

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Graham Merrett
U.S. Patent No.: 11,089,450 Attorney Docket No. 50095-0264IP1
Issue Date: August 10, 2021
Application No.: 16/714,113
Filing Date: December 13, 2019
Title: MESSAGING SERVICE IN A WIRELESS COMMUNICATIONS
 NETWORK

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: 29 August 2025

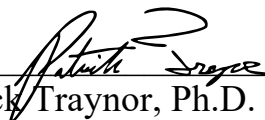
By: 
Patrick Traynor, Ph.D.

TABLE OF CONTENTS

| | | |
|-------|---|----|
| I. | QUALIFICATIONS AND BACKGROUND INFORMATION..... | 4 |
| II. | LEGAL PRINCIPLES..... | 10 |
| | A. Anticipation..... | 10 |
| | B. Obviousness..... | 10 |
| III. | OVERVIEW OF CONCLUSIONS FORMED..... | 12 |
| IV. | BACKGROUND KNOWLEDGE ONE OF SKILL IN THE ART WOULD HAVE HAD PRIOR TO THE PRIORITY DATE OF THE '450 PATENT | 12 |
| V. | INTERPRETATIONS OF THE '450 PATENT CLAIMS AT ISSUE..... | 13 |
| VI. | THE '450 PATENT..... | 13 |
| | A. Overview of the '450 Patent..... | 13 |
| | B. Prosecution History of the '450 Patent | 15 |
| VII. | OVERVIEW OF PRIOR ART REFERENCES..... | 15 |
| | A. Overview of Horvath..... | 15 |
| | B. Overview of Tsampalis | 21 |
| | C. Overview of Chatterjee | 26 |
| | D. Overview of Kansal..... | 27 |
| | E. Overview of Ribaldo | 29 |
| | F. Overview of BenYoseph | 29 |
| | G. Overview of Lin | 30 |
| VIII. | GROUND 1A: CLAIMS 1, 3-4, 7, 9-13, 15, 22, 24, 26-29 ARE OBVIOUS IN VIEW OF THE HORVATH-TSAMPALIS-CHATTERJEE COMBINATION..... | 31 |
| | A. Combining Horvath with Tsampalis | 31 |

| | | |
|-------|---|-----|
| B. | Combining Horvath and Tsampalis with Chatterjee..... | 40 |
| C. | Analysis with Respect to Claims 1, 3-4, 7, 9-13, 15, 22, 24, 26-29 ... | 48 |
| IX. | GROUND 1B: CLAIMS 6, 8, 17-18, 21, 23, 25 ARE OBVIOUS IN VIEW OF THE HORVATH-TSAMPALIS-CHATTERJEE-KANSAL COMBINATION..... | 85 |
| A. | Combining Horvath, Tsampalis and Chatterjee with Kansal..... | 85 |
| B. | Analysis with Respect to Claims 6, 8, 17-18, 21, 23, 25 | 87 |
| X. | GROUND 1C: CLAIMS 2, 16 ARE OBVIOUS IN VIEW OF THE HORVATH-TSAMPALIS-CHATTERJEE-RIBAUDO COMBINATION | 94 |
| A. | Combining Horvath, Tsampalis and Chatterjee with Ribaudo | 94 |
| B. | Analysis with Respect to Claims 2, 16..... | 95 |
| XI. | GROUND 1D: CLAIM 5 IS OBVIOUS IN VIEW OF THE HORVATH-TSAMPALIS-CHATTERJEE-BENYOSEPH COMBINATION | 96 |
| A. | Combining Horvath, Tsampalis and Chatterjee with BenYoseph..... | 96 |
| B. | Analysis with Respect to Claim 5 | 98 |
| XII. | GROUND 1E: CLAIMS 14, 19-20, 30 ARE OBVIOUS IN VIEW OF THE HORVATH-TSAMPALIS-CHATTERJEE-LIN COMBINATION | 98 |
| A. | Combining Horvath, Tsampalis and Chatterjee with Lin | 98 |
| B. | Analysis with Respect to Claims 14, 19-20, 30 | 100 |
| XIII. | CONCLUSION..... | 101 |

DECLARATION OF DR. PATRICK TRAYNOR

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

I. QUALIFICATIONS AND BACKGROUND INFORMATION

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

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

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

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

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

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

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

7. I have published over 100 articles in top conferences and journals in the areas of information security, mobile systems, and networking. Many of my results are highly cited, and I have received multiple "Best Paper" Awards. I have

also written a book entitled “Security for Telecommunications Networks”, which is used in wireless and cellular security courses at a number of top universities.

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

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

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

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

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

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

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

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

- APPLE-1001 U.S. Patent No. 11,089,450 (“the ’450 Patent”)
- APPLE-1002 File History of U.S. Patent No. 11,089,450
- APPLE-1004 U.S. Pub. No. 2007/0254681 (“Horvath”)
- APPLE-1005 U.S. Pub. No. 2004/0203956 (“Tsampalis”)
- APPLE-1007 Chatterjee et al., “Instant Messaging and Presence Technologies for College Campuses.” IEEE Network, May/June 2005. (“Chatterjee”)
- APPLE-1008 U.S. Pub. No. 2005/0243978 (“Son”)
- APPLE-1009 UK Pub. No. 2432482 (“Beaumont”)
- APPLE-1010 U.S. Patent No. 9,408,077 (“David”)
- APPLE-1011 U.S. Patent No. 6,940,844 (“Purkayastha”)
- APPLE-1012 U.S. Patent No. 7,702,342 (“Duan”)
- APPLE-1013 U.S. Patent No. 8,819,145 (“Gailloux”)
- APPLE-1016 U.S. Pub. No. 2005/0037762 to Gurbani et al. (“Gurbani”)
- APPLE-1017 U.S. Patent No. 9,167,401 to Helferich (“Helferich”)
- APPLE-1019 PCT Pub. No. WO 2006/029331 (“Henderson”)
- APPLE-1020 U.S. Patent No. 7,236,472 (“Lazaridis”)
- APPLE-1025 Qi et al., 2004, July. “Multimedia Messaging Service.” Available at https://www.zte.com.cn/global/about/magazine/zte-communications/2004/1/en_68/162264.html (“Qi”)

- APPLE-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. 2008/0153459 (“Kansal”)
- APPLE-1044 U.S. Pub. No. 2007/0030824 (“Ribaudó”)
- APPLE-1045 U.S. Pub. No. 2005/0233737 (“Lin”)
- APPLE-1046 U.S. Pub. No. 2008/0176538 (“Terrill”)
- APPLE-1047 IMS Share Technote, available at https://www.sharetechnote.com/html/Handbook_IMS_SIP_Header_Expire.html
- APPLE-1048 RFC 3680: A Session Initiation Protocol (SIP) Event Package for Registrations (March 2004)
- APPLE-1049 U.S. Patent No. 7,472,163 (“Ben-Yoseph”)
- APPLE-1050 RFC 2778: A Model for Presence and Instant Messaging (February 2000)
- APPLE-1051 U.S. Pub. No. 2008/0090597 (“Celik”)
- APPLE-1052 U.S. Pub. No. 2006/0168204 (“Appelman”)
- APPLE-1053 RFC 3261: SIP: Session Initiation Protocol (June 2002)
- APPLE-1054 U.S. Pub. No. 2008/0034043 (“Gandhi”)
- APPLE-1055 Subramanya et al., Mobile Communications—An Overview, IEEE Potentials (2005)
- APPLE-1056 RFC 3856: A Presence Event Package for the Session Initiation Protocol (SIP)
- 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 '450 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 ’450 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 '450 Patent are obvious over Horvath in view of Tsampalis.

IV. BACKGROUND KNOWLEDGE ONE OF SKILL IN THE ART WOULD HAVE HAD PRIOR TO THE PRIORITY DATE OF THE '450 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 '450 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 '450 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 '450 PATENT

A. Overview of the '450 Patent

24. The '450 patent generally describes techniques for messaging on mobile devices. *See* APPPLE-1001. The Abstract of the '450 Patent refers to a method that includes "receiving a first message formatted according to an SMS format, by a first mobile wireless device from a second mobile wireless device, via

a mobile operator base station,” “subscribing, by the first mobile wireless device, to a service for transmitting and receiving packet switched messages, via the Internet and the mobile operator base station,” “transmitting, by the first mobile wireless device, after the subscribing, a request including at least information corresponding to at least one mobile phone number of the second mobile wireless device, to determine whether the second mobile wireless device corresponds to a subscriber of the service.” APPLE-1001, Abstract; *see also id.*, Cl. 1.

25. FIG. 3 is a flowchart that illustrates one method for formatting an outgoing message according to information about the recipient’s messaging capabilities:

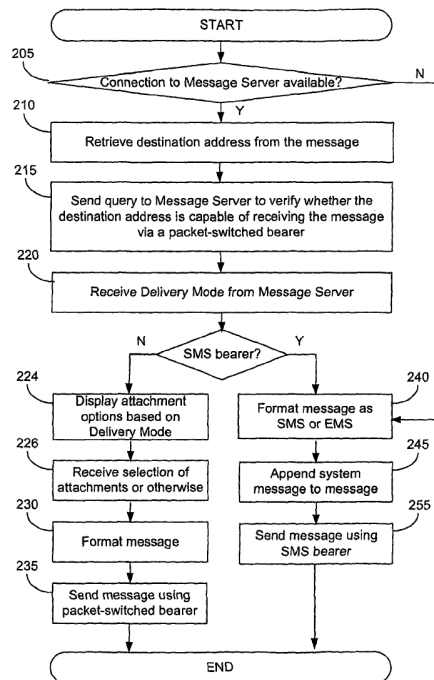


FIG. 3

APPLE-1001, FIG. 3

B. Prosecution History of the ‘450 Patent

26. During prosecution, the Examiner allowed the claims without a prior art rejection and did not consider any of the art applied in this Petition. APPLE-1002. However, as discussed in §§VIII-XII, the application never should have been allowed. All features recited in the Challenged Claims are disclosed in one or more of Horvath, Tsampalis, Chatterjee, Kansal, Ribaud, BenYoseph, Lin, and the claimed combinations of these features would have been obvious before the Critical Date.

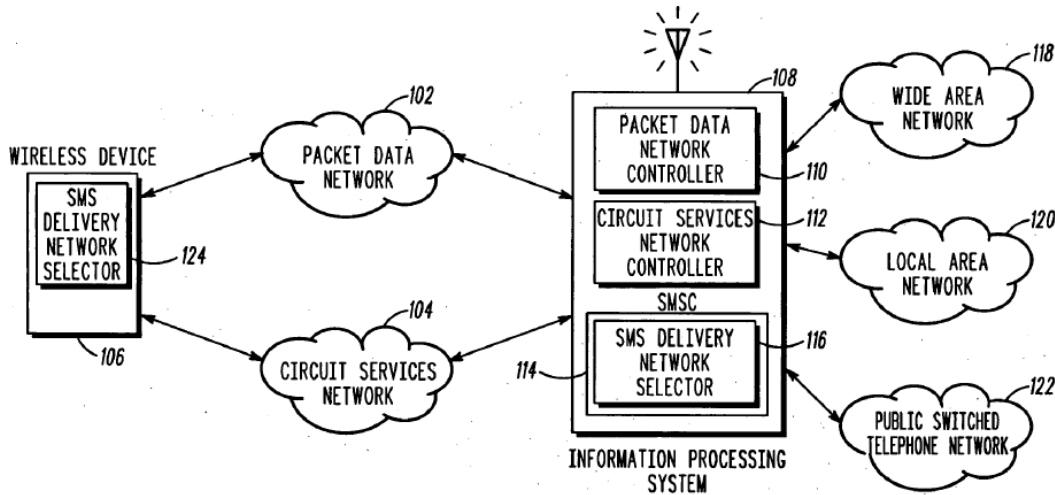
VII. OVERVIEW OF PRIOR ART REFERENCES

A. Overview of Horvath¹

27. Horvath discloses a method and system for “transmitting short message service messages” with “a wireless device such as a mobile phone” 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

¹ The general descriptions of this and other references and combinations are incorporated into each subsection and mapping of the claims that includes citations to these references. All emphasis is added unless otherwise indicated.

network 104,” “based on [a] registration status of the wireless device.” *Id.*, [0007]-[0008], [0024], [0061], FIGS. 1 (below), 2, 4.

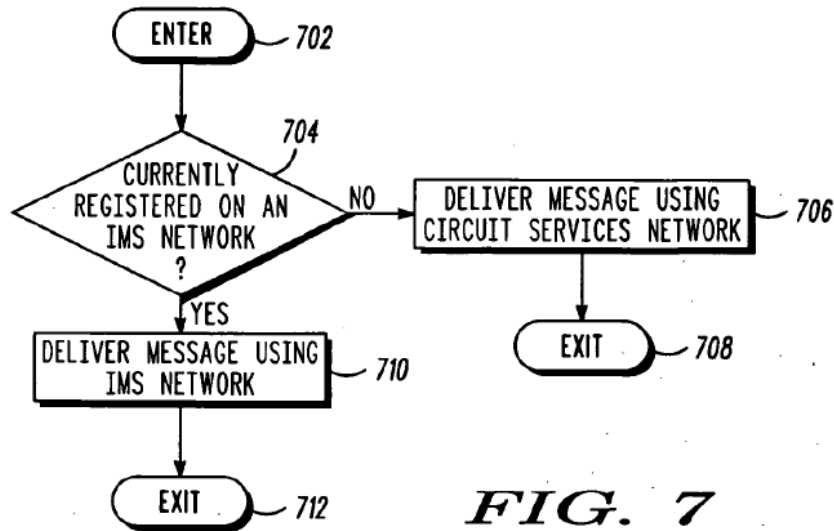


100
FIG. 1

APPLE-1004, FIG. 1

28. As shown in FIG. 1, when wireless device 106 desires to transmit/send a SMS message (operating as a sender device) to another device, “the wireless device 106 first determines if it [*i.e.*, the sending wireless device] is registered on the packet data network 102,” and based on this determination, an “SMS delivery network selector 124” residing on the wireless device 106 “selects a network 102, 104 for the wireless device 106 to transmit [the] SMS message on.” APPLE-1004, [0050], [0062] (“[I]f the wireless device 106 is registered on the packet data network 102, the SMS delivery network selector 124 selects the packet data network 102 for transmission of the SMS message. If the wireless device is

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



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

29. Although Horvath focuses on the selective use of packet switched or circuit switched bearers for delivery of SMS messages, Horvath notes that wireless device 106 can transmit other types of messages as well, including enhanced messaging service (“EMS”) messages, multimedia service (“MMS”) messages, and instant messages (“IM”). APPLE-1004, [0025], [0038]-[0039] (“An IMS system also includes application servers that host and execute services for the wireless device 106. A service for example, is SMS, MMS, ...and the like.”). A session initiation protocol (“SIP”) network operates atop the packet data network 102 to establish communication sessions and carry encapsulated SMS messages

between wireless devices and a server when the circuit switched network 104 is not used. *Id.* [0041], [0033] (“The SIP network is used for establishing instant messaging, ... and other real-time communications over the Internet.”), [0050], FIG. 5.

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

² The SIP network is supported by an “Internet Protocol multimedia subsystem” (IMS) core and is capable of transmitting rich **multimedia** data.

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

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

APPLE-1004, [0034]; *see also* APPLE-1012 (describing IMS networks in further detail).

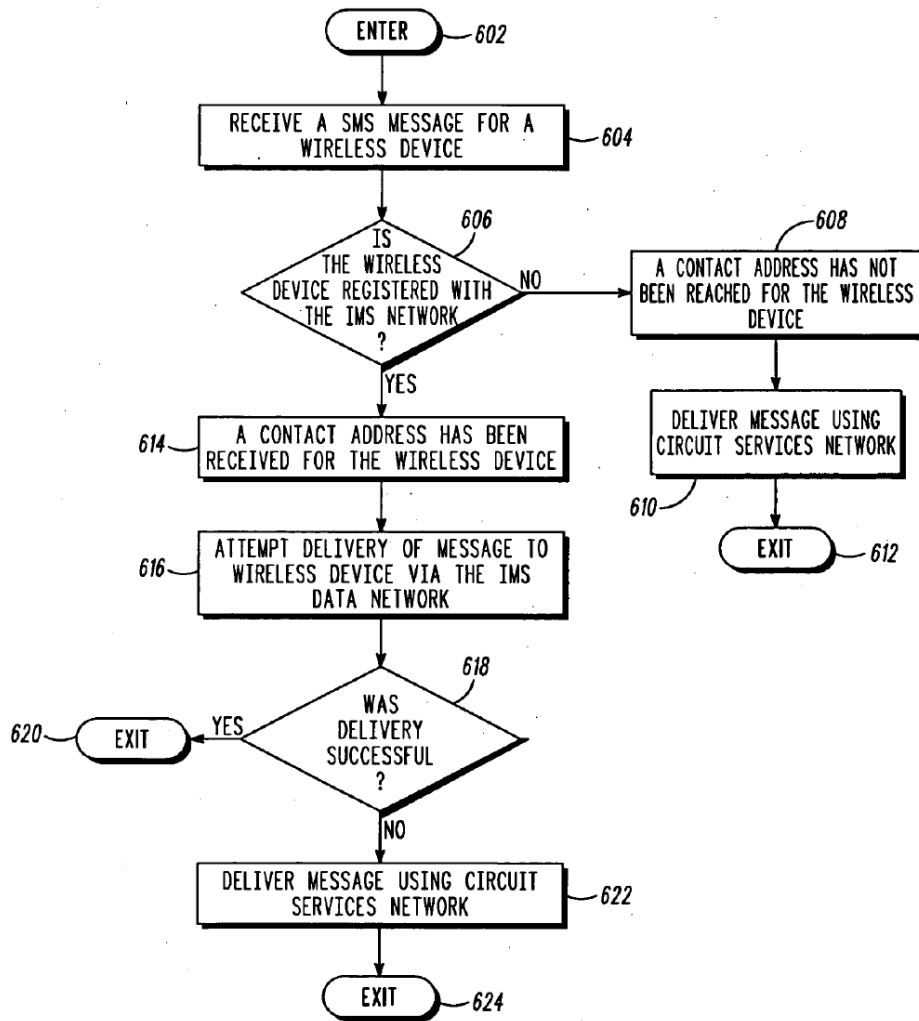
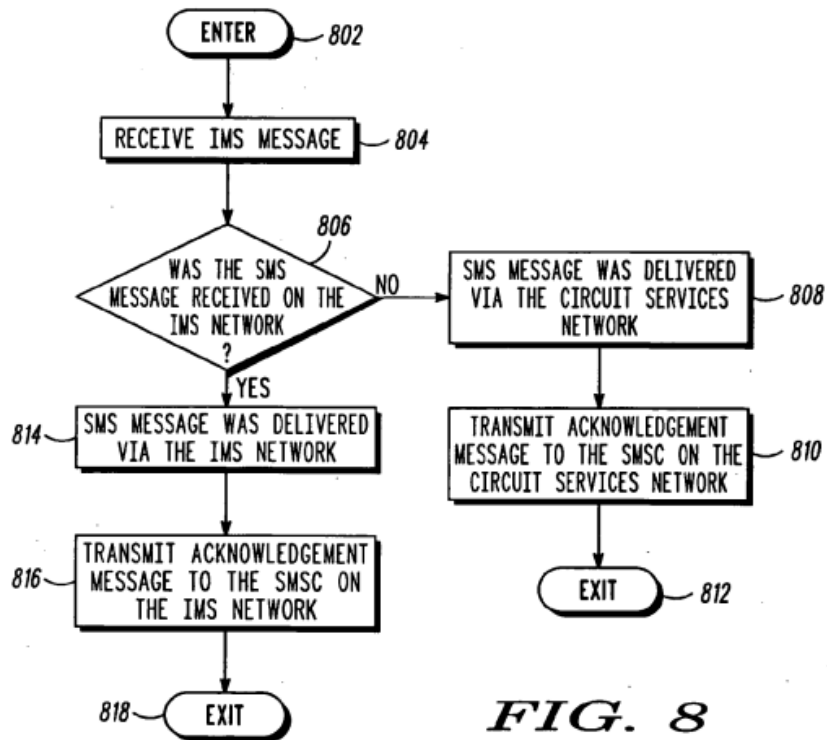


FIG. 6

APPLE-1004, FIG. 6 (Server Perspective)

32. FIG. 8 is a flowchart that illustrates “an exemplary process of a wireless device receiving a SMS message” (APPLE-1004, [0016], *see also id.* [0080]):



APPLE-1004, FIG. 8 (Wireless Device Perspective)

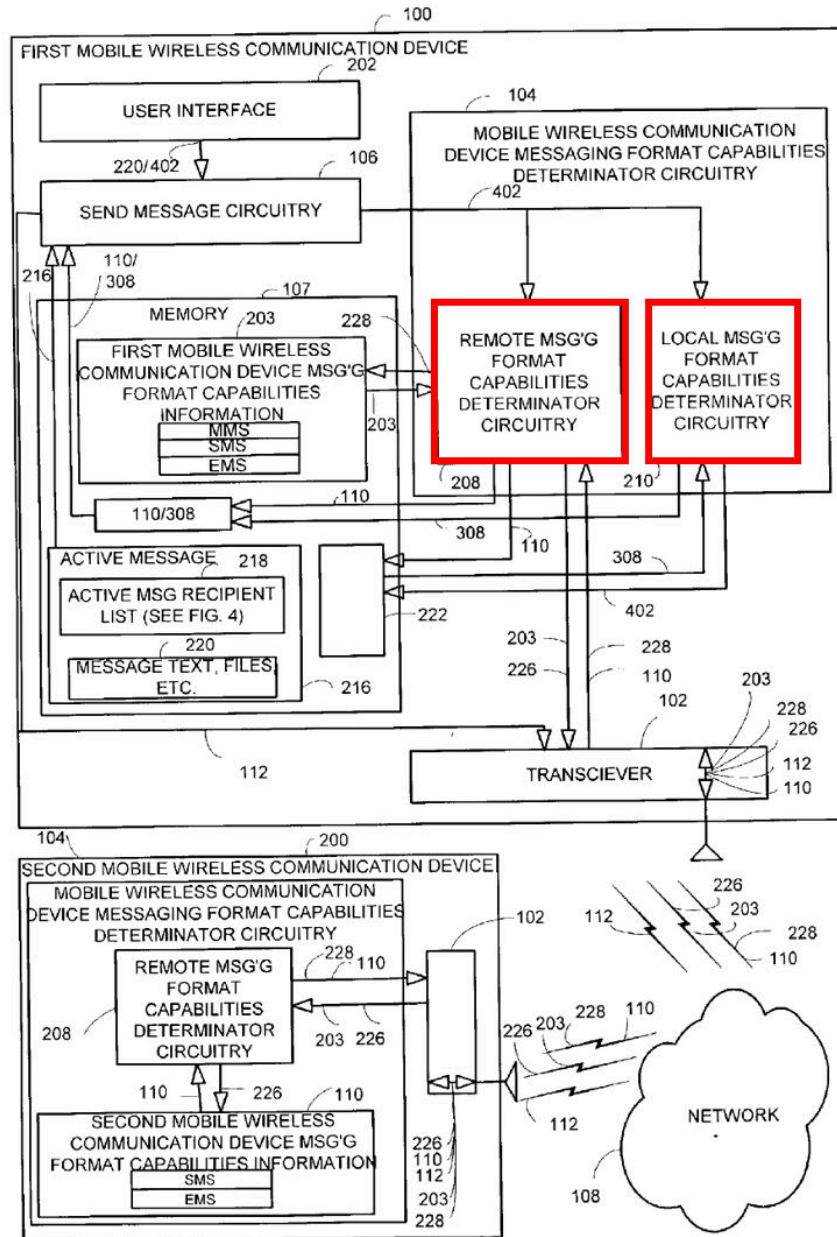
B. Overview of Tsampalis

33. Tsampalis describes a “method and apparatus for providing wireless messaging” in which a first mobile wireless communication device 100 (*i.e.*, a sender device) obtains, either locally or via “a web server” or other “network element,” “messaging format capabilities information 110” of a second mobile wireless communication device 200 (*i.e.*, a recipient device) before the sender device sends a message. *See e.g.*, APPLE-1005, Title, Abstract, [0029]-[0039], FIGS. 1, 2 (below, highlighting the local and remote messaging format capabilities determinator circuitries residing on the first wireless device), 5-7. The messaging format capabilities information 110 (MFCI) indicates the types of messages (*e.g.*,

SMS, MMS, EMS) that the intended recipient device is capable of processing.

APPLE-1005, [0022]-[0024].

