireless device, which would have been telephone number), *wherein the numeric identifier is retrieved, by the first mobile wireless device, from a message being composed* (e.g., the send message circuitry of the sending mobile wireless device invokes the remote message format capabilities determinator circuitry 208 while an “active message” is being composed).

Element [25e]: determines that an email address is associated with the numeric identifier and that the email address is associated with a second mobile wireless device;

180. As I previously discussed for Element [1d], one network element in which a POSITA would have found obvious to store MFCI is the HSS. *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.*

181. Indeed, Kansal describes that “[t]he contact record for an individual may comprise identifying information such...telephone numbers (e.g., home, work, mobile, fax, pager), e-mail address (e.g., home, work, primary, alternative), IM screen names, SMS identifier, MMS identifier,... and so forth.” APPLE-1042, [0037]. “The contacts database 142 also may be used or accessed when composing and/or sending messages.” APPLE-1042, [0038]. And Quon teaches that “the service phonebook may have various features, but preferably it contains at least contact names and associated contact information, such as mobile or land-based

phone numbers, instant messaging screen names, email addresses, and the like.” APPLE-1029, [0029]. In other words, it was known to create profiles that associated all of a user’s public identities.

182. Thus, a POSITA would have found obvious that the MFCI and service-subscription information for the registered wireless mobile devices would have included any available contact addresses for the services associated with the registered wireless mobile devices. *See* APPLE-1004, [0075]; APPLE-1005, [0029], [0031]; APPLE-1042, [0037]-[0038]; APPLE-1076, [0011] (teaching that databases within the IMS network were known to “be used to map a dialed telephone number to an SIP/telephone uniform resource identifier (URI), an email address URI, an instant messaging (IM) URI (for presence or chat), a website address, etc.”); APPLE-1074, [0010] (recognizing that a “single subscriber may have multiple identities, including different identities for phone-based services, such as voice and SMS or MMS, as well as identities for other communication channels such as instant messaging and e-mail”), [0052] (describing a network element that maps the various identities across communication channels); APPLE-1082, [0009] (describes “provid[ing] a single, controlled contact point” that bundles “the private and office personal communication and IT services such as fixed and mobile phones, email, IM, SMS, etc.”).

183. Accordingly, a POSITA would have found it obvious, in Horvath-Tsampalis-Kansal-Quon, that the server system (*e.g.*, information processing system 108) *determines that an email address is associated with the numeric identifier and that the email address is associated with a second mobile wireless device* (*e.g.*, the subscriber profiles stored by the HSS would include all of a user's public identities, such the user's telephone numbers and email addresses, and as a user provided these various public identities through interactions with the IMS system, the HSS would determine associations between identities and devices in order to map all of a user's contact information).

Element [25f1]: sends, based on the determination that the email address is associated with the second mobile wireless device, a first response to the first request, to the first mobile wireless device,

184. As I previously discussed for Element [25e], a POSITA would have found obvious that the MFCI and service-subscription information for the registered wireless mobile devices would have included any available contact addresses for the services associated with the registered wireless mobile devices. A POSITA would have found obvious, for similar reasons to those described in §VII.E(i), *supra*, providing a sending mobile wireless device with more detailed information about the receiving mobile wireless device, including information about all available contact addresses, would help the sending user determine how and where to send a message and what content should be included.

185. Including these contact addresses in the response to the MFCI request would have been made possible where the HSS determined associations between identities and devices in order to map all of a user's contact information. *See, e.g., APPLE-1076, [0011].* Accordingly, a POSITA would have found it obvious, in Horvath-Tsampalis-Kansal-Quon, that the server system (*e.g., information processing system 108*) ***sends, based on the determination that the email address is associated with the second mobile wireless device*** (*e.g., a response containing information about all available contact addresses was made possible because the HSS determined associations between identities and devices and therefor the response is “based on” those associations*), ***a first response to the first request, to the first mobile wireless device*** (*e.g., the HSS providing a response to the MFCI request that included information about all available contact addresses*).

Element [25f2]: the first response indicating that a message to the second mobile wireless device is to be sent via the service;

186. *Supra*, §VIII.A, Analyses of Elements [1e2]-[1f].

Element [25g]: receives a second request, from the first mobile wireless device, the second request comprising another phone number which is different than the numeric identifier; and

187. *Supra*, §VIII.A, Analysis of Element [1g] (the “second phone number” recited in Elements [1g]-[1i] corresponds to the “another phone number” recited in Element [25g]).

Element [25h]: sends a second response to the second request, to the first mobile wireless device, the second response indicating that a message to a third mobile wireless device is not to be sent via the service.

188. *Supra*, §VIII.A, Analyses of Elements [1g]-[1h] (the “second phone number” recited in Elements [1g]-[1i] corresponds to the “third mobile wireless device” recited in Element [25h]). Because the MFCI in the response indicated that the “third mobile wireless device” had limited messaging capabilities, the second response ***indicating that a message to a third mobile wireless device is not to be sent via the service.*** Tsampalis describes “embodiments [that] include no user prompts whatsoever” with respect to the format transformation of messages being sent, which would have resulted in an automatic transformation away from any message format that the MFCI indicates a recipient is not capable of receiving (***not [being] sent via the service***). See APPLE-1005, [0033], [0053]-[0055], [0062].

