

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Graham Merrett
U.S. Patent No.: 11,012,827 Attorney Docket No. 50095-0266IP1
Issue Date: May 18, 2021
Appl. Serial No.: 17/114,645
Filing Date: December 8, 2020
Title: RANDOM NUMBER DERIVED MESSAGE TRANSMISSION
 TO A THIRD PARTY PROVIDER

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: 4 November 2025

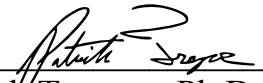
By: 
Patrick Traynor, Ph.D.

Table of Contents

I.	QUALIFICATIONS AND BACKGROUND INFORMATION.....	4
II.	LEGAL PRINCIPLES.....	11
	A. Anticipation.....	11
	B. Obviousness	12
III.	OVERVIEW OF CONCLUSIONS FORMED	13
IV.	BACKGROUND KNOWLEDGE ONE OF SKILL IN THE ART WOULD HAVE HAD PRIOR TO THE PRIORITY DATE OF THE '827 PATENT	13
V.	INTERPRETATIONS OF THE '827 PATENT CLAIMS AT ISSUE.....	14
VI.	THE '827 PATENT	15
	A. Overview of the '827 Patent.....	15
	B. Prosecution History of the '827 Patent.....	16
VII.	OVERVIEW OF PRIOR ART REFERENCES.....	16
	A. Overview of Horvath	18
	B. Overview of Tsampalis.....	23
	C. Overview of Tumminaro	28
	D. Overview of Dorenbosch.....	29
	E. Overview of Kansal	33
	F. Overview of Cottrell	35
	G. Overview of Lin.....	37
VIII.	GROUND 1A: CLAIMS 1, 7, 11, 16-21, 23, 25-27, 29-30 ARE OBVIOUS IN VIEW OF THE HORVATH-TSAMPALIS-TUMMINARO COMBINATION	37
	A. Combining Horvath, Tsampalis and Tumminaro	37
	B. Analysis with Respect to Claims 1, 7, 11, 16-21, 23, 25-27, 29-30.....	46
IX.	GROUND 1B: CLAIMS 2-3, 8, 28 ARE OBVIOUS IN VIEW OF THE HORVATH-TSAMPALIS-TUMMINARO-DORENBOSCH COMBINATION	125
	A. Combining Horvath, Tsampalis, Tumminaro and Dorenbosch.....	125
	B. Analysis with Respect to Claims 2-3, 8, 28.....	129
X.	GROUND 1C: CLAIMS 9, 12-13, 22, 24 ARE OBVIOUS IN VIEW OF THE HORVATH-TSAMPALIS-TUMMINARO-KANSAL COMBINATION	139
	A. Combining Horvath, Tsampalis, Tumminaro and Kansal.....	139
	B. Analysis with Respect to Claims 9, 12-13, 22, 24.....	142

XI.	GROUND 1D: CLAIMS 4-6 ARE OBVIOUS IN VIEW OF THE HORVATH-TSAMPALIS-TUMMINARO-COTTRELL COMBINATION	149
	A. Combining Horvath, Tsampalis, Tumminaro and Cottrell.....	149
	B. Analysis with Respect to Claims 4-6.....	152
XII.	GROUND 1E: CLAIMS 10, 14-15 ARE OBVIOUS IN VIEW OF THE HORVATH-TSAMPALIS-TUMMINARO-LIN COMBINATION.....	153
	A. Combining Horvath, Tsampalis, Tumminaro and Lin	153
	B. Analysis with Respect to Claims 10, 14-15.....	155
XIII.	CONCLUSION.....	159

DECLARATION OF DR. PATRICK TRAYNOR

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

I. QUALIFICATIONS AND BACKGROUND INFORMATION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- APPLE-1001 U.S. Patent No. 11,012,827 (“the ’827 Patent”)
- APPLE-1002 File History of U.S. Patent No. 11,012,827
- 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-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-1017 U.S. Patent No. 9,167,401 (“Helferich”)
- APPLE-1021 U.S. Patent No. (US 8,006,190) (“Quoc”)
- APPLE-1025 Qi et al., 2004, July. “Multimedia Messaging Service.” Available at https://www.zte.com.cn/global/about/magazine/zte-communications/2004/1/en_68/162264.html (“Qi”)
- APPLE-1026 RFC 3261 – SIP: Session Initiation Protocol. Available at <http://www.faqs.org/rfcs/rfc3261.html>. June 2002.
- APPLE-1032 U.S. Pub. No. 2008/0261577 (claiming priority to Provisional App. No. 60/913,187) (“Celik”)
- APPLE-1033 U.S. Provisional App. No. 60/913,187

- APPLE-1034 U.S. Pub. No. 2007/0233615 (“Tumminaro”)
- APPLE-1035 EP Pub. No. 1662812 (“Empower”)
- APPLE-1036 International Pub. No. WO 2007/052264 (“Agiv”)
- APPLE-1037 T-Mobile webpage <https://www.t-mobile.com/home-internet/the-signal/internet-help/the-complete-wifi-history>
- APPLE-1039 U.S. Pub. No. 2002/0173308 (“Dorenbosch”)
- APPLE-1040 PCT Pub. 2005/001660 (“Cottrell”)
- APPLE-1041 U.S. Pub. No. 2005/0233737 (“Lin”)
- APPLE-1042 U.S. Pub. No. 2005/0198124 (“McCarthy”)
- APPLE-1043 RFC 2778 – A Model for Presence and Instant Messaging (Feb. 2000, *available at* <https://datatracker.ietf.org/doc/html/rfc2778>)
- APPLE-1044 RFC 3428 – Session Initiation Protocol (SIP) for Instant Messaging (December 2002), *available at* <https://datatracker.ietf.org/doc/html/rfc3428>
- APPLE-1045 Open Mobile Alliance, Multimedia Messaging Service Encapsulation Protocol, Approved Version 1.2 (March 1, 2005), *available at* https://www.openmobilealliance.org/release/MMS/V1_2-20050301-A/OMA-MMS-ENC-V1_2-20050301-A.pdf
- APPLE-1046 U.S. Patent. No. 9,467,530 (“Belimpasakis”)
- APPLE-1047 Krakow, Wireless Industry Pushes TV for Your Cell Phone, NBC News (Feb. 14, 2006), *available at* <https://www.nbcnews.com/id/wbna11345651>
- APPLE-1048 3G/UMTS Towards Mobile Broadband and Personal Internet, A White Paper from The UMTS Forum (October 2005), *available at* https://www.3gpp.org/ftp/pcg/pcg_15/docs/pdf/PCG15_22.pdf

- APPLE-1049 ETSI TS 133.203 v7.3.0, Digital Cellular Telecommunications System (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G Security; Access Security for IP-based Services (Sept. 2006), *available at* https://www.etsi.org/deliver/etsi_ts/133200_133299/133203/07.03.00_60/ts_133203v070300p.pdf
- APPLE-1050 U.S. Patent No. 7,069,008 (“Hill”)
- APPLE-1051 U.S. Pub. No. 2005/0125547 (“Ahonen”)
- APPLE-1052 U.S. Patent No. 9,036,620 (“Procopio”)
- APPLE-1053 U.S. Pub. No. 2008/0153459 (“Kansal”)
- APPLE-1054 U.S. Pub. No. 2005/0002407 (“Shaheen”)
- APPLE-1055 U.S. Pub. No. 2008/0198811 (“Deshpande”)
- APPLE-1056 U.S. Pub. No. 2006/0282518 (“Karaoguz”)
- APPLE-1057 U.S. Pub. No. 20070110076 (“Brouwer”)
- APPLE-1058 Le Bodic, Mobile Messaging Techs. and Services: SMS, EMS and MMS, Wiley Press (2nd Ed.) (2005)
- APPLE-1059 WIRELESS Waypoint, Understanding SS7 and Intelligent Networks, *available at* <https://wirelesswaypoint.com/understanding-ss7-and-intelligent-networks>
- APPLE-1060 U.S. Patent No. 8,190,878 (“Stern”)
- APPLE-1061 U.S. Pub. No. 2008/0293378 (“Hinton”)
- APPLE-1062 Merriam-Webster Dictionary – “Subscribe”
- APPLE-1063 RFC 2779 – Instant Messaging / Presence Protocol Requirements, *available at* <https://www.rfc-editor.org/rfc/pdf/rfc2779.txt.pdf>

- APPLE-1064 RFC 3856 – A Presence Event Package for the Session Initiation Protocol (SIP), *available at* <https://www.rfc-editor.org/rfc/pdf/rfc3856.txt.pdf>
- APPLE-1065 U.S. Pub. No. 2008/0120427 (“Ramanathan”)
- APPLE-1066 Trillian Pro v1.0 webpage (“Trillian”)
- APPLE-1067 U.S. Pub. No. 2007/0004461 (“Bathina”)
- 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 ’827 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 '827 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 '827 Patent are obvious over Horvath in view of Tsampalis, Tumminaro, Dorenbosch, Kansal, Cottrell, and Lin.

IV. BACKGROUND KNOWLEDGE ONE OF SKILL IN THE ART WOULD HAVE HAD PRIOR TO THE PRIORITY DATE OF THE '827 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 '827

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 '827 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 '827 PATENT

A. Overview of the '827 Patent

24. The '827 Patent describes techniques for messaging over wireless networks in which a sending wireless device selects a bearer for sending a message based on information indicating whether an intended recipient of the message is a subscriber of a service for receiving messages via a packet-switched messaging service. APPLE-1001, 2:31-3:2, 7:45-9:57, Abstract. The Abstract summarizes the disclosed techniques as follows:

A mobile wireless device may transmit message content intended for a third party provider, to a server associated with the service, which forwards a message comprising the message content intended for the third party provider, to the third party provider. The message forwarded to the third party provider may be derived at least in part from a random number. The message forwarded to the third party provider may not be identical to a message transmitted by the mobile wireless device comprising the message content intended for the third party provider. The message transmitted by the mobile wireless device comprising the message content intended for the third party provider may include at least one information element which is not included in the message forwarded to the third party provider.

APPLE-1001, Abstract.

25. FIG. 1 is a diagram of an example messaging system in the '827 Patent:

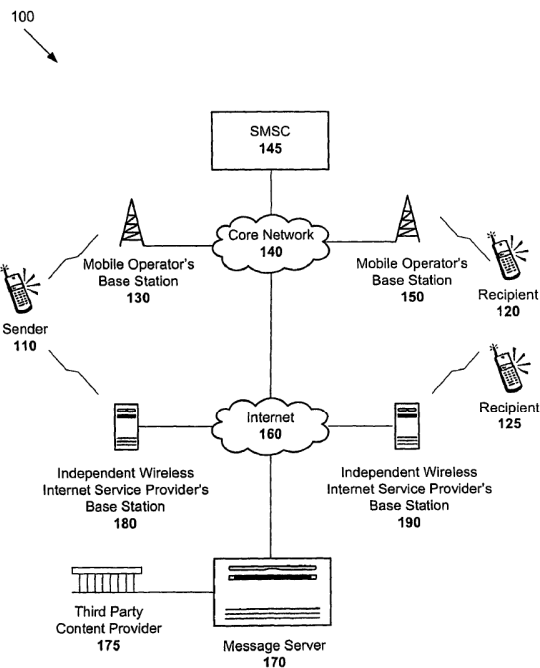


FIG. 1

APPLE-1001, FIG. 1

B. Prosecution History of the '827 Patent

26. No prior art rejections were discussed during prosecution of the application that issued as the '827 Patent. The only rejection was for obviousness-type double patenting over a related patent, which was withdrawn following the applicant's submission of a terminal disclaimer. APPLE-1002, 21-22, 50-54.

VII. OVERVIEW OF PRIOR ART REFERENCES

27. Horvath, Tsampalis, Tumminaro, Dorenbosch, Kansal, Lin, and Cottrell are all analogous art, each being in the field of endeavor (mobile messaging over wireless networks) and reasonably pertinent to the problems said to be

addressed by the '827 Patent. APPLE-1001, Title, Abstract; APPLE-1004, Title, Abstract; APPLE-1005, Title, Abstract; APPLE-1053, Abstract; APPLE-1034, Title, Abstract, [0031]; APPLE-1039, Abstract; APPLE-1040, Abstract; APPLE-1041, Title, Abstract; *infra*, §§VIII-XII. Like the '827 Patent, Horvath, Tsampalis, Tumminaro, Dorenbosch, Kansal, Lin, and Cottrell each seek to provide users with a wider range of messaging options. APPLE-1001, 3:18-25; *See* APPLE-1004, [0009] (ability to select wider range of message delivery networks); APPLE-1005, [0065] (“ability to select a format in which to send a message based upon the messaging capabilities of the intended recipient(s) of the message”); APPLE-1039, [0002] (improving use of instant messaging on mobile devices); APPLE-1053, [0009] (“a mobile computing device may send and receive messages of different types”); APPLE-1034, Title, Abstract, [0031] (messaging options for mobile payment transactions); APPLE-1041, Abstract (ability to use mobile messaging for “instant messaging conferencing”), [0017]-[0018]; APPLE-1040, [0018] (improving privacy in messaging through a “secure network privacy service”), [0009].

A. Overview of Horvath¹

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

¹ General descriptions provided for 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.

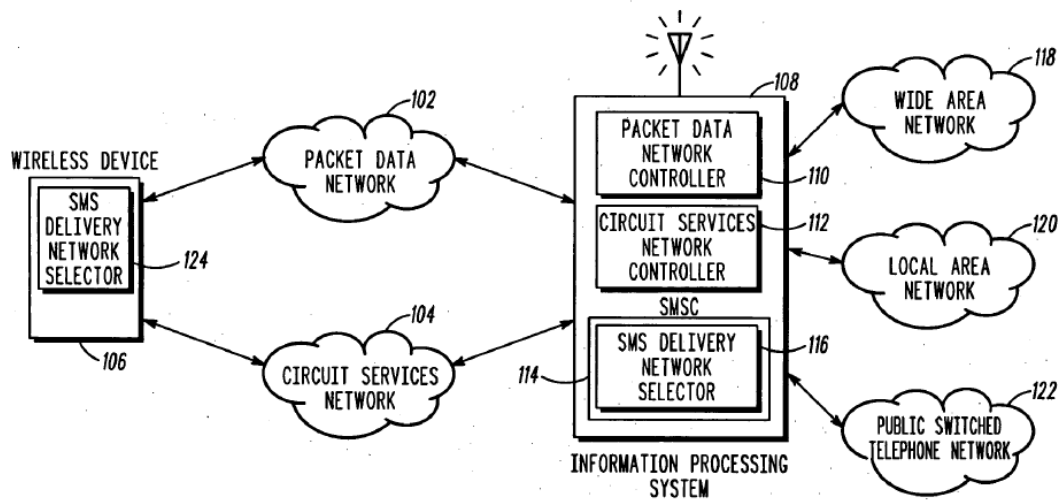
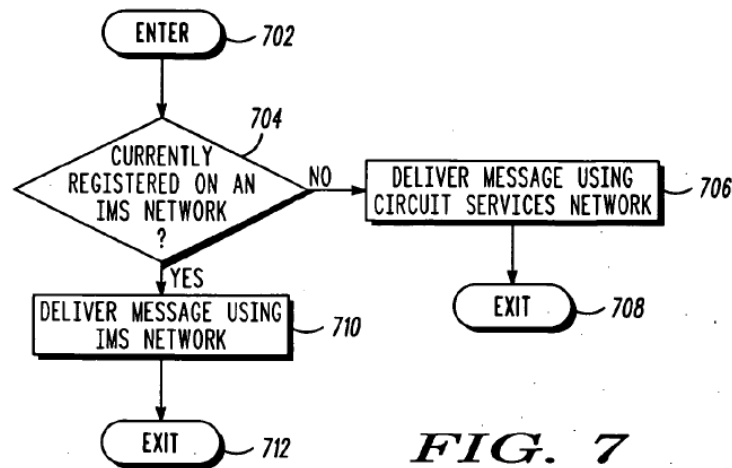


FIG. 1

APPLE-1004, FIG. 1

29. As shown in FIG. 1, wireless device 106 can function both as a sender device that sends messages destined for remote recipient device(s) and as a recipient device that receives message(s) sent from remote sender device(s). When wireless device 106 is instructed to send an SMS message (operating as a sender device), “the wireless device 106 first determines if it [*i.e.*, the sending wireless device] is registered on the packet data network 102,” and based on this determination, an “SMS delivery network selector 124” residing on the wireless device 106 “selects a network 102, 104 for the wireless device 106 to transmit [the] SMS message on.” APPLE-1004, [0050], [0062] (“[I]f the wireless device 106 is registered on the packet data network 102, the SMS delivery network selector 124 selects the packet data network 102 for transmission of the SMS message. If the wireless device is not

registered on the packet data network 102, the SMS delivery network selector 124 selects the circuit services network 104 for transmission of the SMS message.”), [0078], FIGS. 1, 4, 7.



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

30. 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.

31. 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]-[0076], FIGS. 1, 2, 3, 6. By delivering messages to wireless devices over a packet-data network rather

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

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].

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

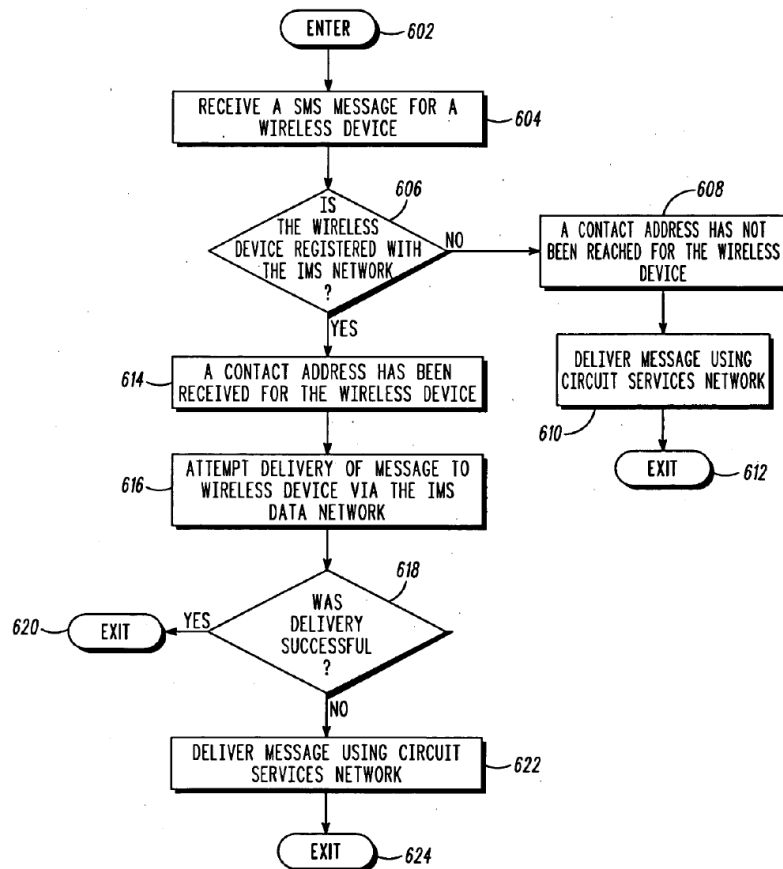
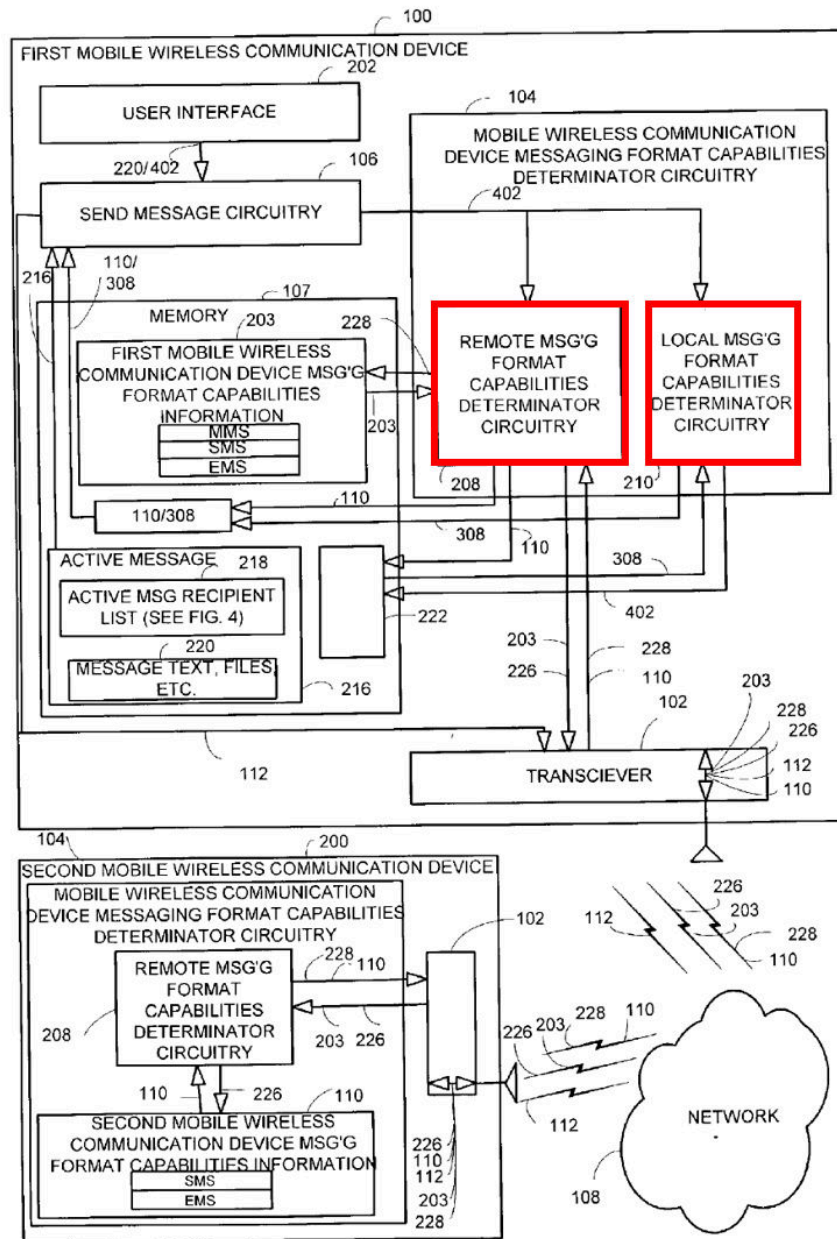


FIG. 6
APPLE-1004, FIG. 6 (SMSC Perspective)

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.