FIG. 2

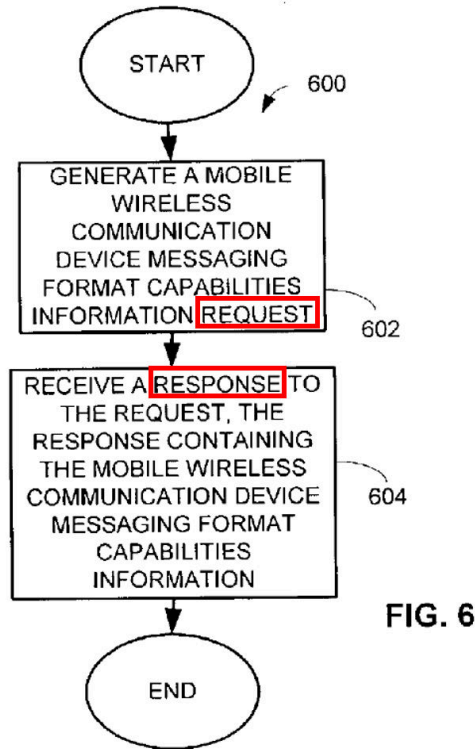


APPLE-1005, FIG. 2 (Annotated)

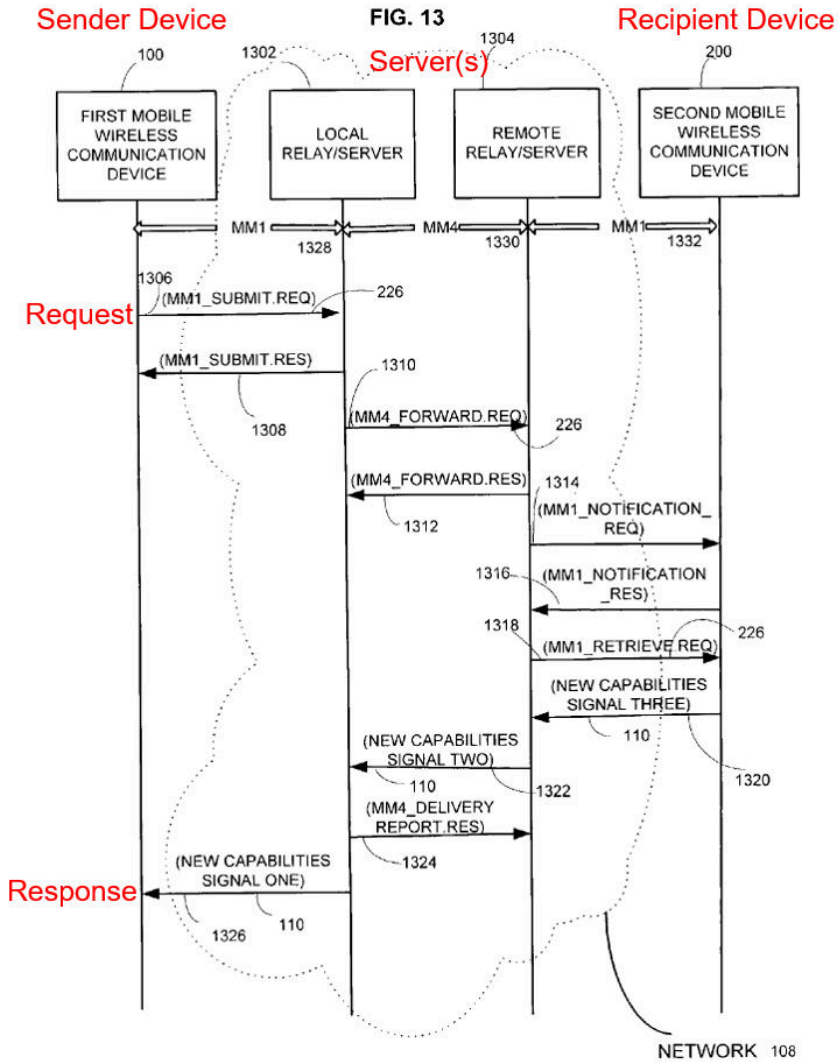
34. According to Tsampalis, when recipient device 200's format capabilities information 110 "must be retrieved remotely," the sender device 100 generates and sends a "mobile wireless communication device messaging format capabilities information **request**" to a remote web server, and "receiv[es] a **response** [*e.g.*, from the web server] to the request where the response contains the second mobile wireless communication device messaging format capabilities information 110." APPLE-1005, [0024], [0027], [0042] (both generation of the request and reception of the response "may be accomplished using the remote messaging format capabilities determinator circuitry 208" or "other suitable circuitry"), [0034], [0056]-[0057] ("request and retrieve the second mobile wireless communication device messaging format capabilities information 110," "a second mobile wireless communication device messaging format request 226," "new capabilities signal one 1326 [including] at least the second mobile wireless communication device messaging format capabilities information 110"), FIGS. 6 (below), 13 (below).

35. In some examples, Tsampalis explains that "the second mobile wireless communication device messaging format capabilities information 110 is stored" in "a network element within the network 108" such as "a web server." *Id.*, [0039], [0057] ("note that some embodiments store the second mobile wireless communication device messaging format capabilities information 110 at the

remote relay/server 1304, and for such embodiments, signals 1314, 1316, 1318 and 1320 are not used”). In such cases, the first (sender) device can retrieve the second (recipient) device’s MFCI 110 from a remote server using signaling like that shown in FIG. 13 (below). *Id.*; *see also id.*, [0056]-[0060], FIGS. 13-15.



APPLE-1005, FIG. 6 (Annotated)



APPLE-1005, FIG. 13 (Annotated)

36. Tsampalis further explains that the first (sender) device can store the second (recipient) device's MFCI 110 in a phonebook, and can use the second (recipient) device's MFCI 110 to select a suitable message format and corresponding transmission mode (e.g., an SMS, MMS, or EMS transmission) for sending the message based on the capabilities of the second (recipient) device. APPLE-1005, [0041], [0060]-[0064], FIGS. 5, 16.

C. Overview of Chatterjee

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

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

■ Table 1. *Instant messaging systems.*

APPLE-1007, Table 1

D. Overview of Kansal

38. 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 describes arranging and correlating received messages of different types with a particular recipient. APPLE-1042, [0009]; [0040]-[0043]; [0066]-[0069]. The wireless device can display a “messaging user interface” that “display[s] a messaging thread comprising correlated messages of different message types.” APPLE-1042, [0009], [0045]-[0046], [0054]-[0056], [0062]-[0064], [0070], [0077]-[0078], FIGs. 2-3 (shown below).



FIG. 2

APPLE-1042, FIG. 2

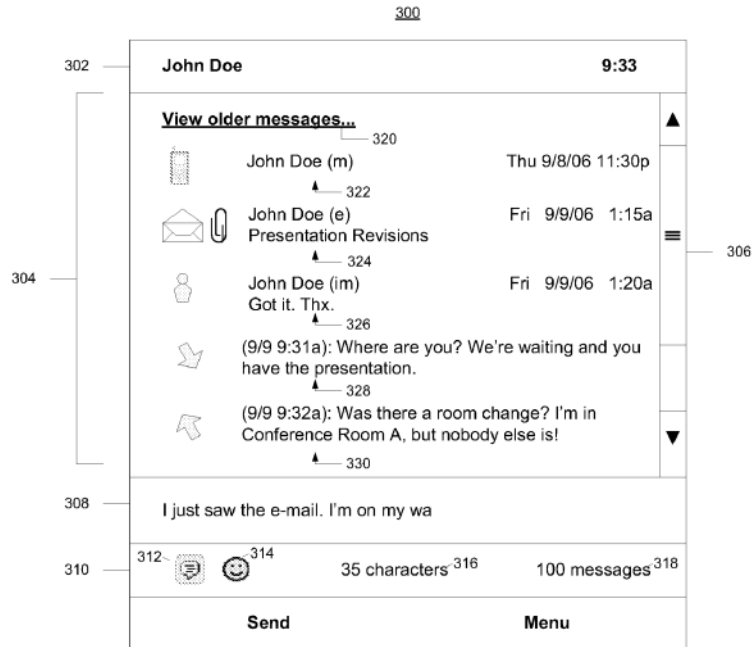


FIG. 3

APPLE-1042, FIG. 3

E. Overview of Ribaudo

39. Ribaudo describes techniques for providing a messaging communication connection between mobile devices based on a proximity determination. APPLE-1044, Title, Abstract, [0079]. Ribaudo describes using the same XMPP messaging and presence protocol discussed in Chatterjee to provide a “decentralized” instant messaging between devices. APPLE-1044, [0079], [0140], [0170], [0220]. Ribaudo explains that the instant “messaging connection” between devices can use “BLUETOOTH.” APPLE-1044, [0079]; *see also* [0066] (“BLUETOOTH-enabled mobile devices 12 on the same personal area network.”).

F. Overview of BenYoseph

40. BenYoseph describes techniques for “providing a set of bulk sender behavior policies and monitoring compliance by a bulk message sender with the set of policies.” EX1049, Abstract. “The bulk sender behavior policies may include a requirement that the bulk sender ... not send more than a predetermined amount of digital communications that are returned to the bulk message sender as undeliverable over a predetermined time interval” and “accept more than a predetermined amount of digital communications that are returned to the bulk message sender as undeliverable over a predetermined time interval.” *Id.*, 2:15-35. “The bulk sender behavior policies may further include a requirement that the bulk message sender not send future e-mails to an e-mail address of a recipient if an e-mail sent to the e-mail address is designated as undeliverable to a permanent delivery failure.” *Id.*, 2:36-58, 7:47-58, 11:15-33 (“mailbox ... may be full and unable to accept more emails”), 32:14-40; *generally id.*, 4:31-6:9.

G. Overview of Lin

41. Lin discloses “a method for establishing a real-time session-based IM system or data exchange system between mobile devices over a digital mobile network system that supports data packet-based communications.” APPLE-1045, [0006]. As part of Lin’s method, “[t]he initiating mobile device [] transmits its IP address, including its TCP port number, the user's personal conference number and the user’s PIN (to authenticate the user as the moderator) in an SMS text message

to [a] telephone number of [a] server 420.” *Id.*, [0017], FIG. 4; *see also id.*, Abstract, [0014]-[0016], FIGs.2-3.

VIII. GROUND 1A: CLAIMS 1, 3-4, 7, 9-13, 15, 22, 24, 26-29 ARE OBVIOUS IN VIEW OF THE HORVATH-TSAMPALIS-CHATTERJEE COMBINATION

A. Combining Horvath with Tsampalis

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

43. As described above, Horvath’s sender device determines whether to send an outgoing SMS message to a server system (*e.g.*, Information Processing

System 108 / SMSC 114) over a packet data network or a circuit switched network based on whether the sender is currently registered with a session initiation protocol (“SIP”) network on the packet data network. *Supra*, §VII.A (Horvath); APPLE-1004, [0004], [0074]-[0076], FIG. 6 (below). The server system in turn determines whether to forward the SMS message to the intended recipient device over a packet data network or a circuit switched network based on whether the recipient is registered on the packet data network. *Id.*

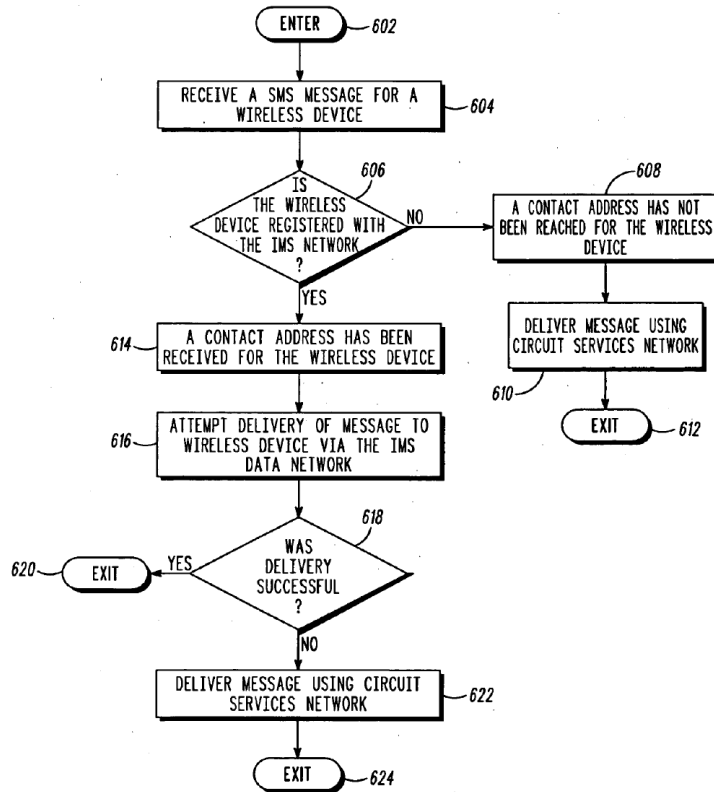


FIG. 6

APPLE-1004, FIG. 6 (Server Perspective)

44. By diverting SMS messages from the circuit switched network to the packet data network when a device is registered on a packet data network, Horvath's system beneficially reduces load and "unnecessary overhead" on the circuit switched network. APPLE-1004, [0004], [0009]. Notwithstanding these benefits, however, a POSITA would have recognized that Horvath's system was still ripe for improvement. For example, although Horvath acknowledges additional messaging services apart from SMS (e.g., MMS, EMS, IM), Horvath provides little detail about the additional messaging services. APPLE-1005, [0025], [0039]. Additionally, a POSITA would have appreciated that some users did not necessarily subscribe to each of these messaging services and users often had limited messaging capabilities that precluded them from receiving or processing richer media formats beyond SMS (e.g., MMS, EMS, IM). Consequently, the sender risked sending a message in a format that the recipient would be incapable of processing or presenting to a user. *Id.* This, in turn, resulted in failed message deliveries, re-transmission attempts that further burdened the network, increased processing load on messaging servers, and frustration by users who expected messages to be delivered in one format but which ultimately could not be delivered as expected. APPLE-1005, [0003]-[0004].

45. In view of these known problems with a multi-modal messaging environment like Horvath's in which different mobile device users subscribed to

messaging services (*e.g.*, SMS, MMS, EMS, IM), a POSITA would have turned to Tsampalis for specific guidance on how to improve the user experience and better manage and coordinate messaging formats in such an environment. *Supra*, §VII.A (Horvath); §VII.B (Tsampalis). In particular, Tsampalis describes an effective solution for improving messaging in such an environment by sharing the recipient's messaging format capabilities information with the sender. *Supra*, §VII.B. A POSITA reviewing Horvath and Tsampalis would have found it obvious to implement Horvath's system in accordance with Tsampalis's suggestions for a sender device to obtain and use messaging format capabilities information of a recipient device to determine how to format and transmit an outgoing message to the recipient. Multiple reasons would have prompted a POSITA to combine Horvath's and Tsampalis's teachings in this manner well before the Critical Date of the '450 Patent (July 24, 2007).

46. **First**, a POSITA would have combined Horvath and Tsampalis such that the sender would obtain and use a recipient's messaging format capabilities information to enhance users' messaging experiences and ensure that the format of outgoing messages is compatible with the messaging format capability of the recipients' device before the message is sent. Tsampalis itself expressly acknowledges the benefits flowing from these techniques, noting that "the determining of the message capabilities of a target mobile wireless communication

device before sending a message to such target device[] ... can enhance a user's experience by allowing a user to determine whether to attempt to send or modify a message based on the messaging capabilities of the intended recipient(s) of the message" and "by providing the user the ability to select a format in which to send a message based upon the messaging capabilities of the intended recipient(s) of the message." APPLE-1005, [0065]. Horvath also already considers the challenge of encoding in different network standards, which would further prompt a POSITA to combine with Tsampalis for teachings on formatting compatibility. *See e.g.*, APPLE-1004, [0050] (describing message encoding using "IS-637" versus very different "ANSI-41" standard).

47. **Second**, a POSITA would have sought to leverage Tsampalis-like messaging format capabilities information in Horvath's system to permit the sender to make more frequent and reliable use of enhanced messaging formats such as MMS and IM. Enhanced messaging formats such as MMS and IM generally offer richer messaging capabilities than SMS, such as the ability to support extended character counts for longer messages and the ability to attach/include multimedia files with the message. APPLE-1007, 8 ("IM&P [*i.e.*, Instant Messaging and Presence] service is more media-rich than traditional applications such as mail, phone, and email. By using IM&P, we can deliver voice, video, and data together to various endpoints."); APPLE-1025, Introduction ("The

most significant characteristic of MMS is to support multimedia contents. It can send not only texts, but also images, videos and audios. Therefore, MMS applications are much richer than those of SMS.”). A POSITA would have understood that the enhanced messaging capabilities of MMS and IM were often desirable for situations where users desired to communicate more than the short, text-based messages that could be accommodated by SMS. If the recipient’s messaging capabilities are unknown, however, some senders are biased toward not using any of the enhanced messaging features of MMS or IM to ensure the message is successfully delivered to the recipient using a more basic service (*e.g.*, SMS). But intentional avoidance of enhanced messaging features offered by MMS or IM is unnecessary if the recipient is in fact capable of receiving MMS or IM messages, and Tsampalis’s proposal to share the recipients’ messaging format capabilities information with the sender would allow a sender to use these rich messaging features more frequently and reliably with confidence that the recipient can successfully receive them.

48. **Third**, a POSITA would have sought to leverage Tsampalis-like messaging format capabilities information in Horvath’s system to make better, more selective use of SMS when the recipient has limited messaging capabilities. As Tsampalis explains, some users do not subscribe to MMS and are incapable of receiving or processing messages other than SMS or similar text-based messages.

APPLE-1005, [0061]-[0063]. By obtaining the recipients' messaging format capabilities information in advance of sending a message, the sender can ensure the message is appropriately sized and formatted according to the restrictions imposed by SMS and the limited messaging capabilities of the recipient. Likewise, the sender can avoid making use of richer features associated with formats such as MMS or IM that the recipient could not receive or process.

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

send the message, before sending a message that will later be bounced back”); [0022]-[0023], [0025].

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

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

52. **Seventh**, a POSITA would have found it obvious to combine the teachings of Horvath with Tsampalis because the combination merely involves the

application of a known technique to a known system to achieve predictable results. Tsampalis recognized a known problem with dynamic messaging environments like Horvath's in which users have different messaging format capabilities, and yet, Tsampalis's teachings would help address this problem in a straightforward manner that was well within the skill of a POSITA. A POSITA would have further recognized that at the time of the claimed invention, some users were still charged on a per SMS basis, and being selective about how messages were sent could save costs for both the sender and the receiver. APPLE-1009, 1 ("Sending an SMS message to a mobile telephone carries an attached cost for sending the message over the mobile network...A user of a mobile device whilst in a location with WiFi (or other form of) internet access would authenticate with the remote registration server and this would indicate to the Routing System that it was possible for that mobile device to receive text messages via the internet rather than via GSM SMS messages offering substantial cost savings to the sending party. Replies could also be made over the internet providing further costs savings."). Accordingly, the combination would have been obvious.

53. Likewise, a POSITA would have reasonably expected success implementing the combination, especially since the resulting system could be implemented with conventional software and hardware techniques (*e.g.*, general-purpose processors on mobile devices executing programmable instructions) with

messaging formats (*e.g.*, SMS, MMS, IM) that were well-defined and commonly implemented by the Critical Date of the '450 Patent. Further, the techniques that would be integrated from Tsampalis in the Horvath-Tsampalis combination are fully compatible with Horvath's and would not disturb the ability of Horvath's system to transmit or deliver SMS messages over either a packet-based or circuit switched network. Indeed, Horvath and Tsampalis both describe multi-modal wireless devices that are physically and logically compatible with each other. As discussed above, Horvath and Tsampalis are also both analogous art to the '450 Patent, each being in the same field of endeavor and reasonably pertinent to the problems said to be addressed by the '450 Patent. For example, like the '450 Patent, Horvath and Tsampalis both describe methods and systems for mobile messaging over wireless networks. *Id.*; *supra*, §§VI.A, VII.A-B.³

B. Combining Horvath and Tsampalis with Chatterjee

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

54. Horvath and Tsampalis each describe conventional mobile messaging services for wireless devices, including SMS, MMS, and EMS. APPLE-1004, [0025] (“Text messaging standards such as Short Message Service (‘SMS’), Enhanced Messaging Service (‘EMS’), Multimedia Messaging Service (‘MMS’), and the like are also included in the networks 102, 104.”); APPLE-1005, [0002] [0024] (“FIG. 1 illustrates a mobile wireless communication device such as a cellular telephone, two-way pager, or other device employing non-real-time store-and-forward messaging (e.g., SMS, EMS, MMS).”). While SMS, MMS, and EMS feature prominently in Horvath and Tsampalis, a POSITA would have appreciated that additional services were also commonly used for messaging on wireless devices by the Critical Date. For example, Horvath notes that its “IMS system also includes application servers that host and execute services for the wireless device 106,” where the services can include “SMS, MMS, caller ID, call waiting, push-to-talk, voicemail, and the like.” APPLE-1005, [0039]. Horvath also explains that “[t]he SIP network is used for establishing instant messaging, telephone calls, and other real-time communications over the Internet.” *Id.*, [0033]. Notably, Horvath acknowledges the option for additional messaging services such as instant messaging, although Horvath leaves many of the implementation details of these additional services to a POSITA. A POSITA interested in pursuing additional messaging services as suggested by Horvath would have turned to references like

Chatterjee for further detail about the capabilities of these services and how to implement them.

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

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

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

57. **Second**, a POSITA would have implemented instant messaging in the combination system to expand the capabilities of the device and keep current with the growing popularity of instant messaging in the timeframe leading up to the ’450 Patent. APPLE-1007, 4 (“Although IM started as a consumer-grade technology, it was quickly adopted by many businesses that saw its advantages in enabling quick communications and providing presence information. ... This new phenomenon is now impacting schools and college campuses.”).

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

59. **Fourth**, a POSITA would have considered IM to be a desirable messaging format to implement in the combination system because it “is more media-rich than traditional applications such as mail, phone, and email,” and IMs

can deliver not only text but also “voice, video, and data together to various endpoints.” APPLE-1007, 8. Further, “the delivered messages” can “integrate ... with existing systems and infrastructure” thereby “sav[ing] both time and money.” APPLE-1007, 8.

60. **Fifth**, a POSITA would have implemented presence capabilities in the combination system to better inform users of the instant messaging service when other users are available to receive instant messages. APPLE-1007, 4 (“By using presence information, an IM system enables us to search for a specific user, check the user’s status, and send short messages. ... We are also aware, in this case, whether or not the user is open to communicating at this time.”). To the extent presence is not obvious given that it is part of the SIP standard, Chatterjee makes it explicit. APPLE-1056 (a 2004 RFC already establishing the availability of presence functionality for SIP), Abstract (“This document describes the usage of the Session Initiation Protocol (SIP) for subscriptions and notifications of presence”); APPLE-1007, 4 (“By using presence information, an IM system enables us to search for a specific user, check the user’s status, and send short messages. ... We are also aware, in this case, whether or not the user is open to communicating at this time.”).

61. **Sixth**, it would have been obvious in view of Chatterjee to extend Tsampalis’s messaging format capabilities information in the combination system

to further indicate an intended recipient's instant messaging capability (e.g., in addition to SMS, MMS, EMS capabilities), and there would be no incompatibility between Tsampalis's teachings and the addition of instant messaging as an identifiable messaging capability of a device. A POSITA would have understood that identifying additional messaging capabilities of the intended recipient of a message, including information indicating whether the intended recipient is capable of receiving instant messages, would further Tsampalis's goal of enabling the sending device to select an optimal message format before sending a message, thereby enhancing the user's experience and reducing attempts to transmit a message in a format that the recipient is either incapable of receiving or that does not make best use of the recipients' messaging capabilities. APPLE-1005, [0065], [0003]-[0004]. Tsampalis identifies SMS, MMS, and EMS as "non-real-time store and-forward messaging format capabilities," but Tsampalis does not restrict the messaging format capabilities information from further including other messaging formats. On the contrary, Tsampalis contemplates that any suitable messaging format can be indicated in the messaging format capabilities information. APPLE-1005, [0022] (describing non-real time store-and-forward as a mere example of messaging format capabilities information ("*such as*")), [0025] (explaining that messaging format capabilities information can include "data representing that the device can process messages that are in an SMS format, EMS format, or *another*

suitable format”). Indeed, a POSITA would have desired to inform the sender of all messaging format capabilities of the recipient, including IM, to provide the sender with comprehensive information that would better allow the sender to optimize its selection of a format for messaging the recipient. *See also* APPLE-1007, 6 (describing known option for “store-and-forward” IM services). A POSITA also would have recognized messaging format capabilities information to be distinct from presence information about the intended recipient of a message, and the provision of messaging format capabilities information would be useful both on its own and together with IM presence information. For example, messaging format capabilities information allows a sender to identify and compare all or a least multiple different message formats that the intended recipient’s device is capable of receiving and processing, thereby allowing the sender to make an intelligent selection of an optimal format for a message. APPLE-1005, [0022]-[0025]. This functionality could not be realized from IM presence information alone, however, because such presence information only indicates the recipient’s willingness and/or availability to receive instant messages (not other formats). Additionally, messaging format capabilities information accounts for the capabilities of an intended recipient’s device to actually “process” messages of a particular format, whereas IM presence information can indicate that a recipient is available on one of multiple devices with no guarantee that the intended recipient

is currently present on a device that is necessarily capable of receiving/processing the IMs, depending on the particular presence indicators employed. APPLE-1005, [0025] (“data representing that the device can process messages” that are in particular formats).