Claim [26]: The system of claim 25, wherein the server system determines that the second mobile wireless device is inactive, subsequent to the second response being sent; wherein the server system provides information indicating that messages to the second mobile wireless device should not be sent via the service, to a plurality of mobile wireless devices.

189. *Supra*, §VIII.A, Analysis of Claim [9] (regarding determination of a device being “inactive,” which a POSITA would have known could be determined at any time. *Supra*, §VIII.A, Analysis of Element [25h] (where the indication that a message should not be sent would have been sent ***to a plurality of mobile wireless***

devices when a plurality of mobile wireless devices each request the MFCI of the same mobile wireless device with limited capabilities).

Claim [27]: The system of claim 25, wherein the server system performs a short message service (SMS) based authentication procedure on a phone number associated to the first mobile wireless device and adds the phone number associated to the first mobile wireless device to a subscriber address list subsequent to the SMS based authentication procedure; wherein at least one message to the second mobile wireless device is routed via the email address and via the service.

190. *Supra*, §VIII.A, Analyses of Elements [1c] (authentication via SMS), [18d] (adding the phone number to a subscriber list subsequent to authentication), and Claim [5] (message sent to receiver device via IM service where screen name is the same as the e-mail address).

Claim [28]: The system of claim 25, wherein a plurality of mobile wireless devices are associated with the numeric identifier.

191. *Supra*, §VIII.A, Analysis of Claim [26].

Claim [29]: The system of claim 28, wherein the server system receives message content from the first mobile wireless device and provides the message content to each one of the plurality of mobile wireless devices associated with the numeric identifier.

192. *Supra*, §VIII.A, Analyses of Element [18h] and Claim [26].

Claim [30]: The system of claim 25, wherein the second response to the second request indicates that a message being composed on the first mobile wireless device should be sent via SMS; wherein at least one message to the second mobile wireless device is routed via the email address and via the service.

193. *Supra*, §VIII.A, Analyses of Claims [5] & [27] (at least one message to the second mobile wireless device is routed via the email address and via the IM service).

194. As I previously discussed for Elements [1g]-[1h], certain wireless mobile device's MFCI would indicate that they had limited messaging capabilities. *See, e.g.*, APPLE-1005, [0003] (describing receiving mobile devices "capable of only receiving messages in" SMS), [0034] (describing a receiving mobile devices as having "limited messaging capabilities"), [0061]-[0062]; APPLE-1029, [0029]; APPLE-1042, [0078]; APPLE-1053, 2:9-17.

195. For at least some wireless mobile devices with limited capabilities, the MFCI would indicate it is only capable of receiving SMS, so the sending mobile phone would send an SMS message to the receiving mobile phone. *See id.* 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 networks], and/or availability of a recipient to receive messages of a certain format." APPLE-1042, [0078].

196. Tsampalis describes "embodiments [that] include no user prompts whatsoever" with respect to the format transformation of messages being sent, which would have resulted in an automatic transformation to an SMS message format when

the MFCI indicates the receiving mobile wireless device is only capable of receiving SMS (*should be sent via SMS*). See APPLE-1005, [0033], [0053]-[0055], [0062].

IX. CONCLUSION

197. For all the reasons I have noted in the foregoing paragraphs, claims 1-30 of the '601 Patent are obvious in view of the references discussed above.

198. 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 malware through cellular infrastructure.

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

Frank Park Georgia Institute of Technology

Fall 2008–Spring 2010

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

Ferdinand Schober Georgia Institute of Technology

Fall 2009–Summer 2010

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

4. M.S. Students Supervised

Chaitrali Amrutkar Georgia Institute of Technology

Fall 2008–Spring 2009

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

Logan Blue University of Florida

Fall 2015–Spring 2016

Investigated problems of cellular and network security.

David Dewey Georgia Institute of Technology

Fall 2009–Spring 2010

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

Christopher Grayson Georgia Institute of Technology

Fall 2012–Fall 2013

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

Young Seuk Kim Georgia Institute of Technology

Fall 2012–Fall 2013

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

Daniel Komaromy Georgia Institute of Technology

Fall 2008–Summer 2009

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

Nigel Lawrence Georgia Institute of Technology

Fall 2011–Spring 2012

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

Philip Marquardt Georgia Institute of Technology

Fall 2009–Present

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

Rishikesh Naik Georgia Institute of Technology

Fall 2008–Spring 2010

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

Ashish Nautiyal University of Florida

Fall 2015–Spring 2016

Research on connecting telephone calls to the larger authentication infrastructure.

Nilesh Nipane Georgia Institute of Technology

Fall 2008–Spring 2010

Research on creating provably anonymous networks on a base of secure function evaluation. Now with VMWare.

Walter “Nolen” Sciafe Georgia Institute of Technology

Spring 2012–Spring 2014

Developed the OnionDNS architecture, which prevents domain delisting attacks by leveraging a Tor hidden service. Joined Ph.D. program at UF.