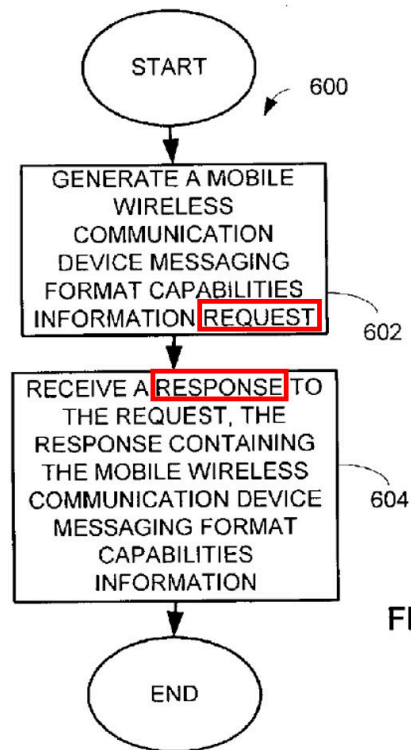
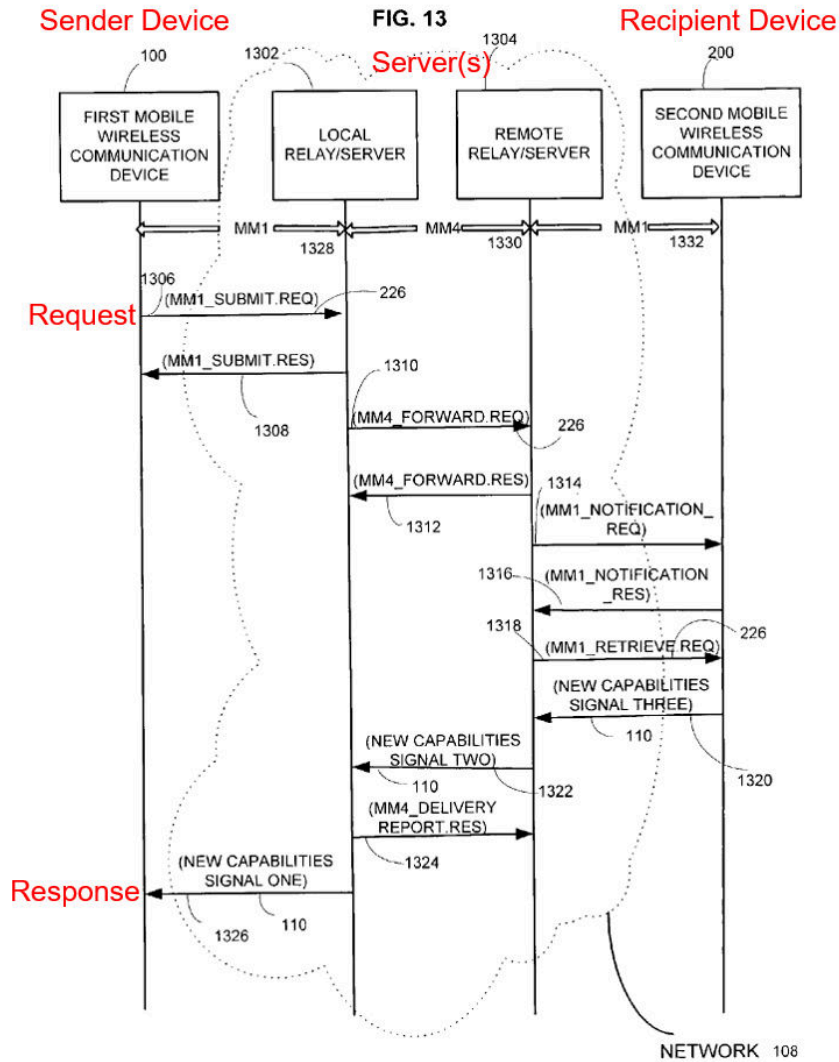


FIG. 6

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 Tumminaro

37. Tumminaro describes “a mobile payment system where consumers may conduct transactions using a mobile device such as a mobile telephone, smartphone, personal digital assistant or similar portable wireless handheld device.” APPLE-1034, Abstract. “Transactions may be requested through any number of means including SMS messaging, Web, e-mail, instant messenger, a mobile client application, an instant messaging plug-in application or ‘widget.’” *Id.*, [0031], [0350]. For example, Tumminaro discloses techniques that “provide[] for the initiation of [a] financial transaction by way of SMS text message. The SMS message starts with a key word that provides the type of transaction requested” and “[a]fter the key word, the amount is entered,” followed by “the target telephone number.” *Id.*, [0205]-[0206]. The sending device can also add “a unique sequence number” such as “a random number” to the message that uniquely identifies the transaction and “help[s] prevent spoof attacks, “fraud,” and “duplication of financial transactions.” *Id.*, [0607]-[0608]. Transaction requests are sent from the sending mobile phone “to the mobile operator” and are “then routed to [a] payment server through a secure Internet connection.” *Id.*, [0202].

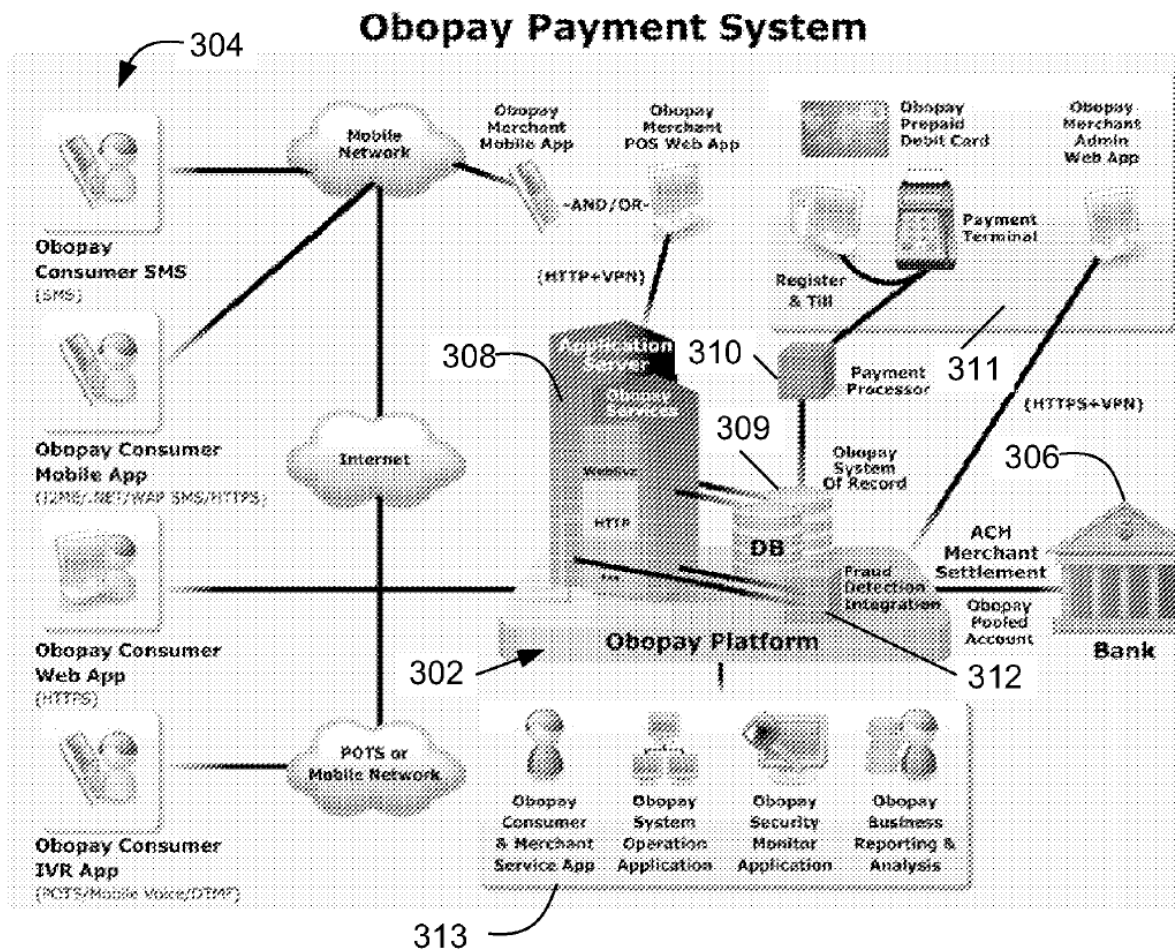


Fig. 3

APPLE-1034, FIG. 3

D. Overview of Dorenbosch

38. Dorenbosch explains that then-conventional “IM systems typically rel[ied] on a best-effort delivery mechanism in which a message intended for a target buddy is delivered if the IM login server determines that the target buddy is available.” APPLE-1039, [0005]. “If the IM login server determine[d] that the

target buddy is not available, the message [was] dropped.” *Id.* Indeed, Dorenbosch attributes “considerable delay” and “high cost” to establishing and maintaining an open IM session connection over a circuit-switched mobile network. *Id.*, [0006]. As illustrated in FIG. 1 (below), Dorenbosch mitigates these issues with “an instant message proxy that is capable of maintaining the availability status of a mobile subscriber when the communicati[on] to the subscriber is temporarily broken.” APPLE-1039, [0002]. Dorenbosch teaches two related techniques that (1) help reduce dropped messages and (2) “minimize system connection overhead in a manner that also minimizes the amount of latency introduced into the system,” respectively. *See* APPLE-1039, [0020], [0024], [0029], [0030], [0036], [0039]-[0040].

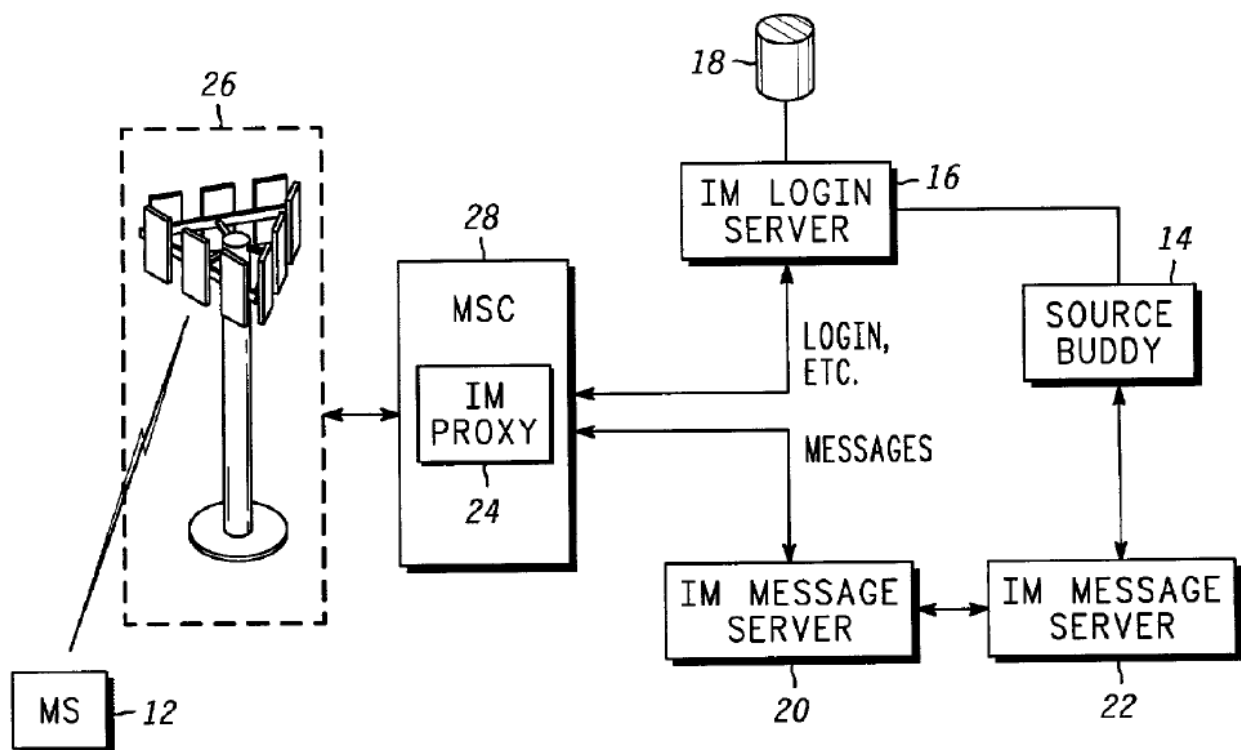


FIG. 1 10

APPLE-1039, FIG. 1

39. In one aspect, Dorenbosch describes “an IM session involving [a] mobile subscriber 12 and multiple buddies, such as conventional subscribers 14, 14' and 14”, in which [an] IM proxy 24 stores and bundles IMs in its buffer 36 from the conventional subscribers 14, 14' and 14” based on predetermined participant parameters.” APPLE-1039, [0036]. “When the IM proxy 24' determines that download parameters have been met, the IM proxy 24' establishes a connection with the mobile subscriber 12 and at 122 downloads the stored and bundled messages to the mobile subscriber 12.” APPLE-1039, [0037]. Two examples of download

parameters are: (1) when “more than a predetermined number of messages are stored” and (2) “a predetermined buffer memory threshold is exceeded.” APPLE-1039, [0040]. To illustrate, the proxy “flushes the IM proxy buffer” by sending the stored messages to the mobile device when the number of messages stored in the IM proxy’s buffer exceed a threshold number of messages, or when those messages exceed a threshold amount of that buffer’s memory. APPLE-1039, [0039]-[0040].

40. In another aspect of Dorenbosch’s system, if a mobile IM subscriber temporarily loses network coverage and is therefore unavailable to receive messages, the IM proxy will continue to store messages in the message buffer and retry sending the message(s) (*e.g.*, a predetermined number of times within a predetermined time period) before dropping the message(s) from the buffer. APPLE-1039, [0020], [0024]. Dorenbosch describes a retry counter and timer that “enable the IM proxy 24 to maintain its IP connection with the IM login server 16, and therefore maintain the mobile subscriber’s registered status with the IM login server 16, when the mobile subscriber 12 becomes temporarily unavailable due to roaming or the like.” APPLE-1039, [0020]. In this way, even when a mobile subscriber has poor network coverage, the Dorenbosch interface reflects availability of the mobile subscribers. APPLE-1039, [0024]; *see also id.* [0030]. Only after the mobile subscriber “becomes unavailable for receiving instant messages for a period of time that exceeds the number of retries allotted by and programmed into the retry

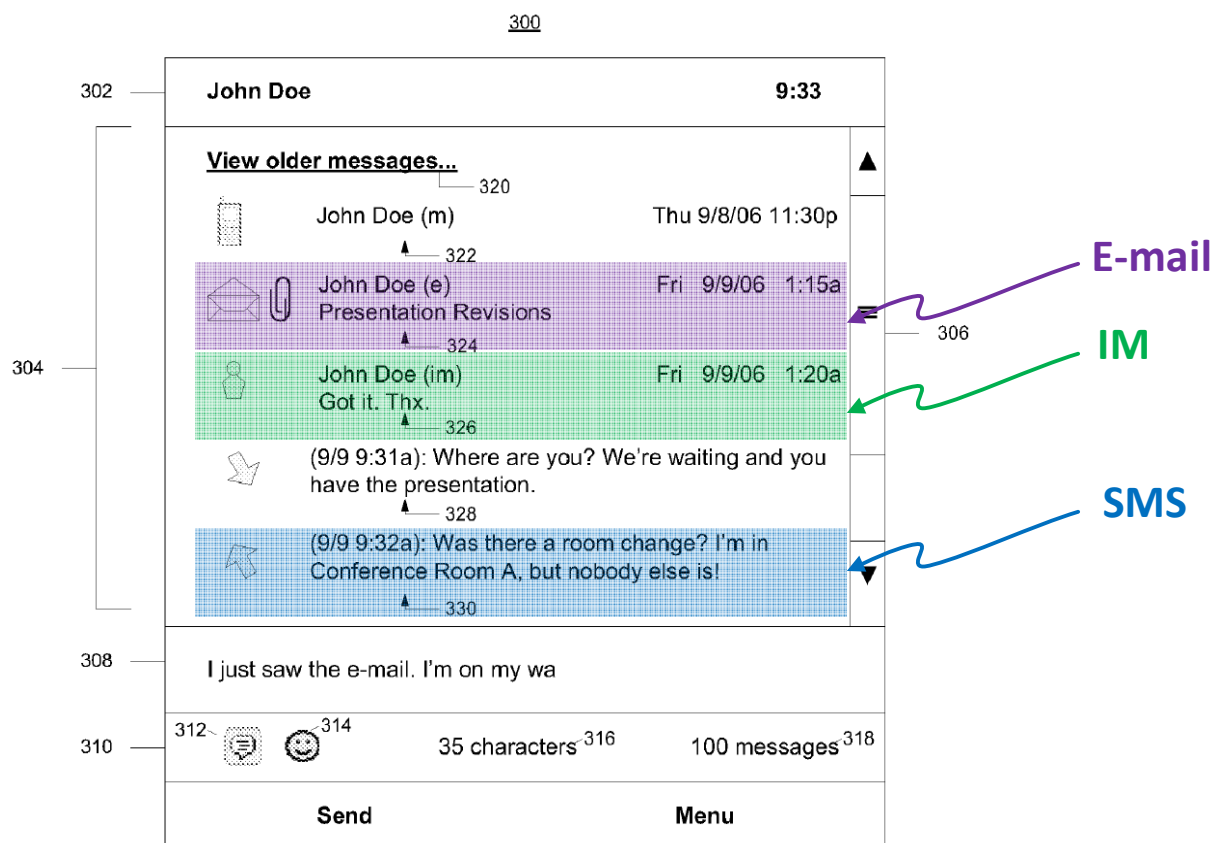
counter and/or the predetermined time period allotted by the timer” will the IM proxy drop “its connection with the IM login server 16” and “indicat[e] to the IM server 16 that the mobile subscriber 12 is unavailable.” APPLE-1039, [0028]-[0029].

41. A POSITA would have understood that implementing these two aspects of Dorenbosch’s disclosure together would achieve the benefits of each individually. When implemented together, Dorenbosch’s IM proxy bundles messages in a message buffer until “more than a predetermined number of messages are stored,” at which point the proxy attempts to forward the bundled messages to the mobile subscriber. APPLE-1039, [0038]-[0040]. The IM proxy will maintain a connection with the IM login server even when the mobile subscriber temporarily loses network coverage, and other IM subscribers will continue to see the mobile subscriber as “available” and be able to send the mobile subscriber messages. APPLE-1039, [0024], [0030]. If the IM proxy attempts to forward the bundle of messages to the mobile subscriber and is not able, the IM proxy will retry sending the bundle a certain number of times within a certain period, after which it will drop the message(s) and indicate to the IM login server that the mobile subscriber is unavailable. APPLE-1039, [0020], [0024], [0029].

E. Overview of Kansal

42. Like Horvath and Tsampalis, Kansal describes mobile messaging services for sending and receiving messages of different formats. APPLE-1053,

Abstract, [0009], [0035] (“an IM application,” “an SMS application,” and “an MMS application”). Kansal presents a tool for correlating and aggregating for display all messages received by a “particular recipient,” including each of several message types/formats (*e.g.*, SMS, IM, MMS), without regard for the network over which the messages are received. APPLE-1053, [0009]; [0040]-[0043]; [0066]-[0069]; FIGs. 2-3 (shown below).



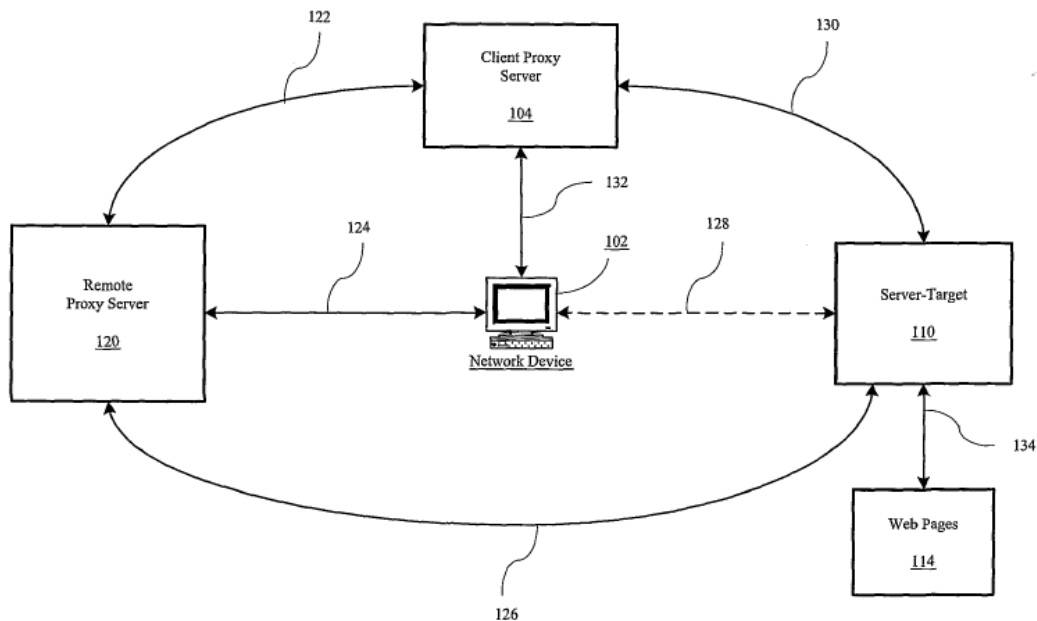
APPLE-1053, FIG. 3 (Annotated)

43. As shown above, Kansal describes a “unified messaging UI” from which a user may view received messages of various messaging types and may select from a variety of types when composing and sending a response, demonstrating the

utility and viability of integration. APPLE-1053, [0062], [0077]-[0078]. In particular, the unified messaging UI “display[s] a messaging thread comprising correlated messages of different message types,” including “SMS messages, MMS messages, as well as, telephone messages, voicemail messages, fax messages, video conferencing messages, IM messages, and e-mail messages.” APPLE-1053, [0009], [0045]-[0046], [0054]-[0056], [0062]-[0064], [0070], [0077]-[0078], FIGs. 2-3.

F. Overview of Cottrell

44. Cottrell describes a “secure network privacy system” that enhances security and protects users’ privacy by intercepting and modifying communications between a network device and a target server. APPLE-1040, [002]-[009], [019]-[022], [024], [0051], FIGs. 1-2, 5. FIG. 1 is a block diagram representing major components of Cottrell’s system, including a network device 102, a client proxy server 104, and a server-target 110:



APPLE-1040, FIG. 1

45. Cottrell explains that “the Remote Proxy Server 120 relay[s] data from the client on the Network Device 102 to the Server-Target 110 hosting the content or service the Network Device 102 may be attempting to connect to and/or access.” APPLE-1041, [022]. The Remote Proxy Server intercepts communications between the network device 102 and Server-Target 110 and performs various privacy-enhancing operations including “adding, changing, or removing text, data, information, scripts, or other content” sent by or directed to the network device 102. *Id.* The Remote Proxy Server can “replace sensitive information like-email addresses or credit card numbers with either false information or alternative information” to shield the sensitive information from the Server-Target. *Id.*, [024]. The substituted information can include “personal information related to the user,

such as real name, address, phone number, etc., with alternative information for purposes of identity protection, privacy, and tracking prevention.” *Id.*, [051].

G. Overview of Lin

46. 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-1041, [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, 7, 11, 16-21, 23, 25-27, 29-30 ARE OBVIOUS IN VIEW OF THE HORVATH-TSAMPALIS-TUMMINARO COMBINATION

A. Combining Horvath, Tsampalis and Tumminaro

47. Like the ’827 Patent, Horvath describes techniques for selectively transmitting wireless messages via different transmission bearers, including techniques for transmitting messages over either a packet-data network or a circuit-services network. APPLE-1001, 2:64-3:27; APPLE-1004, [0001], [0007], [0024]-[0026], [0050], [0061]-[0062], FIGS. 1, 4, 7; *supra*, §VII.A (Horvath Overview). In seeking to keep the circuit-services network “unnecessarily burdened with SMS traffic,” Horvath proposes defaulting to use of a packet-data network for

transmission of messages whenever the sending and receiving devices are registered with the IMS on the packet-data network. *See e.g.*, APPLE-1004, [0004], [0006]-[0009], [0021], [0039] (goal to provide “capacity relief on the circuit services network 104”), [0081] (desire to “provide dynamic optimization of the resources available” and to “optimiz[e] network resources”). With this approach, Horvath diverts some of the load otherwise carried by and burdening the circuit switched network. APPLE-1004, [0004], [0009]. Still, a POSITA would have recognized that Horvath’s system was ripe for improvement. For example, although Horvath describes messaging services apart from SMS (*e.g.*, MMS, EMS, IM), Horvath leaves various implementation details relating to these services to the discretion of a POSITA. APPLE-1005, [0025], [0039]. Additionally, a POSITA would have appreciated from Horvath that different users did not all subscribe to the same messaging services, leaving some users with relatively limited messaging capabilities that precluded them from receiving or processing richer media formats beyond SMS (*e.g.*, MMS and IM), despite other users sending messages in those richer media formats. Without more, this leaves a Horvath sender device vulnerable to sending a message in a format that a Horvath recipient device would be incapable of processing or presenting to a user. And while Horvath describes example uses of mobile messaging for facilitating communication between mobile devices, Horvath does not specifically address the wide range of uses of mobile messaging that were

known by the mid-2000s, including messaging to obtain services from a third-party provider.

(i) ***Tsampalis's Message-Format-Capabilities Determination***

48. In a multi-modal messaging environment like Horvath's in which different mobile device users subscribed to different messaging services (*e.g.*, SMS, MMS, EMS, IM), a POSITA would have been led by Tsampalis to improve the user experience and better manage and coordinate messaging formats. *Supra*, VII.A (Horvath Overview); §VII.B (Tsampalis Overview). Tsampalis describes an effective solution for improving messaging in such an environment by sharing information about the recipient's messaging capabilities with the sender. *Supra*, §VII.B. For multiple reasons, a POSITA reviewing Horvath and Tsampalis would have found it obvious to implement Horvath's system in accordance with Tsampalis's suggestions for a sender device to obtain and use messaging capabilities information of a recipient device to determine how to format and transmit an outgoing message to the recipient.

49. 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 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” SMS encapsulated in a SIP MESSAGE versus encoding and transmission according to the “ANSI-41” standard).

50. Second, a POSITA would have sought to leverage Tsampalis-like messaging format capabilities information in Horvath’s system to permit the sender to make more frequent and reliable use of enhanced messaging formats such as MMS and IM. Enhanced messaging formats such as MMS and IM generally offer richer messaging capabilities than SMS, such as the ability to support extended character counts for longer messages and the ability to attach/include multimedia files with the message. APPLE-1007, Page 8 (“IM&P [*i.e.*, Instant Messaging and Presence]

service is more media-rich than traditional applications such as mail, phone, and email. By using IM&P, we can deliver voice, video, and data together to various endpoints.”); APPLE-1025, Introduction (“The most significant characteristic of MMS is to support multimedia contents. It can send not only texts, but also images, videos and audios. Therefore, MMS applications are much richer than those of SMS.”). A POSITA would have understood that the enhanced messaging capabilities of MMS and IM were often desirable for situations where users desired to communicate more than the short, text-based messages that could be accommodated by SMS. If the recipient’s messaging capabilities were unknown, however, some senders would have been biased toward not using any of the enhanced messaging features of MMS or IM to ensure the message was 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.