62. Finally, a POSITA would have found it obvious to apply an IM&P service based on Chatterjee in combination with Horvath-Tsampalis because the combination merely involves the use of well-known techniques for instant messaging and presence to a known system to achieve predictable results. A POSITA would have reasonably expected success implementing the combination, especially since the resulting system could be implemented with conventional software and hardware on mobile devices using IM&P services that were well-established by the Critical Date. APPLE-1007, 10 (describing IM “available on the cell phone”), 4 (IM has been “quickly adopted”); APPLE-1045, [0002] (describing known techniques for “establish[ing] an instant messaging conferencing session ... among multiple mobile devices”). Notably, Horvath explicitly describes the option of using a SIP network for instant messaging, and Chatterjee expands on IM&P services such as SIMPLE that were specifically developed to operate on SIP networks, or Jabber that was capable of interfacing with an SIP server. APPLE-1007, 5-8, FIG. 2 (depicting “SIMPLE components”), FIG. 3 (depicting “Foreign IM gateway (Jabber to SIP)”). Chatterjee is also

analogous art to the '450 Patent and fully compatible with Horvath and Tsampalis, each being in the same field of endeavor and reasonably pertinent to the problems said to be addressed by the '450 Patent. For example, like the '450 Patent, Tsampalis describes methods and systems for mobile messaging over wireless networks (e.g., using IM).

C. Analysis with Respect to Claims 1, 3-4, 7, 9-13, 15, 22, 24, 26-29

Element [1pre]: A method comprising:

63. To the extent the preamble is limiting, the Horvath-Tsampalis-Chatterjee combination renders obvious [1pre]⁴. For example, Horvath is titled “method and system for delivery of short message service messages.” APPLE-1004, Title. Horvath describes a “method and device for transmitting at least one short messaging service message” where the method includes a wireless device “receiving at least one short message service message request associated with a short message service message” (e.g., an SMS message). APPLE-1004, Abstract; *see also id.* [0002], [0006]-[0007], [0045]-[0048], [0050], [0074]-[0080], FIGs. 1, 5-7. Horvath likewise describes an ability of the wireless device to transmit

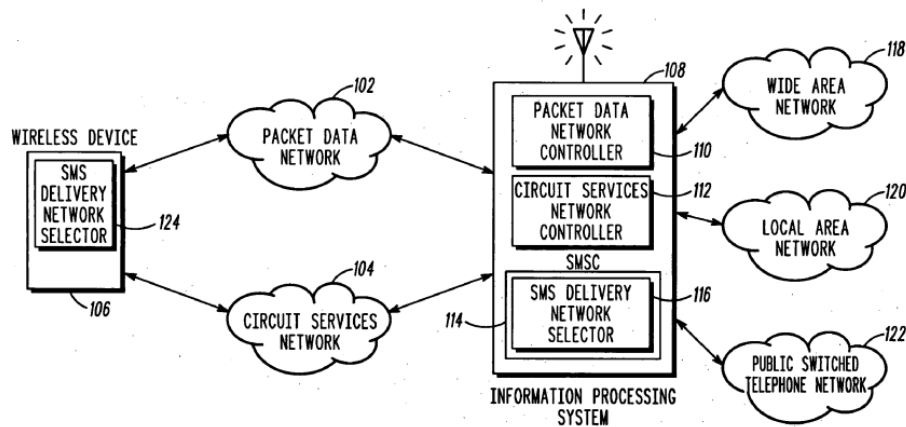
⁴ This Declaration incorporates the description of the Horvath-Tsampalis-Chatterjee combination from §§VIII.A-B into the analysis of each element of the Challenged Claims.

enhanced messaging service (“EMS”) messages, multimedia messaging service (“MMS”) messages, and instant messages. APPLE-1004, [0025], [0033].

Element [1a]: receiving a first message, by a first mobile wireless device from a second mobile wireless device, via a mobile operator base station, wherein the first message is formatted according to a short message service (SMS) format;

64. The Horvath-Tsampalis-Chatterjee combination renders obvious [1a]. As discussed above, Horvath discloses methods for transmitting and receiving SMS messages from a wireless device. *Supra* [1pre]; §VII.A.

65. For example, Horvath discloses a “wireless device 106” that communicates on “either the packet data network 102 or the circuit services network 104.” APPLE-1004, Title, [0001]-[0002], [0007], [0014], [0021], [0024]-[0026], [0031], [0033], [0039]-[0040], [0044]-[0050], [0060]-[0070], [0077]-[0080] FIGs. 1 (shown below), 2, 4, 6-8.



100
FIG. 1

APPLE-1004, FIG. 1

66. Horvath's receiving wireless device (*first mobile wireless device*) receives an SMS message from another wireless device (*second mobile wireless device*) via either the "packet data network" or the "circuit services network." APPLE-1004, [0045]-[0046] (explaining that the "SMS message" can be delivered to the "recipient device through the packet data network"); [0047]-[0048] (explaining that the "SMS message" can be delivered "to the recipient device through the traditional circuit services network method") [0079]-[0080] (describing an example method for a "Wireless Device Receiving a SMS Message" over either a "packet data network" or a "circuit services network."), FIG. 8; *see also id.* [0002], [0033], [0050], [0062]-[0063], FIGs. 1, 4, 7. The SMS message is formatted according to an SMS format. APPLE-1004, [0025] ([t]ext messaging standards such as Short Message Service ('SMS')); *see also* [0002], [0021].

67. Finally, Horvath teaches that the receiving wireless device (*first mobile wireless device*) can receive an SMS message *via a mobile operator base station*. For example, Horvath explains that both the "packet data network 102" and the "circuit services network 104" can be operated over cellular and other mobile networks. APPLE-1004, [0024]-[0027] (describing EV-DO, GPRS, UMTS, CDMA, GSM mobile networks); [0029] ("communicatively couples the wireless communications device 106 to ... a public switched telephone network 122 through the packet data network 102 and the circuit services network 104"), FIGs.

1-3; *see also id.*, [0002]. A POSITA would have understood and at least found obvious that receiving an SMS message over a cellular network would be received “via a mobile operator base station.” APPLE-1055, 1 (a “base station (BS)[] ... acts as a relay of the signals it receives”), 2-5.

Element [1b]: subscribing, by the first mobile wireless device, to a service for transmitting and receiving packet switched messages, via the Internet and the mobile operator base station;

68. The Horvath-Tsampalis-Chatterjee combination renders obvious [1b]. As further described below, the receiving wireless device (***first mobile wireless device***) in the combination subscribes to an instant messaging service (***service for transmitting and receiving packet switched messages***) via the Internet and the mobile operator base station.

69. Horvath discloses a “session initiation protocol (“SIP”) network” that is “used for establishing **instant messaging**.” APPLE-1004, [0033], *see also id.* [0025], [0038]-[0039] (“An IMS system also includes application servers that host and execute services for the wireless device 106.”). Horvath also describes determining “which application server(s) to forward the SIP message associated with the wireless device 106 so that the services **subscribed** to by the device 106 can be provided.” APPLE-1004, [0038], *see also id.* [0031] (“service(s) **subscribed** to by the wireless device 106.”), [0039], *see also id.* [0033], [0041], [0050], FIG. 5. “[R]egistration events” are sent to the “SMSC 114, which is acting

as an SIP application server.” APPLE-1004, [0041]. Horvath describes using a “subscriber profile” as part of the registration/authentication process of the wireless device to determine which application servers “are to be notified that they are to provide services for the wireless device.” *Id. see also id.*, [0050], [0071]-[0073], FIG. 5 (Step 510). A POSITA would have understood or at least found obvious from these disclosures that “establishing instant messaging” would require a subscription or involve subscribing to an IM service, such as at one of the application servers. *See also* APPLE-1007, Table 1 (disclosing various example IM services), p. 5 (describing users of IM services as “subscribers”); APPLE-1050, 1 (“A present and instant messaging system allows users to **subscribe** to each other ...”). In more detail, Horvath explains that each wireless device must register with the IMS to access services over SIP, and that each registered device has a profile including “subscription related information” maintained in a database by a registrar for the IMS (e.g., home subscriber server 210). APPLE-1004, [0035], [0036] (“The wireless device 106 is assigned to a specific P-CSCF 206 for the duration of the device’s subscription to the IMS network.”). Horvath also explains that “[t]he SIP network is used for establishing instant messaging” and that the IMS system “includes application servers that host and execute services for the wireless device 106.” APPLE-1004, [0033], [0039] (“A service for example, is SMS, MMS, ... and the like.”). A POSITA would have understood from

Horvath's disclosure and knowledge of IMS/SIP that instant messaging is one of the services of the IMS system supported by SIP such that devices capable of establishing instant messaging sessions would need to have subscription information in the IMS system and would have subscribed to an instant messaging service (e.g., an IM service hosted by application server(s)). APPLE-1004, [0033]; APPLE-1046, [0003] (S-CSCF "provides services to the user that the user is subscribed to"), [0027] (describing details of "a user (IMS) subscription"), [0029] ("Within the IMS service network, application servers (Ass) are provided for implementing IMS service functionality."), [0034] ("an application server must store ... a service configuration for each IMPU" of subscribed users), [0093], FIG. 2. Chatterjee provides additional details about known instant messaging services including services like SIMPLE implemented using SIP and Jabber/SMPP services that all involve subscriptions to the IM service. APPLE-1007, 5 (AIM "increased its subscribers to ten million users"), 8 ("A contact in the roster item indicates that the user has subscribed"), 8 ("subscribed, ..., unsubscribed" presence statuses). In short, a POSITA would have understood or at least found obvious that IM services like those described in Horvath and Chatterjee are services for transmitting and receiving packet switched messages.

70. A POSITA also would have understood based on Horvath's and Chatterjee's teachings that an instant messaging service is a service for

transmitting and receiving packet switched messages. *Cf.* APPLE-1001, 1:66-2:1 ('450 Patent admitting that “instant messaging” is performed “via an IP network”). Indeed, Horvath’s “SIP network” is a type of packet data network. APPLE-1004, [0024] (“In one embodiment, the packet data network 102 is an Internet Protocol (‘IP’) connectivity network, which provides data connections at much higher transfer rates than [*sic*] a traditional circuit services network.”), [0033]-[0034], [0037] (messages are sent over the SIP network in “**SIP packets**”), [0046]; *see also id.* [0004], [0074]-[0076], FIG. 6. Moreover, Chatterjee teaches well-known protocols for IM including SIP/SIMPLE and Jabber/XMPP, both of which enable transmitting and receiving packet switched messages from a wireless device. APPLE-1007, 1, 7-8 (“the network packet with message Hello! sent from Alice@foobar.com to Bob@foobar.com is represented in Box 1. The network packet was captured on the source machine (Alice’s machine) using Ethereal Network Protocol Analyzer available at <http://www.ethereal.com>. The packet is not an exact illustration of all the details. It just gives an overview of how the information is stored and transferred on the network...”), Boxes 1, 2.

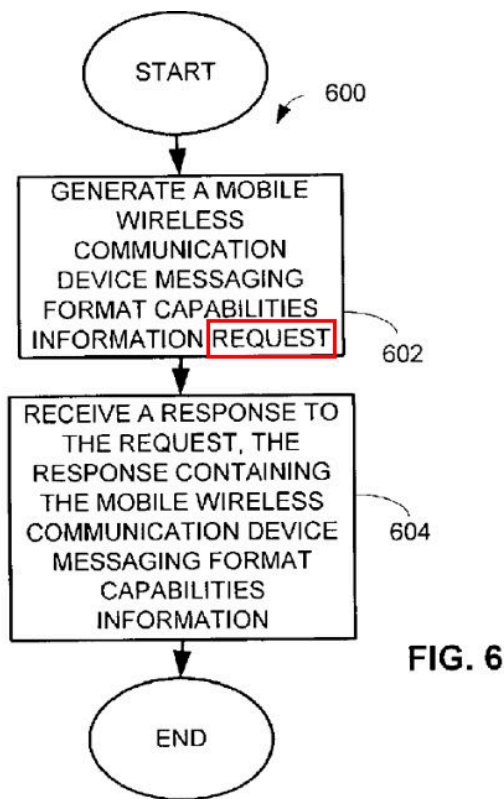
71. Finally, Horvath’s and Chatterjee’s teachings would have rendered obvious subscribing to the IM service “via the Internet and the mobile operator base station.” For example, Horvath expressly teaches that “[t]he **SIP network** is used for establishing **instant messaging**, telephone calls, and other real-time

communications **over the Internet.**”; *see also* APPLE-1004, [0033]; APPLE-1007, 1, 5, 7-8 (Box 1; Box 2). Because SIP operates on the packet data network 102 for establishing instant messaging over the Internet, a POSITA would have understood or at least found it obvious that subscriptions to the IM service would also be made over the Internet as was common before the Critical Date. APPLE-1007, 4 (“IM systems exist in various Internet communities”), 6 (“interoperate across the Internet”). Further, Horvath explains that the wireless device can communicate over the packet data network 102 using a cellular or mobile operator network such as EV-DO, GPRS, UMTS, or the like, in which case it would have been obvious that the subscription to the IM service would be made via the Internet and a mobile operator base station of the network. *Supra* [1a]; APPLE-1004, [0026]-[0027], *see also id.*, [0002].

Element [1c]: transmitting, by the first mobile wireless device, after the subscribing, a request including at least information corresponding to at least one mobile phone number of the second mobile wireless device, to determine whether the second mobile wireless device corresponds to a subscriber of the service;

72. The Horvath-Tsampalis-Chatterjee combination renders obvious [1c]. As discussed above, Horvath’s wireless device 106 (***first mobile wireless device***) in the combination implements Tsampalis’s technique for sending a “second mobile wireless communication device messaging format capabilities information request” to determine the second device’s messaging capabilities. *Supra* §§VII.B-

C, VIII.A-B; APPLE-1005, [0024], [0027], [0042], [0034], [0056]-[0057], FIGs. 6 (step “602”), 7; *see also id.* Title, Abstract, [0001], [0022]-[0024][0029]-[0039] FIGs. 1-2, 5-7, 13). Tsampalis explains that the wireless device generates the “messaging format capabilities information request” by entering a “recipient ID,” which is illustrated as being a phone number. APPLE-1005, [0033], FIGs. 3-4 (showing the recipient ID in the phone number format); *see also id.* [0024], [0027], [0031]-[0032], [0034]-[0037], [0039] [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”); [0046]; [0056]-[0060] (“request and retrieve the second mobile wireless communication device messaging format capabilities information 110,” “a second mobile wireless communication device messaging format request 226,” “new capabilities signal one 1326 [including] at least the second mobile wireless communication device messaging format capabilities information 110”), FIGs. 6 (below, step 602), 13-15.



APPLE-1005, FIG. 6 (Annotated)

73. As explained above in the overview of the Horvath-Tsampalis-Chatterjee combination, it would have been obvious to implement Tsampalis’s messaging format capabilities information request, which includes information corresponding to a phone number of the recipient (e.g., second mobile wireless device), to determine whether the second mobile wireless device is also subscribed to the instant messaging service (e.g., “to determine whether the second mobile wireless device corresponds to a subscriber of the service”). *Supra* §§VIII.A-B; *infra*, [1d]. As discussed above in [1b] (and below in [1d]), a POSITA would have understood or at least found obvious that capabilities information for a second

device indicating that a device is capable of receiving and processing IMs would have also served as an indication that the device corresponds to a subscriber of the IM service (i.e., a service for transmitting/receiving packet switched messages) since receiving/processing IMs requires an IM subscription.⁵ APPLE-1003, ¶73; *supra*, [1b]; *infra*, [1d]. Requesting a recipient's messaging format capabilities information after the subscribing also would have been obvious because a user of the first mobile wireless device would naturally be interested in the intended

⁵ Even if some other uncommon protocols support instant messaging via a circuit-switched bearer, that would does not detract from the fact that IM is predominantly a service for receiving messages via a packet switched bearer. In fact, Horvath explicitly discloses that its IM sessions are established over SIP, on the packet data network 102 (i.e., a packet-switched bearer), and Chatterjee describes IM packets transmitted over the Internet. APPLE-1004, [0033]; APPLE-1007. Nothing in the plain language of the claim requires that the service never be capable of communicating messages via a circuit-switched bearer. Thus, determining whether the destination address corresponds to a subscriber for receiving an outgoing message via a Horvath- or Chatterjee-like IM service is tantamount to determining whether the whether the destination address corresponds to a subscriber of a service for transmitting and receiving packet switched messages.

recipient's IM capability after subscribing to the IM service, which is when the sender would actually be able to send IMs as a suitable messaging format if the intended recipient was also capable of receiving IMs.

73A. Moreover, to be clear, a POSITA would have understood the indications of supported messaging formats in Tsampalis's messaging format capabilities information to represent not only a device's physical capabilities or potential to receive messages of a particular format (e.g., SMS, EMS, MMS, IM), but also whether the device actually has a subscription to the respective messaging services for the formats identified in its capabilities information such that the device would be capable of utilizing those services as needed to receive the messages. This is evident from Tsampalis's explanation that "messaging format capabilities information 110 may be data representing that the device can *process* messages." APPLE-1005, [0025]; *see also id.*, [0022] ("send a message ... in a format that can be *processed* by the target mobile wireless communication device"). Tsampalis sought to reduce failed message delivery attempts by providing senders with the target device's messaging capabilities information so that senders would be less likely to attempt transmission of messages in formats that could not actually be delivered to the recipient. APPLE-1005, [0065], [0002]-[0004], [0022]-[0023]. If the capabilities information was based only on the physical capability of the device without account for whether the device was subscribed to the corresponding

messaging services, Tsampalis would not have achieved the goals it proclaims to achieve. For example, this would have left the recipient of the capabilities information with a misleading indication that a target device was capable of receiving a message in a particular format, even if messages in that format could never actually be delivered to or processed by the target device due to the target device's lack of subscription to a service (e.g., an MMS subscription). This is inconsistent with Tsampalis's disclosure and not how a POSITA would have understood Tsampalis's descriptions of capabilities information or the problems and solutions described therein. Instead, a POSITA would have understood Tsampalis's messaging format capabilities information to indicate the capabilities of the target device to ultimately receive and process messages of different types/formats, which is itself indicative of whether the target device corresponds to a subscriber of each of the different messaging services for different message formats (e.g., SMS, MMS, EMS, IM).

74. As another example, Chatterjee discloses that after a user has subscribed to an IM service, the user can use his/her device to transmit a request to subscribe to presence information for a contact. APPLE-1007, 7 ("When users add contacts to their list, they subscribe to these contacts' presence information. In this case, a watcher sends a SUBSCRIBE request to a PA. Once the subscription has been made, any change to the contact's presence information is conveyed to the

user who added the contact. This is done by transferring a NOTIFY message using SIP from PA to watcher [15].”), 8 (“A contact in the roster item indicates that the user has subscribed to the contact’s presence information.”), Table 2 (showing functionality is implemented in both SIP/SIMPLE and Jabber/XMPP); *see also supra* §§VII.C, VIII.A-B; *infra* [1d]. A POSITA also would have known that conventional IM services like those disclosed in Horvath and Chatterjee allowed users to fetch a contact’s current presence status by transmitting requests. APPLE-1007, 5 (“Fetchers pull the value of presence information for a specificpresentity.”); APPLE-1050 (“A special kind of FETCHER is one that fetches information on a regular basis. This is called a POLLER.”); APPLE-1053, 11 (“Each transaction consists of a request ...”). The contact can be identified in the request by a phone number of the contact’s mobile device (e.g., the second mobile wireless device), for example. APPLE-1004, [0035] (“A tel-URI, for example is the telephone number assigned to the wireless device 106.”); APPLE-1005, [0031]-[0033], [0042], FIGs. 3 and 6 (disclosing requests for capabilities information including “recipient IDs” as phone numbers). A request for presence information for a contact in this context renders obvious a type of request to determine whether the second mobile wireless device corresponds to a subscriber of the IM service at least because the contact would not be present on the IM service if the contact were not a subscriber. APPLE-1004, [0035] (explaining that “subscription related

information” for authorized users must be stored), [0038] (“services subscribed to by the device 106”). Thus, an indication that the contact is present would indicate that the contact has subscribed to the IM service. *Id.* Furthermore, a POSITA would have known or at least found obvious that presence indications that a user is not available can also indicate that a user is not subscribed, for example, due to expiration of the contact’s registration or subscription, deactivation of the subscriber, or due to the subscriber affirmatively deregistering and unsubscribing. APPLE-1048, 9.

Element [1d]: receiving, by the first mobile wireless device, a response to the request indicating that the second mobile wireless device corresponds to a subscriber of the service; and

75. The Horvath-Tsampalis-Chatterjee combination renders obvious [1d]. For example, Tsampalis discloses receiving a response to the “messaging format capabilities request,” discussed above. *See supra* [1c]; *see also* APPLE-1005, [0024], [0027], [0034], [0042]-[0043], [0056]-[0057], FIGs. 6 (below step 604), 7, 13. Tsampalis explains that this response “contains the second mobile wireless communication device messaging format capabilities information.” APPLE-1005, [0042]-[0043], *see also id.* [0022]-[0024], [0027].

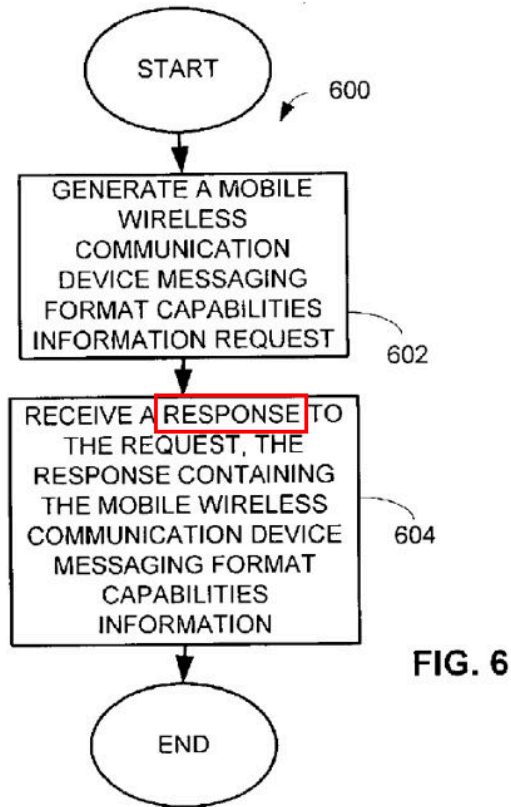


FIG. 6

APPLE-1005, FIG. 6 (Annotated)

76. As discussed above, it would have been obvious for the response including “messaging format capabilities information” to indicate whether the second wireless device is also subscribed to the instant messaging service. *Supra*, §§VIII.A-B. For example, based on Tsampalis’s teachings, a POSITA would have understood and found obvious that the IM transmitting wireless device in the Horvath-Tsampalis-Chatterjee system determines whether the destination address (e.g., phone number) of the intended recipient of an outgoing message is a subscriber of the IM service (*i.e., to determine whether the second mobile wireless device corresponds to a subscriber of the service*) by checking whether IM is an

available message format for the intended recipient as indicated by the recipient's messaging format capabilities information. *Supra* §§VII.C; VIII.A-B. Because a wireless device subscribes to an IM service to receive IM messages, a POSITA would have understood and found obvious that the transmitting wireless device in the Horvath-Tsampalis-Chatterjee combination would determine whether the destination address (*e.g.*, phone number) of the intended recipient of an outgoing message is a subscriber of an IM service by checking whether IM is an available message format for the intended recipient as indicated by the recipient's messaging format capabilities information, based on Tsampalis's teachings. APPLE-1005, [0022]-[0025], [0041], [0056]-[0065], FIGS. 5-6, 13; *supra*, §VII.C.

77. It also would have been obvious for the first mobile device to receive a response to a request for the presence information of a contact associated with the second mobile wireless device that indicates whether the second device corresponds to a subscriber of the IM service, as discussed above in connection with [1c]. *Supra*, [1c]; APPLE-1007, 7 ("Once the subscription has been made, any change to the contact's presence information is conveyed to the user who added the contact. This is done by transferring a NOTIFY message using SIP from PA to watcher [15]."), 8 ("A contact in the roster item indicates that the user has subscribed to the contact's presence information."), Table 2; APPLE-1050, 14

(“notify it immediately of changes in the PRESENCE INFORMATION”), 3 (“fetches [presence] information on a regular basis”).