Tyler Tucker University of Florida

Fall 2018–Spring 2021

Evaluating the security of Bluetooth radios.

5. M.S. Special Problems Students

Siddhant Deshmukh University of Florida

Fall 2016–Present

Developed tools for analysis of mobile digital financial services.

Chinmay Gangakhedkar Georgia Institute of Technology

Spring 2009

Research on multi-factor authentication using mobile phones.

Christopher Grayson Georgia Institute of Technology

Spring 2013

Research on continuous authentication using mobile phones.

Aarushi Karnany University of Florida

Fall 2016–Present

Developed tools for analysis of mobile digital financial services.

Rohit Matthews Georgia Institute of Technology

Spring 2011

Developed mobile phone-based tools for measuring performance and reachability throughout the Internet.

Ashwin Narasimhan Georgia Institute of Technology

Spring 2009

Research on developing efficient security mechanisms for the IMS cellular core.

Aamir Poonawalla Georgia Institute of Technology

Spring 2010

Helped develop a call provenance infrastructure, which included both networking and machine learning components.

Erin Reddick Georgia Institute of Technology

Fall 2008–Fall 2009

Research on IPTV security with GTRI.

Lalanthika Vasudevan Georgia Institute of Technology

Spring 2009

Research on developing efficient security mechanisms for the IMS cellular core.

6. Undergraduate Special Problems Students

Ethan Shernan Georgia Institute of Technology

Spring 2014

Developed an infrastructure for detecting billing bypass fraud attacks.

Young Seuk Kim Georgia Institute of Technology

Fall 2011–Spring 2012

Developed a mobile phone application for taking measurements of cellular networks.

Dane Van Dyck Georgia Institute of Technology

Summer 2009

Research on virtualization support for mobile phones.

E. Teaching Honors and Awards

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

II. RESEARCH AND CREATIVE SCHOLARSHIP

A. Thesis

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

B. Published Journal Papers (Refereed)

1. Cassidy Gibson, Vanessa Frost, Katie Platt, Washington Garcia, Luis Vargas, Sara Rampazzi, Vincent Bindschaedler, Patrick Traynor, and Kevin Butler. Analyzing the Monetization Ecosystem of Stalkerware. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2022. (Acceptance rate: 24%).
2. Bradley Reaves, Luis Vargas, Nolen Scaife, Dave Tian, Logan Blue, Patrick Traynor, and Kevin Butler. Characterizing the Security of the SMS Ecosystem with Public Gateways. *ACM Transactions on Privacy and Security (TOPS)*, 22(1), 2018.
3. Patrick Traynor, Kevin Butler, Jasmine Bowers, and Bradley Reaves. FinTechSec: Addressing the Security Challenges of Digital Financial Services. *IEEE S&P Magazine*, 15(5):85–89, 2017.
4. Nolen Scaife, Henry Carter, Rachel Jones, Lyrissa Lidsky, and Patrick Traynor. OnionDNS: A Seizure-Resistant Top-level Domain. *International Journal of Information Security (IJIS)*, 2017.
5. Bradley Reaves, Jasmine Bowers, Nolen Scaife, Adam Bates, Arnav Bharatiya, Patrick Traynor, and Kevin Butler. Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World. *ACM Transactions on Privacy and Security (TOPS)*, 2017.
6. Henry Carter and Patrick Traynor. OPFE: Outsourcing Computation for Private Function Evaluation. *International Journal of Information and Computer Security (IJICS)*, 2017.
7. Stephan Heuser, Bradley Reaves, Praveen Kumar Pendyala, Henry Carter, Alexandra Dmitrienko, William Enck, Negar Kiyavash, Ahmad-Reza Sadeghi, and Patrick Traynor. Phonion: Practical Protection of Metadata in Telephony Networks. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2017.
8. Bradley Reaves, Jasmine Bowers, Sigmond A. Gorski III, Olabode Anise, Rahul Bobhate, Raymond Cho, Hiranava Das, Sharique Hussain, Hamza Karachiwala, Nolen Scaife, Byron Wright, Kevin Butler, William Enck, and Patrick Traynor. *droid: Assessment and Evaluation of Android Application Analysis Tools. *ACM Computing Surveys (CSUR)*, 2016.
9. Chaitrali Amrutkar, Young Seuk Kim, and Patrick Traynor. Detecting Mobile Malicious Webpages in Real Time. *IEEE Transactions on Mobile Computing (TMC)*, To Appear 2016.
10. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Outsourcing Secure Two-Party Computation as a Black Box. *Journal of Security and Communication Networks (SCN)*, To Appear 2016.
11. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Secure Outsourced Garbled Circuit Evaluation for Mobile Devices. *Journal of Computer Security (JCS)*, 24(2):137–180, 2016.
12. Adam Bates, Kevin Butler, Micah Sherr, Clay Shields, Patrick Traynor, and Dan Wallach. Accountable Wiretapping -or- I Know They Can Hear You Now. *Journal of Computer Security (JCS)*, 23(2):167–195, 2015.
13. Henry Carter, Chaitrali Amrutkar, Italo Dacosta, and Patrick Traynor. For Your Phone Only: Custom Protocols for Efficient Secure Function Evaluation on Mobile Devices. *Journal of Security and Communication Networks (SCN)*, 7(7):1165–1176, 2014.