51. Third, 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 understood that integration of Tsampalis’s techniques in the combination would enhance the sender’s ability to select 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.

52. Fourth, a POSITA would have found it obvious to combine the teachings of Horvath with Tsampalis because the combination merely involves the application of a known technique to a known system to achieve predictable results. Here, Tsampalis recognized a known problem with dynamic messaging environments like Horvath’s 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.

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 '827 Patent. Further, the techniques that would be integrated from Tsampalis in the Horvath-Tsmpalis combination are fully compatible with Horvath's and would not disturb the ability of Horvath's system to transmit or deliver SMS messages over either a packet-based or circuit switched network.

(ii) ***Tumminaro's Mobile Messaging for
Mobile Payment Transactions***

54. In view of the multi-modal messaging capabilities of the Horvath-Tsmpalis wireless device 106, a POSITA would have looked to references that describe useful applications of mobile messaging services that could be implemented using the Horvath-Tsmpalis system. Tumminaro is one such reference. *Supra*, § VII.C (Tumminaro Overview). As discussed above, Tumminaro describes an application of mobile messaging for conveniently conducting payment transactions with a mobile phone. *Supra*, § VII.C. For multiple reasons, a POSITA reviewing Horvath, Tsmpalis, and Tumminaro would have found it obvious to further modify the Horvath-Tsmpalis system described above (*supra*, § VIII.A(i)) by applying Tumminaro's techniques for a wireless device to use mobile messaging services (e.g., SMS, MMS, IM) to initiate and conduct transactions with a third-party provider based on parameters specified in messages transmitted by the wireless device.

55. First, a POSITA would have further combined the Horvath-Tsmpalis system with Tumminaro to beneficially achieve "a mobile payment system (MPS)

or mobile person-to-person payment system that allows fast and easy money transactions.” APPLE-1034, [0032]. Tumminaro recognized that “[t]he mobile phone is becoming more and more ubiquitous around the world” and “[m]any people carry a mobile phone or similar portable communications device, even if they do not carry a wallet around with them as they go about their daily lives.” APPLE-1034, [0032]. Integration of Tumminaro’s mobile payment techniques in the Horvath-Tsampalis system would have allowed users to more conveniently conduct transactions at various places with their mobile phones and wireless devices without the inconvenience of additionally carrying cash or a wallet that would otherwise be needed for such transactions.

56. Second, a POSITA would have been motivated to apply Tumminaro’s mobile payment techniques in combination with Horvath-Tsampalis to achieve the express benefits of mobile payment transactions described in Tumminaro. For example, Tumminaro explains that its electronic payment system “encourage[s] cash to stay in the bank (instead of consumer’s pockets),” “are safe and traceable,” “occur in near-real-time,” “are accessible to anyone, an-time and any-place,” “optimize load or unload processing (*i.e.*, performing load or unload within bank when possible),” “facilitates electronic payments in a cross carrier or cross network manner,” and “facilities electronic payments in a cross device or cross channel manner (*i.e.*, mobile, e-mail, Web, instant messenger).” APPLE-1034, [0034].

57. Third, a POSITA would have pursued the combination with Tumminaro to make better and more expansive use of existing messaging capabilities on the Horvath-Tsampalis wireless device. Horvath and Tsampalis describe multi-modal messaging environments that allow a user to make use of a variety of different messaging formats and capabilities (*e.g.*, IM, MMS, SMS), and application of Tumminaro's techniques would further improve the messaging environment in the combination by allowing the wireless device to not only message with other users but also with a payment server that facilitates various forms of payment and financial transactions.

58. Fourth, a POSITA would have found it obvious to combine the teachings of Horvath and Tsampalis with Tumminaro because the combination merely involves the application of a known technique to a known system to achieve predictable results. Here, Horvath and Tsampalis each describe multi-modal messaging environments capable of sending a variety of messages from a wireless device and Tumminaro describes a known option for using the same types of messaging capabilities described in Horvath and Tsampalis to conduct mobile payment transactions. The combination is thus straightforward and well within the skill of a POSITA.

59. A POSITA would have reasonably expected success applying Tumminaro's mobile payment techniques in combination with Horvath and

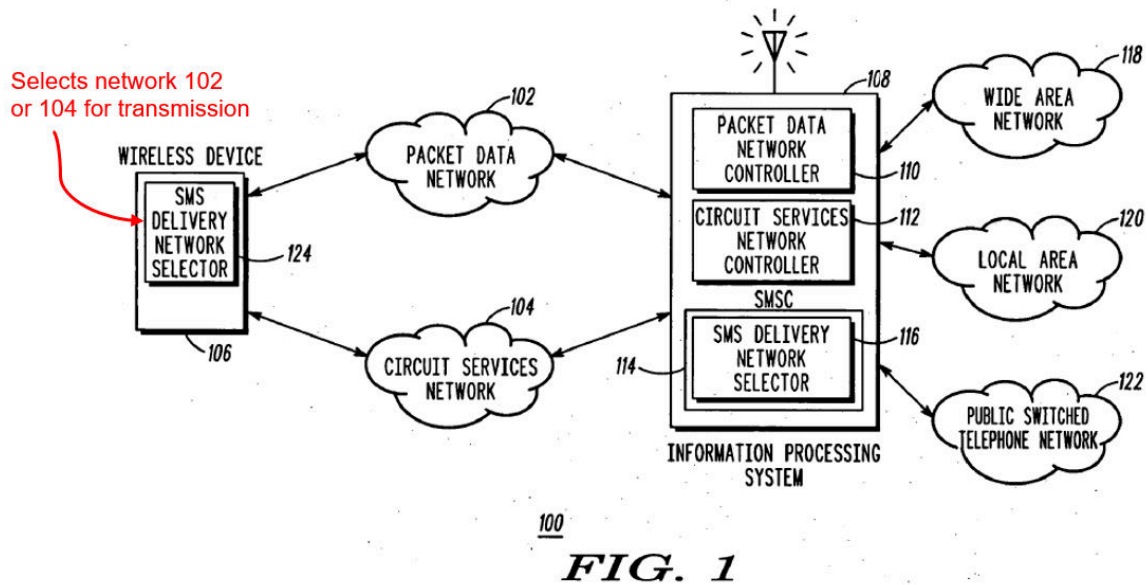
Tsampalis, especially since the system in the resulting combination could be implemented with conventional software and hardware (e.g., general-purpose processors on mobile devices executing programmable instructions) with messaging formats (e.g., SMS, MMS, IM) that were well-defined and commonly implemented before the Critical Date of the '827 Patent.

B. Analysis with Respect to Claims 1, 7, 11, 16-21, 23, 25-27, 29-30

Element [1pre]: A mobile wireless device that transmits (i) at least some messages to at least some recipient devices that correspond to subscribers of a service for receiving packet-switched messages, wherein the service includes a server that receives packet-switched messages transmitted via the service to recipient devices that correspond to subscribers of the service, and (ii) at least some messages over a cellular network to at least some recipient devices that do not correspond to subscribers of the service, the mobile wireless device comprising:

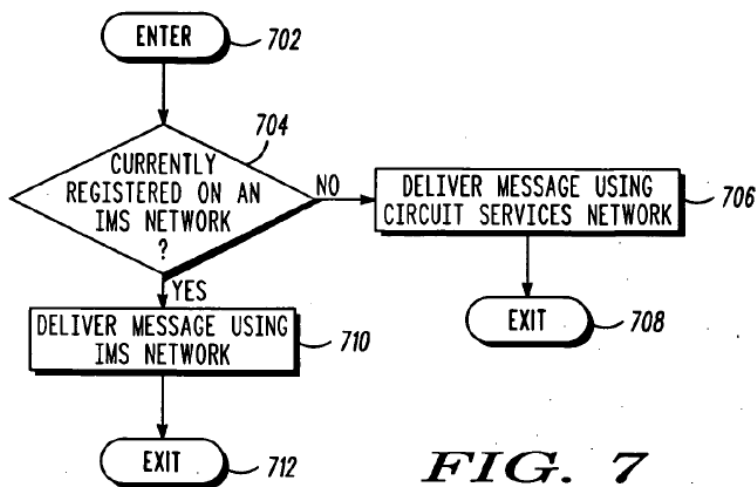
60. To the extent the preamble is limiting, Horvath-Tsampalis-Tumminaro renders [1pre] obvious. Horvath's FIG. 1 (below) shows an example "wireless device 106" (***a mobile wireless device***³) that transmits messages on "either [a] packet data network 102 or [a] circuit services network 104." APPLE-1004, [0014], [0060]-[0070], FIG. 4; *see also id.*, FIGS. 2, 4. "The SMS delivery network selector 124 selects a network 102, 104 for the wireless device 106 to transmit a SMS message on." APPLE-1004, [0062].

³ Bold and italicized text corresponds to claim language.



APPLE-1004, FIG. 1 (Annotated)

61. Horvath's FIG. 7 (below) further shows the sending mobile phone "select[ing] a network for transmitting a [] message based on what network the wireless device is registered with." APPLE-1004, [0078]; *see also id.*, [0009], [0050].



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

62. According to Horvath, wireless device 106 sends short message service (SMS) messages, “through a circuit services network” “using the traditional circuit services network method (for example, ANSI-41 procedures)” if wireless device 106 “is unregistered with” “a registrar associated with a session initiation protocol [SIP] network for communicating over a packet data network.” APPLE-1004, [0002], [0006]-[0007], [0050]. The circuit-services network 104 is included in a **cellular network** such as a “Global System for Mobile Communications (GSM)” network that provides “mobile text messaging” and “voice services” including “push-to-talk over cellular communications.” APPLE-1004, [0025]-[0026].

63. A short message service center (SMSC) 114 receives SMS messages transmitted by the sending wireless device 106 over the circuit-services network 104, and “[i]f the recipient device is not registered on the packet data network 102” (*e.g.*, if the recipient device is not registered with the “registrar associated with a session initiation protocol [SIP] network for communicating over a packet data network”), then “the SMSC 114 delivers the SMS message to the recipient device through the traditional circuit services network method (for example, ANSI-41 procedures)” over circuit-services network 104. APPLE-1004, [0047]; *see also id.*, [0002], [0006]-[0007], [0050], [0053], [0062], FIG. 7. Horvath explains a recipient device “may not be registered on the packet data network 102 because it was never registered to begin with, because it deregistered, or because it lost its coverage.” *Id.*,

[0047]. A recipient device that “was never registered to begin with” does “*not correspond to [a] subscriber*” of the IMS or its supported services.

64. On the other hand, when the sending wireless device 106 “[is] registered with the [SIP] registrar,” device 106 sends “SIP message[s]” in “SIP packets” (*packet switched messages*) “through the [SIP] network communicating over the packet data network.” APPLE-1004, [0002], [0006]-[0007], [0017], [0024], [0034], [0037] (messages are sent over the SIP network in “SIP packets”), [0038], [0039], [0041], [0050], [0078], FIG. 7. Horvath explains that “an Internet Protocol multimedia subsystem (‘IMS’) core [] supports the SIP network,” and the “IMS system [] includes application servers that host and execute services for the wireless device 106” such as SMS, MMS, and instant messaging (“IM”) services. APPLE-1004, [0033]-[0034], [0039]; *see also id.*, [0033] (“The SIP network is used for establishing instant messaging...and other real-time communications over the Internet.”), [0039] (“A service for example, is SMS, MMS, ... and the like.”). The IM and MMS messaging services are each a “*service for receiving packet-switched messages*” as claimed.

65. SMS is another service supported by the IMS, and Horvath’s detailed description of SIP messaging for the SMS service exemplifies how a POSITA would have understood SIP messaging for the IM and MMS services to similarly operate. For example, Horvath explains how the SMS service routes

SMS messages over the SIP network from a sending device to a receiving device by having the sending device “encode[] the IS-637 content” of an SMS message “as the payload of [a] SIP MESSAGE” that is delivered over the SIP network to the recipient device, which then extracts the SMS message from the SIP MESSAGE. APPLE-1004, [0050]. Because SIP MESSAGEs were developed for the specific purpose of instant messaging and encapsulating any of a wide range of payloads for routing through a SIP network, a POSITA would have understood or it would have been obvious for Horvath’s SIP MESSAGES to encapsulate MMS and IM messages for the MMS and IM services described in Horvath, respectively, similar to the encapsulation of SMS messages for the SMS service. APPLE-1044, 1 (“[T]HE MESSAGE method, an extension to the Session Initiation Protocol (SIP) that allows the transfer of Instant Messages. ... MESSAGE requests carry the content in the form of MIME body parts.”), 3 (SIP MESSAGES “carry the instant message content in the request body”), 4 (SIP MESSAGE “body can be of any MIME type”); APPLE-1045, 5 (describing MMS MIME type “application/vnd.wap.mms-message”), 4 and 7 (“MMS PDUs” are “based on the well-known message structure of Internet email which is defined in ... [RFC2045],” “Multipurpose Internet Mail Extensions (MIME) Part One”); APPLE-1007, 3-4 (“By introducing SIP extensions, MESSAGE, SUBSCRIBE, and NOTIFY methods ..., SIP can deliver presence information and IMs.”).

66. Horvath further discloses that the recipients of SIP MESSAGES are registered with the IMS and are subscribers to supported messaging services (*e.g.*, IM, MMS) (*subscribers of the service*). For example, Horvath describes how “application servers ... host and execute services for the wireless device 106” and how the “application server[s]” are configured for “transmitting/delivering” messages “through the packet data network 102 using the IMS network.” APPLE-1004, [0039]. Recipient devices “subscribe[]” to the services hosted by the application servers, and if a subscribed device is currently registered, then the application server (*e.g.*, SMSC 114) delivers SIP MESSAGES for corresponding services to the wireless devices 106 that are the intended recipients of the messages. *Id.*, [0035] (“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.”), [0038] (“determines which application server(s) to forward the SIP message associated with the wireless device 105 so that the services subscribed to by the device 106 can be provided”), [0046] (“upon receiving notification of the device having registered at the registrar, determines that the recipient device is registered on the packet data network 102” and “delivers the SMS message to the recipient device through the packet data network 102 via the SIP network”), [0053], [0062].

67. Horvath discloses that the IMS core that supports the SIP network is comprised of functional components including a proxy-call-session-control function (P-CSCF) 206, an interrogating/serving-call-session-control function (I,S-CSCF) 208, and “a registrar such as a home subscriber server (‘HSS’) 210.” APPLE-1004, [0033]-[0034], FIG. 2; *generally id.*, [0031]-[0050]. Application servers can also optionally be included in the IMS core.⁴ APPLE-1004, [0034], [0039]. The components of the IMS core (*server*) “can reside on the same ... information

⁴ Because application servers generally implement services independently of each other, it would have been obvious that some application servers (*e.g.*, IM and MMS application servers) could be implemented within the IMS core while other application servers (including SMSC 114) are implemented outside the IMS core. APPLE-1004 (“each respective component can reside in the same or separate information processing system”). For Grounds 1A-1E, SMSC 114 is not part of the IMS core and does not form part of the mapping to the “*server*” recited in [1pre]. APPLE-1004, [0034]. The IM and MMS application servers are optionally part of the mapping to the claimed “*server*.”

processing system.”⁵ APPLE-1004, [0038]. Horvath identifies SMSC 114 separately from the P-CSCF 206, I,S-CSCF 208, and HSS 210, and explains that “[i]n one embodiment, the SMSC 114 is also part of the IMS core.” APPLE-1004, [0034]. A POSITA thus would have understood that Horvath contemplates further embodiments where the SMSC 114 is not part of the IMS core or is at least not part of the same server as P-CSCF 206, I,S-CSCF 208, and HSS 210. The IMS core receives SIP MESSAGES (*packet-switched messages*) that are to be delivered via a

⁵ The specific attributes of the “servers” recited in claim 1 do not further define the structure of the “mobile wireless device” that is the subject of claim 1’s preamble. For example, whether a server “receives packet-switched messages transmitted via the service to recipient devices that correspond to subscribers of the service,” “maintains a subscriber list,” or “forwards a message ... to [a] third-party provider” are not further limitations on the claimed “mobile wireless device.” Multiple elements of the Challenged Claims likewise recite limitations that do not limit the “mobile wireless device.” Specifically, at least elements [1pre], [1g], [1n], [4], [5], [6], [8], [11b], [11c], [15b], [15c], [20], and [26] suffer from this problem and are not entitled to patentable weight for purposes of validity. Grounds 1A-1E nonetheless confirm that these features were well known and obvious to a POSITA before the Critical Date.

messaging service (e.g., SMS, MMS, IM) to subscribing recipient devices. For example, “[t]he P-CSCF 206 ... is the first contact point for a wireless device 106 registered in the IMS network” and “[a]ll signaling messages are intercepted by the P-CSCF 206 allowing the P-CSCF 206 to inspect the messages.” APPLE-1004, [0036]. The S-CSCF 208 likewise “inspect[s] each message” and “determine[s] 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.” *Id.*, [0038]. The application servers “transmit[]/deliver[]” messages to recipient devices. APPLE-1004, [0039]; *see also id.*, [0045] (“If the SMSC 114 determines that the recipient device is registered on the packet data network 102, the SMSC 114 delivers the SMS message to the recipient device through the packet data network 102 via IMS.”)

68. Accordingly, the Horvath-Tsampalis-Tumminaro sending wireless device 106 (*mobile wireless device*) transmits at least some SIP MESSAGES (*packet-switched messages*) to at least some recipient devices that correspond to subscribers of an IM or MMS service (*service for receiving packet-switched messages*). The MMS and IM services are implemented with the IMS core (*server*) that receives SIP MESSAGES (*packet-switched messages*) transmitted via the service to recipient devices that correspond to subscribers of the service. The sending device 106 also transmits at least some messages (e.g., SMS messages) over

a circuit-services component 104 of a *cellular network* to at least some recipient devices that do not correspond to subscribers of the IMS or associated IM or MMS services.

Element [1a]: a wireless local area network (WLAN) transceiver that transmits messages from the mobile wireless device to a WLAN base station and subsequently over the Internet to the server that receives packet-switched messages transmitted via the service to recipient devices that correspond to subscribers of the service, before delivery to a recipient device;

69. Horvath-Tsampalis-Tumminaro renders Element [1a] obvious. Horvath discloses that the wireless device 106 (*mobile wireless device*) “is a dual mode device capable of communicating on either the packet data network 102 or the circuit services network 104.” APPLE-1004, [0061]; *see also id.*, [0060], [0062], FIG. 4. Wireless device 106 transmits and receives radio signals over a selected network by alternately coupling its antenna 404 to transmitter 410 or receiver 408 “through a transmit/receive switch 406.” *Id.*, [0061]-[0062]. Device 106 also includes an “SMS delivery network selector 124 [that] selects a network 102, 104 for the wireless device 106 to transmit a SMS message on.” *Id.*, [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” encoded in a SIP MESSAGE (*packet-switched message*). *Id.*, [0062], [0050], [0078], FIG. 7.

70. As discussed in [1pre], *supra*, a POSITA would have found it obvious that the sending wireless device 106 transmits SIP MESSAGES carrying embedded MMS or IM messages to the IMS core (*server*) for delivery to recipient devices corresponding to subscribers of the MMS or IM services (*service*), and the IMS core receives these SIP MESSAGES *before delivery to the recipient device*. APPLE-1004, [0050], [0077]-[0078], FIG. 7; *supra*, Ground 1A, Analysis of Element [1pre].

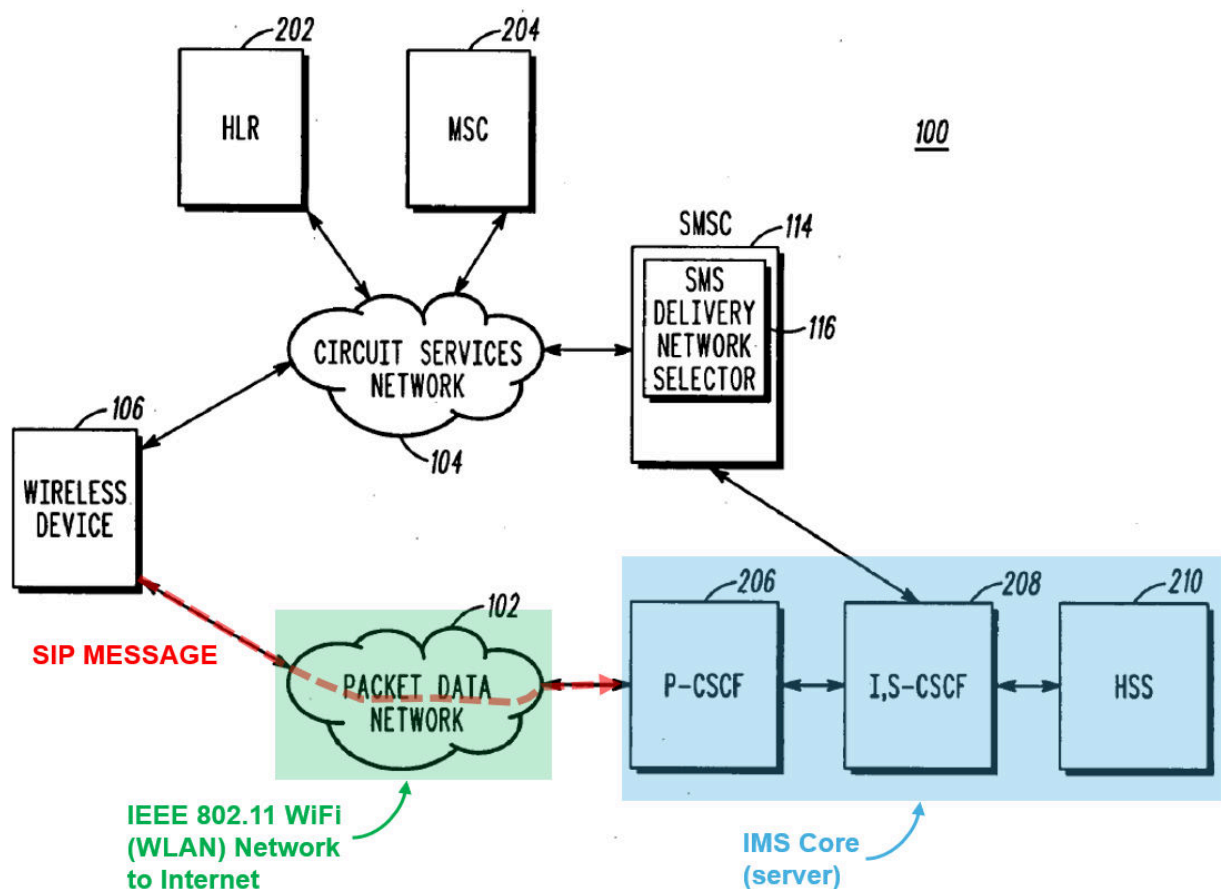


FIG. 2

APPLE-1004, FIG. 2 (Annotated)

71. Further, a POSITA would have found it obvious to implement the packet-data network 102 to include *a wireless local area network (WLAN)*.

Specifically, Horvath teaches that “packet data network 102 is an Internet Protocol (‘IP’) connectivity network, which provides data connections at much higher transfer rates than [*sic*] a traditional circuit services network,” and can comprise “an 802.11 network.” APPLE-1004, [0024]. A POSITA would have understood and found obvious that a common type of 802.11 network was a wireless LAN. APPLE-1011, 5:1-33 (“WLAN capabilities including...technology version (such as 802.11[*g*])”), 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, 4; APPLE-1037. A mobile device communicating via an 802.11 network communicates with a WLAN access point, which is a type of base station (***WLAN base station***). APPLE-1046, FIG. 4, 13: (mobile station “coupled to one or more wireless access points...configured to communicate with the mobile station in accordance with techniques such as...WLAN techniques”).