Element [1e]: formatting a second message in accordance with a message format of the service, subsequent to the subscribing and based at least in part on the response;

78. The Horvath-Tsampalis-Chatterjee combination renders obvious [1e]. For example, Tsampalis discloses that a first mobile wireless device, “using the messaging format capabilities information, then send[s] a message to a target mobile wireless communication device in a format that can be processed by the target mobile wireless communication device.” APPLE-1005, [0022]; *see also id.*, [0025] (“sends message 112, in a format identified in the second mobile wireless communication device messaging format capabilities information 110”), [0041], FIG. 5 (504), FIG. 8 (504), FIG. 9 (504). In the combination, which integrates an IM service as taught in Horvath and Chatterjee, it would have been obvious based on Tsampalis to configure the first mobile wireless device to format messages in accordance with the recipient device’s capabilities. *Id.*; *supra*, §§VIII.A-B. Thus, the first mobile wireless device would format the second message as an instant message, based on the intended recipient device’s messaging format capabilities information (***response***) indicating that the second device is capable of receiving instant messages as a subscriber of an IM service. *Id.* For example, if the intended recipient is able to receive IMs, it would have been obvious that the sender in

many cases would prefer to send IMs as opposed to other message formats due to the comparatively lower cost of transmitting messages over packet data networks and the ability to achieve real-time communications through instant messaging. Similarly, if presence information (an alternative mapping of “*response*”) returned to the first mobile wireless device indicates that the intended recipient of the second message is currently active on the IM service, it would have been obvious to format the second message as an IM for similar reasons, including to establish real-time communications with the intended recipient while the intended recipient is presently available to receive IMs.

79. Finally, it would have been obvious to a POSITA to format the second message as an IM in accordance with the IM message format of the IM service *subsequent to the subscribing* because subscribing to the IM service would be an ordinary predicate to sending the message as an IM over the IM service. *Supra*, [1b]. A wireless device would not ordinarily format a message according to a service it is not capable of using to send the message when it is not subscribed. *Supra*, §§VII.C, VIII.A-B.

Element [1f]: wherein the message format of the service is not a short message service (SMS) message format, a multimedia message service (MMS) message format or an enhanced message service (EMS) message format;

80. The Horvath-Tsampalis-Chatterjee combination renders obvious [1f]. As discussed above, the second message is formatted according to an IM format as

taught in Horvath and Chatterjee. *Supra* [1e]; *see also supra* §§VII.C, VIII.A-B. The various IM formats disclosed in Chatterjee include SIP/SIMPLE and Jabber/XXMP, for example, which are plainly not SMS/MMS/EMS message formats.

Element [1g]: wherein the first message is received prior to the subscribing.

81. The Horvath-Tsampalis-Chatterjee combination renders obvious [1g]. To start, Horvath expressly describes a scenario where it would have been obvious for the first message (SMS message) to be received prior to subscribing. In particular, Horvath explains that “[i]f the recipient wireless device is not registered on the packet data network 102, the SMSC 114 delivers the SMS message to the recipient wireless device through the traditional circuit services network method.” APPLE-1004, [0047]. As explained above the SIP network/packet data network is “used for establishing instant messaging.” APPLE-1004, [0033]. A POSITA would have understood that one reason that the recipient wireless device may not be registered on the packet data network 102 is because the recipient wireless device has not subscribed to services on the packet data network, such as instant messaging or packet-based SMS services. Accordingly, it would have been obvious that the SMS message (e.g., the first message) in this scenario would be received prior to the subscribing to the IM service.

82. Moreover, a POSITA would have understood that many mobile messaging users receive messages on a frequent basis from a variety of contacts at various times. Indeed, a contact may decide to send a first user a message at any time for any reason. Accordingly, it would have been obvious for the first message to be received by the first mobile wireless device before the subscribing as a predictable and natural consequence of the user of the second mobile wireless device deciding to send the first message at any time before a user of the first mobile wireless device decides to subscribe to the service.

Claim [3]: The method of claim 1, further comprising: formatting the second message for transmission over a wireless local area network (WLAN).

83. The Horvath-Tsampalis-Chatterjee combination renders obvious Claim 3. As explained above, Horvath's first mobile wireless device formats the second message in an IM format for transmission over Horvath's "packet data network 102." *Supra* [1b], [1f]. Horvath explains that "packet data network 102 is an Internet Protocol ('IP') connectivity network, which provides data connections at much higher transfer rates than [*sic*] a traditional circuit services network," and the "SIP network" on the packet data network 102 is "used for establishing instant messaging...and other real-time communications over the Internet." APPLE-1004, [0024], [0033]. Horvath explicitly discloses that the packet data network 102 can include "an 802.11 network," commonly known as Wi-Fi (a *WLAN* that operates based on the IEEE 802.11 standards). APPLE-1004, [0021], [0024], [0033]-[0034],

[0050]. Accordingly, it would have been obvious that, by formatting the the second message as an IM message, the second message would be formatted for transmission over a WLAN. APPLE-1011, 5:1-33 (“WLAN capabilities including...technology version (such as 802.11[])”), 6:27-32 (“WLAN 802 protocols...IEEE 802 networks”), FIG. 5B; APPLE-1009, 1 (“New generation mobile phones in addition to GSM capability also have the ability to access the internet via 802.11 g, b and other related wireless protocols.”), 3 (“The mobile GSM device would have an operating system capable of running an application which could subscribe and log into a registration server when the device gained access to the internet via a route such as bluetooth, Wifi (802.11 b,g or other)...”), 4 (“Wi-Fi is an abbreviation for wireless fidelity and is used to refer generically to any type of wireless network based on the IEEE 802.11 standard or similar form of IP based wireless communication”) APPLE-1037 (“When did Wi-Fi become popular? ... 2004: The first Wi-Fi-certified devices (cell phones, PDAs and TVs) hit the market.”); *see also* APPLE-1004, [0033]-[0034] (“The wireless device 106 can connect to the IMS network using different methods, which all use standard IP.”).

Claim [4]: The method of claim 1, further comprising: transmitting, after a change of the first mobile wireless device to a new handset, information indicating that subscribers of the service should no longer be formatting messages of the service for the first mobile wireless device.

84. The Horvath-Tsampalis-Chatterjee renders obvious Claim 4. Horvath explains how a wireless device can “deregister” from the IMS core, which as explained below, occurs when the device transmits a deregistration message (e.g., a SIP REGISTER message with Expire=0), thereby leaving the device unable to receive messages on the packet data network. APPLE-1004, [0047], [0053], [0075]. For example, a predictable scenario in which the first mobile wireless device would deregister from the IMS core is when a user of the first mobile wireless device changes to a new handset. This is because users often register with the IMS core using a phone number, e.g., a phone number associated with the first device, and the user would deregister the phone number of the first device in favor of registration for a new number associated with the new handset when the handset is changed. To this point, a POSITA would have appreciated that IMS users are assigned IMS Public User Identifies (IMPUs) that “are used by any user to request communications to other users. A user might for example include an IMPU ... on a business card,” and an IMPU can use “telecom numbering” in “the form of a SIP URI ... or the ‘tel:’-URI format.” APPLE-1046, [0017]-[0019]; *see also* APPLE-1004, [0035] (“tel-URI, for example is the telephone number assigned to the wireless device 105”); APPLE-1046, [0006]-[0030], FIG. 2. When a user’s IMPU is defined according his/her phone number (“telecom numbering”), it would have been obvious that a user would seek to update his/her IMPU upon obtaining a new

handset associated with a new phone number so that the IMPU would correspond to the new phone number of the new handset rather than the old phone number of the first wireless device.

85. Updating an IMPU involves registering the new IMPU defined by the new phone number and deregistering (also referred to as “unregistering”) the IMPU defined by the old phone number. De/unregistering from an IMS and SIP network conventionally transmission of an unregister message from the user’s device (e.g., the first mobile wireless device) to the IMS core, such as a SIP REGISTER message with Expires=0, to indicate that a user of the first mobile device has changed handsets. APPLE-1047 (“If expires header is set to be Zero in REGISTER message, it means ‘DeREGISTER’.”); APPLE-1048, 9 (“The unregistered event occurs when a REGISTER request sets the expiration time of that contact to zero.”). A POSITA would have recognized that the transmitted message to de/unregister the phone number of the first device from the IMS represents an indication that subscribers of the service should no longer format messages of the service for the first mobile wireless device. For instance, by requesting to de/unregister the phone number of the first device, the transmitted message would indicate that subscribers should not format IM messages to be addressed to the IMPU defined by the retired phone number of the first device as the IMS core would automatically notify other subscribers of the de/unregistration

of the IMPU associated with the prior device (e.g., the first mobile wireless device). APPLE-1048, 9 (“a NOTIFY is sent”), FIG. 2 (“unregistered”); APPLE-1004, [0043] (“registration notification”), [0075].

Claim [7]: The method claim 1, further comprising: authenticating a mobile phone number of the first mobile wireless device to the service prior to receiving the response.

86. The Horvath-Tsampalis-Chatterjee renders obvious Claim 7. For example, Horvath describes authenticating its wireless devices 106, e.g., through authenticating an identifier such as a phone number of wireless device 106 during registration with the SIP/IMS network. APPLE-1004, FIG. 5 (“S-CSCF authenticates and registers the wireless device” at step 508), [0035] (“The HSS 210 comprises a database including profiles associated with each wireless device 106 registered with the IMS. A profile, for example, includes subscription related information. **The HSS 210 also performs authentication and authorization** of the wireless device 106....The HSS 210 also includes **information to identify** each registered wireless device 106 such as a telephone uniform resource identifier (‘tel-URI’) A tel-URI, for example is the **telephone number assigned to the wireless device 106.**”), [0036], [0040]; APPLE-1046, [0004] (“IMS authenticates the user”).

87. In more detail, Horvath explains the SIP registration process for the wireless device 106 with the S-CSCF component of the remote server(s), during

which “authentication and authorization” of the wireless device 106, through the database HSS containing “profiles associated with each wireless device 106” identified by *e.g.*, “the telephone number assigned to the wireless device 106,” is also performed. APPLE-1004, [0035]-[0036], [0038], [0040]- [0041], [0072]-[0073], [0076], FIGS. 2, 5; *supra*, §VII.C.

88. Through authentication with the remote server(s), wireless device 106 is also authenticated to the instant messaging service (*authenticating...to the service*), which is a service for sending and receiving packet switched messages real time. APPLE-1004, [0033], [0038]-[0039] (“An application server [providing messaging service(s) such as instant messaging] interfaces with the S-CSCF component of the I, S-CSCF 20S using SIP.”), [0041] (“A subscriber profile sent to the S-CSCF includes the filter criteria which are used by the S-CSCF to determine the application servers that are to be notified that they are to provide services for the wireless device 106. In one embodiment, part of the filter criteria includes conditions such that, when the conditions are satisfied, the S-CSCF notifies the SMSC 114 that the wireless device 106 has registered with the packet data network 102.... The SMSC 114 does not have to authenticate the wireless device 106 because the S-CSCF 206 has already done so.”), [0073]; APPLE-1007, 4 (“Instant messaging (IM)...enables [message] exchanges in real time”), 7, Boxes 1 & 2. Horvath’s teachings in this regard are consistent with conventional

techniques for authenticating users to an IM service by the Critical Date. APPLE-1009, pages 1 (“A user of a mobile device whilst in a location with WiFi (or other form of) internet access would authenticate with the remote registration server and this would indicate to the Routing System that it was possible for that mobile device to receive text messages via the internet rather than via GSM SMS messages”), 3 (“The registration server could be either a dedicated solution using normal web based protocols such as http post or get, or via SIP, SMPP or other protocol which allows authentication with a remote device.”), 5 (“A Routing System consisting of a gateway system containing a registration server capable of authenticating remote mobile devices via IP and identifying the device via a unique identifier which can be related to the devices GSM mobile number via lookup in a database or other information storage system”), 6 (“A Routing System utilising [sic] of Software capable of being installed and operated on a mobile device which authenticates with a remote database to signify it’s accessibility via an IP based route.”); APPLE-1043, §3 (“INSTANT MESSAGE SERVICE...May require authentication of SENDER USER AGENTS and/or INSTANT INBOXES...PRESENCE SERVICE...May require authentication of PRESENTITIES, and/or WATCHERS”); APPLE-1009); *see also* APPLE-1004, [0033] (“The SIP network is used for establishing instant messaging...and other real-time communications over the Internet.”). When the phone number of the first

mobile wireless device (e.g., tel-URI) is registered in SIP or other network implementing the IM service, it would have been obvious for that phone number to be authenticated according to Horvath's teachings. APPLE-1004, [0035].

89. Because the first mobile wireless device in the Horvath-Tsampalis-Chatterjee combination transmits the request and receives the response after the subscribing (*supra*, [1c]-[1d]), and because authentication occurs during the subscribing and subsequent registrations to the network (as described above in the analysis of this claim element and *supra* with respect to [1b]), it would have been obvious that authentication would occur prior to receiving the response. APPLE-1004, [0033], [0035]-[0036], [0038]-[0039], [0040]-[0041], [0072]-[0073], [0076], FIGS. 2, 5. This would also be obvious to improve security by ensuring the phone number of the first mobile wireless device was properly authenticated before the device requests or obtains messaging format capabilities information or presence information about the second device.

Claim [9]

90. *Supra*, [1pre]-[1g]^{6,7}

⁶ This Declaration addresses in the analysis of all corresponding limitations of claim 1 how those limitations are rendered obvious even when performed by the first mobile wireless device, as recited in the preamble of claim 9.

Claim [10]: The method of claim 9, wherein at the time of transmitting the request, the first mobile wireless device does not have in memory a user name or email address associated with the second mobile wireless device.

91. The Horvath-Tsampalis-Chatterjee combination renders obvious Claim 10. As discussed above, Tsampalis teaches transmitting a “second mobile wireless communication device messaging format capabilities information request” using a recipient ID (e.g., a phone number) for the second user device. *Supra* [1c]-[1d]; §§VII.B, VIII.A-B. Likewise, Horvath discusses registering the wireless devices phone numbers to allow the S-CSCF to forward messages to the associated application servers (such as an IM server). APPLE-1004, [0035] (“tel-URI”), [0038]-[0039], [0041], [0073]. Accordingly, both Tsampalis and Horvath describe a system that at the time of transmitting the request, the wireless device would only need a phone number associated with the second wireless device to transmit the request. As there is no need for the first wireless device to have a separate user name or email address of the second wireless device to transmit the request, it would have been obvious that in many cases the first wireless device would not

⁷ This Declaration addresses in the analysis of all corresponding limitations of claim 1 how those limitations are rendered obvious when performed by the first mobile wireless device, as recited in the preambles of claims 9 and 24.

have these items stored in memory when transmitting the request (e.g., if the user has not yet fully populated an entry in an address book with these items).

Claim [11]: The method of claim 9, further comprising: formatting the second message for transmission over a wireless local area network (WLAN).

92. The Horvath-Tsampalis-Chatterjee combination renders obvious Claim 11. *Supra*, Claim 3.

Claim [12]: The method of claim 9, wherein the information corresponding to at least one mobile phone number of the second mobile wireless device is retrieved from the first message.

93. The Horvath-Tsampalis-Chatterjee combination renders obvious Claim 12. As discussed above, Horvath teaches receiving an SMS message as the first message before subscribing to the IM service. *Supra*, [1a], [1c], [1g]. As also discussed, the combination implements Tsampalis' teachings for sending a "second mobile wireless communication device messaging format capabilities information request," including a phone number corresponding to the second device, to determine the second device's messaging capabilities. APPLE-1005, [0024]-[0025], FIGs. 2-3, 6; *supra* [1c]-[1d]; §VII.B. Because the first message is an SMS message that originated from the second mobile wireless device, SMS messages conventionally indicate the phone number of the device that originated the message, and the first mobile wireless device transmits a request that includes information corresponding to the phone number of the second mobile wireless device, it would have been obvious to use second device's phone number from the SMS message as

the phone number used to send the request per Tsampalis' teachings (or as a tel-URI to send a presence request per Horvath's and Chatterjee's teachings). This would have been an obvious way to obtain contact information that specifies the second wireless device as the first device has already received a message from the second device containing the second device's phone number. It was well known how to retrieve a phone number from an SMS message. APPLE-1051, [0035] ("When the recipient's phone receives the SMS message, the recipient's phone recognizes that the SMS message includes contact information by analyzing the arrangement of the SMS message. The recipient's phone automatically prompts the recipient to add the caller's contact information to the recipient's contact information.").

Claim [13]: The method of claim 9, further comprising: receiving presence information associated with the second mobile wireless device after the subscribing; and displaying the presence information associated with the second mobile wireless device.

94. The Horvath-Tsampalis-Chatterjee combination renders obvious Claim 13. For example, Chatterjee describes various IM and presence applications and standards. 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"), 4 ("IM systems, with the ability of providing presence information, enables a user to know the availability of other users. By using presence information, an IM system enables us

to search for a specific user, check the user's status, and send short messages. Popular IM applications include AOL™ Instant Messenger (AIM), ICQ™ (“I Seek You”), MSN™ or WindowsXP™ Messenger, and Yahoo™ Messenger....there are times when we may need an instant response from one in a group of users. It takes a while just to find one of the users in that group, who might be available or not. In IM applications, if we have that group of users on our ‘buddy list,’ we can tell at a glance if any of them are logged onto the network, and whether they have been active recently. We are also aware, in this case, whether or not the user is open to communicating at this time. If they are, we can send a quick IM and communicate further.””); *see also supra* §§VII.C, VIII.A-B. A POSITA would have known that “[a] presence and instant messaging system allows users to subscribe to each other and be notified of changes in state,” and therefore it would have been understood or at least obvious that presence information would be received by first mobile device after subscribing to the IM service. It was also well known before the Critical Date to display presence information of other subscribers of an IM service such as the second mobile wireless device, e.g., in a buddy list or message, and a POSITA would have been motivated to implement the first mobile wireless device to display such information to inform a user of the first device of the presence status of the second device and its availability to receive IMs. APPLE-1052, [0012] (“display presence information”), FIGs. 3, 6A-6B); APPLE-1010, 8:52-54

(“Presence status indicates online status (e.g., offline, online and busy, online and available, etc.) for the destination user.”); APPLE-1019, page 9, lines 30-31 (“the client device can receive an automatic update of presence information from other client devices and/or a server”); APPLE-1020, 1:40-45 (“An instant messaging server keeps track of the online status of each of its subscribed users (often referred to as presence information), and when someone from a user’s buddy list is online, the service alerts that user and enables immediate contact with the other user.”); APPLE-1016, [0015] (“a wireless communication network 100 including a mobile switching center (MSC) 102”), [0025] (“The MSC 102 includes...an SMS connection and transmission module 208.”), [0026] (“The SMS connection and transmission module 208 examines the user profile 108 to determine the user selections for handling of SMS transmissions and to determine the conditions that prevail with respect to the telephone 104B. A”).

Elements [15pre], [15b]-[15f]

95. *Supra*, [1pre], [1b]-[1f].

Element [15a]: receiving a first message, by a first mobile wireless device from a second mobile wireless device, via a mobile operator base station, wherein the first message is formatted according to a multimedia message service (MMS) format;

96. The Horvath-Tsampalis-Chatterjee combination renders obvious [15a]. As discussed above, Horvath’s wireless device receives can receive messages on a packet data network. *Supra*, [1a]. Horvath also explains that the messages

delivered over the packet data network can be formatted according to an MMS format. APPLE-1004, [0025], [0039]. As also explained above, Horvath teaches and renders obvious receipt of messages including MMS messages over a packet data network on a cellular network *via a mobile operator base station*. *Supra* [1a]; APPLE-1004, [0024]-[0027], *see also id.*, [0002]; APPLE-1005, [0002]-[0003], [0024], [0026] (Tsampalis further describing receipt of MMS messages by a mobile wireless device).

Element [15g]: wherein the first message is received prior to the subscribing.

97. A POSITA would have found it obvious that the first message formatted as an MMS message would be received prior to the subscribing for the same reasons as the first message formatted as an SMS message being received before the subscribing as described above with respect to [1g]. *Supra*, [1g]. Indeed, the first mobile wireless device would be capable of receiving an MMS message at any time, including before the subscribing, just as an SMS message.

Claim [22]: The method of claim 15, further comprising: transmitting, via hypertext transfer protocol, after a change of the first mobile wireless device to a new handset, information indicating that subscribers of the service should no longer be formatting messages of the service for the first mobile wireless device.

98. The Horvath-Tsampalis-Chatterjee combination renders obvious Claim 22 for the reasons described with respect to Claim 4. *Supra*, Claim 4. Additionally, a POSITA would have found it obvious to transmit the message to de/unregister the phone number of the first device from the IMS (*information*

indicating that subscribers of the service should no longer be formatting messages of the service for the first mobile wireless device) via hypertext transfer protocol (HTTP) because the IMS operates on the Internet, where HTTP is used for request/response interactions between clients and servers, and on a SIP network that uses HTTP-based protocols. APPLE-1053, §7 (“much of SIP’s message and header field syntax is identical to HTTP/1.1”).

Elements [24pre], [24b]-[24f]:

99. *Supra*, [1pre]⁸, [1b]-[1f].

Element [24a]: receiving a first message, from a second mobile wireless device, via a mobile operator base station, wherein the first message is formatted according to a multimedia message service (MMS) format;

100. *Supra*, [15a].

Element [24g]: wherein the first message is received prior to the subscribing.

101. *Supra*, [15g].

Claim [26]: The method of claim 24, wherein at the time of transmitting the request, the first mobile wireless device does not have in memory a user name or email address associated with the second mobile wireless device.

102. The Horvath-Tsampalis-Chatterjee combination renders obvious Claim 26. *Supra* Claim 10.

⁸ This Declaration addresses in the analysis of all corresponding limitations of claim 1 how those limitations are rendered obvious even when performed by the first mobile wireless device, as recited in the preamble of claim 24.

Claim [27]: The method of claim 24, further comprising: registering a user name or email address with the service.

103. The Horvath-Tsampalis-Chatterjee combination renders obvious Claim 27. For example, Horvath discloses that “the wireless device 106 registers with the IMS network,” and that the registered information can include “a telephone uniform resource identifier (‘tel-URI’) and/or a SIP uniform resource identifier (‘SIP-URI’). APPLE-1004, [0034]-[0035]. Chatterjee further discloses that each user of the service is associated with a user name, and the user names can be in the form of an e-mail address. APPLE-1007, 7-8 (“Alice@foobar.com,” “Bob@foobar.com”) Box 1, Box 2. A POSITA would have understood or at least found obvious that the user names or email addresses for the IM service would be registered with the service to permit later authentication or recognition of particular users, e.g., by maintaining the user names or email addresses in a home subscriber server or similar database of registered information. APPLE-1004, [0035] (“HSS 210 comprises a database ...”); APPLE-1007, 7 (“Each of these SIMPLE components registers with the SIMPLE provider to send and receive messages” over the IM servers.).

Claim [28]: The method of claim 24, further comprising: receiving an indication that the mobile phone number of the second mobile wireless device is authenticated to the service.

104. The Horvath-Tsampalis-Chatterjee combination renders obvious Claim 28. When the second receiving mobile device is capable of receiving IMs,

the second device would be authenticated on the IM service. For example, Chatterjee explains that in the SIMPLE IM service, “[e]ach of the[] SIMPLE components registers with the SIMPLE provider to send and receive messages.” APPLE-1007, 7. Horvath further teaches that an IMS core that implements an IM service includes a P-CSCF 206 that “authenticates” wireless devices to the network. APPLE-1004, [0036], [0072]; *see also id.*, [0033] (“The SIP network is used for establishing instant messaging[] ...”), FIG. 5 (508). Because a mobile device first authenticates to access applications and services (e.g., instant messaging) on the network as taught in Horvath, an indication received by the first mobile wireless device that the second mobile wireless device is on the IM service would indicate that the second device is authenticated to the service. For example, as Chatterjee teaches, a presence watcher on a first mobile wireless device can receive an indication from a presence agent that a second device is currently active/available to receive IMs. APPLE-1007, p. 7, FIGS. 1-2. The received active/available presence information indicates that the second device is active/available, which means that the second device has authenticated with the service. *Id.*

Claim [29]: The method of claim 24, further comprising: transmitting, by the first mobile wireless device, an indication that a user of the first mobile wireless device has changed a handset.

105. The Horvath-Tsampalis-Chatterjee combination renders obvious Claim 29. *Supra*, Claims 4, 22.

IX. GROUND 1B: CLAIMS 6, 8, 17-18, 21, 23, 25 ARE OBVIOUS IN VIEW OF THE HORVATH-TSAMPALIS-CHATTERJEE-KANSAL COMBINATION

A. Combining Horvath, Tsampalis and Chatterjee with Kansal

106. As discussed above, the Horvath-Tsampalis-Chatterjee combination provides a wireless mobile device capable of messaging using different messaging services including, SMS, MMS, and IM. *Supra*, §VIII.A-B. It would have been obvious to apply Kansal's suggestion for a messaging UI to display messages formatted according to these different formats within a single application UI. In fact, multiple reasons would have prompted a POSITA to implement this combination.

107. **First**, a POSITA would have been motivated to apply Kansal's suggested user interface to the wireless device in the resulting combination to improve the user's experience with mobile messaging services involving messages of different types (e.g., SMS, MMS, IM). This would have predictably achieved Kansal's stated goals to meet the "need for an improved apparatus and methods for providing enhanced mobile messaging services. APPLE-1042, [0002]. For example, correlating messages in a manner that allows a user to view all messages of various types with a particular user at a glance in a single thread would be advantageous in allowing a user to see all messages sent to particular recipients or received from particular senders within a single interface without needing to

navigate to different messaging applications or interfaces for each different message type. APPLE-1042, [0009]; [0045]-[0046]; [0054]-[0056]; [0062]-[0064]; [0070]; [0077]-[0078]. FIGs. 2-3.