14. Chaitrali Amrutkar, Patrick Traynor, and Paul van Oorschot. An Empirical Evaluation of Security Indicators in Mobile Web Browsers. *IEEE Transactions on Mobile Computing (TMC)*, 14(5), 2015.
15. Andrew Harris, Seymour Goodman, and Patrick Traynor. Privacy and Security Concerns Associated with Mobile Money Applications in Africa. *Washington Journal of Law, Technology & Arts*, 8(3), 2013.
16. Italo Dacosta, Saurabh Chakradeo, Mustaque Ahamad, and Patrick Traynor. One-Time Cookies: Preventing Session Hijacking Attacks with Stateless Authentication Tokens. *ACM Transactions on Internet Technology (TOIT)*, 12(1), 2012.
17. Cong Shi, Xiapu Luo, Patrick Traynor, Mostafa Ammar, and Ellen Zegura. ARDEN: Anonymous netwoRking in Delay tolErant Networks. *Journal of Ad Hoc Networks*, 10(6):918–930, 2012.
18. Patrick Traynor. Characterizing the Security Implications of Third-Party EAS Over Cellular Text Messaging Services. *IEEE Transactions on Mobile Computing (TMC)*, 11(6):983–994, 2012.
19. Italo Dacosta, Vijay Balasubramaniyan, Mustaque Ahamad, and Patrick Traynor. Improving Authentication Performance of Distributed SIP Proxies. *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, 22(11):1804–1812, 2011.
20. Patrick Traynor, Chaitrali Amrutkar, Vikhyath Rao, Trent Jaeger, Patrick McDaniel, and Thomas La Porta. From Mobile Phones to Responsible Devices. *Journal of Security and Communication Networks (SCN)*, 4(6):719 – 726, 2011.
21. Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Brent Waters. Secure Attribute-Based Systems. *Journal of Computer Security (JCS)*, 18(5):799–837, 2010.
22. Patrick Traynor, Kevin Butler, William Enck, Kevin Borders, and Patrick McDaniel. malnets: Large-Scale Malicious Networks via Compromised Wireless Access Points. *Journal of Security and Communication Networks (SCN)*, 2(3):102–113, 2010.
23. Patrick Traynor. Securing Cellular Infrastructure: Challenges and Opportunities. *IEEE Security & Privacy Magazine*, 7(4), 2009.
24. Kevin Butler, Sunam Ryu, Patrick Traynor, and Patrick McDaniel. Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems. *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, 20(12):1803–1815, 2009.
25. Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta. Mitigating Attacks On Open Functionality in SMS-Capable Cellular Networks. *IEEE/ACM Transactions on Networking (TON)*, 17(1), 2009.
26. Patrick Traynor, Michael Chien, Scott Weaver, Boniface Hicks, and Patrick McDaniel. Non-Invasive Methods for Host Certification. *ACM Transactions on Information and System Security (TISSEC)*, 2008.
27. Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta. Exploiting Open Functionality in SMS-Capable Cellular Networks. *Journal of Computer Security (JCS)*, 16(6):713–742, 2008.
28. Patrick Traynor, Raju Kumar, Heesook Choi, Sencun Zhu, Guohong Cao, and Thomas La Porta. Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks. *IEEE Transactions on Mobile Computing (TMC)*, 6(6), 2007.

C. Published Books and Parts of Books

1. Andrew Harris, Frank S. Park, Seymour Goodman, and Patrick Traynor. *Emerging Privacy and Security Concerns for Digital Wallet Deployment*. Privacy in America: Interdisciplinary Perspectives. Scarecrow Press, July 2011.
2. Kevin Butler, William Enck, Patrick Traynor, Jennifer Plasterr, and Patrick McDaniel. *Privacy Preserving Web-Based Email*. Algorithms, Architectures and Information Systems Security, Statistical Science and Interdisciplinary Research. World Scientific Computing, November 2008.
3. Patrick Traynor, Patrick McDaniel, and Thomas La Porta. *Security for Telecommunications Networks*. Number 978-0-387-72441-6 in Advances in Information Security Series. Springer, August 2008.

D. Edited Proceedings

None.