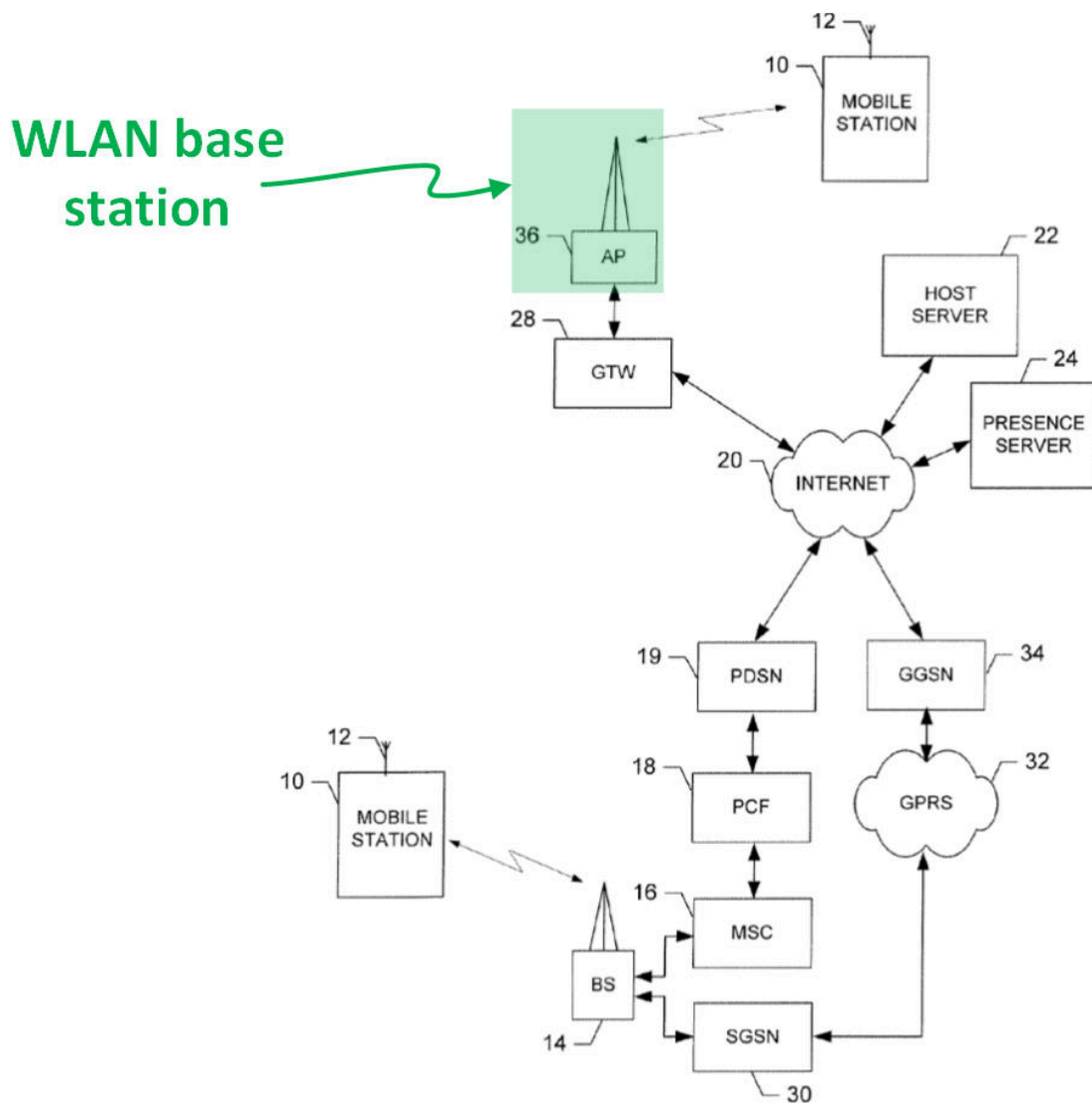


FIG. 4

APPLE-1046, FIG. 4 (Annotated)

72. Horvath also discloses that “[t]he SIP network is used for establishing ... communications over the Internet” and that the IMS core is for an “Internet Protocol multimedia subsystem.” APPLE-1004, [0033]-[0034]. Accordingly, it would have been obvious that Horvath-Tsampalis-Tumminaro’s sending wireless device 106 (*mobile wireless device*) includes a dual-mode

transmitter 410 and receiver 408 (collectively, a ***WLAN transceiver***) that transmits messages from the wireless device 106 to an IEEE 802.11 WLAN access point (***WLAN base station***) and subsequently over the Internet to the IMS core (***server***) that receives SIP MESSAGES (***packet-switched messages***) transmitted via the MMS or IM services (***service***) to recipient devices that correspond to subscribers of either service, before delivery to the recipient devices.

Element [1b]: a cellular transceiver that transmits messages from the mobile wireless device to a cellular base station before delivery to a recipient device, wherein the cellular transceiver and the cellular base station communicate using a radio communications protocol that supports transmission of multimedia messages comprising at least one of images, audio clips or videos;

73. Horvath-Tsampalis-Tumminaro renders Element [1b] obvious. As I previously discussed in Analysis of Element [1a], Horvath discloses that the wireless device 106 (***mobile wireless device***) “is a dual mode device capable of communicating on either the packet data network 102 or the circuit services network 104.” APPLE-1004, [0061]; *see also id.*, [0060], [0062], FIG. 4. Wireless device 106 transmits and receives radio signals over a selected network by alternately coupling its antenna 404 to transmitter 410 or receiver 408 “through a transmit/receive switch 406.” *Id.*, [0061]-[0062]. Device 106 also includes an “SMS delivery network selector 124 [that] selects a network 102, 104 for the wireless device 106 to transmit a SMS message on.” *Id.*, [0062]. “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”
“using the traditional circuit services network method (for example, ANSI-41 procedures).” *Id.*, [0062], [0050], [0078], FIG. 7.

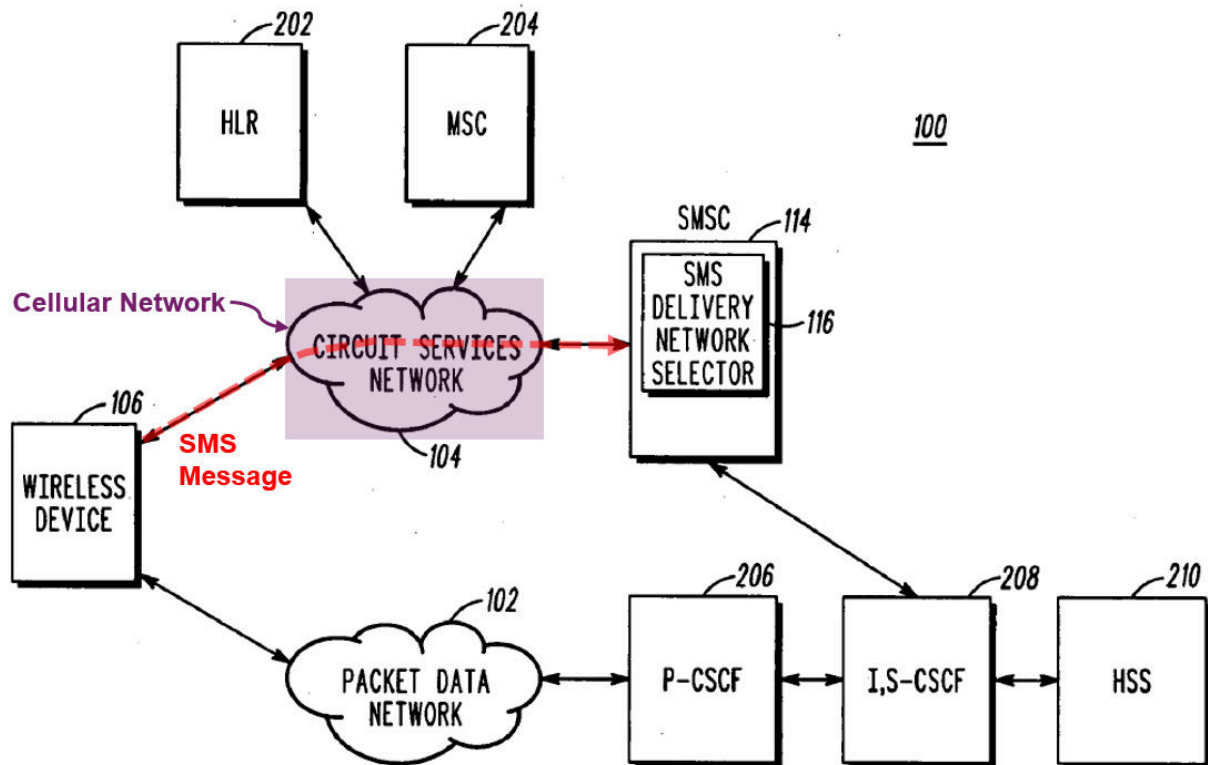


FIG. 2

APPLE-1004, FIG. 2 (Annotated)

74. Further, a POSITA would have found obvious that the circuit-services network 104 includes a *cellular network* having at least one cellular base station such that the wireless device would transmit SMS messages to a cellular base station before delivery to a recipient device. For example, Horvath discloses that circuit-

services network 104 is provided on a *cellular network* such as a “Global System for Mobile Communications (GSM)” network that provides “mobile text messaging” and “voice services” including “push-to-talk over cellular communications.” APPLE-1004, [0025]-[0026]. As shown in the following diagram, a mobile device communicating over a cellular network communicates with a base station of the cellular network. APPLE-1046, FIG. 4, 12:54-13:60 (“an antenna 12 for transmitting signals to and for receiving signals from one or more base stations (BS’s),” which are “part of one or more cellular or mobile networks that each includes elements required to operate the network”).

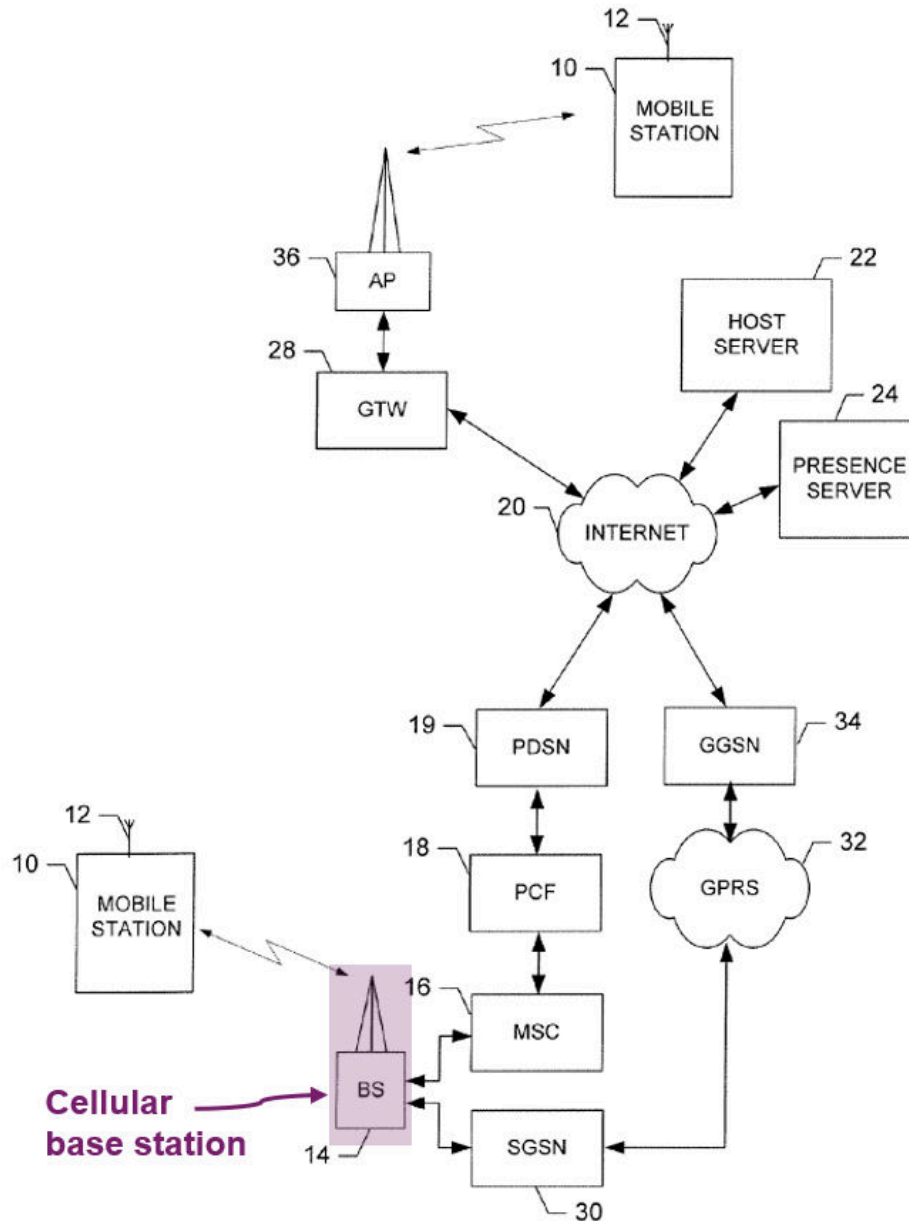


FIG. 4

APPLE-1046, FIG. 4 (Annotated)

75. Horvath also discloses that the wireless device's transmitter 410 and receiver 408 can further communicate over a cellular network included in the packet-data network 102. In particular, "packet data network 102, in one embodiment,

comprises an Evolution Data Only ('EV-DO') network, a General Packet Radio Service ('GPRS') network, a Universal Mobile Telecommunications System ('UMTS') network, ... or the like." APPLE-1004, [0024]. A POSITA would have known that EV-DO, GRPS, and UMTS networks define radio communications protocols that support transmission of multimedia messages comprising at least one of images, audio clips, or videos. APPLE-1048, 1 ("Consumers can send picture messages to their friends' phones or download the latest games and polyphonic ringtones – and now ..., they can view news bulletins, sports highlights and music videos streamed to their mobile handset."), 2-24; APPLE-1047 (describing multimedia capabilities of GPRS, UMTS, EV-DO); *cf.* APPLE-1001, 10:10-18 & FIG. 6C ('827 Patent identifying "GPRS, 3G, 3.5G" as "wireless protocols ... used in the data link layer to deliver the message"). For the reasons discussed above, a mobile device communicating via GPRS, EV-DO, or UMTS would also communicate with a base station of a cellular network. APPLE-1046, FIG. 4, 12:54-13:60.

76. Accordingly, it would have been obvious that Horvath-Tsampalis-Tumminaro's sending wireless device 106 (*mobile wireless device*) includes a dual-mode transmitter 410 and receiver 408 (collectively, a *cellular transceiver*) that transmits messages from the wireless device 106 to a cellular base station before delivery to a recipient device, where the cellular transceiver and the cellular base

station communicate using EV-DO, GPRS, or UMTS protocols (*a radio communications protocol that supports transmission of multimedia messages comprising at least one of images, audio clips, or videos*).

Element [1c]: wherein the mobile wireless device connects via the WLAN base station to the server that receives packet-switched messages transmitted via the service to recipient devices that correspond to subscribers of the service;

77. Horvath-Tsampalis-Tumminaro renders Element [1c] obvious. As I previously discussed in Analysis of Element [1a], the combination's sending wireless device 106 (*mobile wireless device*) includes a dual-mode receiver 408 and transmitter 410, the latter of which transmits messages to an 802.11 WiFi access point (*WLAN base station*) and subsequently over the Internet to the IMS core (*server*) that receives SIP messages (*packet-switched messages*) transmitted via an MMS or IM service to recipient devices that correspond to subscribers of the service. APPLE-1004, [0024], [0060]-[0062], FIGs. 1-2, 4; *supra*, [1a]. Horvath further discloses that "[t]he wireless device 106 can connect to the IMS network using different methods, which all use standard IP." APPLE-1004, [0034]. "[W]hen a wireless device 106 wants to access the packet data network 102, the wireless device 106 registers with the IMS network." *Id.* "The P-CSCF 206 is a SIP proxy and is the first contact point for a wireless device 106 registered in the IMS network." *Id.*, [0036]. Accordingly, it would have been obvious that Horvath-Tsampalis-Tumminaro's sending wireless device 106 connects via the 802.11 WiFi access point

(*WLAN base station*) to the IMS core (*server*). APPLE-1049, 24 (“the P-CSCF, if it does not have a TCP connection towards the UE yet, shall set up a TCP connection”).

Element [1d]: wherein the mobile wireless device connects via the cellular base station to the server that receives packet-switched messages transmitted via the service to recipient devices that correspond to subscribers of the service;

78. Horvath-Tsampalis-Tumminaro renders Element [1d] obvious. As I previously discussed in Analysis of Element [1b], the combination’s sending wireless device 106 (*mobile wireless device*) includes a dual-mode receiver 408 and transmitter 410, the latter of which transmits messages to a cellular base station via packet-based cellular protocols such as UMTS, GPRS, or EV-DO. APPLE-1004, [0024], [0060]-[0062], FIGs. 1-2, 4; *supra*, [1b]. Horvath further discloses that “[t]he wireless device 106 can connect to the IMS network using different methods, which all use standard IP.” APPLE-1004, [0034]. “[W]hen a wireless device 106 wants to access the packet data network 102, the wireless device 106 registers with the IMS network.” *Id.* “The P-CSCF 206 is a SIP proxy and is the first contact point for a wireless device 106 registered in the IMS network.” *Id.*, [0036]. Accordingly, it would have been obvious that Horvath-Tsampalis-Tumminaro’s sending wireless device 106 connects via the cellular base station to the IMS core (*server*) via GPRS, UMTS, or EV-DO. APPLE-1049, 24 (“the P-CSCF, if it does not have a TCP connection towards the UE yet, shall set up a TCP connection”).

Element [1e]: wherein the mobile wireless device transmits packet-switched messages using a packet-switched bearer supported by the WLAN base station and transmits packet-switched messages using a packet-switched bearer supported by the cellular base station; and

79. Horvath-Tsampalis-Tumminaro renders Element [1e] obvious. For context, a POSITA would have known that “various bearers in the mobile network technology” include, for example, “SMS, USSD (Unstructured Supplementary Services Data), CSD (Circuit Switched Data) and packet-switched bearers, such as *e.g.*, GPRS (General Packet Radio Service) etc.” APPLE-1051, [0014]; *see also* APPLE-1050, 4:42-46. The ’827 Patent describes that a “conventional SMS bearer” may be used on a circuit-switched network (*e.g.*, GSM), whereas a “packet-switched bearer may be a HSDPA, WCDMA, CDMA2000, GPRS or similar data bearer,” and “[t]he packet-switched bearer may also [be] supported by other wireless technologies such as Bluetooth, WiFi, WiMax.” APPLE-1001, 2:51-60. In general, messages sent over a circuit-switched network are sent via a circuit-switched bearer and messages sent over a packet-switched network are sent via a packet-switched bearer. Thus, when an SMS message is sent over a circuit-switched network⁶, it is

⁶ Some packet-switched networks support SMS messages, and in those cases, an SMS bearer would also be a packet-switched bearer. *See, e.g.*, APPLE-1054, [0091]. However, in other cases, SMS sent over a packet-switched network

utilizing an SMS bearer, which is a type of circuit-switched bearer. *See* APPLE-1001, 2:51-60, APPLE-1050, 4:42-46. On the other hand, for messages sent over the packet-switched network, such as the SIP MESSAGEs taught by Horvath, the bearer (*e.g.*, 802.11 WiFi, GPRS, UMTS, or EV-DO) is a packet-switched bearer. *See* APPLE-1004, [0024] (identifying GPRS as an example of its packet-switched network 102), [0040]-[0041], [0050] (describing the delivery of a SIP MESSAGE over a packet-switched network).

80. In this context, it would have been obvious that Horvath-Tsampalis-Tumminaro's sending wireless device 106 (*mobile wireless device*) transmits SIP MESSAGEs (*packet-switched messages*) using an 802.11 WiFi bearer (*a packet-switched bearer supported by the WLAN base station*) when connected to the 802.11 network, and transmits packet-switched messages using GPRS, EV-DO, or UMTS bearers (*a packet-switched bearer supported by the cellular base station*) when connected to a cellular data network. APPLE-1004, [0024]-[0027], FIGs. 1-2; *supra*, [1a]-[1b]. Indeed, Horvath contemplates that the wireless device 106 is

is encapsulated in a packet-switched bearer. *See, e.g.*, APPLE-1004, [0050] (describing encoding SMS content as the payload of an SIP message); APPLE-1054, [0166] (describing encapsulating SMS data "in IP format before delivery to the WLAN").

capable of communicating on a range of networks using respective bearers corresponding to the different networks and services provided. *See* APPLE-1004, [0061] (“dual-mode device capable of communicating on either the packet data network 102 or the circuit services network 104”), [0064] (“wireless device 106[] ... also includes an optional local wireless link 416 that allows the wireless device 106 to directly communicate with another wireless device”), [0022] (“wireless device is intended to broadly cover many different types of devices that ... operate in a wireless communication system”), [0027] (“support any number of wireless devices 106” and also “allow for mesh networking”). Horvath also describes how a communication system can include multiple types of packet-switched networks including 802.11 WiFi, EV-DO, GPRS, UMTS, wide area networks 118, and local area networks 120. APPLE-1004, [0024]-[0028], FIG. 2. In this context, it would have been obvious for the sending wireless device 106 to be capable of transmitting via packet-switched bearers on multiple types of networks including 802.11 WiFi and cellular data networks. This is reinforced by Tumminaro, which likewise discloses wireless devices configured to communicate messages over both WiFi and cellular data networks. *See, e.g.*, APPLE-1034, [0161] (“Various communication protocols may be used to facilitate communication”), [0162] (“a wireless network using a protocol such as Wi-Fi”), [0534] (“mobile networks based on all three cellular technologies, with GSM, CDMA, and TDMA”), [1161] (“cellular

telephones”), [0256]-[0257], [045], [0456], [0534], [1160]-[1163]. Not only is the option of transmitting messages via both WiFi and cellular data networks expressly disclosed in Horvath and Tumminaro, but a POSITA would have known that mobile devices were commonly implemented to connect to both WiFi and cellular data networks before the Critical Date and this was obvious to provide the device with greater access to services on different networks in more areas than would otherwise be possible if the device were limited to use of a single packet-switched bearer. *Infra*, [1j]-[1k]; APPLE-1055, [0028]-[0030], FIG. 2; APPLE-1056, [0002]-[0009]; APPLE-1068, Abstract (“portable devices to communicate ... via both cellular and WiFi”), [0006], [0032]-[0034].

Element [1f]: a message client that retrieves, from a message, information corresponding to at least one mobile phone number of a wireless device of an addressed recipient;

81. Horvath-Tsampalis-Tumminaro renders Element [1f] obvious. Horvath explains that the sending wireless device 106 (***mobile wireless device***) sends messages to recipient wireless devices over one or more packet-data networks 102 and/or circuit-services networks 104. APPLE-1004, [0050], [0078], FIGs. 1-2, 7. Horvath discloses “information to identify” each wireless device registered to the SIP network and the IMS core, *e.g.*, a “destination address” (also referred to as “contact address” or “IMS contact address”), “such as a telephone uniform resource identifier (‘tel-URI’),” *e.g.*, “the telephone number assigned to the wireless device

106.” APPLE-1004, [0035] (“A tel-URI, for example is the telephone number assigned to the wireless device 106.”), [0045], [0050], [0073] (“the contact address (for example, tel-URI) of the wireless device 106”), [0076].

82. Horvath’s functionality for receiving information associated with a destination address of a recipient is maintained in the combination with Tsampalis, which similarly describes conventional addressing techniques where the sending device receives phone numbers of intended messaging recipients while actively composing a message. APPLE-1005, [0033]-[0034], [0061]. Tsampalis teaches that an “active message” being composed by a user of the sending mobile phone contains a “recipient ID” received from the user, *e.g.*, a phone number in the form of a MSISDN. *See* APPLE-1005, FIG. 4 (below, showing “recipient ID” 402 list in the form of telephone numbers), [0032]-[0033], [0046], [0061], [0064], FIGS. 3-4, 7, 10; APPLE-1052, 12:53-60; APPLE-1053, [0037]-[0038], [0066], [0072] (“the address bar 504 may comprise a ‘To’ field which may display the contact name...through reverse look up in the contact records or the telephone number of the recipient”).