108. **Second**, providing a single thread of messages would have predictably improved the user interface by providing additional contextual information for a user of the wireless device. For example, Kansal explains that the thread can be “sorted in various ways such as by time of receipt.” APPLE-1042, [0049]; *see* FIGs. 2-3. In addition to improving the user experience (as described in the first reason), Kansal’s UI suggestions would provide additional contextual information that would otherwise not be readily conveyed. For example, as shown in FIG. 3 of Kansal, the chronologically ordered communication events (e.g., missed call at 218 and urgent email request at 216) would beneficially provide additional context for the later received text message (e.g., at 214). APPLE-1042, FIG. 3. As another example, the same user interface in FIG. 3 includes a “message count 208” indicating the number of messages and unread items across services. APPLE-1042, [0048]. A POSITA would have sought to implement Kansal’s user interface to provide this additional contextual information to a user.

109. **Third**, Kansal’s techniques are fully compatible with the types of messaging formats disclosed in each of Horvath, Tsampalis, and Chatterjee (e.g., SMS, MMS, IM), and these formats are expressly identified in Kansal as services

that can be integrated within its messaging interface. *See supra* §§VII.A-B, D VIII.A-B. Applying Kansal’s suggestion for a unified messaging interface for each of these services in the context of references with the same services to obtain a substantially similar result would have been obvious. Moreover, Kansal is analogous art to both the ’450 Patent and Horvath, Tsampalis, and Chatterjee, especially as each are in the same field of endeavor and reasonably pertinent to the problems said to be addressed by the ’450 Patent (e.g., mobile messaging). A POSITA would have reasonably expected success implementing the combination as the messaging and communication protocols involved were all well known before the Critical Date.

B. Analysis with Respect to Claims 6, 8, 17-18, 21, 23, 25

Claim [6]: The method of claim 1, further comprising: displaying, by the first mobile wireless device, in a single interface, the second message and an MMS message.

110. The Horvath-Tsampalis-Chatterjee-Kansal combination renders obvious Claim 6. As discussed above, the combination implements Kansal’s messaging user interface, which displays a message thread of various types including “MMS messages” and “IM messages” within a single interface at the mobile wireless device. APPLE-1042, [0046]; *see also id.*, [0009]; [0045]-[0046]; [0054]-[0056]; [0062]-[0064]; [0070]; [0077]-[0078]. FIGs. 2, 3 (shown below). For example, the message thread 304 “includes a message 326 comprising a sent

IM message” (*second message*) and other types of messages that can include “MMS messages” as well. APPLE-1042, [0062]-[0064], [0046].

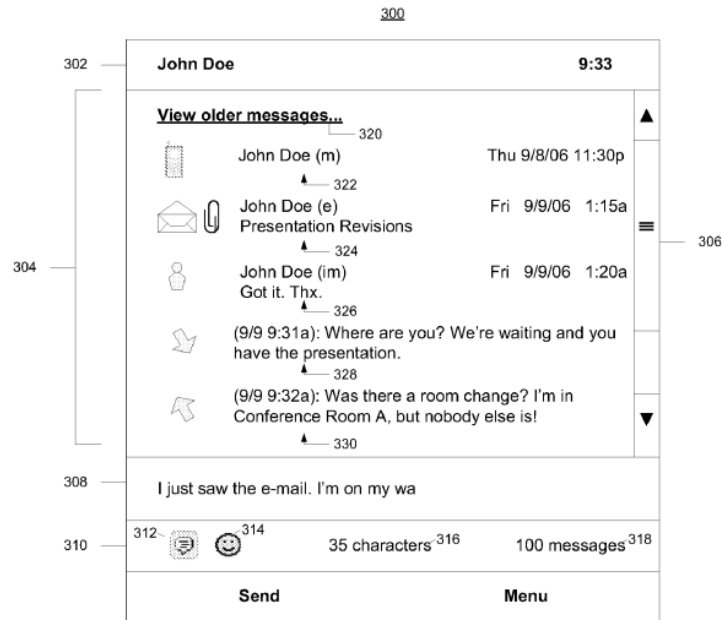


FIG. 3

APPLE-1042, FIG. 3

Claim [8]: *The method of claim 6, wherein the single interface provides an option to add, to a message, a voice attachment for subsequent playback by the second mobile wireless device, after the subscribing; wherein the single interface does not provide the option to add, to a message, a voice attachment for subsequent playback by the second mobile wireless device, before the subscribing.*

111. The Horvath-Tsampalis-Chatterjee-Kansal combination renders obvious Claim 6. For example, the combination incorporates Horvath’s and Chatterjee’s teachings for implementing an instant messaging service. *Supra* §§VII.A, C, VIII.A-B. Chatterjee explains that the IM service “is more media-rich” because it can be used to deliver “deliver voice, video, and data together.”

APPLE-1007, 8, 11 (“integrated voice, video, and data services in IM systems.”). These teachings are supplemented by Kansal’s express disclosure for including a selectable menu item to “Record Sound” as an option to add a voice recording attachment to a message. APPLE-1042, [0073], FIG. 5; *see also id.*, [0074]-[0078] (“add media”), [0060], FIG. 3 (314). Like Chatterjee, Kansal explains that this message (e.g., the message with the voice recording attachment) can be an IM message. APPLE-1042, [0078] (“the user may compose a message in one format (e.g., SMS) and then convert or send the message in another format (e.g., MMS, e-mail, IM, etc.)”); *see also id.* [0045] (“the messaging UI used to display the message thread generally may be supported by a particular messaging application such as ... IM application 135”). [0064] (“using various types of messages”); [0071] (“the embodiments, however, are not limited in [the SMS] context.”). Tsamaplis also recognized that some messaging formats are capable of handling multimedia attachments while others are not, and that “any attached/inserted multimedia files” to be sent as an SMS message “will be lost.” APPLE-1005, [0062].

112. Kansal explains that “the messaging UI 500 may automatically or seamless convert” between messaging formats based on whether a user has attached a media file to the message. APPLE-1042, [0077]-[0078]. However, Kansal’s ability to seamlessly convert messaging formats assumes that the user

currently subscribes to a messaging service having a messaging format capable of handling multimedia attachments (e.g., MMS, IM). Before the user subscribes to the IM service, if the user were only subscribed to SMS, the voice recording or other media file could not be attached to an SMS message. APPLE-1005, [0062]; APPLE-1042, [0077]. In this context, it would have been obvious not to provide the option to add to the SMS message a voice attachment (Sound Recording) before the user subscribes to the IM service or other service capable of handling media attachments. For example, Tsampalis describes the option of removing a media file from a composed/active message before it is sent as an SMS, but a POSITA would have recognized that the options of (i) permitting the attachment of a media file (e.g., voice attachment) during message composition that would be removed before sending (e.g., sending as an SMS message), or (ii) preventing the attachment of a media file during message composition in the first instance would be a matter of obvious design choice. For example, a POSITA would have chosen the latter option in at least some cases to provide an earlier indication to the user that the message will not be able to be sent with a voice attachment. A POSITA would have desired to restrict attachments during message composition if either the sender or receiver had limited messaging capabilities since the attachments could not be delivered in either case. Thus, it would have been obvious to provide the option of adding a voice attachment after subscribing to the IM service, and not

to provide that option before the subscribing. In fact, imposing restrictions/constraints on message attachments was well known before the Critical Date. APPLE-1054, [0011] (“attachment constraints can be specified”), [0022]-[0025].

Claim [17]: The method of claim 15, further comprising: retrieving information representative of at least one electronic mail (email) address corresponding to a third mobile wireless device; wherein the third mobile wireless device is a wireless device of a third subscriber of the service.

113. The Horvath-Tsampalis-Chatterjee-Kansal combination renders obvious Claim 17. For example, Kansal discloses a “contact database 142” that stores contact records for wireless devices (e.g., including a contact record associated with a “*third mobile wireless device.*”). APPLE-1042, [0037]-[0038]. The contact record can include “identifying information such as ... e-mail address” and “IM screen names.” *Id.* That a contact record for a single contact can include both an e-mail address and IM screen name would have indicated or at least rendered obvious to a POSITA that the contact (e.g., a third subscriber) can have an email address corresponding to a third mobile device that is also a subscriber to the IM service. *See also* APPLE-1042, [0042], [0051]; APPLE-1005, [0041], [0060]-[0064], FIGs. 5, 16.

Claim [18]: The method of claim 17, further comprising: transmitting a message to the second mobile wireless device and to the third mobile wireless device, via the service.

114. The Horvath-Tsampalis-Chatterjee-Kansal combination renders obvious Claim 18. As discussed, both the claimed “second mobile wireless device” and “third mobile wireless device” can be subscribers to the service. *Supra*, Ground 1A at [1d]-[1f], Ground 1B at Claim 17. Accordingly, it would have been obvious to transmit IM messages to both the second and third devices from the first device using an IM service like that described in Horvath, Chatterjee, and Kansal. For example, Tsampalis explicitly teaches that a message can be sent to multiple users who are subscribers to a particular service. APPLE-1005, [0061]-[0063] (“multiple remote recipients”), FIG. 16; *see also* APPLE-1007, 4, 8.

Elements [21pre]-[21a]: The method of claim 15, further comprising: receiving, in a single interface, the second message and an SMS message;

115. The Horvath-Tsampalis-Chatterjee-Kansal combination renders obvious [21pre]-[21a] for similar reasons to those described above with respect to Claim 6. *Supra*, Claim 6. As discussed above, the combination implements Kansal’s messaging user interface, which displays a message thread of various types including “SMS messages” and “IM messages” (*i.e.*, the claimed “second message”) within a single interface at the mobile wireless device. APPLE-1042, [0046]; *see also id.*, [0009]; [0045]-[0046]; [0054]-[0056]; [0062]-[0064]; [0070]; [0077]-[0078]. FIGs. 2-3.

Element [21b]; wherein the single interface provides an option to add a voice attachment for subsequent playback by the second mobile wireless device, after the subscribing.

116. The Horvath-Tsampalis-Chatterjee combination renders obvious Element [21b] for the reasons described above with respect to Claim 8. *Supra*, Claim 8.

Claim [23]: The method of claim 21, further comprising: displaying an option to add one or more attachments, based at least in part on the response.

117. The Horvath-Tsampalis-Chatterjee-Kansal combination provides the additional features recited in Claim 23 for the same reasons described above with respect to Claim 8 that it would have been obvious to display an option to add attachments (e.g., a voice attachment). *Supra*, Claim 8, [1d]. For example, it would have been obvious to restrict the ability to add attachments to a message if the response indicates that the intended recipient of the message has limited messaging capabilities and cannot receive message formats (e.g., IM) that support attachments. APPLE-1005, [0062] (attachments “will be lost”); APPLE-1042, [0077]-[0078].

Elements [25pre]-[25a]: The method of claim 24, further comprising: formatting the second message for transmission over a wireless local area network (WLAN);

118. *Supra*, Claim 3.

Elements [25b]-[25c]: and displaying an option to add, to a message being created, a voice attachment for subsequent playback by the second mobile wireless device, after the subscribing; wherein the option is not displayed before the subscribing.

119. *Supra*, Claim 8.

X. GROUND 1C: CLAIMS 2, 16 ARE OBVIOUS IN VIEW OF THE HORVATH-TSAMPALIS-CHATTERJEE-RIBAUDO COMBINATION

A. Combining Horvath, Tsampalis and Chatterjee with Ribaudo

120. As discussed above, the Horvath-Tsampalis- Chatterjee combination provides a wireless mobile device with various messaging services including, SMS, MMS, and IM. *Supra*, §§VIII.A-B. It would have been obvious to further integrate in the combination Ribaudo’s teaching for transmitting IM messages directly over Bluetooth when the first device and second device are in sufficient proximity of each other. In fact, multiple reasons would have prompted a POSITA to implement this combination.

121. **First**, a POSITA would have been motivated to incorporate Ribaudo’s teachings teaching for transmitting IM messages over Bluetooth because doing so would beneficially reduce the load and unnecessary overhead on the packet switched network by diverting IM messages from the packet switched network when the devices are in proximity to establish a Bluetooth connection. APPLE-1004, [0004], [0009]. A POSITA would have been led to this motivation by analogous disclosure in Horvath which explains that Horvath’s system beneficially reduces load and “unnecessary overhead” on the circuit switched network by diverting SMS messages from the circuit switched network to the packet data. . For

a similar benefit, a POSITA would have been motivated to apply Ribaudo's technique in order to predictably reduce the load on the packet switched network.

122. **Second**, a POSITA would have been motivated to incorporate Ribaudo's teachings for transmitting IM messages over Bluetooth to beneficially provide messaging capability for wireless devices in situations where the devices are unable to access a cellular and/or Wi-Fi/WLAN network. Moreover, because Bluetooth provides a direct P2P connection, it often facilitates higher data transmission speeds and lower latency than transmission over remote networks.

123. **Third**, Chatterjee describes instant messaging services using the same well known XMPP protocol that Ribaudo implements for establishing a proximity based instant messaging connection. *See supra* §§VII.C, E.

124. **Fourth**, applying Ribaudo technique involving the same IM protocol disclosed in Chatterjee's to achieve nothing more than predictable results would have been obvious. Moreover, Ribaudio is analogous art to both the '450 Patent and Horvath, Tsampalis, and Chatterjee, especially as each are in the same field of endeavor and reasonably pertinent to the problems said to be addressed by the '450 Patent (e.g., mobile messaging). A POSITA would have reasonably expected success implementing the combination as the messaging and communication protocols involved were all well known before the Critical Date.

B. Analysis with Respect to Claims 2, 16

Claim [2]: The method of claim 1, further comprising: formatting the second message for transmission over a wireless personal area network (WPAN).

Claim [16]: The method of claim 15, further comprising: formatting the second message is for transmission over a wireless personal area network (WPAN).

125. The Horvath-Tsampalis-Chatterjee-Ribaudo combination renders obvious Claims 2, 16. For example, as discussed above, the combination integrates Ribaudo's teachings for providing instant messaging between devices over a "BLUETOOTH" connection. APPLE-1044, [0079]; *see supra* §§VII.E, X.A. This includes formatting the instant message (*i.e.*, the claimed "second message") for transmission over Bluetooth (*i.e.*, the claimed "wireless personal area network (WPAN)"). *Id. see also id.* [0066].

XI. GROUND 1D: CLAIM 5 IS OBVIOUS IN VIEW OF THE HORVATH-TSAMPALIS-CHATTERJEE-BENYOSEPH COMBINATION

A. Combining Horvath, Tsampalis and Chatterjee with BenYoseph

126. It would have been obvious to further modify the Horvath-Tsampalis-Chatterjee combination as described in Ground 1A by integrating BenYoseph's suggested policies that forbid a sender from sending more than a predetermined amount of messages returned as undeliverable and that require a sender to accept more than a predetermined amount of undeliverable messages. *Supra*, §§VIII.A-B, VII.F. Multiple reasons would have prompted a POSITA to implement this combination.

127. **First**, a POSITA would have implemented BenYoseph's suggested techniques in the combination to permit a sending device to send bulk messages while ensuring that the sender acts responsibly and does not overload the system with undeliverable messages. APPLE-1049, 14:44-53 ("does not overload").

128. **Second**, a POSITA would have implemented BenYoseph's suggested techniques in the combination to provide a framework by which messages from a compliant sending device can be differentiated from messages from non-compliant senders or from messages of a different type (e.g., non-bulk messages). APPLE-1049, 4:31-6:9.

129. **Third**, applying BenYoseph's suggested techniques in the combination would have achieved merely predictable results and would have been obvious. Like the Horvath-Tsampalis-Chatterjee system described in Ground 1A, BenYoseph's techniques are specifically applicable to instant messaging, confirming that the techniques are entirely compatible. APPLE-1049, 5:65-6:9. BenYoseph is also analogous art to both the '450 Patent and Horvath, Tsampalis, and Chatterjee, especially as each are in the same field of endeavor and reasonably pertinent to the problems said to be addressed by the '450 Patent (e.g., mobile messaging). A POSITA would have reasonably expected success implementing the combination as the messaging and communication protocols involved were all well known before the Critical Date.

B. Analysis with Respect to Claim 5

Claim [5]: The method of claim 1, wherein the formatting the second message is further based at least in part upon a status indicating that an undelivered message parameter has not been exceeded.

130. BenYoseph teaches policies that forbid a sender from sending more than a predetermined amount of instant messages returned as undeliverable and that require a sender to accept more than a predetermined amount of undeliverable instant messages. APPLE-1049, 2:15-58, 5:65-6:9, 7:47-58, 11:15-33, 32:14-40. As applied in the combination, the first mobile device predictably formats the second message as an instant message based at least in part on an indication that it is compliant with BenYoseph's undeliverable message policies (*a status indicating that an undelivered message parameter has not been exceeded*). *Supra*, §§VII.F, XI.A.

XII. GROUND 1E: CLAIMS 14, 19-20, 30 ARE OBVIOUS IN VIEW OF THE HORVATH-TSAMPALIS-CHATTERJEE-LIN COMBINATION

A. Combining Horvath, Tsampalis and Chatterjee with Lin

131. It would have been obvious to further modify the Horvath-Tsampalis-Chatterjee combination as described in Ground 1A by integrating Lin's suggested techniques for establishing real-time instant messaging sessions between mobile devices by sending SMS messages to invite participants to join the IM session and by sending an SMS message to authenticate with an IM server. *Supra*, §§VIII.A-B,

VII.G. Multiple reasons would have prompted a POSITA to implement this combination.

132. **First**, a POSITA would have implemented Lin's suggested techniques in the combination to provide a convenient method for mobile devices to readily initiate and join instant messaging sessions—even when the users are not all initially logged into a same IM service. APPLE-1045, [0003], [0006].

133. **Second**, a POSITA would have implemented Lin's suggested techniques in the combination because Lin explains that its server-based architecture for mobile IM is more efficient than P2P architectures for more than two devices, while also allowing mobile devices to join the IM session from outside a private network. APPLE-1045,[0005]-[0006].

134. **Third**, a POSITA would have implemented Lin's suggested techniques in the combination because it would allow a mobile device initiating an IM session to securely authenticate with a server as a moderator using a commonly available messaging format (SMS), thereby improving security and convenience. APPLE-1045, [0017].

135. **Fourth**, applying Lin's suggested techniques in the combination would have achieved merely predictable results and would have been obvious. Like the Horvath-Tsampalis-Chatterjee system described in Ground 1A, Lin's techniques are specifically applicable to instant messaging and would have been

entirely compatible. APPLE-1045, Abstract, [0006]. Lin is also analogous art to both the '450 Patent and Horvath, Tsampalis, and Chatterjee, especially as each are in the same field of endeavor and reasonably pertinent to the problems said to be addressed by the '450 Patent (e.g., mobile messaging). A POSITA would have reasonably expected success implementing the combination as the messaging and communication protocols involved were all well known before the Critical Date.

B. Analysis with Respect to Claims 14, 19-20, 30

Claim [14]: The method of claim 9, further comprising: receiving an over the air (OTA) configuration message, wherein the OTA configuration message includes at least one parameter for establishing a server connection with a server of the service.

136. The Horvath-Tsampalis-Chatterjee-Lin combination renders obvious Claim 14. For example, based on Lin's teachings, to initiate or join an IM session, the first mobile wireless device receives "through an offline process (e.g., email, phone call, letter, etc.), ... a phone number associated with the server (e.g., a toll-free number), a personal conference number, and a PIN." APPLE-1045, [0018]-[0019], FIG. 4. The server's phone number is a "unique identification number ... that may be used by the mobile devices to contact the server through the page-mode messaging service (e.g., SMS)." *Id.*, [0018]. When the first mobile device receives the server's unique identification number by a phone call or other over-the-air (OTA) process (e.g., SMS, mobile email), it receives an OTA configuration message that includes at least one parameter (e.g., the unique identification number

of the server) for establishing a server connection with a server of the IM service.

Id.

Claim [19]: The method of claim 15, further comprising: transmitting, by the first mobile wireless device, a short message service (SMS) message for authentication to the service.

Claim [20]: The method of claim 15, wherein the first mobile wireless device is authenticated to the service via SMS.

Claim [30]: The method of claim 24, wherein the subscribing includes transmitting an SMS message for authentication to the service.

137. The Horvath-Tsampalis-Chatterjee-Lin combination renders obvious Claims 19, 20, and 30. For example, as applied in the combination, Lin discloses a first mobile wireless device that initiates an instant messaging session by performing operations that include transmitting an SMS message for authentication to the IM service such that the first mobile wireless device is authenticated to the IM service via SMS. APPLE-1045, [0017] (“The initiating mobile device [] transmits its IP address, including its TCP port number, the user's personal conference number and the user's PIN (to *authenticate* the user as the moderator) in an SMS text message to [a] telephone number of [a] server 420.”; *see also id.*, Abstract, [0014]-[0016], FIG. 4; *supra*, §§VII.G, XII.A; APPLE-1004, FIG. 5 (“S-CSCF authenticates and registers the wireless device” at step 508), [0035], [0036], [0040].

XIII. CONCLUSION

138. For all the reasons I have noted in the foregoing paragraphs, claims 1-30 of the '450 Patent are obvious in view of the references discussed above.

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

APPENDIX A

Patrick Gerard Traynor

Professor

Associate Chair for Research in CISE

John and Mary Lou Dasburgh Preeminent Chair in Engineering

Department of Computer & Information Science & Engineering (CISE)

University of Florida

1889 Museum Rd,

Gainesville, FL 32611 USA

`traynor@cise.ufl.edu`

`http://www.cise.ufl.edu/~traynor`

Table of Contents

| | |
|--|-----------|
| EDUCATIONAL BACKGROUND | 4 |
| EMPLOYMENT HISTORY | 4 |
| CURRENT FIELDS OF INTEREST | 4 |
| I. TEACHING | 6 |
| A. Courses Taught | 6 |
| B. Continuing Education | 6 |
| C. Curriculum Development | 6 |
| D. Individual Student Guidance | 7 |
| E. Teaching Honors and Awards | 12 |
| II. RESEARCH AND CREATIVE SCHOLARSHIP | 13 |
| A. Thesis | 13 |
| B. Published Journal Papers (Refereed) | 13 |
| C. Published Books and Parts of Books | 15 |
| D. Edited Proceedings | 15 |
| E. Conference Presentations | 15 |
| E.1. Conference Papers with Proceedings (Refereed) | 15 |
| E.2. Conference Presentations with Proceedings (Non-Refereed) | 22 |
| E.3. Conference Presentations without Proceedings | 22 |
| F. Other | 22 |
| F.1. Submitted Journal Papers | 22 |
| F.2. Refereed Research Reports | 23 |
| F.3. Software | 23 |
| F.4. Published Papers (Non-Refereed) | 23 |
| F.5. Books in Preparation | 23 |
| F.6. Workshops and External Courses | 23 |
| G. Research Proposals and Grants (Principal Investigator) | 24 |
| H. Research Proposals and Grants (Contributor) | 26 |
| I. Research Honors and Awards | 28 |
| III. SERVICE | 29 |
| A. Professional Activities | 29 |
| A.1. Memberships and Activities in Professional Societies | 29 |
| A.2. Conference Committee Activities | 29 |
| B. On-Campus Committees | 30 |
| B.1. University of Florida | 30 |
| B.2. Georgia Tech | 31 |
| C. Special Assignments | 31 |
| D. Ph.D. Examining Committees | 31 |
| E. External Member of M.S. Examining Committee | 35 |
| F. Consulting and Advisory Appointments | 35 |
| G. Civic Activities | 35 |
| IV. NATIONAL AND INTERNATIONAL PROFESSIONAL RECOGNITION | 36 |
| A. Honors and Awards | 36 |
| B. Invited Conference Session Chairmanships | 36 |
| C. Professional Registration | 36 |
| D. Patents | 36 |
| E. Editorial and Reviewer Work for Technical Journals and Publishers | 37 |
| F. Expert Witness Services | 39 |
| V. OTHER CONTRIBUTIONS | 41 |
| A. Seminar Presentations (Invited Papers and Talks at Meetings and Symposia) | 41 |

B. Special Activities 45

EDUCATIONAL BACKGROUND

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

EMPLOYMENT HISTORY

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

CURRENT FIELDS OF INTEREST

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

Recognizing this, my research focuses on three specific themes: (1) developing efficient techniques to allow telephony providers and customers to authenticate the origin of incoming calls; (2) measuring and improving the security of emerging mobile financial systems and (3) efficient and strong privacy-preserving

techniques for mobile devices. Additionally, I have significant expertise in fraud detection, particularly for payment systems.