E. Conference Presentations

E.1. Conference Papers with Proceedings (Refereed)

1. 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 Nittroveri, 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. Lius Vargas, Logan Blue, Vanessa Frost, Christopher Patton, N. Scaife, K. Butler, and P. Traynor. Digital Healthcare-Associated Infection Analysis of a Major Multi-Campus Hospital System. In *Proceedings of the ISOC Network & Distributed Systems Security Symposium (NDSS)*, 2019. (Acceptance Rate: 17.1%).
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 Shernan, Henry Carter, Dave Tian, Patrick Traynor, and Kevin Butler. More Guidelines Than Rules: CSRF Vulnerabilities from Noncompliant OAuth 2.0 Implementations. In *Proceedings of the International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA)*, 2015. (Acceptance Rate: 22.7%).
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, Franzi Roesner, Apu Kapadia, Eakta Jain.
Amount: \$7,500,000 for 5 years
Awarded October 2022
2. **ROCKY: Reliable Obfuscated Communications Kit for everYone**
Sponsor: DARPA Resilient Anonymous Communication for Everyone (RACE) – Broad Agency Announcement
Investigator(s): Thomas Shrimpton (PI), Patrick Traynor, Kevin Butler, Vincent Bindschaedler, Nadia Heninger
Amount: \$1,600,000 over 4 years
Awarded May 2019
3. **WiFiUS: Collaborative Research: SELIOT: Securing Lifecycle of Internet-of-Things**
Sponsor: NSF CNS WiFiUS
Investigator(s): Gene Tsudik (PI), Patrick Traynor
Amount: \$300,000 for 2 years
Submitted December 2016
4. **Cloud-based Oblivious Spectrum Mapping and Allocation**
Sponsor: NSF CNS EARS
Investigator(s): John Shea (PI), Tan Wong, Patrick Traynor
Amount: \$532,952 for 2 years
Submitted May 2016
5. **DURIP: Developing Research Capability in Cyber-Physical Systems at the University of Florida**
Sponsor: Small
Investigator(s): Kevin Butler (PI), Patrick Traynor, My Thai
Amount: \$200,000 for 2 years
Submitted: June 2015
6. **Securing the New Converged Telephony Landscape**
Sponsor: NSF TWC: Small
Investigator(s): Mustaque Ahamad (PI) and Patrick Traynor
Amount: \$500,000 for 3 years
Submitted: December 2012
7. **Facilitating Free and Open Access to Information on the Internet**
Sponsor: NSF Trustworthy Computing
Investigator(s): Nick Feamster (PI), Wenke Lee, Patrick Traynor, Hans Klein, Roger Dingledine, Michael Freedman and Edward W. Felten
Amount: \$1,500,000 for 4 years
Awarded: June 2011
8. **Monitoring Free and Open Access to Information on the Internet**
Sponsor: Google Focus Program
Investigator(s): Nick Feamster (PI), Wenke Lee, Mustaque Ahamad, Patrick Traynor, Henry Owen, Ellen Zegura, Zvi Galil

Amount: \$1,000,000 for 2 years
Awarded: November 2011

9. **Dynamic-attribute-based Disclosure of Health Information in Emergency Care Scenarios**

Sponsor: Health Systems Institute (HSI) Seed Grant Program
Investigator(s): Doug Blough (PI), Mustaque Ahamad, Patrick Traynor and Jim Jose
Amount: \$50,000 over 1 year
Awarded: August 2009

10. **Federal Cyber Service Scholarships at Georgia Tech**

Sponsor: NSF SFS Scholarships
Investigator(s): Seymour Goodman (PI), Patrick Traynor
Amount: \$1,250,682 over 5 years
Awarded: June 2009

11. **Security for IMS-Enabled Converged Applications**

Sponsor: US Department of Defense
Investigator(s): Mustaque Ahamad (PI), Patrick Traynor (PI), Michael Hunter, Russ Clark
Amount: \$146,121 for 1 year
Awarded: August 2008

2. Pending

Removed for external version.

I. Research Honors and Awards

1. Fellow, Center for Financial Inclusion at Accion, 2017.
2. Sloan Research Fellow, Alfred P. Sloan Foundation, 2014.
3. Best Paper, The ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec); Budapest, Hungary, 2013.
4. Best Student Paper, The Information Security Conference (ISC); Passau, Germany, 2012
5. Lockheed Inspirational Young Faculty Award, 2012
6. Best Demo, "Is Browsing the Internet on Your Mobile Phone Secure?" Chaitrali Amrutkar (Ph.D Advisee), CoC Research Day, 2011
7. Best Poster, "(sp)iPhone: Decoding Vibrations From Nearby Keyboards Using Mobile Phone Accelerometers" Arunabh Verma, Henry Carter (MS, Ph.D Advisees), CoC Research Day, 2011
8. National Science Foundation CAREER Award, 2010
9. Pennsylvania State University Alumni Association Dissertation Award, 2007
10. Pennsylvania State University CSE Graduate Research Assistant Award, 2007
11. AT&T Wireless Fellowship, 2005

III. SERVICE

A. Professional Activities

A.1. Memberships and Activities in Professional Societies

1. Senior Member, Association for Computing Machinery (ACM)
2. Senior Member, Institute of Electrical and Electronics Engineers (IEEE)
3. Member, USENIX Advanced Computing Systems Association (USENIX)