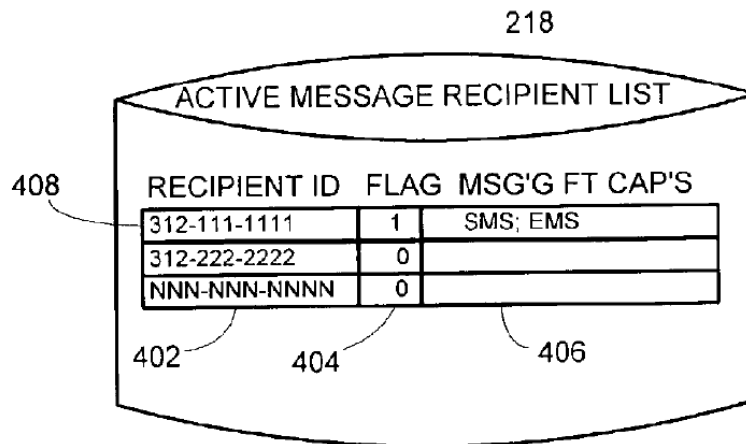
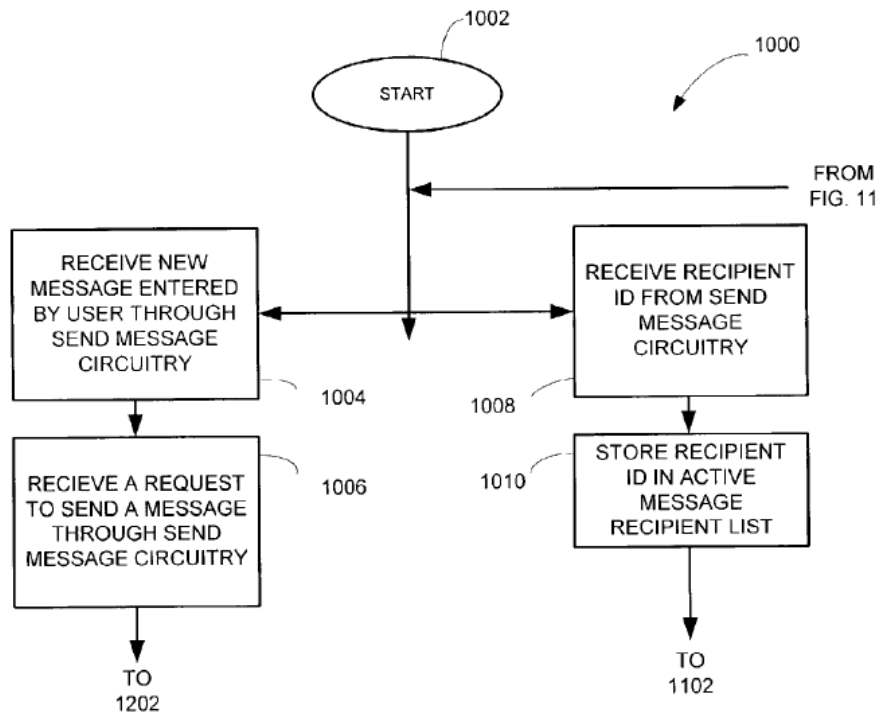


FIG. 4

APPLE-1005, FIG. 4

83. Referring to FIG. 10 (below), Tsampalis explains, “[a]s shown in Block 1004, the method includes [] receiving a new unformatted message 110 entered by a user” and “[b]lock 1008 demonstrates the method including the receiving of a next recipient ID 402 as the recipient ID is entered in the send message circuitry 106.” APPLE-1005, [0046], FIG. 10. Tsampalis describes that as a user enters message text and an active message recipient list into the sending mobile phone’s user interface, “the mobile wireless communication device messaging format capabilities determinator circuitry 104...retrieve[s] the [receiving] mobile wireless communication device [MFCI] 110 associated with the” recipient ID of a receiving mobile phone entered into the active message recipient list. APPLE-1005, [0033]; *see also id.*, [0046]; *infra*, [1g]-[1h].

FIG. 10



APPLE-1005, FIG. 10

84. It also would have been obvious that the combination's sending wireless device 106 (*mobile wireless device*) includes a “*message client*” that performs the “*retriev[ing]*” operation recited in [1f]. For example, Horvath describes the wireless device 106 executing software to carry out messaging functions substantially similar to those performed by the software client described in the '827 Patent. APPLE-1004, [0061]-[0062], FIG. 4 (depicting memory 412 and processor 402); *cf.* APPLE-1001, 5:2-3 (“the invention is a software program to implement the method”), 5:49 (“a message client 114 runs on the mobile device”).

Moreover, implementing a message client on the Horvath-Tsampalis-Tumminaro device would have been obvious to ensure the sender was provisioned with software adequate to carry out the messaging functions of the combination as described herein. These functions align with the types of functions that were commonly performed by messaging clients before the Critical Date. APPLE-1008, [0002], [0004], [0038]; APPLE-1009, pp. 3, 6; APPLE-1017, 34:63-66; APPLE-1021, 4:66-5:6, 9:57-64; *see also* APPLE-1005, [0024] (Tsampalis describing its circuitries on a sender wireless device for determining recipient messaging capabilities and for sending messages as “software modules”), [0027], [0046], FIGS. 3-4, 7, 10.

85. For each of these reasons, Horvath-Tsampalis-Tumminaro renders obvious a sending mobile phone (*e.g.*, wireless device 106) including a message client that *retrieves, from a message, information corresponding to at least one mobile phone number of a wireless device of an addressed recipient* (*e.g.*, the send message circuitry 106 retrieving a “destination address” or “recipient ID” from an active message being composed by the user of the sending mobile phone, and the messaging format capabilities determinator circuitry 104 retrieving the MFCI 110 corresponding to the “destination address” or “recipient ID” of the message, where the “destination address” or “recipient ID” is a telephone number in the form of a tel-URI or MSISDN).

Element [1g]: wherein the WLAN transceiver: (i) transmits a request, including at least information corresponding to the mobile phone number of the wireless

device of the addressed recipient, via the WLAN base station and the Internet, to a server that maintains a subscriber list, to determine whether the wireless device of the addressed recipient corresponds to a subscriber of the service; and

86. Horvath-Tsampalis-Tumminaro renders Element [1g] obvious. As I previously discussed for Element [1f], the combination's sending mobile device 106 includes a message client that "retrieve[s] the [receiving] mobile wireless communication device messaging format capabilities information 110 associated with the" recipient ID of an addressed receiving wireless device entered into the active message recipient list. APPLE-1005, [0033]; *see also id.*, [0046]; *supra*, [1f]. As I previously discussed in §VII.B, *supra*, Tsampalis describes that the recipient ID may be the phone's MSISDN, which was known to be "the standard international telephone number used to identify a given subscriber." *See* APPLE-1005, FIGS. 3, 4 (illustrating that the recipient ID may be a telephone number); APPLE-1052, 12:53-60. If the format-capabilities information is not available in the sending mobile phone's local phonebook or the phonebook's information has not been updated within a certain period of time, "the remote message format capabilities determinator circuitry 208 [of the sending mobile phone] is then invoked and generates a second mobile wireless communication device messaging format capabilities information request 226." APPLE-1005, [0033]-[0034], FIGs. 6, 13.

87. The requested messaging format capabilities information 110 for the receiving mobile phone may be "stored in a location other than within the second

mobile wireless communication device 200, for example, such as a network element within the network 108” (e.g., a “web server”), and the sending mobile phone directs the request to the network element. APPLE-1005, [0039], [0056]-[0057]. In at least one obvious implementation, the “web server” described by Tsampalis would be included in or combined with one or both of Horvath’s HLR 202 or HSS 210 (the latter of which is part of the “IMS core”), because Horvath’s HLR and HSS are “network elements within the networks” and store similar information as Tsampalis’s web server. See APPLE-1004, [0035], [0044], FIG. 2. Specifically, Horvath’s HLR “comprises a database including information associated with a wireless device subscribing to the circuit services network 104,” which includes “service(s) subscribed to by the wireless device 106.” APPLE-1004, [0031]. Similarly, Horvath’s HSS “comprises a database including profiles associated with each wireless device 106 registered with the IMS,” and these profiles “include[] subscription related information,” as well as capability information indicating whether each wireless phone is configured to receive messages through the packet-data network. APPLE-1004, [0035], [0044]. Indeed, Tsampalis teaches that, “while inputting the active message 216, the first mobile wireless communication device 100 will transparently contact the network talking to the address(es), (e.g., the MSISDN(s)), of the recipients(s), and try to talk with their home location register

(HLR) to find out if they are capable of receiving” certain types of messages. APPLE-1005, [0061].

88. As noted above, Horvath and Tsampalis teach that the HLR and HSS “include[] information to identify each registered wireless device 106 such as...the telephone number assigned to the wireless device.” See APPLE-1004, [0031], [0035], [0047]; APPLE-1005, [0061]. Thus, to obtain the format-capabilities information, it would have been obvious for the combination’s sending device 106 to transmit a request that included the telephone number or other form of “destination address” or “recipient ID” (*information corresponding to the mobile phone number of the wireless device of the addressed recipient*) of the receiving device to the “network element within the network” (e.g., HLR 202 and/or HSS 210), so that the network element would be able to look up the profile of the receiving device, including the receiving device’s capabilities and relates subscription information. See APPLE-1004, [0035], [0044]; APPLE-1005, [0033], [0039], [0046], [0056]-[0057], [0061]; *see also* APPLE-1053, [0068] (“a telephone number may be used to correlate and thread together different types of messages such as telephone messages, voicemail messages, fax messages, SMS messages, and MMS messages”).

89. As I previously discussed for Elements [1a] and [1c], the sending wireless device 106 includes a WLAN transceiver that allows the sending device 106 to connect and communicate with the IMS core (including HSS 210) via an

802.11 access point (*WLAN base station*) and over the Internet. APPLE-1004, [0024]-[0025], [0060]-[0062], FIGs. 1-2, 4; *supra*, [1a], [1c]. In this context, it would have been obvious for the sending wireless device's request to be transmitted via the 802.11 access point and over the Internet to the HLR 202 and/or HSS 210, particularly when the wireless device 106 is connected to the 802.11 network. APPLE-1004, [0024]-[0025], FIG. 2; APPLE-1004, [0004], [0009] (describing desire to unburden the circuit-services network and communicate over packet-data networks (*e.g.*, 802.11 WLAN) where possible).

90. It also would have been obvious that the combination system's HLR 202 and/or HSS 210 would provide a "*server that maintains a subscriber list*" and that the request sent from the sending wireless device 106 (*mobile wireless device*) would constitute a request to "*determine whether the wireless device of the addressed recipient corresponds to a subscriber*" of an MMS or IM service (*service*). For examples, as discussed above, HLR 202 and HSS 210 store information regarding the "service(s) subscribed to by the wireless device 106." APPLE-1004, [0031], [0035], [0044]; APPLE-1005, [0061]. Horvath and Tsampalis describe that two such services to which a wireless device may be subscribed are MMS and IM services. *See* APPLE-1004, [0002], [0025], [0033] ("instant messaging"), [0039] ("A service for example, is SMS, MMS, caller ID, call waiting, push-to-talk, voicemail, and the like"); APPLE-1005, [0002]-[0003], [0058]-[0063]; *supra*, [1pre].

The HLR 202, HSS 210, or both, thus maintain a ***subscriber list*** indicating which services each device is subscribed to.

91. A POSITA would have found obvious that the sending wireless device's request to the HLR 202 and/or HSS 210 in the Horvath-Tsampalis-Tumminaro combination would seek not just the recipient's capabilities information for the example services discussed in Tsampalis (*e.g.*, SMS, EMS, and MMS) but rather to seek information about *all* the services to which the recipient is subscribed (*e.g.*, SMS, EMS, MMS, and IM). Tsampalis describes how its author sought to overcome the problem of “[b]eing unable to process the message due to the incompatibility of its messaging service capabilities with that of the format of the received message.” APPLE-1005, [0003]. In other words, Tsampalis recognizes that format capabilities information is related to the messaging services to which a mobile phone is subscribed, and therefore suggests that the format capabilities information itself indicates subscriber information. Moreover, requests for such subscription and registration information along with format-capabilities information was well known long before the alleged invention of the '827 Patent. APPLE-1046, 1:24-50 (“there are many different protocols or services that can be used for exchanging content,” including MMS and e-mail), 5:29-33, 7:28-8:45 (describing a sending mobile phone requesting and receiving from a presence server a “resource file,” which includes “information, such as the protocols and connectivity bearers

supported by, the capabilities of, and/or the security associations relating to respective devices operated by, or otherwise associated with, the” receiving mobile phone), 12:25-36; APPLE-1050, [0103] (“information related to the subscriber...and settings related to the purchased/subscribed service(s)”), [0107], [0115] (“delivery decision comprises delivery instructions with regard to destination device(s) and/or content and/or format and/or layout of the message to be delivered”), [0122] (describing a sending device receiving information about the destination device of a message to make a “delivery decision”), [0127]; APPLE-1064, 2 (“SIP location services already contain presence information, in the form of registrations”); APPLE-1063, 1 and 7-8 (describing presence information returned to requesting devices); APPLE-1043 and APPLE-1007 (describing known motivations to return presence information, which would include information in the form of registrations indicating subscriber status in the Horvath-Tsampalis-Tumminaro combination). Thus, a POSITA would have found obvious, for reasons similar to those expressly discussed in Tsampalis, that providing a sending mobile phone with more detailed information about the recipient, including their subscriber information, will help the sender determine how and where to send a message and what content should be included. *See supra* §VIII.A(i) (providing similar motivations for the Tsampalis combination).

92. Accordingly, it would have been obvious that Horvath-Tsampalis-Tumminaro's sending wireless device 106 transmits a *request*, including a telephone number, recipient ID, or destination address (*information corresponding to the mobile phone number of the wireless device of the addressed recipient*), via the 802.11 access point (*WLAN base station*) and the Internet, to *a server that maintains a subscriber list* (e.g., the network element within the network 108, such as HLR 202 and/or HSS 210, that contains the format capabilities and subscription-related information), *to determine whether the wireless device of the addressed recipient corresponds to a subscriber of the service* (e.g., MMS or IM service).

Element [1h]: (ii) receives a response from the server that maintains the subscriber list, via the WLAN base station and the Internet, indicating whether the wireless device of the addressed recipient corresponds to a subscriber of the service, wherein a negative response indicates that the wireless device of the addressed recipient is not a subscriber of the service;

93. Horvath-Tsampalis-Tumminaro renders Element [1h] obvious. As I previously explained for Element [1g], it would have been obvious for the combination's sending wireless device 106 to transmit a request via a WLAN base station and the Internet to a server that maintains a subscriber list (e.g., the network element within the network 108, such as HLR 202 and/or HSS 210, that contains the format capabilities and subscription-related information), to determine whether the wireless device of the addressed recipient corresponds to a subscriber of the service (e.g., SMS, MMS, or IM service). *Supra*, [1g].

94. Tsampalis goes on to teach that “the method includes receiving a response to the request where the response contains the second mobile wireless communication device messaging format capabilities information 110, as shown in step 604.” APPLE-1005, [0042]; *see also id.*, [0057] (“In response, the remote relay/server 1304 then sends a new capabilities signal two 1322 (including a second mobile wireless communication device messaging format capabilities information 110) to the local relay/server 1302,” which sends this to the sending mobile phone). Because the combination’s HLR 202 and/or HSS 210 store the messaging capabilities information and receive the request for such information from the sending mobile phone (*see supra*, [1g]), a POSITA would have understood and found obvious that the response described by Tsampalis would have been sent from the HLR 202 and/or HSS 210 to the sending wireless device 106. The response would include information about all the services to which the recipient is subscribed (*e.g.*, SMS, EMS, MMS, and IM). *Id.*; *supra*, [1g]. The response would also predictably be returned over the same connection as the request was sent such that the response would be received by the sending wireless device via the 802.11 access point (***WLAN base station***) and the Internet. APPLE-1005, FIG. 13 (showing requests and responses communicated over the same signaling lines); *supra*, [1g] (explaining how it would be obvious also to transmit the request via the WLAN base station and the Internet).

95. A POSITA also would have understood that the HLR 202 and/or HSS 210 would provide a response to every request for capabilities and related subscription information, regardless of which capabilities or services are indicated as being subscribed to in the profile associated with the addressed recipient. *See, e.g.,* APPLE-1005, [0035], [0042], [0057]-[0060] (not conditioning a response to a format capabilities request on the information contained therein). It was well known that some wireless devices (*e.g.,* mobile phones) had limited messaging capabilities. *See, e.g.,* APPLE-1005, [0003] (describing receiving mobile phones “capable of only receiving messages in” SMS), [0034] (describing a receiving mobile phones as having “limited messaging capabilities”), [0061]-[0062]; APPLE-1053, [0078] (describing messaging decision based on “availability of a recipient to receive messages of a certain format”); APPLE-1053, 2:9-17 (“each device may have a different range of connectivity...and different capabilities for handing different types and sizes of content”). Accordingly, a POSITA would have understood and found obvious that, for certain receiving devices, the HLR 202 and/or HSS 210 would provide a response when the phone number of the receiving device is not associated with a subscriber of either the MMS or IM services (or any messaging service). *See, e.g.,* APPLE-1004, [0047] (describing a case where “the recipient device is not registered on the packet data network 102”), [0053]. For example, it would have been obvious to provide a response indicating whether or not the

recipient device is a subscriber capable of processing messages formatted according to each messaging service including MMS and IM. *See, e.g.,* APPLE-1005, FIGs. 3-4 (depicting example receiving devices capabilities information for certain devices including SMS and EMS, but not MMS, indicating negative responses for MMS), [0033]-[0034], [0051] (“limited messaging capabilities” not including MMS), [0060] (“MMS=‘yes’; EMS=‘no’; and SMS=‘yes’”).

96. Thus, in the Horvath-Tsampalis-Tumminaro combination, it would have been obvious that the sending wireless device 106 would receive a *response* from the *server that maintains a subscriber list* (e.g., the network element within the network 108, such as HLR 202 and/or HSS 210), via the 802.11 access point (*WLAN base station*) and the Internet, containing information *indicating whether the wireless device of the addressed recipient corresponds to a subscriber of the service* (e.g., MMS or IM service), where a *negative response indicates that the wireless device of the addressed recipient is not a subscriber of the service* (e.g., a response indicating that the device has “limited capabilities” or a response that otherwise fails to indicate that the device is subscribed to the MMS or IM services).

Element [1i]: wherein the mobile wireless device selects a packet-switched bearer for transmission of a message to the addressed recipient via the server that receives packet-switched messages transmitted via the service to recipient devices that correspond to subscribers of the service, based at least in part on the response indicating that the addressed recipient corresponds to a subscriber of the service;

97. Horvath-Tsampalis-Tumminaro renders Element [1i] obvious. For example, Tsampalis discloses that a sending wireless device can set a “default format” for outgoing messages, and the sending device will format a message for transmission according to the “default format” if the recipient is a subscriber to the messaging service associated with the default format. APPLE-1005, [0062] (“[A] message may be initially formatted in the default messaging capabilities of the sending device, (e.g., MMS format), and if necessary, may be reformatted in a new format, (e.g., SMS), before being sent.”), [0036]-[0037], [0048]-[0054], [0062], [0064], FIG. 11. Tsampalis explains that rich formats that support multimedia attachments and longer body text are often preferable over formats having more limited capabilities such as SMS, and a rich format can be set as the default format or otherwise preferred over limited capability formats (e.g., SMS). *Id.*, [0062]-[0064].

98. As I previously discussed for Element [1pre], the sending wireless device 106 in the Horvath-Tsampalis-Tumminaro combination may send messages in different formats including SMS, MMS, and IM via corresponding SMS, MMS, and IM services. *Supra*, [1pre]; *see also supra*, [1g]-[1h]. MMS and IM are both rich formats that support multimedia attachments and longer message lengths than SMS. Based on Tsampalis’s teaching that rich messaging formats are often preferable over SMS when the recipient is capable of receiving a richly formatted

message, a POSITA would have found it obvious to set either MMS or IM as the default messaging format to leverage the enhanced capabilities of those formats over SMS since both are rich messaging formats. The Horvath-Tsampalis-Tumminaro sending device would thus format messages as MMS or IM messages for transmission via a SIP-supported MMS or IM service by default under certain conditions including that the sending device is registered with the IMS core and the recipient's capabilities information indicates that the recipient is a subscriber of the MMS or IM services and capable of receiving MMS or IM messages, respectively. APPLE-1004, [0050], [0078], FIG. 7.

99. Also as I previously discussed for Element [1pre], MMS and IM are both packet-switched messaging services, and when MMS or IM are utilized in a SIP network like Horvath's, it would have been understood and obvious that the sending device 106 encapsulate MMS and IM messages in SIP MESSAGES that the sending device sends to the IMS core, and which are then routed to corresponding MMS or IM application servers for further processing and delivery to addressed recipient devices. APPLE-1004, [0033], [0039], [0050], [0076]; *supra*, [1pre]. Because the SIP network operates on a packet-data network 102 and SIP MESSAGES are sent in "SIP packets" (*packet-switched messages*), a POSITA also would have found obvious that the sending wireless device selects a *packet-switched bearer* (e.g., an 802.11 WiFi bearer when the sending device is connected to the

802.11 network or a cellular-based GPRS, EV-DO, or UMTS data bearer when the sending device is only connected to a cellular network) for transmission of a SIP MESSAGE containing either an MMS or IM-formatted message to the addressed recipient via the IMS core (*server*). APPLE-1004, [0024], [0031], [0037], [0050] and [0078] (selecting packet data network transmission when registered), FIGs. 2, 7; *supra*, [1pre], [1e].

100. The Horvath-Tsampalis-Tumminaro sending device's selection of a *packet-switched bearer* would also be *based at least in part on the response indicating that the addressed recipient corresponds to a subscriber of the [MMS or IM] service* since transmission of MMS and IM messages (*e.g.*, encapsulated in SIP MESSAGES) require a packet-switched bearer, and as suggested by Tsampalis, the sending device applies the default rich-messaging format (*e.g.*, MMS or IM) if the response indicates that the recipient is a subscriber capable of receiving messages via the corresponding rich-messaging service (*e.g.*, MMS or IM service). *Supra*, [1e]. For example, Tsampalis teaches that the device can provide the user with an option to "abort" and therefore "prevent[] the sending of [a] message to any recipient with limited capabilities in any format," meaning that, in this case, the sending device's determination to select a packet-switched bearer for transmission is based on the addressed recipient's capabilities information indicating that the recipient corresponds to a subscriber of a rich-messaging service (*e.g.*, IM or MMS service)

because the transmission could otherwise be aborted (the packet-switched bearer would not be selected for transmission) if the recipient has “limited messaging capabilities” and thus does not correspond to a subscriber of a rich-messaging service (*e.g.*, IM or MMS service). APPLE-1005, [0053], [0062], FIG. 12. More generally, the Horvath-Tsampalis-Tumminaro sending device implements Tsampalis’s teachings to format and transmit a message in a rich format (*e.g.*, MMS, IM) using a packet-switched bearer by default whenever the sending and receiving devices are both capable of communicating richly formatted messages, and thus the selection of a packet-switched bearer for transmission of such messages is based at least in part on the response indicating that the addressed recipient is a subscriber of a service for receiving richly formatted messages (*e.g.*, MMS, IM). APPLE-1005, [0053], [0062]-[0063]; *see also* APPLE-1004, [0050], [0076]-[0078], FIG. 7.

101. A POSITA also would have found it obvious in some implementations to “abort” or defer transmission of a message containing multimedia attachments (or that otherwise exceed the capabilities of SMS) if either the sending or recipient device is incapable of transmitting or receiving MMS or IM messages because the message would either fail to be delivered if the default MMS or IM format were maintained or the multimedia attachments would be lost if the message were converted to SMS. APPLE-1006, [0062], [0050]-[0055], FIG. 12; APPLE-1004, [0050], [0078], FIG. 7. The selection of a packet-switched bearer for transmission

of MMS or IM messages using SIP (rather than formatting the message as an SMS and sending via a circuit-switched SMS bearer) was also obvious to further Horvath's goal of unburdening the circuit-switched network 104 of message traffic and instead utilizing the packet-data network 102 for such messaging when available. APPLE-1004, [0004], [0009].

Element [1j]: wherein if a packet-switched bearer is selected for message transmission via the server that receives packet-switched messages transmitted via the service to recipient devices that correspond to subscribers of the service, the mobile wireless device chooses for message transmission the packet-switched bearer supported by the WLAN base station or the packet-switched bearer supported by the cellular base station;

Element [1k]: wherein the mobile wireless device transmits a message to the addressed recipient via the cellular base station, at least where the packet-switched bearer supported by the WLAN base station is not chosen for message transmission;

102. Horvath-Tsampalis-Tumminaro renders Elements [1j]-[1k] obvious. As I previously discussed for Element [1e], it would have been obvious for the combination's sending wireless device 106 (***mobile wireless device***) to be configured with the capability of transmitting SIP MESSAGES (***packet-switched messages***) on both an 802.11 WiFi data bearer (***a packet-switched bearer supported by a WLAN base station***) and a GPRS, EV-DO, or UMTS data bearer (***a packet-switched bearer supported by a cellular base station***). APPLE-1004, [0024]-[0027], [0060]-[0062], FIGs. 1-2m 4; APPLE-1034, [0161]-[0162], [0534], [1161], [0256]-[0257], [045], [0456], [0534], [1160]-[1163]; *supra*, [1e]. Although the sending device has

capabilities for transmitting on multiple packet-switched bearers, Horvath contemplates the selection of a single packet-switched bearer for transmission of a given message (*e.g.*, a SIP MESSAGE). *See* APPLE-1004, [0061] (“communicating on either” network), [0050] and [0078] (describing single transmission of message on packet data network 102 when sender is registered with the IMS). Accordingly, it would have been obvious for the Horvath-Tsampalis-Tumminaro sending device 106 to choose one of the packet-switched bearers (*e.g.*, the 802.11 WiFi data bearer or the GPRS, EV-DO, or UMTS data bearer) for transmission of a SIP MESSAGE over packet-data network 102 to the IMS core.