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

I. TEACHING

A. Courses Taught

| Semester/Year | Course Number & Title | Number of Students | Comments |
|---------------|---|--------------------|-------------------|
| Fall 2024 | CNT 4007 Computer Networks 1 | 310 | Revamped Course |
| Fall 2023 | CIS 6930 Cellular and Mobile Network Security | 19 | New Topics |
| Fall 2022 | CNT 5410 Computer and Network Security | 75 | New Topics |
| Fall 2021 | CNT 5410 Computer and Network Security | 45 | New Topics |
| Fall 2019 | CNT 5410 Computer and Network Security | 28 | New Topics |
| Fall 2018 | CIS 6930 Cellular and Mobile Network Security | 16 | New Course |
| Fall 2017 | CNT 5410 Computer and Network Security | 27 | New Topics |
| Fall 2016 | CNT 5410 Computer and Network Security | 60 | New Topics |
| Spring 2016 | CNT 5410 Computer and Network Security | 13 | New Topics |
| Spring 2015 | CNT 5410 Computer and Network Security | 12 | New Topics |
| Fall 2014 | CNT 5410 Computer and Network Security | 30 | New Course |
| Spring 2014 | CS 6262 Network Security | 55 | New Projects |
| Fall 2013 | CS 3251 Computer Networks I | 73 | Expanded Syllabus |
| Spring 2013 | CS 6262 Network Security | 65 | All New Projects |
| | CS 8001 Information Security Seminar | 20 | New Speakers |
| Fall 2012 | CS 8803 Cellular & Mobile Network Security | 17 | New Topics |
| | CS 8001 Information Security Seminar | 20 | New Speakers |
| Spring 2011 | CS 8001 Information Security Seminar | 20 | New Speakers |
| Fall 2011 | CS 6262 Network Security | 27 | Expanded Syllabus |
| | CS 8001 Information Security Seminar | 35 | New Speakers |
| Spring 2011 | CS 3251 Computer Networks I | 61 | Expanded Syllabus |
| | CS 8001 Information Security Seminar | 20 | New Speakers |
| Fall 2010 | CS 8803/4803 Cellular & Mobile Network Security | 16 | New Course |
| | CS 8001 Information Security Seminar | 31 | New Speakers |
| Fall 2009 | CS 6262 Network Security | 55 | Expanded Syllabus |
| Spring 2009 | CS 3251 Computer Networks I | 45 | Expanded Syllabus |
| Fall 2008 | CS 8003 Destructive Research | 10 | New Course |

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

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

B. Continuing Education

None.

C. Curriculum Development

University of Florida

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

CIS 6930 Cellular and Mobile Network Security: *Fall 2018, 2023.* Developed an entirely new course around security issues facing cellular and mobile networks. Students learned about wireless basics, spectrum issues, core network architectures (GSM, ISDN, IMS, SIP), air interfaces (2G-5G), mobility management, authentication, mobile phone operating systems (Android, iPhone), Android security, congestion and denial of service, privacy and eavesdropping. Students also complete a research project and aim towards publishing this work at a major venue. My aim is for this class to become part of the regular offering of security courses. Semester projects were also judged and encouraged using a “venture capital” model, in which students had to pretend as if they were pitching their ideas for a start-up company to potential investors.

CNT 5410 Computer and Network Security: *Fall 2014-2022.* Totally rewrote the syllabus and slide material, giving the class its first major overhaul in a number of years. While many old themes remain, new lecture blocks including Web Security, Cellular Security and Social Engineering were developed from scratch. This new course material was made available to all other faculty members teaching this class, who have since used my slides and syllabus.

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

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

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

D. Individual Student Guidance

1. Research Scientists Supervised

None.

2. Ph.D. Students Graduated

Hadi Abdullah University of Florida

Fall 2016–Summer 2022

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

Chaitrali Amrutkar Georgia Institute of Technology

Fall 2009–Fall 2013

Her research discovered vulnerabilities in mobile web browsers and developed techniques to detect malicious mobile web pages. Joined Oracle in Spring 2014.

- Logan Blue** University of Florida
Fall 2016–Summer 2022
Investigated biological feature reconstruction from voice recordings. Now: Research Scientist at Harbor Labs
- Jasmine Bowers** University of Florida
Fall 2015–Summer 2020
Her research focuses on mobile applications, and the development of tools for building secure systems. Now: Research Scientist, MITRE
- Henry “Hank” Carter** Georgia Institute of Technology
Fall 2010–Spring 2016
Developing techniques for secure function evaluation for privacy-preserving applications on constrained mobile devices. Now: Assistant Professor, Villanova University
- Italo Dacosta** Georgia Institute of Technology
Fall 2008–Summer 2012
Co-advised with Mustaque Ahamad. Research on scaling performance of SIP network components. Graduated Summer 2012, currently research scientist at EPFL.
- David Dewey** Georgia Institute of Technology
Fall 2011–Summer 2015
Investigated compiler techniques to remove software vulnerabilities from code. Now CTO of MailChimp.
- Cassidy Gibson** University of Florida
Fall 2019–Spring 2025
Investigated compiler techniques to remove software vulnerabilities from code. Now CTO of MailChimp.
- Christian Peeters** University of Florida
Fall 2016–Summer 2022
Develop techniques to detect and defend against call and message interception attacks in cellular networks. Now: Research Scientist at Harbor Labs
- Brad Reaves** University of Florida
Fall 2014–Spring 2017
Develop strong authentication techniques for cellular networks. Now: Assistant Professor at North Carolina State University.
- Nolen Scaife** University of Florida
Fall 2014–Spring 2019
Developed techniques to detect credit card skimming. First: Assistant Professor at the University of Colorado Boulder. Now: Director, Global Cyber Intelligence at Walmart
- Imani Sherman** University of Florida
Fall 2018–Summer 2021
Developing usable interfaces against robocalls. Co-advised with Juan Gilbert. Now: Assistant Professor at the University of California, San Diego
- Luis Vargas** University of Florida
Fall 2016–Summer 2021
Developing techniques for network-based detection and mitigation of malware in a healthcare environment. Now: Data Scientist at the Alethia Group

2. Ph.D. Students Supervised

Nathaniel Bennett University of Florida

Fall 2022–Present

Finding vulnerabilities in cellular core networks via fuzzing.

Seth Layton University of Florida

Fall 2020–Present

Detecting deepfakes in audio samples.

Allison Lu University of Florida

Fall 2022–Present

Measuring repeatability in computer security.

Daniel Olszewski University of Florida

Fall 2019–Present

Removing unwanted/insecure features from software.

Tyler Tucker University of Florida

Fall 2021–Present

Evaluating the security of Bluetooth/cellular radios.

Kevin Warren University of Florida

Fall 2019–Present

Detecting deepfake audio through linguistic information.

3. Ph.D. Students - Other

Saurabh Chakradeo Georgia Institute of Technology

Fall 2010–Spring 2013

Research exploring malicious mobile applications. Left to join Facebook.

Brendan Dolan-Gavitt Georgia Institute of Technology

Spring 2009

Research project on using kernel type graphs to detect dummy structures.

Ryon Kennedy University of Florida

Fall 2020–Spring 2023

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

Eric (Yu) Liu Georgia Institute of Technology

Fall 2008

Research on the spread of malware through cellular infrastructure.

Chaz Lever Georgia Institute of Technology

Fall 2011–Spring 2014

Developing techniques to measure the spread of malware in cellular networks. Left Georgia Tech to create a startup.

Frank Park Georgia Institute of Technology

Fall 2008–Spring 2010

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

Ferdinand Schober Georgia Institute of Technology

Fall 2009–Summer 2010

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

4. M.S. Students Supervised

Chaitrali Amrutkar Georgia Institute of Technology

Fall 2008–Spring 2009

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

Logan Blue University of Florida

Fall 2015–Spring 2016

Investigated problems of cellular and network security.

David Dewey Georgia Institute of Technology

Fall 2009–Spring 2010

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

Christopher Grayson Georgia Institute of Technology

Fall 2012–Fall 2013

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

Young Seuk Kim Georgia Institute of Technology

Fall 2012–Fall 2013

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

Daniel Komaromy Georgia Institute of Technology

Fall 2008–Summer 2009

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

Nigel Lawrence Georgia Institute of Technology

Fall 2011–Spring 2012

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

Philip Marquardt Georgia Institute of Technology

Fall 2009–Present

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

Rishikesh Naik Georgia Institute of Technology

Fall 2008–Spring 2010

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

Ashish Nautiyal University of Florida

Fall 2015–Spring 2016

Research on connecting telephone calls to the larger authentication infrastructure.

Nilesh Nipane Georgia Institute of Technology

Fall 2008–Spring 2010

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

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

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

5. M.S. Special Problems Students

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

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

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

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

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

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

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

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

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

6. Undergraduate Special Problems Students

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

Young Seuk Kim Georgia Institute of Technology

Fall 2011–Spring 2012

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

Dane Van Dyck Georgia Institute of Technology

Summer 2009

Research on virtualization support for mobile phones.

E. Teaching Honors and Awards

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

II. RESEARCH AND CREATIVE SCHOLARSHIP

A. Thesis

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

B. Published Journal Papers (Refereed)

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

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

C. Published Books and Parts of Books

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

D. Edited Proceedings

None.

E. Conference Presentations

E.1. Conference Papers with Proceedings (Refereed)

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

8. K. Virgil English, Nathaniel Bennett, Seaver Thorn, Kevin Butler, William Enck, and Patrick Traynor. Examining Cryptography and Randomness Failures in Open-Source Cellular Cores. In *Proceedings of the ACM Conference on Data and Application Security and Privacy (CODASPY)*, 2024. (Acceptance rate: 21.3%)(Best Paper).
9. Seth Layton, Tyler Tucker, Daniel Olszewski, Kevin Warren, Carrie Gates, Kevin Butler, and Patrick Traynor. SoK: The Good, The Bad, and The Unbalanced: Measuring Structural Limitations of Current Deepfake Datasets. In *Proceedings of the USENIX Security Symposium (Security)*, 2024. (Acceptance Rate 18.3%).
10. Imani Munyaka, Daniel Delgado, Juan Gilbert, Jaime Ruiz, and Patrick Traynor. “I used to live in Florida”: Exploring the Impact of Spam Call Warning Accuracy on Callee Decision-Making. In *Symposium on Usable Security and Privacy (USEC)*, 2024.
11. Jianliang Wu, Patrick Traynor, Dongyan Xu, Dave (Jing) Tian, and Antonio Bianchi. Finding Traceability Attacks in the Bluetooth Low Energy Specification and Its Implementations. In *Proceedings of the USENIX Security Symposium (Security)*, 2024. (Acceptance Rate 18.3%).
12. Daniel Olszewski, Allison Lu, Carson Stillman, Kevin Warren, Cole Kitroser, Alejandro Pascual, Divyajyoti Ukirde, Kevin Butler, and Patrick Traynor. “Get in Researchers; We’re Measuring Reproducibility”: A Reproducibility Study of Machine Learning Papers in Tier 1 Security Conferences. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2023. (Acceptance rate: 19.8%).
13. Christian Peeters, Tyler Tucker, Anushri Jain, Kevin Butler, and Patrick Traynor. LeopardSeal: Detecting Call Interception via Audio Rogue Base Stations. In *Proceedings of the ACM International Conference on Mobile Systems, Applications and Services (MobiSys)*, 2023. (Acceptance rate: 21%).
14. Tyler Tucker, Hunter Searle, Kevin Butler, and Patrick Traynor. Blue’s Clues: Practical Discovery of Non-Discoverable Bluetooth Devices. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2023. (Acceptance rate: 14%).
15. Hadi Abdullah, Aditya Karlekar, Saurabh Prasad, Muhammad Sajidur Rahman, Logan Blue, Luke Bauer, Vincent Bindschaedler, and Patrick Traynor. Attacks as Defenses: Designing Robust Audio CAPTCHAs Using Attacks on Automatic Speech Recognition Systems. In *Symposium on Network and Distributed System Security (NDSS)*, 2023. (Acceptance rate: 16%).
16. Daniel Olszewski, Sandeep Sathyanarayana, Weidong Zhu, Kevin Butler, and Patrick Traynor. HallMonitor: A Framework for Identifying Network Policy Violations in Software. In *IEEE Conference on Communications and Network Security (CNS)*, 2022.
17. Hadi Abdullah, Aditya Karlekar, Vincent Bindschaedler, and Patrick Traynor. Demystifying Limited Adversarial Transferability in Automatic Speech Recognition Systems. In *Proceedings of the International Conference on Learning Representations (ICLR)*, 2022. (Acceptance rate: 32%).
18. Logan Blue, Kevin Warren, Hadi Abdullah, Cassidy Gibson, Luis Vargas, Jessica O’Dell, Kevin Butler, and Patrick Traynor. Who Are You (I Really Wanna Know)? Detecting Audio DeepFakes Through Vocal Tract Reconstruction. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2022. (Acceptance rate: 17.2%).
19. Grant Hernandez, Marius Muench, Dominik Maier, Alyssa Milburn, Shinjo Park, Tobias Scharnowski, Tyler Tucker, Patrick Traynor, and Kevin R. B. Butler. FirmWire: Transparent Dynamic Analysis for Cellular Baseband Firmware. In *Symposium on Network and Distributed System Security (NDSS)*, 2022. (Acceptance rate: 16.2%).

20. Christian Peeters, Christopher Patton, Imani N. Sherman, Daniel Olszewski, Thomas Shrimpton, and Patrick Traynor. SMS OTP Security (SOS): Hardening SMS-Based Two Factor Authentication. In *ACM Asia Conference on Computer and Communications Security (ASIACCS)*, 2022. (Acceptance rate: 18.2%).
21. Hadi Abdullah, Muhammad Sajidur Rahman, Christian Peeters, Cassidy Gibson, Washington Garcia, Vincent Bindschaedler, Thomas Shrimpton, and Patrick Traynor. Beyond L_p Clipping: Equalization based Psychoacoustic Attacks against ASRs. In *The Asian Conference on Machine Learning (ACML)*, 2021.
22. Imani Sherman and Daniel Delgado and Juan Gilbert and Jaime Ruiz and Patrick Traynor. Characterizing User Comprehension in the STIR/SHAKEN Anti-Robocall Standard. In *Proceedings of the Annual Research Conference on Communications Information and Internet Policy (TPRC 49)*, 2021.
23. Hadi Abdullah, Kevin Warren, Vincent Bindschaedler, Nicolas Papernot, and Patrick Traynor. The Faults in our ASRs: An Overview of Attacks against Automatic Speech Recognition and Speaker Identification Systems. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2021. (Acceptance rate: 12.1%).
24. Hadi Abdullah, Muhammad Sajidur Rahman, Washington Garcia, Logan Blue, Kevin Warren, Anurag Swarnim Yadav, Tom Shrimpton, and Patrick Traynor. Hear “No Evil”, See “Kenansville”: Efficient and Transferable Black-Box Attacks on Speech Recognition and Voice Identification Systems. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2021. (Acceptance rate: 12.1%).
25. Imani Sherman, Jasmine Bowers, Liz-Laure Laborde, Juan E. Gilbert, Jaime Ruiz, and Patrick Traynor. Truly Visual Caller ID? An Analysis of Anti-Robocall Applications and their Accessibility to Visually Impaired Users. In *IEEE International Symposium on Technology and Society (IEEE ISTAS)*, 2020.
26. Imani Sherman, Jasmine Bowers, Keith McNamara, Juan Gilbert, Jaime Ruiz, and Patrick Traynor. Are You Going to Answer That? Measuring User Responses to Anti-Robocall Application Indicators. In *Proceedings of the ISOC Network & Distributed Systems Security Symposium (NDSS)*, 2020. (Acceptance rate: 17.4%).
27. Joseph Choi, Dave Tian, Grant Hernandez, Christopher Patton, Benjamin Mood, Thomas Shrimpton, Patrick Traynor, and Kevin Butler. A Hybrid Approach to Secure Function Evaluation Using SGX. In *Proceedings of the ACM ASIA Conference on Computer and Communications Security (ASIACCS’19)*, 2019. (Acceptance Rate: 17.0% for full papers).
28. Vanessa Frost, Dave Tian, Christie Ruales, Patrick Traynor, and Kevin Butler. Examining DES-based Cipher Suite Support within the TLS Ecosystem. In *Proceedings of the ACM ASIA Conference on Computer and Communications Security (ASIACCS’19)*, 2019. (Acceptance Rate: 22.0% for all papers).
29. Dave Tian, Joseph Choi, Grant Hernandez, Patrick Traynor, and Kevin Butler. A Practical Intel SGX Setting for Linux Containers in the Cloud. In *Proceedings of the ACM Conference on Data and Application Security and Privacy (CODASPY’19)*, 2019. (Acceptance rate: 23.5%).
30. Nolen Scaife, Jasmine Bowers, Christian Peeters, Grant Hernandez, Imani Sherman, Lisa Anthony, and Patrick Traynor. Kiss from a Rogue: Evaluating Detectability of Pay-at-the-Pump Card Skimmers. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2019. (Acceptance rate: 12.0%).
31. Jasmine Bowers, Imani Sherman, Kevin Butler, and Patrick Traynor. Characterizing Security and Privacy Practices in Emerging Digital Credit Applications. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2019. (Acceptance rate: 25.6%).

32. Hadi Abdullah, Washington Garcia, Christian Peeters, P. Traynor, K. Butler, and J. Wilson. Practical Hidden Voice Attacks against Speech and Speaker Recognition Systems. In *Proceedings of the ISOC Network & Distributed Systems Security Symposium (NDSS)*, 2019. (Acceptance Rate: 17.1%).
33. Lius Vargas, Logan Blue, Vanessa Frost, Christopher Patton, N. Scaife, K. Butler, and P. Traynor. Digital Healthcare-Associated Infection Analysis of a Major Multi-Campus Hospital System. In *Proceedings of the ISOC Network & Distributed Systems Security Symposium (NDSS)*, 2019. (Acceptance Rate: 17.1%).
34. Dominik Wermke, Nicolas Huaman, Yasemin Acar, Bradley Reaves, Patrick Traynor, and Sascha Fahl. A Large Scale Investigation of Obfuscation Use in Google Play. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2018. Acceptance Rate: 20.1%.
35. Nolen Scaife, Christian Peeters, and Patrick Traynor. Fear the Reaper: Characterization and Fast Detection of Card Skimmers. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2018. Acceptance Rate: 19.0%.
36. Dave (Jing) Tian, Grant Hernandez, Joseph Choi, Vanessa Frost, Christie Raules, Kevin Butler, Patrick Traynor, Hayawardh Vijayakumar, Lee Harrison, Amir Rahmati, and Mike Grace. Attention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2018. Acceptance Rate: 19.0%.
37. Luis Vargas, Gyan Hazarika, Rachel Culpepper, Kevin Butler, Thomas Shrimpton, Doug Szajda, and Patrick Traynor. Mitigating Risk while Complying with Data Retention Laws. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2018.
38. Logan Blue, Luis Vargas, and Patrick Traynor. Hello, Is It Me You're Looking For? Differentiating Between Human and Electronic Speakers for Voice Interface Security. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2018.
39. Logan Blue, Hadi Abdullah, Luis Vargas, and Patrick Traynor. 2MA: Verifying Voice Commands via Two Microphone Authentication. In *ACM Asia Conference on Computer and Communications Security (ASIACCS)*, 2018. (Acceptance Rate: 20.0%).
40. Nolen Scaife, Christian Peeters, Camilo Velez, Hanqing Zhao, Patrick Traynor, and David Arnold. The Cards Aren't Alright: Detecting Counterfeit Gift Cards Using Encoding Jitter. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2018. (Acceptance Rate: 10.4%).
41. Christian Peeters, Hadi Abdullah, Nolen Scaife, Jasmine Bowers, Patrick Traynor, Bradley Reaves, and Kevin Butler. Sonar: Detecting SS7 Redirection Attacks Via Call Audio-Based Distance Bounding. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2018. (Acceptance Rate: 10.4%).
42. Tyler Ward, Joseph Choi, Kevin Butler, John M. Shea, Patrick Traynor, and Tan Wong. Privacy Preserving Localization Using a Distributed Particle Filtering Protocol. In *IEEE MILCOM*, 2017. (Acceptance Rate: 56%).
43. Bradley Reaves and Logan Blue and Hadi Abdullah and Luis Vargas and Patrick Traynor and Thomas Shrimpton. AuthentiCall: Efficient Identity and Content Authentication for Phone Calls. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2017. (Acceptance Rate: 16.3%).
44. Jasmine Bowers and Bradley Reaves and Imani N. Sherman and Patrick Traynor and Kevin Butler. Regulators, Mount Up! Analysis of Privacy Policies for Mobile Money Applications. In *Proceedings of the USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2017. (Acceptance Rate: 26.5%).

45. Bradley Reaves, Logan Blue, and Patrick Traynor. AuthLoop: End-to-End Cryptographic Authentication for Telephony over Voice Channels. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2016. (Acceptance Rate: 15.5%).
46. Dave Tian, Nolen Scaife, Adam Bates, Kevin Butler, and Patrick Traynor. Making USB Great Again with USBFILTER. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2016. (Acceptance Rate: 15.5%).
47. Bradley Reaves, Dave Tian, Logan Blue, Patrick Traynor, and Kevin Butler. Detecting SMS Spam in the Age of Legitimate Bulk Messaging. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2016. (Acceptance Rate: 35.0%).
48. Nolen Scaife, Henry Carter, Patrick Traynor, and Kevin Butler. CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. In *IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2016. (Acceptance Rate: 17.6%).
49. Bradley Reaves, Nolen Scaife, Dave Tian, Logan Blue, Patrick Traynor, and Kevin Butler. Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2016. (Acceptance Rate: 13.0%).
50. Benjamin Mood, Debayan Gupta, Henry Carter, Kevin Butler, and Patrick Traynor. Frigate: A Validated, Extensible, and Efficient Compiler and Interpreter for Secure Computation. In *Proceedings of the IEEE European Symposium on Security and Privacy*, 2016. (Acceptance Rate: 17.3%).
51. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Outsourcing Secure Two-Party Computation as a Black Box. In *Proceedings of the International Conference on Cryptology and Network Security*, 2015. (Acceptance Rate: 52.9%).
52. Nolen Scaife, Henry Carter, and Patrick Traynor. OnionDNS: A Seizure-Resistant Top-level Domain. In *Proceedings of the IEEE Conference on Communications and Network Security (CNS)*, 2015. (Acceptance Rate: 28.1%).
53. Bradley Reaves, Nolen Scaife, Adam Bates, Patrick Traynor, and Kevin Butler. Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2015. (Acceptance Rate: 15.7%).
54. Bradley Reaves, Ethan Sherman, Adam Bates, Henry Carter, and Patrick Traynor. Boxed Out: Blocking Cellular Interconnect Bypass Fraud at the Network Edge. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2015. (Acceptance Rate: 15.7%).
55. David Dewey, Bradley Reaves, and Patrick Traynor. Uncovering Use-After-Free Conditions In Compiled Code. In *Proceedings of the International Conference on Availability, Reliability and Security (ARES)*, 2015. (Acceptance Rate: 22%).
56. Ethan Sherman, Henry Carter, Dave Tian, Patrick Traynor, and Kevin Butler. More Guidelines Than Rules: CSRF Vulnerabilities from Noncompliant OAuth 2.0 Implementations. In *Proceedings of the International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA)*, 2015. (Acceptance Rate: 22.7%).
57. Henry Carter, Charles Lever, and Patrick Traynor. Whitewash: Outsourcing Garbled Circuit Generation for Mobile Devices. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2014. (Acceptance Rate: 19.9%).
58. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Secure Outsourced Garbled Circuit Evaluation for Mobile Devices. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2013. (Acceptance Rate: 16.2%).