A.2. Conference Committee Activities

1. Program co-Chair, *IEEE Symposium on Security and Privacy (OAKLAND)*: 2023, 2024
2. Program co-Chair, *USENIX Security Symposium (SECURITY)*: 2019
3. Program co-Chair, *Network and Distributed System Security Symposium (NDSS)*: 2017, 2018
4. Program Chair, *USENIX Workshop on Offensive Technologies (WOOT)*: 2016
5. Program Chair, *ACM Conference on Wireless Network Security (WiSec)*: 2014
6. Program Co-Chair, *Annual Computer Security Applications Conference (ACSAC)*: 2012, 2013
7. Program Chair, *USENIX Workshop on Hot Topics in Security (HotSec)*: 2012
8. Chair Invited Talks Committee, *USENIX Security Symposium (SECURITY)*: 2014
9. Workshops Chair, *IEEE Conference on Communications and Network Security (CNS)*: 2016
10. Program Committee, *USENIX Security Symposium (SECURITY)*: 2008, 2009, 2010, 2013, 2015-2018, 2020-2022
11. Program Committee, *IEEE Symposium on Security and Privacy (OAKLAND)*: 2009-2014, 2022.
12. Program Committee, *ACM Conference On Computer and Communications Security (CCS)*: 2009, 2013-2015, 2017
13. Program Committee, *Network and Distributed System Security Symposium (NDSS)*: 2010, 2013-2016, 2020-2021
14. Program Committee, *IEEE European Symposium on Security and Privacy (Euro S&P)*: 2016
15. Program Committee, *Annual Computer Security Applications Conference (ACSAC)*: 2008, 2009, 2010, 2011, 2015
16. Program Committee, *ACM Conference on Wireless Network Security (WiSec)*: 2009, 2010, 2013, 2015-2021
17. Program Committee, *International Conference on Financial Cryptography and Data Security (FC)*: 2010, 2013
18. Program Committee, *USENIX Symposium on Operating Systems Design and Implementation (OSDI)*: 2016.
19. Program Committee, *ICST Conference on Security and Privacy in Communication Networks (SecureComm)*: 2009, 2010
20. Program Committee, *Privacy Enhancing Technologies Symposium (PETS)*: 2015, 2016

21. Program Committee, *International World Wide Web Conference (WWW)*: 2016
22. Program Committee, *USENIX Workshop on Hot Topics in Security (HotSec)*: 2011
23. Program Committee, *ACM SIGCOMM Workshop on Networking, Systems, and Applications on Mobile Handhelds (MOBIHELD)*: 2010
24. Program Committee, *International Workshop on Mobile Security (WMS)*: 2010
25. Program Committee, *European Symposium on Research in Computer Security (ESORICS)*: 2009, 2011
26. Program Committee, *IEEE Conference on Mobile Ad-hoc and Sensor Systems (MASS)*: 2009, 2010
27. Program Committee, *Information Security Conference (ISC)*: 2010
28. Program Committee, *IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT)*: 2009
29. Program Committee, *Computer Security Architecture Workshop (CSAW)*: 2008
30. Program Committee, *IWCMC Computer and Network Security Symposium*: 2009
31. Program Committee, *IARIA International Conference on Internet Monitoring and Protection (ICIMP)*: 2009
32. Program Committee, *IEEE Workshop on Network Security and Privacy (NSP)*: 2008
33. Program Committee, *IEEE International Workshop on Wireless and Sensor Networks Security (WSNS)*: 2008, 2009
34. Program Committee, *IEEE Conference on Sensor Networks, Ubiquitous and Trustworthy Computing (SUTC)*: 2008
35. Program Committee, *ACM Conference on Computer and Communications Security, Industry and Government Track (CCS I&G)*: 2006, 2007
36. Program Committee, *Workshop on Secure Network Protocols (NPSec)*: 2006
37. Program Committee, *International Conference on Information Systems Security (ICISS)*: 2006, 2009, 2010
38. Program Committee, *IEEE LCN Workshop on Network Security (WNS)*: 2006, 2007, 2008

B. On-Campus Committees

B.1. University of Florida

1. Member, Computer and Information Science and Engineering Steering Committee, 2015-2017.
2. Member, Graduate Recruiting Committee, 2015-2017.
3. Chair, Computer and Information Science and Engineering Industrial Advisory Board, 2014-2015.

B.2. Georgia Tech

1. Member, Massive Open Online Master's (MOOMS) Investigation Committee, 2012-2013.
2. Chair, School of Computer Science Ph.D. Review Committee, 2012.
3. Member, School of Computer Science Ph.D Review Committee, 2011.
4. Faculty Advisor, Grey H@T - Georgia Tech Undergraduate Security Club, 2011-2014.
5. Member, School of Computer Science Ph.D. Review Committee, 2011.
6. Member, School Advisory Committee, School of Computer Science, 2011-2013.
7. Member, School of Computer Science Chair Recruiting Committee, 2011.
8. Member, School of Computer Science Faculty Recruiting Committee, 2010, 2011.
9. Chair, College of Computing Ph.D. Welcome Weekend Committee, 2009, 2010, 2011 (co-chair).
10. Member, College of Computing Ph.D. Recruiting Committee, 2009.
11. Member, Georgia Tech Computer and Network Usage Security Policy (CNUSP) Evaluation Group, 2009.

C. Special Assignments

None.