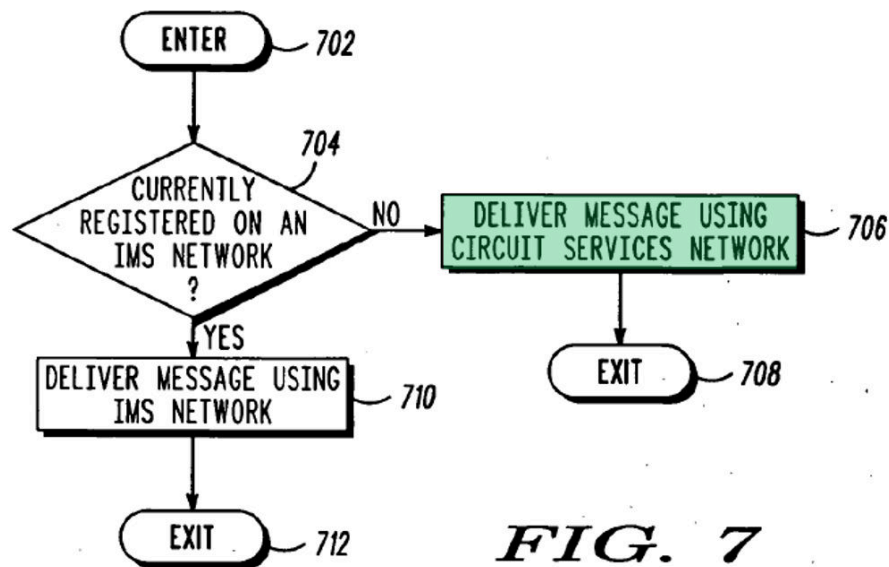
103. As one example, it would have been obvious for the sending device 106 to select a GPRS, EV-DO, or UMTS data bearer only when the sending device 106 is not in range of an accessible 802.11 WLAN access point (or in other limited circumstances), *e.g.*, because a 802.11 WiFi data bearer often provides higher transmission speeds and lower cost of service than the GPRS, EV-DO, or UMTS bearer. APPLE-1055, [0028] (“[W]hen a multi-mode (*e.g.*, WWAN and WLAN) access terminal 202 that is communicating via a WWAN (*e.g.*, a cellular network) enters a home environment, it may be desirable for the access terminal 202 to associate with the WLAN at the home environment (*e.g.*, to obtain access to different services and/or services having better quality of service)”), [0029]-[0030], FIG. 2; APPLE-1056, [0008] (“[W]hen the device is within the area of coverage of a

network that provides high speed Internet access, the device may switch from the network with which it was connected to the network with the high speed Internet access. Similarly, the device may, for example, connect to networks that provide different quality of service, low cost service and/or different services (e.g., voice, data, multimedia, etc.).”), [0002]-[0009]; APPLE-1068, Abstract (“portable devices to communicate ... via both cellular and WiFi”), [0006], [0032], [0034]. In these situations, the Horvath-Tsampalis-Tumminaro wireless device would transmit a SIP MESSAGE to the addressed recipient via the cellular base station (e.g., using a GPRS-EV-DO, or UMTS packet-switched data bearer), *at least where the packet-switched bearer supported by the WLAN base station is not chosen for message transmission* (e.g., where the sending device is not within an authorized 802.11 WLAN coverage area or where the cost, quality, or services offered by the GPRS, EV-DO, or UMTS bearer are determined to make it a better option than an available 802.11 WLAN bearer).

Element [11]: wherein the mobile wireless device transmits a message to the addressed recipient via the cellular base station, and without traversing the server that receives packet-switched messages transmitted via the service to recipient devices that correspond to subscribers of the service, before delivery to the addressed recipient, based at least in part on the response failing to indicate that the addressed recipient corresponds to a subscriber of the service;

104. Horvath-Tsampalis-Tumminaro renders Element [11] obvious. For example, Horvath discloses that when “wireless device 106 desires to transmit a SMS message to another device, the wireless device 106 first determines if it is

registered on the packet data network 102.” APPLE-1004, [0050]. “If the wireless device 106 is not registered on the packet data network 102, the wireless device 106 transmits the SMS messages using the traditional circuit services network method (for example, ANSI-41 procedures).” *Id.*; *see also id.*, [0078] (“If the result of this determination is negative, the wireless device 106[] ... transmits the SMS message through the traditional circuit services network ...”). Horvath’s “process of the wireless device 106 selecting either the packet data network 102 or the circuit services network 104 for transmission of a SMS message” is shown is shown in FIG. 7:



APPLE-1004, FIG. 7 (Annotated)

105. According to Horvath, an SMS message transmitted from the sending device 106 “using the traditional circuit services network method” is sent to the short message service center (SMSC) 114 without traversing the IMS core (*server*). This

follows because the IMS core (*server*) is part of an “Internet Protocol multimedia system” configured to “process SIP signaling packets” transported over the “packet data network 102”—not SMS messages transmitted according to “the traditional circuit services network method,” *e.g.*, using “ANSI-41 procedures.” APPLE-1004, [0034]-[0035], FIG. 2. Horvath specifically distinguishes transmission of an SMS message over the circuit-services network 104 from SMS transmission to the IMS core over the packet-data network 102, the latter of which involves “encod[ing] the IS-637 content” of the SMS message “as the payload of the SIP MESSAGE.” APPLE-1004, [0050]. FIG. 2 specifically illustrates the transmission path of an SMS message from the sending device 106 to the SMSC 114 using the traditional circuit-services method, which never traverses the IMS core:

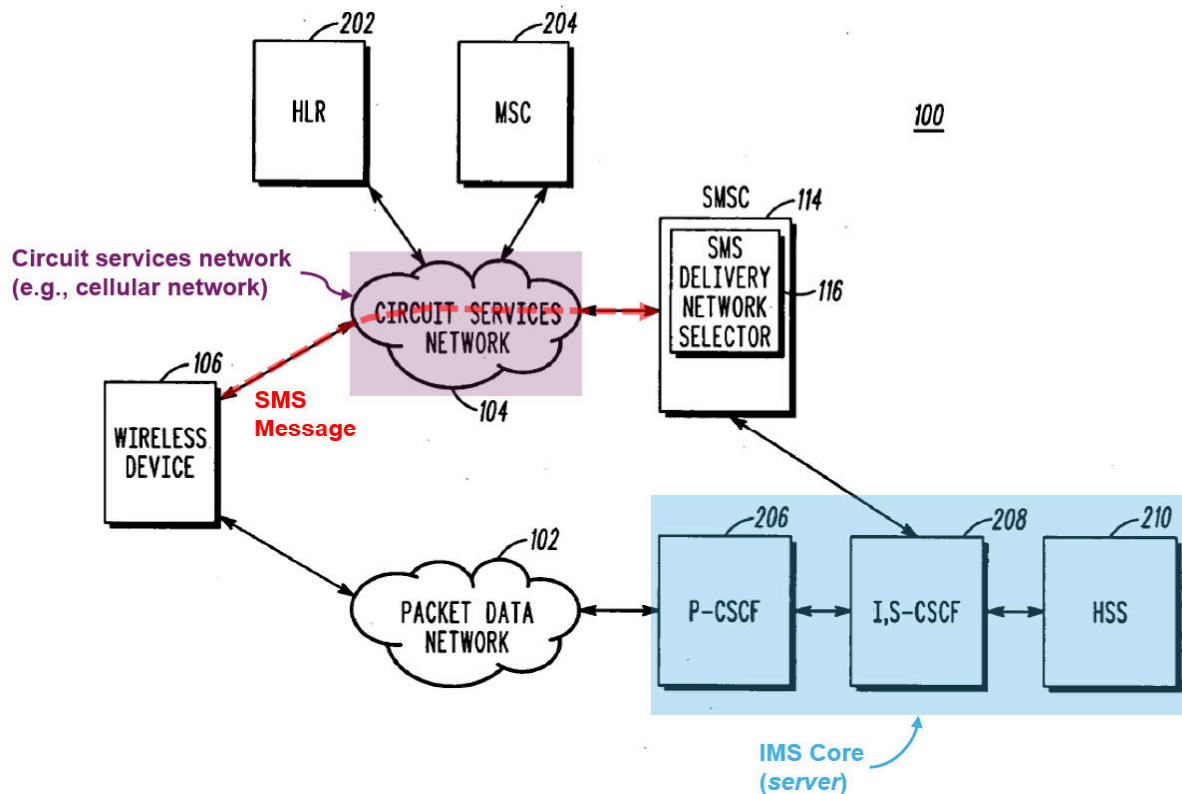


FIG. 2

APPLE-1004, FIG. 2 (Annotated)

See also APPLE-1057, FIG. 1 (depicting mobile device “in an SS7 switched circuit PLMN network 10” transmitting messages to SMSC 11 without traversing IMS Overlay Network 2), [0063]-[0065], FIG. 2; APPLE-1058, 75 (FIG. 3.2) (depicting mobile station transmitting SMS to via cellular base station subsystem to SMSC), 77 (“submitted from an MS to an SMSC”).

106. As I previously discussed for Elements [1b] and [1d], the sending device 106 transmits SMS messages over the circuit-services network 104 *via the cellular base station*. *Supra*, [1b], [1d]. These SMS messages are specifically transmitted via the cellular base station to SMSC 114 *before delivery to the*

addressed recipient. *Id.* To this point, Horvath explains that “when a SMS message request is received by the SMSC 114, the SMSC 114 first determines if the [addressed recipient] device 106 is registered on the packet data network,” and if the recipient device is registered, “[t]he SMSC 114 delivers the SMS message to the recipient device through the packet data network 102 via the SIP network.” APPLE-1004, [0046]. “If the recipient device is not registered on the packet data network 102, the SMSC 114 delivers the SMS message to the recipient device through the traditional circuit services network method (for example, ANSI-41 procedures).” *Id.*, [0047]; *see also id.*, [0048]-[0049], [0053], FIG. 6.

107. Horvath’s functionality for transmitting SMS messages from the sending device 106 over the circuit-services network 104 under appropriate conditions is maintained in the combination with Tsampalis and Tumminaro. And in the combination, the sending device’s determination whether to transmit an SMS message using the traditional circuit-services method is based at least in part on the addressed recipient’s capabilities information in the ***response failing to indicate that the addressed recipient corresponds to a subscriber of the [MMS or IM] service.*** *Id.* For example, the Horvath-Tsampalis-Tumminaro sending device implements Tsampalis’s suggestions for allowing a message to be formatted for transmission as an SMS message if the addressed recipient has “limited messaging capabilities” and is therefore not a subscriber of an IM or MMS service capable of receiving richly

formatted IM or MMS messages. APPLE-1005, [0062]-[0063] (“where the ... messaging format capabilities information 110 does not indicate compatibility with MMS messaging”); APPLE-1004, [0035], [0039]. When the recipient has limited messaging capabilities, the combination’s sending device 106 “inform[s] the associated user ..., and suggests to the user to transform (format the message to an SMS formatted message and send it.” APPLE-1005, [0062]. Automatic conversion to the SMS format also (while still providing the user with an option to abort) would have been obvious in some implementations based on Tsampalis’s teaching that the sending device 100 may “not inform the user” of the recipient’s limited messaging capabilities, thereby providing an even more efficient and seamless process that does not burden the user with choosing among message formats. *Id.*

108. As Tsampalis’s teachings are applied to Horvath, the combination’s sending device 106 would thus transmit an SMS message to the addressed recipient via the cellular base station using the traditional circuit-services method based at least in part on a determination that the recipient has limited messaging capabilities (*failing to indicate that the addressed recipient corresponds to a subscriber of the [MMS or IM] service*). For example, the sending device 106 would transmit an SMS message using the traditional circuit-services method when the addressed recipient has limited messaging capabilities, the sending device is not currently registered with the IMS (*e.g.*, the sending device may de-register at any time

including after receiving the response of [1h] and for any reason including incidentally as a result of moving outside the coverage area of an 802.11 access point that provides access to the packet-data network 102), and no election is made to abort the conversion or formatting of the message as an SMS for transmission. Notably, if the addressed recipient did not have limited messaging capabilities (and was instead a subscriber to a default IM or MMS service), it would have been obvious that the sending device 106 would instead format the message for transmission as an IM or MMS rather than SMS when the sending device is also registered to the IMS, or would defer transmission or “abort [transmission] completely” if the sending device were not registered to the IMS (*e.g.*, to avoid sending a message whose media files are lost and for which the user deems SMS inadequate as suggested in Tsampalis). APPLE-1005, [0052], [0072]; APPLE-1004, [0050], [0078], FIG. 7; *supra*, [1i].

Element [1m]: wherein the mobile wireless device transmits a message limited to one or more binary-encoded characters to the addressed recipient via the cellular base station and through a short message service center (SMSC) before delivery to the addressed recipient, based at least in part on the response failing to indicate that the addressed recipient corresponds to a subscriber of the service;

109. Horvath-Tsampalis-Tumminaro renders Element [1m] obvious. As I previously discussed for Claim [11], the combination’s sending device 106 (***mobile wireless device***) transmits an SMS message to the addressed recipient via the cellular base station and through SMSC 114 before delivery to the addressed recipient, based

at least in part on the response failing to indicate that the addressed recipient corresponds to a subscriber of the IM or SMS service. *Supra*, [11].

110. It was obvious that the SMS message transmitted by the Horvath-Tsampalis-Tumminaro sending device can be *limited to one or more binary-encoded characters*. For example, Tumminaro describes the sending device “encrypt[ing] a message” and sending the message as an “SMS message in binary rather than plain text.” APPLE-1034, [0561]; *see also id.*, [0539], [0566], [0653]-[0655]. Moreover, the SMS messages described in Horvath (and similarly in Tsampalis and Tumminaro) were limited to one or more binary-encoded characters, *e.g.*, up to a maximum of 140 bytes of raw data. This is evident from Horvath’s disclosure that wireless devices 106 and the network carry out SMS messaging according to the SS7 and ANSI-41 protocols. APPLE-1004, [0026], [0033] (“HLR 202 is a signaling system 7 (‘SS7 database’). SS7 is a set of telephony signaling protocols used to achieve connection control in a telephony network.”), [0050] (“transmits the SMS messages using ... ANSI-41 procedures”). SS7 and ANSI-41 protocols impose size limitations on SMS messages—a fact acknowledged even in the background discussion of the ’827 Patent itself. *See* APPLE-1001, 1:36-48 (“[O]ne of its biggest drawbacks is that an SMS message can only carry a small amount of data due to limitations imposed by the Mobile Application Part (MAP) protocol of SS7. An SMS message can only contain up to 160 8-bit alphanumeric

or binary characters ...”); *see also* APPLE-1034, [0539] (describing size-limited “binary SMS messages”); APPLE-1035, [0090] (“Short Messages are messages that contain up to 140 bytes of raw data, or 160 characters in single character sets.”), [0088]-[0094], [0141] (“SS7 bandwidth is limited and expensive”); APPLE-1036, 3:5-11 (“Transmission of the short messages between SMSC and phone can be done through different protocols such as SS7 within the standard GSM MAP framework or TCP /IP within the same standard. Messages are sent with the additional MAP operation forward short message, whose payload length is limited by the constraints of the signaling protocol to precisely 140 bytes (140 bytes = 140 * 8 bits = 1120 bits). In practice, this translates to either 160 7-bit characters, 140 8-bit characters, or 70 16-bit characters.”); APPLE-1059, 3 (“Both ANSI-41 and GSM MAP rely upon SS7 as a signaling protocol ...”).

Element [1n]: wherein the mobile wireless device transmits message content intended for a third party provider, to a server associated with the service, which forwards a message comprising the message content intended for the third party provider, to the third party provider, wherein the message forwarded to the third party provider is derived at least in part from a random number.

111. Horvath-Tsampalis-Tumminaro renders Element [1n] obvious. Tumminaro, for example, discloses “a mobile payment system where consumers may conduct transactions using a mobile device.” APPLE-1034, [0021]. Tumminaro’s “mobile payment platform” allows users to initiate transactions “through any number of means including SMS messaging, Web, e-mail, instant

messenger, a mobile client application, an instant messaging plug-in application or ‘widget.’” *Id.*, [0031]; *see also id.*, [0204]-[0206], [0358] (“SMS messaging, email MMS messaging, instant messaging”), Abstract. Tumminaro explains that a mobile message (*e.g.*, an SMS message) for a payment transaction can include a “key word that provides the type of transaction requested,” “the amount” of the transaction, “the target telephone number,” and optionally additional information. *Id.*, [0204]-[0206]. A message intended for the mobile payment system can further include “a unique sequence number” derived by the mobile device that uniquely identifies the transaction, which can be used to “help prevent spoof attacks,” “prevent fraud,” and “avoid[] duplication of financial transactions.” *Id.*, [0607]-[0608]. In some implementations, “the sequence number may be any number, including a random number.” *Id.*, [0607]. The sequence number can also “be generated using a seed created from a hash function on information such as the telephone number, time of day, or other.” *Id.*; *see also id.*, [0042], [0398]-[0399], [0548], [0552], [0559] (“SMS text message commands [are] sent to the server”), [0615], [0671], FIGs. 54-56.

112. As I previously described in §VIII.A(ii), the combination’s sending device 106 incorporates Tumminaro’s suggested use of mobile messaging services (*e.g.*, SMS, MMS, and/or IM) to conduct mobile payment transactions. *Supra*, §VIII.A(ii). Tumminaro explains that “[w]hen an account holder makes a transaction request from their mobile phone, information is routed to the mobile

operator,” and “[t]he information is then routed to the payment server through a secure Internet connection.” *Id.*, [0202], FIG. 3; *see also id.*, [0139], [0154] (“encompasses many mobile payment system implementations”). In the context of Horvath’s packet-data network 102, which includes an IMS-supported SIP network, and Horvath’s description of SIP MESSAGES carrying SMS, MMS, or IM messages being routed to corresponding application servers, it would have been obvious for the Horvath-Tsampalis-Tumminaro sending device 106 to transmit an SMS, MMS, or IM message containing Tumminaro’s payment transaction parameters in a SIP MESSAGE to the IMS core, which would route the message to an appropriate SMS, MMS, or IM application server (*e.g.*, SMSC 114, MMSC, or IM server), and which would in turn route the message over the Internet to a payment server as taught in Tumminaro. APPLE-1004, [0036]-[0040], [0050], FIG. 2; APPLE-1034, [0202].

113. Accordingly, it would have been obvious that the Horvath-Tsampalis-Tumminaro sending device (*mobile wireless device*) transmits payment transaction requests (*message content*) intended for a *payment server* (third party provider), to the IM or MMS application servers via the IMS core (*server associated with the service*), which forwards the transaction request (*message comprising the message content intended for the third party provider*), to the payment server (*third party provider*). A POSITA would have understood that the IMS core and the IM and

MMS application servers are each *servers associated with the [IM or MMS] service* since the IM and MMS application servers process messages respectively transmitted via the IM and MMS services, and the IMS core handles SIP signaling, authentication, and routing of messages for the IM and MMS services within the SIP network. Further, as discussed above, the message routed to the payment server can include a “random number” that uniquely identifies the transaction associated with the message. APPLE-1034, [0607]-[0608], [0559]. The message forwarded to the payment server (*third party provider*) is therefore *derived at least in part from a random number* since it includes the random transaction number.

114. Although claim 1 does not require that the server associated with the service derive the forwarded message by modifying the message from the mobile wireless device using a random number, it was nonetheless known and obvious before the Critical Date to implement servers that performed these exact operations, *e.g.*, by replacing identifying information in a message with randomized anonymous information before delivering the message to the intended recipient. APPLE-1060, 6:59-7:5 (describing “a service 214 to which emails between the sender and recipient are directed” and which “masks the identity of the sender and recipient ... to protect the anonymity of the [] participants”), 9:30-10:24 (server inserts encrypted ID derived from a “random number”), Abstract, FIGs. 3, 4b; APPLE-1061, Abstract (“A mobile device identifier (such as an MSISDN) that typically accompanies a

mobile device request is replaced with an ‘enriched’ identifier that exposes the mobile device user’s home operator but obfuscates the mobile device's (and, thus, the device user’s) identity.”); APPLE-1040, [024] (“replace sensitive information like-email addresses or credit card numbers with either false information or alternative information”), [051]; *infra*, §VII.F; *cf.*, APPLE-1001, 11:26-36 (“To hide a user’s identity, the message server may dynamically create a random number that maps to the user’s actual mobile number ...”). A POSITA would have found it obvious to similarly replace identifying information in messages sent from the Horvath-Tsampalis-Tumminaro wireless device to the payment server or to other user devices to mask the identity of the sender and provide improved privacy protections and security. A POSITA would have reasonably expected success since such techniques involve conventional message processing techniques that were well known by the Critical Date. *Infra*, §XI.A.

Claim [7]: The mobile wireless device of claim 1, wherein the message limited to one or more binary-encoded characters is further limited to less than a maximum allowable number of binary-encoded characters.

115. Horvath-Tsampalis-Tumminaro renders Claim [7] obvious for each of the reasons discussed above with respect to [1m]. *Supra*, [1m]. For example, the combination’s sending device transmits an SMS message limited to 140 bytes (*e.g.*, 160 7-bit characters, 140 8-bit characters, or 70 16-bit characters) (***limited to less than a maximum allowable number of binary-encoded characters***). *Cf.* APPLE-

1001, 1:42-48 ('827 Patent also disclosing SMS message limited to 160 binary characters).

Claim [11]: The mobile wireless device of claim 1, wherein the request is encapsulated⁷ in hypertext transfer protocol (HTTP) and a message to the addressed recipient is encapsulated in HTTP; wherein the server that receives packet-switched messages transmitted via the service to recipient devices that correspond to subscribers of the service is located outside of the cellular network; wherein the server that maintains the subscriber list is located outside of the cellular network.

116. Horvath-Tsampalis-Tumminaro renders Claim [11] obvious. Tumminaro discloses the conventional practice of encapsulating requests that a client device sends to a server over a packet-switched network (like the request that the sending device 106 sends to the IMS core (*supra*, [1g])) in HTTP. APPLE-1034, [0901] (“A protocol for communicating with the system may be selected, such as HTTPS, HTTP, or SMS.”), [0806] (“changing the protocol (*i.e.*, SMS or HTTP) that they use to send and receive payment information between their mobile device and the server”), [0156], [0161], [0203], [0573]. A POSITA would have found it obvious to encapsulate the request in HTTP as taught in Tumminaro because HTTP was a well known, reliable, and commonly implemented protocol allowing

⁷ The specification of the '827 Patent does not describe encapsulation of any message or data, the word “***encapsulated***” or its alternative forms (*e.g.*, encapsulation/encapsulating/encapsulate) does not appear in the specification.

communication of requests and responses between sending device and the server. For similar reasons, it would have been obvious to encapsulate a message sent from the sending device 106 to the addressed recipient in HTTP (*e.g.*, the addressed recipient may be another user device or a third-party provider like Tumminaro's payment server). Tumminaro describes the benefits of being able to select different messaging protocols for communicating with a sending device, including options that employ HTTP. APPLE-1034, [0901]; *see also id.*, [0156], [0161], [0203], [0573], [0806]; APPLE-1042, [0003]-[0004], [0010], [0035], [0050], [0061]-[0062], [0067] (describing known options for HTTP-based messaging).

117. A POSITA also would have found it obvious that the IMS core (“*server that receives packet-switched messages...*” and “*server that maintains the subscriber list*”) is located outside of the cellular network. As discussed in greater detail above with respect to [11], the sending device 106 transmits an SMS message to the addressed recipient via the cellular base station without traversing the IMS core (*server*) because the IMS core resides in Horvath's packet-data network 102—not the cellular network. *Supra*, [11]; *see also supra* [1pre] and [1g] (mappings to the claimed “server[s]”); APPLE-1004, [0024]-[0025], [0031]-[0034], FIG. 2. For example, where the packet-data network 102 includes an 802.11 network as described in Horvath, the IMS core may reside in the 802.11 network or the Internet (or other portion of the packet data network 102) rather than any cellular network.

APPLE-1004, [0024]-[0025]. Even where the packet-data network 102 includes GPRS, EV-DO, or UMTS, it would have been obvious to implement the IMS core outside the GPRS, EV-DO, or UMTS cellular networks because the IMS is commonly implemented outside the cellular network. APPLE-1052, FIG. 1 (depicting IMS outside of the cellular network); APPLE-1046, FIG. 4 (depicting Internet (where the IMS may be implemented) outside of the cellular network).

Claim [16]: The mobile wireless device of claim 1, further comprising: wherein the mobile wireless device registers a user name tag or handle with the service, wherein the mobile wireless device transmits an authentication identifier for authentication to the service.