59. Chaitrali Amrutkar, Matti Hiltunen, Shobha Venkataraman, Kaustubh Joshi, Patrick Traynor, Trevor Jim, and Oliver Spatscheck. Why is My Smartphone Slow? On The Fly Diagnosis of Poor Performance on the Mobile Internet. In *Proceedings of The 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2013. (Acceptance Rate: 19.6%).
60. Saurabh Chakradeo, Brad Reaves, Patrick Traynor, and William Enck. MAST: Triage for Market-scale Mobile Malware Analysis. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2013. (Acceptance Rate: 15.0%)(Best Paper).
61. Charles Lever, Manos Antonakakis, Brad Reaves, Patrick Traynor, and Wenke Lee. The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2013. (Acceptance rate: 18.8%).
62. Chaitrali Amrutkar, Kapil Singh, Arunabh Verma, and Patrick Traynor. VulnerableMe: Measuring Systemic Weaknesses in Mobile Browser Security. In *Proceedings of the International Conference on Information Systems Security (ICISS)*, 2012. (Acceptance rate: 25%) (Best Paper - SAIC Student Paper Competition (GT)) (Finalist - CSAW AT&T Applied Security Research Best Paper Competition 2012).
63. Chaitrali Amrutkar, Patrick Traynor, and Paul van Oorschot. A Measurement Study of SSL Indicators on Mobile Browsers: Extended Life, or End of the Road? In *Proceedings of the Information Security Conference (ISC)*, 2012. (Acceptance rate: 32%) (Best Student Paper).
64. Italo Dacosta, Mustaque Ahamad, and Patrick Traynor. Trust No One Else: Detecting MITM Attacks Against SSL/TLS Without Third-Parties. In *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, 2012. (Acceptance Rate: 20.2%).
65. Adam Bates, Kevin Butler, Micah Sherr, Clay Shields, Patrick Traynor, and Dan Wallach. Accountable Wiretapping -or- I Know They Can Hear You Now. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2012. (Acceptance Rate: 17.8%).
66. Yacin Nadji, Jon Giffin, and Patrick Traynor. Automated Remote Repair for Mobile Malware. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2011. (Acceptance Rate: 18.5%).
67. Nilesh Nipane, Italo Dacosta, and Patrick Traynor. "Mix-In-Place" Anonymous Networking Using Secure Function Evaluation. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2011. (Acceptance Rate: 18.5%).
68. Philip Marquardt, Arunabh Verma, Henry Carter, and Patrick Traynor. (sp)iPhone: Decoding Vibrations From Nearby Keyboards Using Mobile Phone Accelerometers. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2011. (Acceptance Rate: 13.9%).
69. Philip Marquardt, David Dagon, and Patrick Traynor. Impeding Individual User Profiling in Shopper Loyalty Programs. In *Proceedings of the International Conference on Financial Cryptography and Data Security (FC)*, 2011. (Acceptance Rate: 35.1%).
70. David Dewey and Patrick Traynor. No Loitering: Exploiting Lingering Vulnerabilities in Default COM Objects. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2011. (Acceptance Rate: 20.1%).
71. Vijay Balasubramaniyan, Aamir Poonawalla, Mustaque Ahamad, Michael Hunter, and Patrick Traynor. PinDrOp: Using Single-Ended Audio Features to Determine Call Provenance. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2010. (Acceptance Rate: 17.2%).

72. Patrick Traynor, Joshua Schiffman, Thomas La Porta, Patrick McDaniel, Abhrajit Ghosh, and Farooq Anjum. Constructing Secure Localization Systems with Adjustable Granularity. In *IEEE Global Communications Conference (GLOBECOM)*, 2010. (Acceptance Rate: 35.6%).
73. Patrick Traynor. Characterizing the Security Implications of Third-Party EAS Over Cellular Text Messaging Services. In *Proceedings of the Second IEEE International Conference on Security and Privacy in Communication Networks (SecureComm)*, 2010. (Acceptance Rate: 25.0%).
74. Kapil Singh, Samrit Sangal, Nehil Jain, Patrick Traynor, and Wenke Lee. Evaluating Bluetooth as a Medium for Botnet Command and Control. In *Proceedings of the International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA)*, 2010. (Acceptance Rate: 30.7%).
75. Italo Dacosta and Patrick Traynor. Proxychain: Developing a Robust and Efficient Authentication Infrastructure for Carrier-Scale VoIP Networks. In *Proceedings of the USENIX Annual Technical Conference (ATC)*, 2010. (Acceptance Rate: 17.0%).
76. Frank S. Park, Chinmay Gangakhedkar, and Patrick Traynor. Leveraging Cellular Infrastructure to Improve Fraud Prevention. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2009. (Acceptance Rate: 19.0%).
77. Patrick Traynor, Michael Lin, Machigar Ongtang, Vikyath Rao, Trent Jaeger, Thomas La Porta, and Patrick McDaniel. On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2009. (Acceptance Rate: 18.4%).
78. Brendan Dolan-Gavitt, Abhinav Srivastava, Patrick Traynor, and Jonathon Giffin. Robust Signatures for Kernel Data Structures. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2009. (Acceptance Rate: 18.4%).
79. Italo Dacosta, Vijay Balasubramaniyan, Mustaque Ahamad, and Patrick Traynor. Improving Authentication Performance of Distributed SIP Proxies. In *Proceedings of the Conference on Principles, Systems and Applications of IP Telecommunications (IPTComm)*, 2009. (Acceptance Rate: 43.3%).
80. Patrick Traynor, Kevin Butler, William Enck, and Patrick McDaniel. Realizing Massive-Scale Conditional Access Systems Through Attribute-Based Cryptosystems. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2008. (Acceptance Rate: 17.7%).
81. Patrick Traynor, Patrick McDaniel, and Thomas La Porta. On Attack Causality in Internet-Connected Cellular Networks. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2007. (Acceptance Rate: 12.3%).
82. Sunam Ryu, Kevin Butler, Patrick Traynor, and Patrick McDaniel. Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems. In *Proceedings of the IEEE International Symposium on Security in Networks and Distributed Systems (SSNDS)*, 2007. (Acceptance Rate: 40%).
83. Luke St. Clair, Lisa Johansen, William Enck, Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Trent Jaeger. Password Exhaustion: Predicting the End of Password Usefulness. In *Proceedings of the International Conference on Information Systems Security (ICISS)*, 2006. (Invited Paper).
84. Kevin Butler, William Enck, Jennifer Plasterr, Patrick Traynor, and P. McDaniel. Privacy-Preserving Web-Based Email. In *Proceedings of the International Conference on Information Systems Security (ICISS)*, December 2006. (Acceptance Rate: 30.4%).
85. Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Brent Waters. Secure Attribute-Based Systems. In *Proceedings of the Thirteenth ACM Conference on Computer and Communications Security (CCS)*, November 2006. (Acceptance Rate: 14.8%).

86. Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta. Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks. In *Proceedings of the Twelfth Annual ACM International Conference on Mobile Computing and Networking (MobiCom)*, September 2006. (Acceptance Rate: 11.7%).
87. Patrick Traynor, Michael Chien, Scott Weaver, Boniface Hicks, and Patrick McDaniel. Non-Invasive Methods for Host Certification. In *Proceedings of the Second IEEE International Conference on Security and Privacy in Communication Networks (SecureComm)*, August 2006. (Acceptance Rate: 25.4%).
88. Patrick Traynor, JaeShung Shin, Barat Madan, Shashi Phoha, and Thomas La Porta. Efficient Group Mobility for Heterogeneous Sensor Networks. In *Proceedings of the IEEE Vehicular Technology Conference (VTC Fall)*, September 2006. (Acceptance Rate: 58%).
89. Patrick Traynor, Raju Kumar, Hussain Bin Saad, Guohong Cao, and Thomas La Porta. LIGER: Implementing Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks. In *Proceedings of the 4th ACM International Conference on Mobile Systems, Applications and Services (MobiSys)*, June 2006. (Acceptance Rate: 15.4%).
90. Patrick Traynor, Guohong Cao, and Thomas La Porta. The Effects of Probabilistic Key Management on Secure Routing in Sensor Networks. In *Proceedings of the 2006 IEEE Wireless Communications and Networking Conference (WCNC)*, April 2006. (Acceptance Rate: 38.8%).
91. Patrick Traynor, Heesook Choi, Guohong Cao, Sencun Zhu, and Thomas La Porta. Establishing Pair-Wise Keys In Heterogeneous Sensor Networks. In *Proceedings of the 25th Annual IEEE Conference on Computer Communications (INFOCOM)*, April 2006. (Acceptance Rate: 18%).
92. William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta. Exploiting Open Functionality in SMS-Capable Cellular Networks. In *Proceedings of the Twelfth ACM Conference on Computer and Communications Security (CCS)*, November 2005. (Acceptance Rate: 15%).

Removed for external version.

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

None.

E.3. Conference Presentations without Proceedings

1. Patrick Traynor. Work in Progress Presentations: Fine-Grained Secure Localization for 802.11 Networks. 15th USENIX Security Symposium (SECURITY), August 2006.
2. Patrick Traynor. Work in Progress Presentations: Fundamental Limitations of Sensor Network Security. ACM/USENIX Fourth International Conference on Mobile Systems Applications and Services (MobiSys), June 2006. (Award: Most Entertaining WIP).
3. Patrick Traynor, Heesook Choi, Guohong Cao, and Thomas La Porta. Poster Session: Probabilistic Unbalanced Key Distribution and Its Effects on Distributed Sensor Networks. Workshop on Wireless Security (WiSe), October 2004.

F. Other

F.1. Submitted Journal Papers

None.

F.2. Refereed Research Reports

None.

F.3. Software

1. *GSM Air Interface Simulator*: Developed a full voice, data and SMS capable simulator for the wireless portion of a GSM network. Models communications down to the timeslot for highest possible accuracy. Used in the majority of our work on cellular security.
2. *Malicious Telephony Load Tester*: Built a system on top of the TM1 Telecom Database testing suite to allow for a comparison of malicious traffic of varying composition.

F.4. Published Papers (Non-Refereed)

1. Patrick Traynor. Characterizing the Limitations of Third-Party EAS Over Cellular Text Messaging Services. Technical report, 3G Americas Whitepaper, 2008.
2. Lisa Johansen, Kevin Butler, William Enck, Patrick Traynor, and Patrick McDaniel. Grains of SANs: Building Storage Area Networks from Memory Spots. Technical Report NAS-TR-0060-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, 2007.

F.5. Books in Preparation

None.

F.6. Workshops and External Courses

1. Luis Vargas, Patrick Emami, and Patrick Traynor. On the Detection of Disinformation Campaign Activity with Network Analysis. In *Proceedings of the 2020 ACM SIGSAC Cloud Computing Security Workshop*, CCSW '20, 2020.
2. Siddhant Deshmukh, Henry Carter, Grant Hernandez, Patrick Traynor, and Kevin Butler. Efficient and Secure Template Blinding for Biometric Authentication. In *IEEE Workshop on Security and Privacy in the Cloud (SPC)*, 2016.
3. Debayan Gupta, Benjamin Mood, Joan Feigenbaum, Kevin Butler, and Patrick Traynor. Using Intel Software Guard Extensions for Efficient Two-Party Secure Function Evaluation. In *Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC)*, 2016.
4. Chaitrali Amrutkar and Patrick Traynor. Rethinking Permissions for Mobile Web Apps: Barriers and the Road Ahead. In *Proceedings of the ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, 2012.
5. Nigel Lawrence and Patrick Traynor. Under New Management: Practical Attacks on SNMPv3. In *Proceedings of the USENIX Workshop on Offensive Technologies (WOOT)*, 2012.
6. Andrew Harris, Frank S. Park, Seymour Goodman, and Patrick Traynor. Emerging Privacy Concerns for Digital Wallet Deployment. In *Proceedings of the Workshop on Making Privacy in America*, 2009.
7. Patrick Traynor. Privacy and Security Concerns for Personal and Mobile Health Devices. In *Proceedings of the Workshop to Set A Research Agenda for Privacy and Security of Healthcare Technologies*, 2009.

- Kevin Butler, William Enck, Harri Hursti, Stephen McLaughlin, Patrick Traynor, and Patrick McDaniel. Systemic Issues in the Hart InterCivic and Premier Voting System: Reflections Following Project EVEREST. In *Proceedings of the USENIX/ACCURATE Electronic Voting Technology (EVT) Workshop*, 2008.

G. Research Proposals and Grants (Principal Investigator)

1. Approved and Funded

- Artus Protocol STTR Phase II - Extension**
Sponsor: Office of Naval Research
Investigator(s): Patrick Traynor (PI), Kevin Butler
Amount: *\$300,000 over 2 years*
Awarded: *August 2023*
- Testing Audio Deep Fake Detectors**
Sponsor: Bank of America
Investigator(s): Patrick Traynor (PI), Kevin Butler
Amount: *\$150,000 over 1 year*
Awarded: *August 2023*
- Testing Audio Deep Fake Detectors**
Sponsor: Bank of America
Investigator(s): Patrick Traynor (PI), Kevin Butler
Amount: *\$274,000 over 2 years*
Awarded: *August 2021*
- Deploying Defenses for Cellular Networks Using the AWARE Testbed**
Sponsor: Department of Homeland Security: CISA:
Investigator(s): Patrick Traynor (PI), Kevin Butler, Guofei Gu, Radu Stoleru, Walter Magnussen, P. R. Kumar
Amount: *\$3,100,000 over 4 years*
Awarded: *October 2019*
- SaTC:CORE:Medium: Securing the Voice Processing Pipeline Against Adversarial Audio**
Sponsor: NSF Secure and Trustworthy Cyberspace
Investigator(s): Patrick Traynor (PI), Thomas Shrimpton, Vincent Bindschaedler
Amount: *\$1,199,999 over 4 years*
Awarded: *October 2019*
- Artus Protocol STTR Phase II**
Sponsor: Office of Naval Research
Investigator(s): Patrick Traynor (PI), Kevin Butler
Amount: *\$800,000 over 4 years*
Awarded: *August 2019*
- Evaluating the Security of QR Code-Based Payments**
Sponsor: Discover Financial
Investigator(s): Patrick Traynor (PI)
Amount: *\$50,000 over 1 year*
Awarded: *September 2018*
- Workshop: Addressing the Technical Security Challenges of Emerging Digital Financial Services**
Sponsor: NSF Secure and Trustworthy Cyberspace

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

9. **Designing Strong End-to-End Authentication Mechanisms for Modern Telephony Systems**
Sponsor: NSF Secure and Trustworthy Cyberspace
Investigator(s): Patrick Traynor (PI)
Amount: \$500,000 over 3 years
Awarded: July 2016
10. **Digital Healthcare-Associated Infection: Measurement, Defense and Prevention in a Modern Digital Healthcare Ecosystem**
Sponsor: National Science Foundation
Investigator(s): Patrick Traynor (PI), Kevin Butler, Shigang Chen
Amount: \$1,200,000 over 4 years
Awarded: June 2016
11. **Evaluating and Improving Security in Emerging Branchless Banking Systems**
Sponsor: NSF Secure and Trustworthy Cyberspace
Investigator(s): Patrick Traynor (PI)
Amount: \$500,000 over 3 years
Awarded July 2015
12. **Prevention and Detection of Disallowed Connections in Mobile and Pervasive Systems**
Sponsor: CISE-ECE Harris Endowed Seed Fund Program
Investigator(s): Patrick Traynor (PI), Renato Figueiredo (PI)
Amount: \$40,000 over 1 year
Awarded December 2014
13. **Mobile Excursion Study Support**
Sponsor: Hanscom AFB Electronic Systems Command Development Planning Division (ESC/XR)
Investigator(s): Patrick Traynor (PI), Mustaque Ahamad, Jeff Evans, Chuck Bokath
Amount: \$280,000 over 3 months
Awarded July 2012
14. **Characterizing the Security Limitations of Accessing the Mobile Web**
Sponsor: NSF Secure and Trustworthy Cyberspace
Investigator(s): Patrick Traynor (PI) and William Enck (NC State)
Amount: \$334,000 over 3 years
Awarded July 2012
15. **Mitigating Attacks on Mobile Devices and Critical Cellular Infrastructure**
Sponsor: US Department of Defense - Defense University Research Instrumentation Program (DURIP)
Investigator(s): Patrick Traynor (PI), Jon Giffin, Mustaque Ahamad
Amount: \$210,081 over 1 year
Awarded June 2011
16. **Characterizing and Implementing Efficient Primitives for Privacy-Preserving Computation**
Sponsor: DARPA PROgramming Computation on EncryptEd Data (PROCEED) – Broad Agency Announcement
Investigator(s): Patrick Traynor (PI) and Kevin Butler (UOregon)
Amount: \$580,000 over 4 years
Awarded May 2011

17. **Security for Converged IMS Networks**
 Sponsor: US Department of Defense
 Investigator(s): Patrick Traynor (PI), Mustaque Ahamad and Russ Clark
 Amount: \$242,401 over 1 year
 Awarded August 2010
18. **CAREER: Protecting User Data on Lost, Stolen and Damaged Mobile Phones**
 Sponsor: NSF Trustworthy Computing
 Investigator(s): Patrick Traynor (PI)
 Amount: \$400,000 over 5 years
 Awarded: May 2010
19. **Provably Anonymous Networking Through Secure Function Evaluation**
 Sponsor: NSF Trustworthy Computing
 Investigator(s): Patrick Traynor (PI)
 Amount: \$200,000 over 2 years
 Awarded: July 2009
20. **Characterizing and Mitigating Device-Based Attacks in Cellular Telecommunications Networks**
 Sponsor: NSF Trustworthy Computing
 Investigator(s): Patrick Traynor (PI) and Jonathon Giffin
 Amount: \$450,000 over 3 years
 Awarded: July 2009

2. Pending

Removed for external version.

H. Research Proposals and Grants (Contributor)

1. Approved and Funded

1. **SaTC: Frontier: Securing the Future of Computing for Marginalized and Vulnerable Populations**
 Sponsor: NSF SaTC
 Investigator(s): Kevin Butler (PI), Patrick Traynor, Tadayoshi Kohno, Franzi Roesner, Apu Kapadia, Eakta Jain.
 Amount: \$7,500,000 for 5 years
 Awarded October 2022
2. **ROCKY: Reliable Obfuscated Communications Kit for everYone**
 Sponsor: DARPA Resilient Anonymous Communication for Everyone (RACE) – Broad Agency Announcement
 Investigator(s): Thomas Shrimpton (PI), Patrick Traynor, Kevin Butler, Vincent Bindschaedler, Nadia Heninger
 Amount: \$1,600,000 over 4 years
 Awarded May 2019
3. **WiFiUS: Collaborative Research: SELIOT: Securing Lifecycle of Internet-of-Things**
 Sponsor: NSF CNS WiFiUS
 Investigator(s): Gene Tsudik (PI), Patrick Traynor
 Amount: \$300,000 for 2 years
 Submitted December 2016

4. **Cloud-based Oblivious Spectrum Mapping and Allocation**
 Sponsor: NSF CNS EARS
 Investigator(s): John Shea (PI), Tan Wong, Patrick Traynor
 Amount: \$532,952 for 2 years
 Submitted May 2016
5. **DURIP: Developing Research Capability in Cyber-Physical Systems at the University of Florida**
 Sponsor: Small
 Investigator(s): Kevin Butler (PI), Patrick Traynor, My Thai
 Amount: \$200,000 for 2 years
 Submitted: June 2015
6. **Securing the New Converged Telephony Landscape**
 Sponsor: NSF TWC: Small
 Investigator(s): Mustaque Ahamad (PI) and Patrick Traynor
 Amount: \$500,000 for 3 years
 Submitted: December 2012
7. **Facilitating Free and Open Access to Information on the Internet**
 Sponsor: NSF Trustworthy Computing
 Investigator(s): Nick Feamster (PI), Wenke Lee, Patrick Traynor, Hans Klein, Roger Dingledine, Michael Freedman and Edward W. Felten
 Amount: \$1,500,000 for 4 years
 Awarded: June 2011
8. **Monitoring Free and Open Access to Information on the Internet**
 Sponsor: Google Focus Program
 Investigator(s): Nick Feamster (PI), Wenke Lee, Mustaque Ahamad, Patrick Traynor, Henry Owen, Ellen Zegura, Zvi Galil
 Amount: \$1,000,000 for 2 years
 Awarded: November 2011
9. **Dynamic-attribute-based Disclosure of Health Information in Emergency Care Scenarios**
 Sponsor: Health Systems Institute (HSI) Seed Grant Program
 Investigator(s): Doug Blough (PI), Mustaque Ahamad, Patrick Traynor and Jim Jose
 Amount: \$50,000 over 1 year
 Awarded: August 2009
10. **Federal Cyber Service Scholarships at Georgia Tech**
 Sponsor: NSF SFS Scholarships
 Investigator(s): Seymour Goodman (PI), Patrick Traynor
 Amount: \$1,250,682 over 5 years
 Awarded: June 2009
11. **Security for IMS-Enabled Converged Applications**
 Sponsor: US Department of Defense
 Investigator(s): Mustaque Ahamad (PI), Patrick Traynor (PI), Michael Hunter, Russ Clark
 Amount: \$146,121 for 1 year
 Awarded: August 2008

2. Pending

Removed for external version.

I. Research Honors and Awards

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

III. SERVICE

A. Professional Activities

A.1. Memberships and Activities in Professional Societies

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

A.2. Conference Committee Activities

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

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

B. On-Campus Committees

B.1. University of Florida

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

B.2. Georgia Tech

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

C. Special Assignments

None.

D. Ph.D. Examining Committees

Ph.D. Examining Committees

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

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

External Member of Ph.D. Research Committee

None.

External Member of Ph.D. Examining Committee

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

Ph.D. Thesis Proposal Committees

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

Ph.D. Qualifying Exam Committees—Georgia Tech

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

3. Xinyu Xing, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Wenke Lee.
4. Brad Reaves, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Patrick Traynor.
5. Chaz Lever, College of Computing, Georgia Tech, Spring 2013.
Advisor: Professor Patrick Traynor.
6. Terry Nelms, College of Computing, Georgia Tech, Spring 2012.
Advisor: Professors Mustaque Ahamad and Roberto Perdesci.
7. Saurabh Chakradeo, College of Computing, Georgia Tech, Spring 2012.
Advisor: Professor Patrick Traynor.
8. Henry Carter, College of Computing, Georgia Tech, Spring 2012.
Advisor: Professor Patrick Traynor.
9. David Dewey, College of Computing, Georgia Tech, Spring 2012.
Advisor: Professor Jon Giffin.
10. Chaitrali Amrutkar, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Patrick Traynor.
11. Yacin Nadji, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Wenke Lee.
12. Yogesh Mundada, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Nick Feamster.
13. Hyojoon Kim, College of Computing, Georgia Tech, Fall 2011.
Advisor: Professor Nick Feamster.
14. Ikpeme Erete, College of Computing, Georgia Tech, Spring 2011.
Advisor: Professor Alex Orso.
15. Chaitrali Amrutkar, College of Computing, Georgia Tech, Spring 2011.
Advisor: Professor Patrick Traynor.
16. Brendan Dolan-Gavitt, College of Computing, Georgia Tech, Spring 2011.
Advisor: Professor Wenke Lee and Professor Jon Giffin.
17. Sam Burnett, College of Computing, Georgia Tech, Fall 2010.
Advisor: Professor Nick Feamster.
18. Cong Shi, College of Computing, Georgia Tech, Fall 2010.
Advisor: Professor Mostafa Ammar and Professor Ellen Zegura.
19. Partha Kanuparth, College of Computing, Georgia Tech, Fall 2010.
Advisor: Professor Constantine Dorvolis.
20. Long Lu, College of Computing, Georgia Tech, Spring 2010.
Advisor: Professor Wenke Lee.
21. Virendra Kumar, College of Computing, Georgia Tech, Spring 2009.
Advisor: Professor Alexandra Boldyreva.
22. Frank Park, College of Computing, Georgia Tech, Spring 2009.
Advisor: Professor Patrick Traynor.

23. Italo Dacosta, College of Computing, Georgia Tech, Fall 2008.
Advisor: Professor Mustaque Ahamad and Professor Patrick Traynor.
24. Adam O'Neill, College of Computing, Georgia Tech, Fall 2008.
Advisor: Professor Alexandra Boldyreva.

E. External Member of M.S. Examining Committee

M.S. Thesis Defense Committees None.

F. Consulting and Advisory Appointments

1. Skim Reaper, *Co-Founder and CEO*, 2019-Present.
2. CryptoDrop Anti-Ransomware, *Co-Founder and CEO*, 2017-2018.
3. Pindrop Security, *Research Fellow and Co-Founder*, Spring 2012 - Spring 2014.
4. United States Army (via US Falcon), *Information Assurance Officer Training Program*, Spring 2010.
5. 3G Americas, *Characterizing the Limitations of Third-Party EAS over Cellular Text Messaging Systems*, Fall 2008.

G. Civic Activities

None.

IV. NATIONAL AND INTERNATIONAL PROFESSIONAL RECOGNITION

A. Honors and Awards

1. Fellow, Kavli Foundation, 2017.
2. Fellow, Center for Financial Inclusion at Accion, 2016.
3. Sloan Research Fellow, Alfred P. Sloan Foundation, 2014.

B. Invited Conference Session Chairmanships

1. Session Chair, *Work-in-Progress* at the *USENIX Security Symposium (SECURITY)*, 2016.
2. Session Chair, *Mobile Security* at the *USENIX Security Symposium (SECURITY)*, 2013.
3. Poster Chair, *USENIX Security Symposium (SECURITY)*, 2010, 2011.
4. Session Chair, *Privacy and Anonymity* at the *USENIX Workshop on Hot Topics in Security (HotSec)*, 2011.
5. Session Chair, *Security of Authentication and Protection Mechanisms* at the *IEEE Symposium on Security & Privacy (OAKLAND)*, 2011.
6. Session Chair, *Information Abuse* at the *IEEE Symposium on Security & Privacy (OAKLAND)*, 2010.
7. Session Chair, *RFID Security* at the *ACM Conference on Computer and Communications Security (CCS)*, 2009.
8. Session Chair, *Browser Security Session* at the *USENIX Security Symposium (SECURITY)*, 2009.
9. Session Chair, *Information Security Session* at the *IEEE Symposium on Security and Privacy (OAKLAND)*, 2009.
10. Session Chair, *Work-in-Progress* at the *IEEE Symposium on Security and Privacy (OAKLAND)*, 2009.
11. Session Chair, *Work/Opinions-in-Progress* at the *ISOC Network and Distributed Systems Security (NDSS) Symposium*, 2009.
12. Session Chair, *Privacy Session* at the *USENIX Security Symposium (SECURITY)*, 2008.