D. Ph.D. Examining Committees

Ph.D. Examining Committees

1. Bradley Reaves, Department of Computer and Information Science and Engineering, University of Florida, Summer 2017.
Advisor: Professor Patrick Traynor.
2. Adam Bates, Department of Computer and Information Science and Engineering, University of Florida, Spring 2016.
Advisor: Professor Kevin Butler.
3. Benjamin Mood, Department of Computer and Information Science and Engineering, University of Florida, Spring 2016.
Advisor: Professor Kevin Butler.
4. Henry Carter, College of Computing, Georgia Tech, Fall 2015.
Advisor: Professor Patrick Traynor.
5. David Dewey, College of Computing, Georgia Tech, Fall 2015.
Advisor: Professor Patrick Traynor.
6. Lateef Yusuf, College of Computing, Georgia Tech, Spring 2014.
Advisor: Professor Umakishore Ramachandran.
7. Chaitrali Amrutkar, College of Computing, Georgia Tech, Summer 2013.
Advisor: Professor Patrick Traynor.
8. Long Lu, College of Computing, Georgia Tech, Summer 2013.
Advisor: Professor Wenke Lee.

9. Manos Antonakakis, College of Computing, Georgia Tech, Summer 2012.
Advisor: Professor Wenke Lee.
10. Junjie Zhang, College of Computing, Georgia Tech, Summer 2012.
Advisor: Professor Wenke Lee.
11. Italo Dacosta, College of Computing, Georgia Tech, Summer 2012.
Advisor: Professor Patrick Traynor.
12. Virendra Kumar, College of Computing, Georgia Tech, Summer 2012.
Advisor: Professor Alexandra Boldyreva.
13. Anirudh Ramachandran, College of Computing, Georgia Tech, Summer 2011.
Advisor: Professor Nick Feamster.
14. Vijay Balasubramaniyan, College of Computing, Georgia Tech, Summer 2011.
Advisor: Professor Mustaque Ahamad.
15. Kapil Singh, College of Computing, Georgia Tech, Summer 2011.
Advisor: Professor Wenke Lee.
16. Abhinav Srivastava, College of Computing, Georgia Tech, Summer 2011.
Advisor: Professor Jon Giffin.
17. Adam O'Neill, College of Computing, Georgia Tech, Summer 2010.
Advisor: Professor Alexandra Boldyreva.
18. David Cash, College of Computing, Georgia Tech, Fall 2009.
Advisor: Professor Alexandra Boldyreva.

External Member of Ph.D. Research Committee

None.

External Member of Ph.D. Examining Committee

1. Shannon Eggers, Department of Materials Sciences and Engineering - Nuclear Engineering Program, University of Florida, Fall 2016.
Advisor: Professor Kelly Jordan.
2. Ed Carlisle, Department of Electrical and Computer Engineering, University of Florida, Summer 2016.
Advisor: Professor Alan George.
3. Claudio Marforio, Department of Computer Science, Swiss Federal Institute of Technology Zurich (ETH Zurich), Fall 2015.
Advisor: Professor Srdjan Capkun.
4. Nils Ole Tippenhauer, Department of Computer Science, Swiss Federal Institute of Technology Zurich (ETH Zurich), Spring 2012.
Advisor: Professor Srdjan Capkun.
5. Bongkyoung Kwon, School of Electrical and Computer Engineering, Georgia Tech, Summer 2009.
Advisor: Professor John Copeland.

Ph.D. Thesis Proposal Committees

1. Bradley Reaves, Department of Computer and Information Science and Engineering, Spring 2016.
Advisor: Professor Patrick Traynor.
2. Maliheh Shirvanian, University of Alabama, Birmingham, Spring 2016.
Advisor: Professor Nitesh Saxena.
3. Benjamin Mood, Department of Computer and Information Science and Engineering, Fall 2015.
Advisor: Professor Kevin Butler.
4. Adam Bates, Department of Computer and Information Science and Engineering, Fall 2015.
Advisor: Professor Kevin Butler.
5. Lateef Yusuf, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Umakishore Ramachandran.
6. Long Lu, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Wenke Lee.
7. Chaitrali Amrutkar, College of Computing, Georgia Tech, Fall 2012.
Advisor: Professor Patrick Traynor.
8. Junjie Zhang, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Wenke Lee.
9. Italo Dacosta, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Patrick Traynor.
10. Manos Antonakakis, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Wenke Lee.
11. Abhinav Srivastava, College of Computing, Georgia Tech, Spring 2011.
Advisor: Professor Jon Giffin.
12. Vijay Balasubramaniyan, College of Computing, Georgia Tech, Fall 2010.
Advisor: Professor Mustaque Ahamad.
13. Kapil Singh, College of Computing, Georgia Tech, Fall 2010.
Advisor: Professor Wenke Lee.
14. Anirudh Ramachandran, College of Computing, Georgia Tech, Fall 2010.
Advisor: Professor Nick Feamster.
15. Adam O'Neill, College of Computing, Georgia Tech, Spring 2010.
Advisor: Professor Alexandra Boldyreva.
16. David Cash, College of Computing, Georgia Tech, Spring 2009.
Advisor: Professor Alexandra Boldyreva.