118. Horvath-Tsampalis-Tumminaro renders Claim [16] obvious. Horvath discloses that sending device 106 “registers with the IMS network” and the home subscriber server (HSS) 210 in the IMS core maintains a “database including profiles associated with each wireless device 106 registered with the IMS.” APPLE-1004, [0034]-[0035]. The information stored by HSS 210 “includes information to identify each registered wireless device 106 such as a telephone uniform resource identifier (‘tel-URI’) and/or a SIP uniform resource identifier (‘SIP-URI’).” *Id.*, [0035]. The “SIP registration[] ... allows the S-CSCF to bind the location of the wireless device 106 (for example, the IP address of the device) and the SIP address.” *Id.*, [0038]. The sending device 106 (***mobile wireless device***) thus registers a “tel-URI” and/or a “SIP-URI” (***a user name tag or handle***) with the IMS SIP network, which implements the MMS and IM services (***service***). *Supra*, [1pre]; APPLE-1004,

[0033], [0039]; APPLE-1026, §4 (“SIP URIs are defined in Section 19.1. It has a similar form to an email address, typically containing a username and a host name. In this case, it is sip:bob@biloxi.com, where biloxi.com is the domain of Bob’s SIP service provider.”), §19.1 (“The ‘sip:’ and ‘sips:’ schemes follow the guidelines in RFC 2396 [5]. They use a form similar to the mailto URL... The formal syntax for a SIP or SIPS URI is presented in Section 25. Its general form, in the case of a SIP URI, is: sip:user:password@host:port;uri-parameters?headers”); APPLE-1044, 1-3; APPLE-1045, 4-5, 7.

119. Horvath-Tsampalis-Tumminaro also renders obvious the sending device 106 *transmitting an authentication identifier to the service*. According to Horvath, “[t]he P-CSCF 206 is a SIP proxy and is the first contact point for a wireless device 106 registered in the IMS network.” APPLE-1004, [0036]. “The wireless device 106 locates its respective P-CSCF 206” and “[a]ll signaling messages are intercepted by the P-CSCF 206.” *Id.* “The P-CSCF 206 authenticates the wireless device 106.” *Id.* “[A]fter successful registration of a wireless device 106 with the S-CSCF component of the I, S-CSCF 208, security keys are sent to the P-CSCF 206, which allows it to setup a security association with the wireless device 106.” *Id.*; *see also id.*, [0035]-[0036], [0038], [0040]-[0041], [0072]-[0073], FIG. 5. By locating the P-CSCF 206 and transmitting signaling messages that allow the P-CSCF 206 to perform authentication, the sending device 106 *transmit[s] an authentication*

identifier to the IMS, which implements the MMS and IM services (*service*). See also APPLE-1004 (“P-CSF 206 ... is trusted by the other IMS components” including the application servers, “which therefore do not perform further authentication of the wireless device 106”). Moreover, Horvath explains that “[t]he basic functions of an IMS network should be known to those [of] ordinary skill in the art,” and a POSITA would have understood therefore that the IMS described in Horvath would implement standard SIP authentication protocols in which user agents (*e.g.*, device 106) transmit authentication identifiers to the service. APPLE-1044, 15 (“a signed message/cpim body can provide sender authentication”); APPLE-1026, 193-201 (“SIP provides a stateless, challenge-based mechanism for authentication” involving “usernames,” “passwords,” and similar “credentials”).

Claim [17]: The mobile wireless device of claim 1, wherein the mobile wireless device receives an indication that the wireless device of the addressed recipient is authenticated to the service.

120. Horvath-Tsampalis-Tumminaro renders Claim [17] obvious. As I previously discussed for Elements [1g]-[1h], the combination’s sending device 106 requests and receives messaging capabilities information for the addressed recipient of a message. *Supra*, [1g]-[1h]. Further as I previously discussed for Elements [1g]-[1h], it would have been obvious that the capabilities information returned to the sending device 106 would include an indication whether the addressed recipient is currently registered with the IMS and capable of receiving messages over services

(e.g., MMS, IM) provided by the IMS. *Id.* Information indicating that the addressed recipient is currently registered with the IMS itself constitutes an indication that the addressed recipient is authenticated to the IMS and thus authenticated to the MMS and IM *services* (which are at least partially implemented on the IMS) because the addressed recipient must authenticate to register with the IMS. APPLE-1004, [0035] (“P-CSCF 206 authenticates the wireless device 106” and “after successful registration of a wireless device 106” the P-CSCF 206 “set[s up] a security association with the wireless device 106”), [0040] (“authentication and authorization of the wireless device 106”), [0041], [0072] (“authenticates and registers the wireless device 106 with the IMS core”); APPLE-1044, 15 (“a signed message/cpm body can provide sender authentication”); APPLE-1026, 193-201 (“SIP provides a stateless, challenge-based mechanism for authentication”).

Claim [18]: The mobile wireless device of claim 1, wherein the mobile wireless device is not enabled to transmit messages via the server that receives packet-switched messages transmitted via the service to recipient devices that correspond to subscribers of the service before authentication of the mobile wireless device to the service.

121. Horvath-Tsampalis-Tumminaro renders Claim [18] obvious. Horvath teaches that a sending device 106 communicates via the IMS core (*server*) and SIP network only if the sending device 106 registers with the IMS. APPLE-1004, [0050], [0077]-[0078], FIG. 7. The IMS implements aspects of the IM and MMS services (*service*), and as I previously discussed (*supra*, Claim [17]), each wireless device

106 that registers and communicates through the IMS must first be authenticated. *Supra*, [1pre], [17]; APPLE-1004, [0036]-[0041], [0072], FIG. 5. Accordingly, the Horvath-Tsamaplis-Tumminaro sending device 106 would not be enabled to transmit messages via the IMS core (*server*) before authentication of the device 106 to the IMS, and thus to the MMS and IM services supported by the IMS. For example, just as Horvath teaches that the sending device 106 is not enabled to transmit SMS messages through the IMS over packet data network 102 if the device 106 is not registered (and thus not authenticated) with the IMS, the sending device 106 would likewise not be enabled to transmit MMS or IM messages via the IMS core before authentication and registration since registration and authentication to the IMS core provides the sending device with access to each of the services on the IMS. APPLE-1004, [0036], [0041] (“does not have to authenticate the wireless device 106 because the S-CSCF 206 has already done so”), [0050], [0077]-[0078], FIG. 7.

Claim [19]: The mobile wireless device of claim 1, wherein the mobile wireless device transmits location information.

122. Horvath-Tsmpalis-Tumminaro renders Claim [19] obvious. For example, Horvath discloses that the sending wireless device 106 registers with the IMS by transmitting information that allows the “S-CSCF to bind the location of the wireless device 106 (for example, the IP address of the device) and the SIP address.” APPLE-1004, [0038]; *see also id.*, [0035] (“The HSS 210 also provides information

about the physical location [of wireless devices 106] to requesting entities such as the SMSC 114.”), [0037] (“retrieves the location of the wireless device 106”), [0003] (“transmits ... device’s status and current location”). A POSITA would have understood that the sending device 106 thus transmits ***location information*** (e.g., IP address) to the IMS core to enable the S-CSCF to bind the device’s location information to the SIP address. APPLE-1026, 17 (“Upon initialization, and a periodic intervals, Bob’s SIP phone sends REGISTER messages to a server ... known as a SIP registrar. The REGISTER message associates Bob’s SIP or SIPS URI ... with the machine into which he is currently logged.”); *see also id.*, APPLE-1004, [0070] and FIG. 4 (disclosing GPS module 106 used to “determine the location” of the device 106); *cf.* APPLE-1001, 11:26-30 (minimal description regarding the recited “***location information***”).

123. Also in the combination, Tumminaro discloses that “location technology” can be used to “determine the physical location of the device,” which allows “services made available to the account holder [to] be adjusted based on where they are located.” APPLE-1034, [0613]; *see also id.*, (“locationName •String value that identifies where the transaction occurred, for instance, a store ID or an ATM ID”), [0589], [1059]-[1070]. Accordingly, it would have been obvious further based on Tumminaro’s teachings for the Horvath-Tsampalis-Tumminaro sending device 106 to transmit location information in messages intended for the payment

server (*third-party provider*) to enable the payment server to make location-based service adjustments.

Claim [20]: The mobile wireless device of claim 19, wherein the message forwarded to the third party provider is derived at least in part from the location information.

124. Horvath-Tsampalis-Tumminaro renders Claim [20] obvious. As I previously discussed for Claim [19], the Horvath-Tsampalis-Tumminaro sending device 106 transmits location information in messages intended for the payment server (*third-party provider*) to enable the payment server to make location-based service adjustments. APPLE-1034, [0613], [1078], [0527]-[0528] (“the shopper can conclude a purchase transaction with the payment server handling the details such as ‘ship to’ address and funds transfer....the account holder has the option to select a ‘deliver to the current geographical location’ rather than the account holder’s billing address”), [0589], [1059]-[1070]; *supra*, [19]. Because the payment server implements payment transactions and is responsible for making location-based adjustments, it would have been obvious that the message forwarded to the payment server is derived at least in part from the location information indicating the location of the sending device 106. *Id.*; *see also supra*, [1n]; *cf.* APPLE-1001, 11:26-30.

Claim [21]: The mobile wireless device of claim 1, wherein the mobile wireless device is authenticated to the service, via a mobile phone number of the mobile wireless device, prior to receiving the response.

125. Horvath-Tsampalis-Tumminaro renders Claim [21] obvious. Horvath teaches that a sending device 106 communicates via the IMS core (*server*) and SIP network only if the sending device 106 registers with the IMS. APPLE-1004, [0050], [0077]-[0078], FIG. 7. The IMS implements or is connected to the IM and MMS services (*service*), and as I previously discussed (*supra*, Claim [17]), each wireless device 106 that registers and communicates with the IMS must first be authenticated. *Supra*, [1pre], [17], [18]; APPLE-1004, [0036]-[0041], [0072], FIG. 5. It follows that the sending device 106 would not receive from the IMS a *response* containing an addressed recipient's capabilities information (*supra*, [1g]-[1h]) until the sending device 106 was registered and authenticated with the IMS, and thus authenticated to the IM and MMS services supported by the IMS. *Supra*, [18]. Authenticating prior to receiving the response also would have been obvious to improve security and prevent unauthorized leaks of information about registered devices that would be contained in the response from the IMS to non-authenticated devices. Indeed, Horvath expressly teaches that a wireless device 106 must be registered (and hence authenticated) with the IMS for any messages to be delivered from the IMS to the device 106. APPLE-1004, [0045]-[0047], [0075]-[0076], FIG. 6. Horvath further teaches that the wireless device 106 uses a SIP contact address for registration and authentication, where the contact address can be a "telephone uniform resource identifier ('tel-URI')" corresponding to "the telephone number assigned to the

wireless device 106” (*mobile phone number of the mobile wireless device*). *Id.*, [0035]; APPLE-1026, 36, 60, 157-158 (details of “tel URL”).

Claim [23]: The mobile wireless device of claim 1, wherein the message limited to one or more binary-encoded characters is a signaling system 7 (SS7) message.

126. Horvath-Tsampalis-Tumminaro renders Claim [23] obvious. As I previously described for Element [1m], SMS messages transmitted by the sending device 106 over circuit-services network 104 include *signaling system 7 (SS7)* messages limited to one or more binary-encoded characters. *Supra*, [1m].

Claim [25]: The mobile wireless device of claim 1, wherein a negative response is consistent with the addressed recipient being unknown to the server that maintains the subscriber list.

127. Horvath-Tsampalis-Tumminaro renders Claim [25] obvious. As I previously discussed for Element [1h], *supra*, the sending device 106 in the combination can receive a *negative response indicat[ing] that the wireless device of the addressed recipient is not a subscriber of the service* (e.g., a response indicating that the device has “limited capabilities” or a response that otherwise lacks information indicating that the device is subscribed to the MMS or IM services). *Supra*, [1h]. Horvath further explains that a wireless device “may not be registered ... because it never was registered to begin with,” in which case “an IMS contact address[] ... does not exist” for the device. APPLE-1004, [0047], [0076]. A negative response is thus consistent with the addressed recipient having never

registered with the IMS to begin with such that no IMS contact address exists for the recipient (*unknown to the server that maintains the subscriber list*).

Claim [26]: The mobile wireless device of claim 1, wherein the random number is generated by the server associated with the service which forwards the message comprising the message content intended for the third party provider.

128. Horvath-Tsampalis-Tumminaro renders Claim [26] obvious. As I previously discussed for Element [1n], it would have been obvious for the ***random number*** from which the message forwarded to the payment server (***third party provider***) is derived to be generated by the IMS core or the IM or MMS application servers (***server associated with the service***). *Supra*, [1n]; APPLE-1034, [0021], [0031], [0204]-[0206], [0358], [0559], [0607]-[0608]; APPLE-1060, 6:59-7:5, 9:30-10:24, Abstract, FIGs. 3, 4b; APPLE-1061, Abstract.

Claim [27]: The mobile wireless device of claim 1, wherein the multimedia messages comprising at least one of images, audio clips or videos are multimedia message service (MMS) messages.

129. Horvath-Tsampalis-Tumminaro renders Claim [27] obvious. As I previously explained for Element [1b], the sending device's cellular transceiver and a cellular base station in the combination system communicate using EV-DO, GPRS, or UMTS protocols (***a radio communications protocol that supports transmission of multimedia messages comprising at least one of images, audio clips, or videos***). *Supra*, [1b]. EV-DO, GRPS, and UMTS each define protocols that support ***MMS messages***. APPLE-1004, [0024]-[0025] (“[MMS] and the like are also included in

the networks 102”); APPLE-1048, 6-9 (describing UMTS, GPRS, EV-DO support for multimedia transmissions including MMS).

Element [29pre]: A method comprising:

130. *Supra*, [28pre].

Element [29a]: receiving, from a first mobile wireless device via the Internet, a subscription message for subscribing the first mobile wireless device to a service for receiving packet-switched messages other than short message service (SMS) messages, enhanced messaging service (EMS) messages and multimedia message service (MMS) messages;

131. Horvath-Tsampalis-Tumminaro renders Element [29a] obvious. As I previously discussed with respect to [1pre], Horvath describes “instant messaging” (IM) as a ***service for receiving packet-switched messages*** (other than SMS, EMS, and MMS) that is supported by the IMS on the packet-switched SIP network. APPLE-1004, [0033], [0039], FIG. 2; *supra*, [1pre]; APPLE-1044, 1-4 (RFC disclosing details of SIP-based instant messaging).

132. Horvath also describes that the wireless device 106 “transmit[s] a SIP register message to the IMS core,” which supports the SIP capabilities used to establish instant messaging, and the S-CSCF (part of the SIP network and IMS core) “receives the SIP register message.” APPLE-1004, [0033] [0040] (“The wireless device 106 registers with the S-CSCF component of the I, S-CSCF 208. When the S-CSCF receives a registration request from the wireless device 106, the S-CSCF contacts the HSS 210 for authentication and authorization of the wireless device

106.”), [0071]-[0073] (“The wireless device 106, at step 504, registers with the IMS core by transmitting a SIP register message to the IMS core. The S-CSCF component of the I, S-CSCF 20S, at step 506, receives the SIP register message.”), FIG. 5 (below).

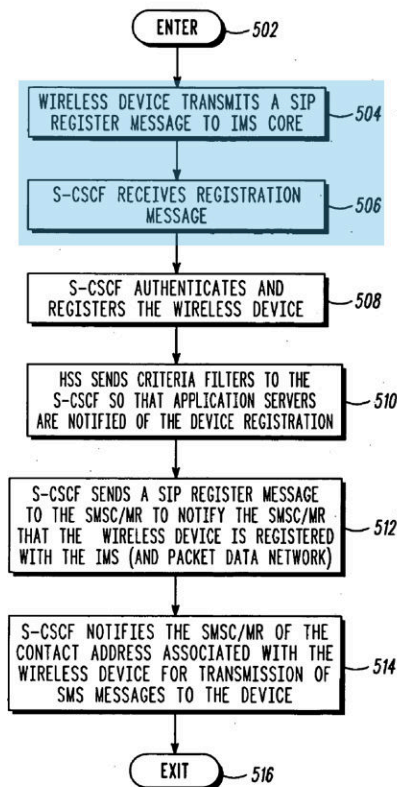


FIG. 5

APPLE-1004, FIG. 5 (Annotated)

133. The “SIP register message” (*subscription message*) received by the IMS core from a first wireless device 106 effects a subscription to the IM service (*for subscribing the first mobile wireless device to a service*) since the registration allows the first wireless device 106 to access services and receive messages via services supported by the SIP network including IM. APPLE-1004, [0034]

(“wireless device 106 registers with the IMS network”), [0038] (“SIP registration[] allows the S-CSCF to bind the location of the wireless device 106 (for example, the IP address of the device) and the SIP address” such that “services subscribed to by the device 106 can be provided”), [0041] (“HSS 210 includes filter criteria for the wireless device 106 that causes registration events to be sent” to a “SIP application server”), [0042] (“subscribes to a registration event package”); APPLE-1026 (“The REGISTER messages associate Bob’s SIP or SIPS URI (sip:bob@biloxi.com) with the machine into which he is currently logged”).

134. Thus, when the IMS core receives a SIP register message from a first wireless device 106, the location (*e.g.*, IP address) is registered with the SIP network and application servers (including an application server for the IM service) are notified of the device 106’s registration. This allows the IM service to deliver IMs and related packet-switched messages from the service (*e.g.*, presence information) to the wireless device 106 using registered location (*e.g.*, IP address) of the device. Accordingly, registration allows the wireless device 106 to receive or access messages from the IM service, indicating that the SIP register message is a ***subscription message*** that effects subscription of the device 106 to the IM service. APPLE-1062. Indeed, Horvath explicitly notes that the device’s registration is stored in “home subscriber server 210,” which “comprises a database including profiles associated with each wireless device 106 registered with the IMS,” where

the “profile[] ... includes subscription related information.” APPLE-1004, [0035]; *see also id.*, [0040]-[0041], [0072]-[0076], FIG. 5. Horvath also acknowledges that “[t]he basic functions of an IMS network should be known to those [of] ordinary skill in the art,” and this being the case, a POSITA also would have found obvious that the first wireless device 106 would send subscription messages to the IMS core both to sign-up for IM service and to receive presence information indicating the availability of other IM users consistent with commonly implemented IMS, SIP, and IM standards. APPLE-1043, 1 (“A presence and instant messaging system allows users to subscribe to each other”); APPLE-1063, 8 (“A SUBSCRIBER MUST be able to request a SUBSCRIPTION to a PRESENTITY’S PRESENCE INFORMATION”); APPLE-1064, (“A presence agent is a SIP user agent which is capable of receiving SUBSCRIBE requests, responding to them, and generating notifications of changes in presence state.”). These additional forms of subscription messages are consistent with Horvath’s teaching to implement instant messaging on the SIP network and to allow the first wireless device 106 to access the IM service and receive presence information indicating the availability of other subscribers of the IM service.

135. In addition, a POSITA would have found obvious that, in the combined system and in accordance with Horvath’s teachings, the IMS core would receive *subscription messages* (e.g., SIP register message or SUBSCRIBE request) from a

first mobile wireless device 106 *via the Internet*, for at least the reasons described for Elements [1a] and 1[g], that messages are received by the IMS core over the Internet when the sending device 106 transmits over packet-data network 102. *Supra*, [1a], [1g]. For example, Horvath discloses the packet network 102 being “an Internet Protocol (‘IP’) connectivity network.” APPLE-1004, [0009], [0021], [0024], [0050]; APPLE-1005, [0028].

Element [29b]: storing information indicating that a first mobile phone number of the first mobile wireless device corresponds to a subscriber of the service, in a subscriber data store;

136. Horvath-Tsampalis-Tumminaro renders Element [29b] obvious. As I previously discussed for Elements [1g] and [29a], Horvath discloses HSS 210 storing a “subscriber profile” (*storing information...in a subscriber data store*) for “each wireless device 106 registered with the IMS.” APPLE-1004, [0035]; *supra*, [1g], [29a]. “A profile[] ... includes subscription related information.” APPLE-1004, [0035]. Further, the IMS system includes “application servers that host and execute services for the wireless device 106,” namely “services subscribed to” including an instant messaging (IM) service. APPLE-1004, [0033], [0038]-[0039]. For example, “[t]he S-CSCF [] determines 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.” *Id.*, [0038]. “The HSS 210 also includes information to identify each registered wireless device 106 such as a

telephone uniform resource identifier (‘tel-URI’),” where the “tel-URI, for example is the telephone number assigned to the wireless device 106.” *Id.*, [0035].

137. Furthermore, Horvath teaches that the IMS core can determines that the wireless device is not registered with the SIP/IMS network establishing IM if “an IMS contact address” such as tel-URI “does not exist for the wireless device,” while if the wireless device is already registered with the SIP/IMS network, then “an IMS contact address...exists for the wireless device.” APPLE-1004, [0072]-[0076]; *see also* [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.”). A wireless device 106 whose tel-URI is registered and associated with the IM service indicate that the device 106 is a subscriber to the IM service.

138. Accordingly, it would have been obvious that the Horvath-Tsampalis-Tumminaro system stores in the IMS core (*e.g.*, within HSS 210) a subscriber profile for a first wireless device 106 indicating that the device is a subscriber of an IM service (*information indicating that a first mobile phone number of the first mobile wireless device corresponds to a subscriber of the service, in a subscriber data store*).

Element [29c]: receiving a first request, from a second mobile wireless device, the first request including at least information corresponding to the first mobile phone number of the first mobile wireless device;

139. Horvath-Tsampalis-Tumminaro renders Element [29c] obvious. For example, as I previously discussed for Element [1g], the IMS core receives a first request from a second mobile wireless device 106 that intends to send a message to a first mobile wireless device 106 for the first mobile wireless device's messaging capabilities information (including subscription related information). *Supra*, [1g].

Element [29d]: determining, via the subscriber data store, in response to receiving the first request, that the first mobile phone number of the first mobile wireless device corresponds to a subscriber of the service;

140. Horvath-Tsampalis-Tumminaro renders Element [29d] obvious. As I previously discussed for Element [1g], the IMS core determines responses to sending wireless devices' requests for the messaging capabilities of intended recipient devices. *Supra*, [1g]. Determining responses to such requests includes determining whether the intended recipient is a subscriber capable of messaging according to each of multiple different formats supported by different messaging services (*e.g.*, SMS, MMS, IM). *Id.* For example, Tsampalis discloses that a recipient device's capabilities information can "assign[]" to each messaging format "an associated value" that indicates "yes" or "no" whether the recipient device supports that format. APPLE-1005, [0060]. In some implementations, a network element (*e.g.*, a server) determines the capabilities of a recipient device in response to a request by generating a "new capabilities signal" that indicates whether the recipient is capable of messaging according to a particular format. *See* APPLE-1005, [0058] (describing

a first value in a new capabilities signal that “indicate[s] that the message type ... is unsupported” and a second value indicating otherwise), [0059], [0057], [0025], [0039], FIGs. 13-15. Horvath likewise discloses that a component of the IMS core (e.g., S-CSCF) determines each service that a wireless device is subscribed to in response to a request so that the request can be forwarded to the application servers for the “services subscribed to by the device 106.” APPLE-1004, [0038]; *see also id.*, [0035] (identifying wireless devices by a “tel-URI” phone number), FIG. 2. As I previously discussed (*supra*, [1g]), the request would be processed by the **subscriber data store** (e.g., the IMS core including HSS 210). *Supra*, [1g]; APPLE-1004, [0035], [0038]-[0044]. Accordingly, it would have been obvious that the Horvath-Tsampalis-Tumminaro combination determines, via the subscriber data store, in response to receiving a first request from a second mobile device, that the first mobile phone number of a first mobile wireless device, corresponds to a subscriber of the IM service.

Element [29e]: transmitting a first response, to the second mobile wireless device, indicating that the first mobile wireless device corresponds to a subscriber of the service;

141. Horvath-Tsampalis-Tumminaro renders Element [29e] obvious for each of the reasons discussed above with respect to Elements [29d] and [1h].

Element [29f]: receiving a second request, from the second mobile wireless device, the second request including at least information corresponding to another phone number; and

Element [29g]: transmitting a second response, to the second mobile wireless device, indicating that the another phone number does not correspond to a subscriber of the service;

142. Horvath-Tsampalis-Tumminaro renders Elements [29f]-[29g] obvious. The IMS core in the combination receives requests and transmits responses like those recited in Elements [29f]-[29g] for each of the reasons described in further detail above with respect to Elements [1g]-[1h] and [29c]-[29e]. *Supra*, [1g]-[1h], [29c]-[29e]. It also would have been obvious for the same mobile device, *e.g. the second mobile device*, to request messaging capabilities information for multiple intended recipient devices that each have different phone numbers. For example, Tsampalis describes scenarios in which “there are multiple remote recipients,” in which case the sending mobile device (*second mobile device*) obtains capabilities information for each recipient and determines how to format and transmit a message to each recipient according to the recipient’s respective capabilities. APPLE-1005, [0062]-[0063], [0035] (“each such recipient ID 402 is checked”). Tsampalis also describes that some recipients may support rich messaging capabilities such as MMS (or IM) while others do not. *Id.* Accordingly, it would have been obvious that the Horvath-Tsampalis-Tumminaro server receives a *second request*, from the sending wireless device 106 (*second mobile wireless device*) including at least *information corresponding to another phone number*, and transmits a *second response* to the

sending wireless device 106 *indicating that the another phone number does not correspond to a subscriber of the service.*

Element [29h]: wherein a server associated with the service receives message content intended for a third party provider, from the second mobile wireless device, and forwards a message comprising the message content intended for the third party provider, to the third party provider, wherein the message forwarded to the third party provider is derived at least in part from a random number.