C. Professional Registration

None.

D. Patents

1. Patrick G. Traynor, Christian Peeters, Bradley G. Reaves, Hadi Abdullah, Kevin Butler, Jasmine Bowers, Walter N. Scaife, "Detecting SS7 Redirection Attacks With Audio-Based Distance Bounding", United State Patent # 11,265,717, Filed March 2019, Issued March 2022.
2. Patrick G. Traynor, Logan E. Blue, Luis Vargas, "Method and Apparatus for Differentiating Between Human and Electronic Speaker for Voice Interface Security", United State Patent # 11,176,960, Filed June 2019, Issued November 2021.
3. Patrick G. Traynor, Bradley G. Reaves, Logan E. Blue Practical End-to-End Cryptographic Authentication for Telephony Over Voice Channels, United State Patent # 11,329,831, Filed November 2018, Issued May 2022.

4. Walter Nolen Scaife, Patrick G. Traynor and Christian Peeters, "Payment Card Overlay Skimmer Detection", United States Patent # 10,496,914, Filed October 2017, Issued December 2019. (See also # 10,936,928)
5. Patrick G. Traynor, David P. Arnold, Walter Nolen Scaife, Christian Peeters, and Camilo Valez Cuervo, "Detecting counterfeit magnetic stripe cards using encoding jitter", United States Patent # 10,803,261, Filed May 2017, Issued October 2020.
6. Patrick G. Traynor, Bradley Reaves, Logan Blue, Luis Vargas, Hadi Abdullah, and Thomas Shrimpton, "Identity and content authentication for phone calls", United States Patent # 10,764,043, Filed Apr 2017, Issued September 2020.
7. Walter Nolen Scaife, Henry Carter, Patrick G. Traynor and Kevin R. B. Butler. "Malware Detection Through User Data Transformation Monitoring", United States Patent # 10,685,114. Filed September 2015, Issued June 2020.
8. Vijay A. Balasubramaniyan, Mustaque Ahamad, Patrick G. Traynor. "Using Single-Ended Audio Features to Automatically Determine Voice Call Provenance", United States Patent, #9,037,113 June 2010, Issued May 2015. (See also #9,516,497 and #10,523,809)
9. Patrick G. Traynor, Byungsook Kim and Farooq Anjum. "Secure Localization for 802.11 Networks with Fine Granularity", United States Patent, #8,107,400, Filed July 2008, Issued January 2012.

E. Editorial and Reviewer Work for Technical Journals and Publishers

Associate Editor:

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

Guest Editor:

Journals

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

Reviewer for:

Journals

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

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

Conferences and Workshops

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

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

F. Expert Witness Services

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

13. *Apple Inc v Seven Networks, LLC*: Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Verdict: Three of four petitions instituted by PTAB. Fourth rejected via discretion, case settled. *August 2019 - November 2020*.
14. *mSIGNIA, Inc. v. InAuth, Inc.*: Expert Witness for the Defendant for Inter Partes Review, Non-Infringement and Invalidity, Trade Secrets (via Quinn Emanuel Urquhart and Sullivan, LLP). Verdict: Dismissed with prejudice. *October 2017 - December 2018*.
15. *Huawei v. T-Mobile*: Expert Witness for the Defendant for Non-Infringement (via WilmerHale LLP, Alston & Bird LLP) Verdict: Settled *June 2016 - December 2017*.
16. *Telefonaktiebolaget LM Ericsson v Apple*: Expert Witness for the Defendant for Non-Infringement, Invalidity (via WilmerHale LLP). Verdict: Settled *June 2015 - December 2015*.
17. *Mayfonk v Nike*: Expert Witness for the Plaintiff for Infringement/Trade Secrets (via Paul Hastings). Verdict: Settled. *June 2015 - November 2015*.
18. *Maxim Integrated Products v Bank of the West*: Expert Witness for the Defendant for Non-Infringement (via Paul Hastings LLP). Verdict: Dismissed with prejudice. *January 2014 - August 2014*.
19. *Maxim Integrated Products v Comerica Inc, et al*: Expert Witness for the Defendant for Non-Infringement (via McKenna, Long & Aldridge LLP). Verdict: Settled. *June 2014 - August 2014*.
20. *William Grecia v. Apple Inc. et al*: Expert Consultant for the Defendant for Invalidity (via Kirkland & Ellis LLP). Verdict: Closed in initial pleadings, dismissed with prejudice. *July 2014 - August 2014*.
21. *Intertrust Technologies Corp. v. Apple Inc.*: Expert Consultant for Defendant for Invalidity and Non-Infringement (via Kirkland & Ellis LLP). Verdict: Settled. *October 2013 - February 2014*.
22. *Maxim Integrated Products v KeyCorp Bank*: Expert Witness for the Defendant for Non-Infringement (via Calfee, Halter & Griswold LLP) Verdict: Settled. *April 2013 - June 2013*.
23. *Intellectual Ventures LLC vs. Check Point; et al.*: Expert Consultant for the Plaintiff for Infringement (via Susman Godfrey LLP), Verdict: Infringement on 2 of 4 patents. *October 2012 - February 2015*.

V. OTHER CONTRIBUTIONS

A. Seminar Presentations (Invited Papers and Talks at Meetings and Symposia)

1. Keynote: Well, It Worked on My Computer: Reproducibility in Computer Security Research. Learning from Authoritative Security Experiment Results (LASER) Workshop, December 2024. École Polytechnique Fédérale de Lausanne (EPFL, Switzerland).
2. Social Engineering and Two-Factor Authentication. Cyber Security Training Eastern Indonesia, August 2024. Financial Innovation Lab (EIFIL) (Denpasar, Bali, Indonesia).
3. DFS Security and Mobile Money Analysis. Cyber Security Training Eastern Indonesia, August 2024. Financial Innovation Lab (EIFIL) (Denpasar, Bali, Indonesia).
4. Keynote: Well, It Worked on My Computer: Reproducibility in Computer Security Research. EPFL Summer Research Institute (SURI), July 2024. École Polytechnique Fédérale de Lausanne (EPFL, Switzerland).
5. Humans vs The Computer Interfaces: The Challenge of Separating Deepfakes/Bots from People. North Central Florida Institute of Internal Auditors (IIA), May 2024.
6. Humans vs The Computer Interfaces: The Challenge of Separating Deepfakes/Bots from People. UF Quest 2: Siri is my Superpower: Communicating with AI, March 2024. University of Florida.
7. Humans vs The Computer Interfaces: The Challenge of Separating Deepfakes/Bots from People. Federal Information Integrity Research and Development (FIIRD) Interworking Group (IWG), March 2024. via NITRD, OSTP.
8. AI driven voice cloning scams. Discussion at the White House with Anne Neuberger (Deputy National Security Advisor for Cyber and Emerging Technologies), Jessica Rosenworcel (Chair of the Federal Communications Commission) and Lina Khan (Chair of the Federal Trade Commission), January 2024. Lead Academic facilitator.
9. Keynote: Well, It Worked on My Computer: Reproducibility, Tech Transfer, and Computer Security Research. National Science Foundation Secure and Trustworthy Cyberspace (SaTC) Vision 2.0 Workshop, March 2023. University of Texas at Dallas.
10. Humans vs The Computer Interfaces: Separating Deepfakes/Bots from People Using Psychoacoustics. UCLA Electrical and Computer Engineering Distinguished Seminar, February 2023. University of California, Los Angeles.
11. Keynote: Exploiting the Gaps Between Human and Machine Understanding of Audio: Frameworks, Attacks, and Defenses. ISCA Symposium on Security and Privacy in Speech Communication (SPSC), November 2021. Virtual.
12. The State of Voice Cloning Technology. Federal Trade Commission (FTC) Workshop on Voice Cloning Technologies, January 2020. Washington, DC.
13. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. North Carolina State University Department of Computer Science Colloquium, January 2020. Raleigh, NC.
14. Moving from research to practice: How to maximize the impact of SaTC projects. National Science Foundation Secure and Trustworthy Cyberspace (SaTC) PI Meeting, October 2019. Alexandria, VA.
15. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. Purdue University Computer Science Excellence Lecture Series, October 2019. West Lafayette, IN.

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

34. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Illinois Science of Security (SoS) Lablet Speaker Series - University of Illinois, Urbana-Champaign, April 2016. Urbana-Champaign, Illinois.
35. New Trends in Cybersecurity: Vulnerabilities in Branchless Banking Systems. United States Departments of State and Justice - Cybersecurity and Cybercrime Workshop for Lusophone Africa, September 2015. Maputo, Mozambique.
36. New Trends in Cybersecurity: Vulnerabilities in Branchless Banking Systems. United States Departments of State and Justice - ECCAS Cybersecurity and Cybercrime Workshop, August 2015. Kinshasa, Democratic Republic of Congo.
37. Chasing Telephony Security: Where the Wild Things... Are? University of Florida - Department Colloquium, January 2014. Gainesville, FL.
38. Chasing Telephony Security: Where the Wild Things... Are? Verizon Wireless RNC/Data Center, October 2013. Alpharetta, GA.
39. Chasing Telephony Security: Where the Wild Things... Are? University of Waterloo - CrySP Speaker Series on Privacy, October 2013. Waterloo, ON, Canada.
40. Analyzing Malicious Traffic in Cellular Networks. GSM Association's (GSMA) Mobile Malware Community Workshop, July 2013. Mountain View, CA.
41. Threats to Mobile Devices. US Federal Trade Commission (FTC) Public Forum - Invited Speaker, June 2013. Washington, D.C.
42. Chasing Telephony Security: Where the Wild Things... Are? University of Wisconsin - Madison, Security Seminar, March 2013. Madison, WI.
43. The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers. Invited Talk: Centre for Secure Information Technologies (CSIT) Queen's University, March 2013. Belfast, Northern Ireland.
44. Chasing Telephony Security: Where the Wild Things... Are? Stanford Security Seminar, March 2013. Stanford, CA.
45. Chasing Telephony Security: Where the Wild Things... Are? University of California, Berkeley, Security Group, March 2013. Berkeley, CA.
46. Chasing Telephony Security: Where the Wild Things... Are? Carnegie Mellon University CyLab Seminar, February 2013. Pittsburgh, PA.
47. Chasing Telephony Security: Where the Wild Things... Are? University of Oregon Department of Computer Science Colloquium, November 2012. Eugene, OR.
48. Chasing Telephony Security: Where the Wild Things... Are? University of Washington Department of Electrical Engineering, Network Security Lab (NSL): Invited Talk, November 2012. Seattle, WA.
49. Needles and Haystacks: Digging for Ground Truth on Mobile Malware. ZISC Workshop on Secure Mobile and Cloud Computing, ETH Zurich, June 2012. Zurich, Switzerland.
50. Panel: Advice for Early Career Faculty. CRA Career Mentoring Workshop, February 2012. Washington, D.C.
51. Research Challenges in Cellular and Mobile Network Security. US-China Software Workshop (Co-Sponsored by NSF and NSFC), September 2011. Beijing, China.

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

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

B. Special Activities

Presentations to Lay Media

1. How technology can fight digital fakery. The Babbage Podcast/The Economist <https://shows.acast.com/theeconomistbabbage/episodes/babbage-how-to-detect-a-deepfake/>, January 2023.
2. Deepfake audio has a tell and researchers can spot it. Ars Technica <https://arstechnica.com/information-technology/2022/09/researchers-use-fluid-dynamics-to-spot-deepfake-voices/>, September 2022.
3. This security tool could help stop the problem of ransomware in its tracks. TheJournal.ie <https://www.thejournal.ie/ransomware-researchers-stop-2875032-Jul2016/>, July 2016.
4. Researchers Unleash Ransomware Annihilation. BankInfoSecurity - <http://www.bankinfosecurity.com/researchers-unleash-ransomware-annihilation-a-9255>, July 2016.
5. CryptoDrop Stops Ransomware by Stopping its Encryption. Security Intelligence - https://securityintelligence.com/news/cryptodrop-stops-ransomware-by-stopping-its-encryption/?utm_source=tfeed&utm_medium=twitter, July 2016.
6. Ransomware 'stopped' by new software. BBC - <http://www.bbc.com/news/technology-36772461>, July 2016.
7. Researchers create effective anti-ransomware solution. Help Net Security - <https://www.helpnetsecurity.com/2016/07/12/anti-ransomware-solution/>, July 2016.
8. Florida U boffins think they've defeated all ransomware. http://www.theregister.co.uk/2016/07/12/ransomware_defeated/, July 2016.

9. This Anti-Ransomware Tool Could Save You Hundreds of Pounds. Huffington Post - http://www.huffingtonpost.co.uk/entry/anti-ransomware-tool-save-hundreds-pounds_uk_57838beee4b0935d4b4b30ba, July 2016.
10. Researchers develop method to stop 100% of ransomware before it encrypts all files. Myce - <http://www.myce.com/news/researchers-develop-method-stop-100-ransomware-encrypts-files-79873/>, July 2016.
11. Desarrollan una solución para detener el ransomware. ComputerHoy - <http://computerhoy.com/noticias/software/desarrollan-solucion-detener-ransomware-47972>, July 2016.
12. Why your antivirus software can't stop ransomware. Futurity - <http://www.futurity.org/ransomware-computer-files-1198242-2/>, July 2016.
13. CryptoDrop Gives Users Hope to Prevent Ransomware Infections in the Future. Softpedia - <http://news.softpedia.com/news/cryptodrop-gives-users-hope-to-prevent-ransomware-infections-in-the-future-506187.shtml>, July 2016.
14. Could this be the answer to the ransomware threat?, Consumer Affairs. Consumer Affairs - <https://www.consumeraffairs.com/news/could-this-be-the-answer-to-the-ransomware-threat-071116.html>, July 2016.
15. Extortion extinction: Researchers develop a way to stop ransomware. Phys.org - <http://phys.org/news/2016-07-extortion-extinction-ransomware.html>, July 2016.
16. Researchers Develop A Way To Stop Ransomware By Watching The Filesystem. Slashdot - <https://yro.slashdot.org/story/16/07/08/2242244/researchers-develop-a-way-to-stop-ransomware-by-watching-the-filesystem>, July 2016.
17. Mohul Ghosh. Trak.in - Digital Money Apps In India Are Unsafe and Unsecured - Researchers. <http://trak.in/tags/business/2015/08/17/digital-money-apps-india-unsafe-unsecured/>, August 2015.
18. Richard Handford. Mobile World Live - Survey finds security holes in mobile money apps. <http://www.mobileworldlive.com/money/news-money/survey-finds-security-holes-in-mobile-money-apps/#.Vc27Y-QTmsQ.twitter>, August 2015.
19. JENNIFER VALENTINO-DEVRIES. Wall Street Journal - Researchers Find Security Flaws in Developing-World Money Apps. <http://blogs.wsj.com/digits/2015/08/11/researchers-find-security-flaws-in-developing-world-money-apps/>, August 2015.
20. Jonathon Cheng. Wall Street Journal - Samsung Phone Studied for Possible Security Gap. <http://online.wsj.com/news/articles/SB10001424052702304244904579276191788427198>, December 2013.
21. N. V. The Economist - The Threat in the Pocket. <http://www.economist.com/blogs/babbage/2013/10/difference-engine-0?fsrc=scn/fb/wl/bl/thethreatinthepocket>, October 2013.

22. Antone Gonsalves. ComputerWorld - Let's Dump Anti-Virus and Move On:. <http://blogs.computerworld.com/mobile-security/22969/lets-dump-av-and-move>, October 2013.
23. Mathew J. Schwartz. InformationWeek - Google: Don't Fear Android Malware. <http://www.informationweek.com/security/mobile/google-dont-fear-android-malware/240162399>, October 2013.
24. Kirsten Doyle. ITWeb - Android Threat Exaggerated, or is it? http://www.itweb.co.za/index.php?option=com_content&view=article&id=68055, October 2013.
25. Danielle Walker. SC Magazine - Mobile malware prevalence expands, but privacy-abusing apps should be top of mind. <http://www.scmagazine.com/mobile-malware-prevalence-expands-but-privacy-abusing-apps-should-be-top-of-mind/article/300597/>, June 2013.
26. Jim Burress. WABE NPR - Mobile Web Browsers Full of Security Risks, Tech Professor Finds. <http://wabe.org/post/mobile-web-browsers-full-security-risks-tech-professor-finds>, December 2012.
27. Mark Huffman. Consumer Affairs - Georgia Tech: mobile browsers fail safety test. <http://www.consumeraffairs.com/news/georgia-tech-mobile-browsers-fail-safety-test-120612.html>, December 2012.
28. Matthew J. Schwartz. Information Week - Blame Screen Size: Mobile Browsers Flunk Security Tests. <http://www.informationweek.com/security/mobile/blame-screen-size-mobile-browsers-flunk/240143999>, December 2012.
29. Jon Gold. Network World - Ga. Tech researchers: Mobile Browsers need better HTTPS indicators. <http://www.networkworld.com/news/2012/120512-mobile-browsers-264846.html>, December 2012.
30. United Press International. Study: Most mobile Web browsers unsafe. http://www.upi.com/Science_News/Technology/2012/12/05/Study-Most-mobile-web-browsers-unsafe/UPI-73431354743353/#ixzz2EGtQsuId, December 2012.
31. Suzanne Choney. Mobile browser woes can fool even experts: report. <http://www.nbcnews.com/technology/mobile-browser-woes-can-fool-even-experts-report-1C7451203>, December 2012.
32. Meghan Kelly. VentureBeat - 3 hot security startups to watch. <http://venturebeat.com/2012/02/27/3-security-startups-to-watch-at-the-2012-rsa-conference/>, February 2012.
33. Jacob Goodwin. Government Security News - RSA 2012 – Pindrop Security can distinguish a fraudulent phone call from a real one. <http://www.gsnmagazine.com/node/25721?c=communications>, February 2012.
34. Matt Liebowitz. Phone hack logs keystrokes from nearby computers. MSNBC.com - http://www.msnbc.msn.com/id/44993238/ns/technology_and_science-security/#.TqU5MNSjPh4, October 2011.
35. Jacob Aron. iPhone keylogger can snoop on desktop typing. New Scientist - <http://www.newscientist.com/article/dn21059-iphone-keylogger-can-snoop-on-desktop-typing.html>, October 2011.

36. iPhone Keylogger Can Snoop on Desktop Typing. Slashdot - <http://mobile.slashdot.org/story/11/10/18/2346222/iphone-keylogger-can-snoop-on-desktop-typing>, October 2011.
37. Robert Lemos. Smart Phones Could Hear Your Password. Technology Review - <http://www.technologyreview.com/computing/38913/?p1=A2>, October 2011.
38. Kevin McCaney. Bad vibrations: How smart phones could steal PC passwords. Government Computer News - <http://gcn.com/articles/2011/10/18/smart-phone-sensors-steal-keystrokes.aspx>, October 2011.
39. PhysOrg. Turning iPhone into spiPhone: Smartphones' accelerometer can track strokes on nearby keyboards. PhysOrg.com - <http://www.physorg.com/news/2011-10-iphone-spiphone-smartphones-accelerometer-track.html>, October 2011.
40. Brid-Aine Parnell. Securo-boffins call for 'self-aware' defensive technologies. The Register - http://www.theregister.co.uk/2011/09/14/self_aware_cyber_security_technologies_should_be_a_top_priority/, September 2011.
41. Clay Dillow. 'PinDr0p' Tech Uses Unique Noise Fingerprints to Trace Calls. Popular Science - <http://www.popsci.com/technology/article/2010-10/pindr0p-tech-tags-phone-calls-unique-fingerprints-trace-call-paths-across-networks>, October 2010.
42. Lewis Page. Voice-routing call fingerprint system fights vishing. The Register - http://www.theregister.co.uk/2010/10/06/voice_fingerprints, October 2010.
43. Science Daily. Voice Phishing: System to Trace Telephone Call Paths Across Multiple Networks Developed. <http://www.sciencedaily.com/releases/2010/10/101005121820.htm>, October 2010.
44. Brian Kalish. To Text or Not to Text During Emergencies. NextGov.com - http://www.nextgov.com/nextgov/ng_20100914_5986.php?oref=topnews, September 2010.
45. Ki Mae Heussner. 'Operation Chokehold': Fake Steve Jobs Rallies iPhone Users to Cripple AT&T Network. ABC News - <http://abcnews.go.com/Technology/GadgetGuide/fake-steve-jobs-rallies-iphone-users-cripple-att/story?id=9355447>, December 2009.
46. Bob Brown. Researchers Set Their Sights on iPhones, Mobile Malware. PC World Magazine - http://www.pcworld.com/article/182005/iphone_worms_mobile_malware.html?tk=rss, November 2009.
47. MacGregor Campbell. Botnets show their disruptive potential. New Scientist Magazine - <http://www.newscientist.com/article/mg20427347.000-mobile-botnets-show-their-disruptive-potential.html>, November 2009.
48. Angela Moscaritolo. Remote repair for infected phones in development. SC Magazine - <http://www.scmagazineus.com/remote-repair-for-infected-phones-in-development/article/157504/>, November 2009.
49. Bob Brown. iPhone worms, other smartphone malware in researchers' sights. Network World - <http://www.networkworld.com/news/2009/111109-smartphone-security-georgia-tech.html?hpg1=bn>, November 2009.

50. Urvaksh Karkaria. GT researchers work to secure cellphones. Atlanta Business Chronicle - <http://atlanta.bizjournals.com/atlanta/blog/atlantech/2009/11/cellphone.html>, November 2009.
51. Making Carriers Shoulder Smartphone Security. http://mobile.slashdot.org/story/09/11/11_2318247/Making-Carriers-Shoulder-Smartphone-Security?art_pos=31, November 2009.
52. Ben Meyer. Georgia Tech to Lead Fight Against Cell Phone Hackers. NBC 11 Atlanta - <http://www.11alive.com/news/local/story.aspx?storyid=132505&catid=3>, July 2009.
53. Illena Armstrong. Safeguarding your mobile networks. SC Magazine - <http://www.scmagazineus.com/Safeguarding-your-mobile-networks/article/138289/>, June 2009.
54. Kelli B. Grant. Four Free Cellphone Apps to Help Manage Your Money. SmartMoney Magazine - <http://www.smartmoney.com/Spending/Deals/4-Great-Free-Finance-Apps-for-Cellphones/>, June 2009.
55. Amanda Hoffstrom. Technology's limitations in alerting campus danger. UWire Magazine - <http://www.uwire.com/Article.aspx?id=3738798>, February 2009.
56. Laura Sydell. Compromise Allows Obama To Keep BlackBerry. National Public Radio - <http://www.npr.org/templates/story/story.php?storyId=99790788>, January 2009.
57. Dennis Carter. Questions abound as emergency alert flops Virginia Tech's text-message alert system failed when the sound of gunfire was heard on campus; officials scramble to understand why. eSchool News - http://www.eschoolnews.com/iphone/top-story/index.cfm?i=56122#_56122, November 2008.
58. Jessica Bauer. Study: Text alerts may fail in real emergency. Diamondback Online - <http://media.www.diamondbackonline.com/media/storage/paper873/news/2008/10/14/News/Study.Text.Alerts.May.Fail.In.Real.Emergency-3485509.shtml>, October 2008.
59. Associated Press. Hackers Expected To Start Targeting Cell Phones. <http://cbs5.com/watercooler/Cell.Phones.Hackers.2.840909.html>, 2008.
60. Associated Press. College alert systems unreliable, study says. http://www.ajc.com/search/content/metro/stories/2008/09/25/college_campus_alerts.html, 2008.
61. Lee Shearer. Study: Campus alerts unreliable. Athens Banner Herald http://www.onlineathens.com/stories/092508/uga_336494829.shtml, 2008.
62. Bill Ray. 3G Americas warns against text warning systems. The Register - http://www.theregister.co.uk/2008/09/18/emergency_text/, 2008.
63. 3G Americas. 3G Americas Highlights New Research Report on Use of Cellular Text Messaging for Emergency Alert Services. 3G Americas http://www.3gamericas.org/English/news_room/DisplayPressRelease.cfm?id=3400&s=ENG, 2008.
64. Evan Koblentz. Web Exclusive: From Messaging to Management Duty. Wireless Week - <http://www.wirelessweek.com/Messaging-to-Management-Duty.aspx>, 2008.
65. Christopher Beam. How Do You Intercept a Text Message? Turn your cell phone into a spy gadget. Slate Magazine <http://www.slate.com/id/2161402/>, 2007.

66. **Jamming Cellphones with Text Messages.** Slashdot <http://it.slashdot.org/it/05/10/05/1839217.shtml?tid=215&tid=172>, 2005.
67. **Cell phone networks at risk?** CNN http://money.cnn.com/2005/10/05/technology/hacker_cellphones/, 2005.
68. **John Schwartz. Text Hackers Could Jam Cellphones, a Paper Says.** The New York Times <http://www.nytimes.com/2005/10/05/technology/05phone.html?ex=1286164800&en=d917b9cd43dfaa31&ei=5090&partner=rssuserland&emc=rss>, 2005.