Ph.D. Qualifying Exam Committees—Georgia Tech

1. Byoungyoung Lee, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Wenke Lee.
2. Yizheng Chen, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Wenke Lee.

3. Xinyu Xing, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Wenke Lee.
4. Brad Reaves, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Patrick Traynor.
5. Chaz Lever, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Patrick Traynor.
6. Terry Nelms, College of Computing, Georgia Tech, Spring 2012.
Advisor: Professors Mustaque Ahamad and Roberto Perdesi.
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. Ikpeeme 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, Byungsuk Kim and Farooq Anjum. "Secure Localization for 802.11 Networks with Fine Granularity", United States Patent, #8,107,400, Filed July 2008, Issued January 2012.

E. Editorial and Reviewer Work for Technical Journals and Publishers

Associate Editor:

- *ACM Transactions on Information and System Security (TISSEC)* 2015-present

Guest Editor:

Journals

- *IEEE Security and Privacy Magazine (S&P)* 2013

Reviewer for:

Journals

- *ACM Transactions on Information and System Security (TISSEC)* 2008, 2009, 2010, 2011, 2012, 2013
- *IEEE Transactions on Dependable and Secure Computing (TDSC)* 2012, 2013
- *IEEE Security and Privacy Magazine (S&P)* 2010, 2011
- *Communications of the ACM (CACM)* 2010
- *Journal of Anesthesia & Analgesia* 2009
- *IEEE Transactions on Mobile Computing (TMC)* 2008, 2010, 2011, 2012, 2013
- *IEEE Transactions on Internet Technology (TOIT)* 2009, 2010
- *ACM Mobile Computing and Communications Review (MC2R)* 2008
- *IEEE/ACM Transactions on Networking (TON)* 2007, 2008
- *Journal of Pervasive and Mobile Computing (PMC)* 2009, 2010

- *IEEE Transactions on Parallel and Distributed Systems (TPDS)* 2005, 2009, 2010
- *IEEE Transactions on Computers (TOC)* 2010
- *Journal of Security and Communication Networks (SCN)* 2008
- *IEEE Communications Letters (CL)* 2007, 2009
- *IEEE Transactions on Wireless Communications (TWC)* 2007
- *Pervasive and Mobile Computing (PMC)* 2007
- *IEEE Transactions on Software Engineering (TSE)* 2007, 2008
- *Journal of Wireless Networks (WiNet)* 2006, 2007, 2008, 2009
- *Journal of Wireless Communications and Mobile Computing* 2006
- *ACM Computing Surveys (ACMCS)* 2006
- *Information Processing Letters (IPL)* 2006
- *IEEE Transactions on Very Large Scale Integration Systems (TVLSIS)* 2006

Conferences and Workshops

- *ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2011
- *ACM Conference on Computer and Communications Security (CCS)*, 2008, 2011
- *IEEE Symposium on Security and Privacy (OAKLAND)* 2007, 2008
- *Computer Security Foundations (CSF)*, 2011
- *IFIP Conference on Data and Applications Security (DBSec)* 2008
- *Financial Cryptography (FC)* 2007, 2008
- *International Conference on VLSI Design (VLSI)* 2007
- *Annual Computer Security Applications Conference (ACSAC)* 2005, 2006, 2007
- *USENIX Workshop on Hot Topics in Security (HotSec)* 2007
- *International Conference on Information Systems Security (ICISS)* 2007
- *IEEE International Conference on Computer Engineering & Systems (ICCES)* 2007
- *International Workshop on Security (IWSec)* 2006, 2007
- *USENIX Security Symposium (SECURITY)* 2006, 2007
- *IEEE Sarnoff Symposium (SARNOFF)* 2007
- *International Conference on New Technologies, Mobility and Security (NTMS)* 2007
- *IEEE Infocom (INFOCOM)* 2007
- *Network and Distributed System Security Symposium (NDSS)* 2007
- *International Workshop on Storage Security and Survivability (IWSSS)* 2006
- *ACM Conference on Computer and Communications Security (CCS)* 2006

- *IEEE GLOBECOM (GLOBECOM) 2006*
- *International Conference on Mobile and Ubiquitous Systems: Networks and Services (MOBIQUITOUS) 2006*
- *IFIP Conference on Data and Applications Security (DBSec) 2006*
- *Emerging Trends in Information and Communications Security (ETRICS) 2006*
- *International Conference on Applied Cryptography and Network Security (ACNS) 2006*
- *ACM Symposium on Access Control Models and Technology (SACMAT) 2006*
- *IEEE Conference on Communication Systems Software & Middleware (COMSWARE) 2006*
- *International Conference on Cryptology in India (IndoCrypt) 2005*
- *IEEE Symposium on New Frontiers in Dynamic Spectrum Access (DySPAN) 2005*
- *European Symposium on Research in Computer Security (ESORICS) 2005*

F. Expert Witness Services

1. *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 Burrell. 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-spiphone-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 Sydel. 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=d917b9cd43d4aa31&ei=5090&partner=rssuserland&emc=rss>, 2005.
- 66.
- 67.
- 68.