143. Horvath-Tsampalis-Tumminaro renders Element [29h] obvious for each of the reasons described above with respect to Element [1n].

Claim [30]: The method of claim 29, wherein the server associated with the service does not receive message content intended for the third party provider from another mobile wireless device associated with the another phone number.

144. Horvath-Tsampalis-Tumminaro renders Claim [30] obvious. As I previously discussed for Element [1n], the IMS core (optionally including IM application servers) or the IM application servers themselves alternately provide a *server associated with the [IM] service* that forwards a message from the sending device 106 (*mobile wireless device*) to a payment server (*third-party provider*). *Supra*, [1n]. Further, for the reasons I previously discussed for Claim [25] and Element [29g], the server determines that *the another phone number* does not correspond to a subscriber of the IM services on the IMS, and this is consistent with *another mobile wireless device associated with the another phone number* being unknown to the IMS servers that maintain the subscriber list. *Supra*, [25], [29g]. Because devices must be registered with the IMS to perform messaging via the IMS

(including the IMS core and application servers), it would have been obvious that neither the IMS core nor the IM application servers would receive message content from the *another mobile wireless device associated with the another phone number* that is not registered with the IMS and not subscribed to the IM services. *Id.*; *see also supra*, [21]. Per Horvath’s teachings, a device that is not registered with the IMS would transmit the message as an SMS to the SMSC 114 (which would then be responsible for forwarding the message to the payment server), bypassing the IMS core and IM application servers. APPLE-1004, [0050], [0077]-[0078], FIG. 7; APPLE-1034, [0021], [0204]-[0206], [0358] (“SMS messaging”). Even if the *another mobile wireless device* sent the message as an IM using SIP protocols, it would have been obvious that a different IMS server including a different P-CSCF 206, *i.e.*, a server other than the *server associated with the [IM or MMS] service*) would receive the message if the *another mobile wireless device* were located in a different region or the DHCP protocol otherwise assigned the device a different P-CSCF 206. APPLE-1004, [0036]-[0038].

IX. GROUND 1B: CLAIMS 2-3, 8, 28 ARE OBVIOUS IN VIEW OF THE HORVATH-TSAMPALIS-TUMMINARO-DORENBOSCH COMBINATION

A. Combining Horvath, Tsampalis, Tumminaro and Dorenbosch

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

operating real-time IM services using wireless devices, as contemplated by Horvath and Tumminaro, and provided in the Horvath-Tsampalis-Tumminaro combination of Ground 1A. APPLE-1004, [0033] (describing the SIP network “establishing instant messaging”); APPLE-1065, [0007] (describing that when networks are unreliable “messages sent by real-time messaging clients often fail to get delivered to the recipient”). Dorenbosch discloses techniques that mitigate the impact of unreliable wireless networks on IM services. APPLE-1039, [0005] (describing that “mobile station participant may move in and out of service during an IM session, [and] it may not be possible for the mobile station to maintain a reliable connection with the login server,” which leads to “inadvertently dropped” messages), [0021] (describing that the disclosed techniques “minimize[] the occurrence of instant messages intended for the mobile subscriber being dropped”).

146. As described in §VII.D, Dorenbosch describes an IM proxy caching and bundling IM messages for more efficient use of network overhead, maintaining presence status for IM subscribers, attempting redelivery of messages that are directed to IM subscribers who lose network coverage, and adjusting recipient IM subscriber presence status when the cached messages cannot be delivered after a number of retries. APPLE-1039, [0020], [0024], [0029], [0030], [0039]-[0040]. It would have been obvious to integrate Dorenbosch’s techniques into the combination to enhance IM communications on the packet-switched networks described in

Horvath and provided in the combination. Multiple reasons would have prompted a POSITA to integrate Dorenbosch's techniques in the combination in this manner.

147. First, a POSITA would have been motivated to apply Dorenbosch's message bundling and delivery retry techniques to the combination to reduce the number of dropped messages when communicating through IM. APPLE-1039, [0021], [0024], [0026], [0030]. "Because a mobile station participant may move in and out of service during an IM session, it may not be possible for the mobile station to maintain a reliable connection with the login server." APPLE-1039, [0005]. "If the connection is lost, messages targeted at the mobile station will be inadvertently dropped." APPLE-1039, [0005]. Dorenbosch's IM proxy maintains a consistent connection with the IM server so that it can cache messages and retry delivering them when a mobile device temporarily loses network connection, which "minimizes the occurrence of instant messages intended for the mobile subscriber being dropped." APPLE-1039, [0021], [0024], [0026], [0030].

148. Second, a POSITA would have been motivated to apply Dorenbosch's message-bundling and delivery-retry techniques to the combination to decrease overhead in the wireless system, furthering Horvath's similar goals. *Compare* APPLE-1004, [0004]-[0005] (identifying the need to overcome the problem of "creat[ing] unnecessary overhead" in the wireless system), [0039] *with* APPLE-1039, [0036]-[0038] (describing bundling techniques to "minimize system connection

overhead in a manner that also minimizes the amount of latency”). Dorenbosch recognized that a “circuit-switched mobile network [like the one taught in Horvath] has both a considerable delay associated with an IM connection set-up and a high cost associated with maintaining an open connection during an IM session,” and Dorenbosch’s message-bundling techniques ease this high cost. APPLE-1039, [0006], [0033], [0036]-[0037].

149. Third, a POSITA would have found obvious that maintaining a connection to the IM system on behalf of the mobile device, *e.g.*, with an IM proxy, would have allowed the “the mobile subscriber [to] continue[] to appear available to IM buddies when the mobile subscriber is roaming or temporarily out of service even after the IM proxy unsuccessfully attempts to send an instant message to the mobile subscriber.” APPLE-1039, [0030]. A POSITA would have readily recognized that this would have created a more pleasing experience for users of both the sending and receiving devices, as it would have prevented the unpleasant appearance that the receiving device is frequently transitioning between available and unavailable status. *See* APPLE-1065, [0007] (describing the poor user experience of unreliable network connections).

150. A POSITA would have reasonably expected success implementing the combination as the messaging and communication protocols involved were all well known before the Critical Date. Further, the techniques integrated from Dorenbosch

in the combination are fully compatible with Horvath's, Tsampalis's, and Tumminaro's teachings and would not disturb the ability of Horvath's system to transmit or deliver messages over either a packet-based or circuit-switched network, the use of capabilities-based messaging techniques taught by Tsampalis, or Tumminaro's mobile payment transactions.

B. Analysis with Respect to Claims 2-3, 8, 28

Claim [2]: The mobile wireless device of claim 1, wherein the mobile wireless device selects a packet-switched bearer for transmission of a message to the addressed recipient via the server that receives packet-switched messages transmitted via the service to recipient devices that correspond to subscribers of the service, based at least in part on the response indicating that the addressed recipient corresponds to a subscriber of the service and based at least in part upon a status indicating that an undelivered message parameter has not been exceeded.

151. Horvath-Tsampalis-Tumminaro-Dorenbosch renders Claim [2] obvious. As I previously discussed in Ground 1A for Elements [1g]-[1h], *supra*, a POSITA would have found obvious that the response from the HLR 202 and/or HSS 210 containing messaging capabilities information would include information about the services to which the wireless device 106 is subscribed (e.g., IM). Accordingly, where the sending wireless device and the recipient device are both registered with an IM service like that described in each of Horvath, Tumminaro, and Dorenbosch, a POSITA would have further found obvious that the sending device would select to send the message over the packet-switched messaging service (e.g., the IM service) via the IMS core (*server*) using ***a packet-switched bearer*** (e.g., 8012.11 or GPRS,

EV-DO, or UMTS bearers). *See Supra*, Ground 1A at [1i]; APPLE-1004, [0033]; APPLE-1039, [0017], [0022] (“communicating with the IM proxy 24, it should be understood that multiple source buddies (either mobile or conventional subscribers) are capable of communicating with multiple target buddies (either mobile or conventional subscribers) via the functionality implemented at the IM proxy 24”). For example, Tsampalis describes how rich message formats that require a packet-switched bearer, which includes IM in the combination, can be set as the default format for sending a message, and which would be selected if the addressed recipient does not have limited messaging capabilities. APPLE-1005, [0062]-[0064]; *supra*, [1i].

152. As I previously explained in §IX.A, a POSITA would have found it obvious to modify the system of the combination based on the Dorenbosch techniques to enhance communications via the IM service provided by Horvath’s packet-switched network. In the combination, Dorenbosch’s IM proxy—either integrated into the information processing system 108 or implemented as an application server of the IMS system—“functions to set up a connection, such as an IP connection, with the IM login server 16 for the mobile subscriber 12 and for facilitating information flow between the IM login server 16 and the mobile subscriber 12 once the connection is established.” APPLE-1004, [0038]-[0039] (“[a]n IMS system also includes application servers that host and execute services

for the wireless device 106”); APPLE-1039, [0019] (“IM proxy 24 is preferably housed within a mobile services switching center (MSC) 28” or “in proximity to the MSC 28”).

153. As I previously explained in §VII.D, the two aspects of Dorenbosch’s IM proxy bundle messages in a message buffer until “more than a predetermined number of messages are stored,” at which point it will attempt to forward the bundled messages to the mobile subscriber (*e.g.*, the combination’s sending and receiving mobile phones). APPLE-1039, [0038]-[0040]. The IM proxy will maintain a connection with the IM login server even when the mobile subscriber temporarily loses network coverage, and other IM subscribers will continue to see the mobile subscriber as having an “available” presence and be able to send the mobile subscriber messages. APPLE-1006, [0024], [0030]. If the IM proxy attempts to forward the bundle of messages to the mobile subscriber and is unable, the IM proxy will retry sending the bundle a certain number of times within a certain period, after which it will drop the message(s) and indicate to the IM login server that the mobile subscriber is unavailable. APPLE-1006, [0020], [0024], [0029]. In other words, when the number of messages cached by the IM proxy reaches the threshold number and the IM proxy tries but fails to send the bundle of messages to the IM subscriber, any sending mobile phones will no longer be able to send the IM subscriber messages, because the IM login server will list the IM subscriber as unavailable.

This would have been predictable to a POSITA because the IM proxy (and messaging systems generally) have limited storage capacities and it is prohibitive to store large numbers of messages for many users for an extended period of time. It would have been obvious that after a certain point, the IM proxy would drop messages that are no longer relevant or that are less relevant or otherwise less likely to be successfully delivered than more recent messages.

154. Accordingly, a POSITA would have found obvious that, in the Horvath-Tsampalis-Tumminaro-Dorenbosch combination, sending wireless device 106 selects a *packet-switched bearer* for transmission of a message (e.g., an IM message) via the IMS core (*server*) further based upon *a status indicating that an undelivered message parameter has not been exceeded* (e.g., a status indicating that the addressed recipient is available to receive IMs, which is based on the IM proxy being able to continue to receive an acknowledgement that the second receiving mobile phone is receiving bundled messages, where the IM proxy caches IMs for the addressed recipient until a threshold number of messages have been stored, at which point the IM proxy will attempt to deliver the messages to the addressed recipient).

Claim [3]: The mobile wireless device of claim 1, wherein the mobile wireless device transmits a message limited to one or more binary-encoded characters to the addressed recipient via the cellular base station and through a short message service center (SMSC) before delivery to the addressed recipient, based at least in part on the response indicating that the addressed recipient corresponds to a

subscriber of the service and based at least in part on a status indicating that an undelivered message parameter has been exceeded.

155. Horvath-Tsampalis-Tumminaro-Dorenbosch renders Claim [3] obvious. As I previously discussed in Ground 1A with respect to Elements [11] and [1m], a POSITA would have found it obvious that the combination's sending device 106 transmits an SMS message limited to one or more binary-encoded characters to an addressed recipient via a cellular base station through an SMSC before delivery to the addressed recipient based at least in part on the response failing to indicate that the addressed recipient corresponds to a subscriber of a packet-switched messaging service (*e.g.*, the IM service). *Supra*, Ground 1A at [11]-1m]. A POSITA considering the teachings of Dorenbosch further would have found it obvious for the combination's sending device to send the same type of SMS message limited to one or more binary-encoded characters to an addressed recipient via a cellular base station through an SMSC before delivery to the addressed recipient even when the response ***indicat[es] that the addressed recipient corresponds to a subscriber of the service*** if a status of the addressed recipient ***indicate[s] that an undelivered message parameter has been exceeded.***

156. For example, as I previously discussed for Claim [2], when the number of messages cached by the IM proxy in the Horvath-Tsampalis-Tumminaro-Dorenbosch system reaches a threshold number and the IM proxy tries but fails to send the bundle of messages to an IM subscriber, any sending mobile phones will

no longer be able to send the IM subscriber messages, because the IM login server will list the IM subscriber as unavailable. *Supra*, [2]. Accordingly, if the addressed recipient were only subscribed to IM and SMS messaging services, but the addressed recipient were unavailable (*a status indicating that an undelivered message parameter has been exceeded*) and the sending device lost data network coverage or was not otherwise currently registered with the IMS, it would have been obvious based on Horvath's, Tsampalis's, and Dorenbosch's teachings to format and transmit the message via a cellular base station using SMS to ensure the message could be successfully delivered to the recipient sooner, rather than waiting for the recipient to possibly become available later on the IM service. APPLE-1005, [0062]-[0063]; APPLE-1004, [0050], [0077]-[0078], FIG. 7; *supra*, §§VII.D, IX.A, Analysis of Claim [2].

Claim [8]: The mobile wireless device of claim 1, wherein a message to the addressed recipient is queued for later delivery using the service if the wireless device of the addressed recipient corresponds to a subscriber of the service, and the wireless device of the addressed recipient, at a time of message transmission, is unable to connect to the server that receives packet-switched messages transmitted via the service to recipient devices that correspond to subscribers of the service.

157. As I previously discussed in §IX.A and for Claim [2], the IM proxy in the Horvath-Tsampalis-Tumminaro-Dorenbosch combination *queues a message* (e.g., an IM) *to the addressed recipient for later deliver using the service* (e.g., the IM service) *if the wireless device of the addressed recipient corresponds to a*

subscriber of the service and, at a time of message transmission is unable to connect to the server (e.g., the IMS core and application servers that implement aspects of the IM service, which can include IM application servers, IM proxy, IM login system). APPLE-1004, [0047] (“The wireless device 106 may not be registered ... because it never was registered to begin with, because it deregistered, or because it lost its coverage.”), [0045]-[0048], [0075]-[0076], FIG. 6; APPLE-1039, [0020], [0024], [0028]-[0029], [0036]; *supra*, §§VII.D, IX.A. Claim [3] was therefore obvious.

Element [28pre]: A system comprising:

158. To the extent the preamble is limiting, the Horvath-Tsampalis-Tumminaro-Dorenbosch combination renders a “***system***” as recited in Element [28pre]. APPLE-1004, Title (“METHOD AND SYSTEM FOR DELIVERY OF SHORT MESSAGE SERVICE MESSAGES”), Abstract, [0011] (“exemplary wireless communication system”), [0021] (“the system of the present invention”); APPLE-1005, [0001], [0006], FIG. 1; *supra*, Ground 1A at [1pre].

Element [28a]: a mobile wireless device; and

159. *Supra*, Ground 1A at [1pre].

Element [28b]: a server that receives message content intended for a third party provider, from the mobile wireless device;

160. *Supra*, Ground 1A at [1pre], [1n].

Element [28c]: wherein the mobile wireless device transmits (i) at least some messages to at least some recipient devices that correspond to subscribers of a

service for receiving packet-switched messages, wherein the service includes a server that receives packet-switched messages transmitted via the service to recipient devices that correspond to subscribers of the service, and (ii) at least some messages over a cellular network to at least some recipient devices that do not correspond to subscribers of the service;

161. *Supra*, Ground 1A at [1pre].

Element [28d]: wherein the mobile wireless device comprises a wireless local area network (WLAN) transceiver that transmits messages from the mobile wireless device to a WLAN base station and subsequently over the Internet to the server that receives packet-switched messages transmitted via the service to recipient devices that correspond to subscribers of the service, before delivery to a recipient device;

162. *Supra*, Ground 1A at [1a].

Element [28e]: wherein the mobile wireless device comprises a cellular transceiver that transmits messages from the mobile wireless device to a cellular base station before delivery to a recipient device, wherein the cellular transceiver and the cellular base station communicate using a radio communications protocol that supports transmission of multimedia messages comprising at least one of images, audio clips or videos;

163. *Supra*, Ground 1A at [1b].

Element [28f]: wherein the mobile wireless device connects via the WLAN base station to the server that receives packet-switched messages transmitted via the service to recipient devices that correspond to subscribers of the service;

164. *Supra*, Ground 1A at [1c].

Element [28g]: wherein the mobile wireless device connects via the cellular base station to the server that receives packet-switched messages transmitted via the service to recipient devices that correspond to subscribers of the service;

165. *Supra*, Ground 1A at [1d].

Element [28h]: wherein the mobile wireless device transmits packet-switched messages using a packet-switched bearer supported by the WLAN base station

and transmits packet-switched messages using a packet-switched bearer supported by the cellular base station; and

166. *Supra*, Ground 1A at [1e].

Element [28i]: wherein the mobile wireless device comprises a message client that retrieves, from a message, address information consisting of only one mobile phone number of a wireless device of an addressed recipient, during composition of the message;

167. Horvath-Tsampalis-Tumminaro-Dorenbosch renders Element [28i] obvious. As I previously discussed for Element [1f], the combination's sending device 106 retrieves, from a message, address information in the form of a mobile phone number of a wireless device of an addressed recipient during composition of the message. *Supra*, Ground 1A at [1f]. A POSITA would have found it obvious that the retrieved address information consists of "only one" mobile phone number, for example, when the wireless device of the addressed recipient has only one phone number, as was commonly the case by the mid-2000s Critical Date of the '827 Patent (July 24, 2007).

Element [28j]: wherein the WLAN transceiver: (i) transmits a request, including at least information corresponding to the mobile phone number of the wireless device of the addressed recipient, via the WLAN base station and the Internet, to a server that maintains a subscriber list, to determine whether the wireless device of the addressed recipient corresponds to a subscriber of the service; and

168. *Supra*, Ground 1A at [1g].

Element [28k]: (ii) receives a response from the server that maintains the subscriber list, via the WLAN base station and the Internet, indicating whether the wireless device of the addressed recipient corresponds to a subscriber of the service, wherein a negative response indicates that the wireless device of the addressed recipient is not a subscriber of the service;

169. *Supra*, Ground 1A at [1h].

Element [28l]: wherein the mobile wireless device selects a packet-switched bearer for transmission of a message to the addressed recipient via the server that receives packet-switched messages transmitted via the service to recipient devices that correspond to subscribers of the service, based at least in part on the response indicating that the addressed recipient corresponds to a subscriber of the service and based at least in part upon a status indicating that an undelivered message parameter has not been exceeded;

170. *Supra*, Ground 1A at [1i] and Ground 1B at [2].

Element [28m]: wherein if a packet-switched bearer is selected for message transmission via the server that receives packet-switched messages transmitted via the service to recipient devices that correspond to subscribers of the service, the mobile wireless device chooses for message transmission the packet-switched bearer supported by the WLAN base station or the packet-switched bearer supported by the cellular base station;

171. *Supra*, Ground 1A at [1j].

Element [28n]: wherein if the mobile wireless device chooses the packet-switched bearer supported by the WLAN base station for message transmission, the mobile wireless device performs message transmission to the server that receives packet-switched messages transmitted via the service to recipient devices that correspond to subscribers of the service;

172. *Supra*, Ground 1A at [1pre]-[1a], [1j].

Element [28o]: wherein the mobile wireless device transmits a message to the addressed recipient via the cellular base station, at least where the packet-switched bearer supported by the WLAN base station is not chosen for message transmission;

173. *Supra*, Ground 1A at [1k].

Element [28p]: wherein the mobile wireless device transmits a message to the addressed recipient via the cellular base station, and without traversing the server that receives packet-switched messages transmitted via the service to recipient devices that correspond to subscribers of the service, before delivery to

the addressed recipient, based at least in part on the response failing to indicate that the addressed recipient corresponds to a subscriber;

174. *Supra*, Ground 1A at [11].

Element [28q]: wherein the mobile wireless device transmits a message limited to one or more binary-encoded characters to the addressed recipient via the cellular base station and through a short message service center (SMSC) before delivery to the addressed recipient, based at least in part on the response indicating that the addressed recipient corresponds to a subscriber of the service and based at least in part on a status indicating that an undelivered message parameter has been exceeded;

175. *Supra*, Ground 1B at [3]; *see also* Ground 1A at [1pre], [1m]; Ground 1B at [2].

Element [28r]: wherein a message to the addressed recipient is queued for later delivery using the service if the wireless device of the addressed recipient corresponds to a subscriber of the service having a status indicating that an undelivered message parameter has not been exceeded, and the wireless device of the addressed recipient, at a time of message transmission, is unable to connect to the server that receives packet-switched messages transmitted via the service to recipient devices that correspond to subscribers of the service;

176. *Supra*, Ground 1B at [8].

Element [28s]: wherein the server that receives the message content intended for the third party provider forwards a message comprising the message content intended for the third party provider, to the third party provider, wherein the message forwarded to the third party provider is derived at least in part from a random number.

177. *Supra*, Ground 1A at [1n].

X. GROUND 1C: CLAIMS 9, 12-13, 22, 24 ARE OBVIOUS IN VIEW OF THE HORVATH-TSAMPALIS-TUMMINARO-KANSAL COMBINATION

A. Combining Horvath, Tsampalis, Tumminaro and Kansal

178. The combination provides a mobile wireless device capable of messaging using different messaging services including, SMS, MMS, and IM. *Supra* §§VIII.A, VII.E. Kansal suggests using a unified messaging UI for precisely this kind of environment, with variously formatted messages integrated within a single application interface. APPLE-1053, [0077]-[0078], [0086]. Multiple reasons would have prompted a POSITA to implement this combination.

179. First, a POSITA would have been motivated to apply Kansal's suggested unified-messaging user interface to the wireless device in the combination to improve the user's experience with mobile messaging services involving messages of different types (*e.g.*, SMS, MMS, IM). This would have predictably achieved Kansal's stated goals to meet the "need for an improved apparatus and methods for providing enhanced mobile messaging services." APPLE-1053, [0002]. For example, correlating messages in a manner that allows a user to view all messages of various types involving a particular user at a glance in a single thread would advantageously allow a user to see all messages received from particular senders within a single interface without needing to navigate to different messaging applications or interfaces for each different message type. APPLE-1066, 1-2 (a multi-protocol messaging application providing "a powerful and efficient user experience."); APPLE-1053, [0009], [0045]-[0046], [0054]-[0056], [0062]-[0064], [0070], [0077]-[0078], FIGs. 2-3.

180. 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-1053, [0049]; *see* FIGs. 2-3. In addition to improving the user experience (as described in the first reason), Kansal’s unified UI would provide additional contextual information that would otherwise not be readily conveyed. For example, as shown in FIG. 3 of Kansal, the chronologically ordered communication events (*e.g.*, missed call at 218 and urgent email request at 216) would beneficially provide additional context for the later received text message (*e.g.*, at 214). APPLE-1053, FIG. 3. A POSITA would have sought to implement Kansal’s user interface to provide this additional contextual information to a user.

181. Third, 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.

182. A POSITA would have reasonably expected success implementing the combination as the messaging and communication protocols involved were all well known before the Critical Date. Further, the techniques integrated from Kansal in the combination are fully compatible with Horvath’s, Tsampalis’s, and Tumminaro’s teachings and would not disturb the ability of Horvath’s system to

transmit or deliver messages over either a packet-based or circuit-switched network, the use of capabilities-based messaging techniques taught by Tsampalis, or Tumminaro's mobile payment transactions.

B. Analysis with Respect to Claims 9, 12-13, 22, 24

Claim [9]: The mobile wireless device of claim 1, further comprising: a display that displays presence information associated with the wireless device of the addressed recipient; wherein the mobile wireless device receives the presence information associated with the wireless device of the addressed recipient if the wireless device of the addressed recipient corresponds to a subscriber of the service.

183. Horvath-Tsampalis-Tumminaro-Kansal renders obvious Claim [9]. Horvath discloses that the sending device 106 has a “visual notification (or indication interface 440)” that “can be used as an alert by displaying a sequence of colored lights or a single flashing light on [a] display 444 or LEDs...when the wireless device 106 receives a message, or the user missed a call,” where display 444 is “for displaying information to the user of the wireless device 106.” APPLE-1004, [0068], [0070], FIG. 4 (below).

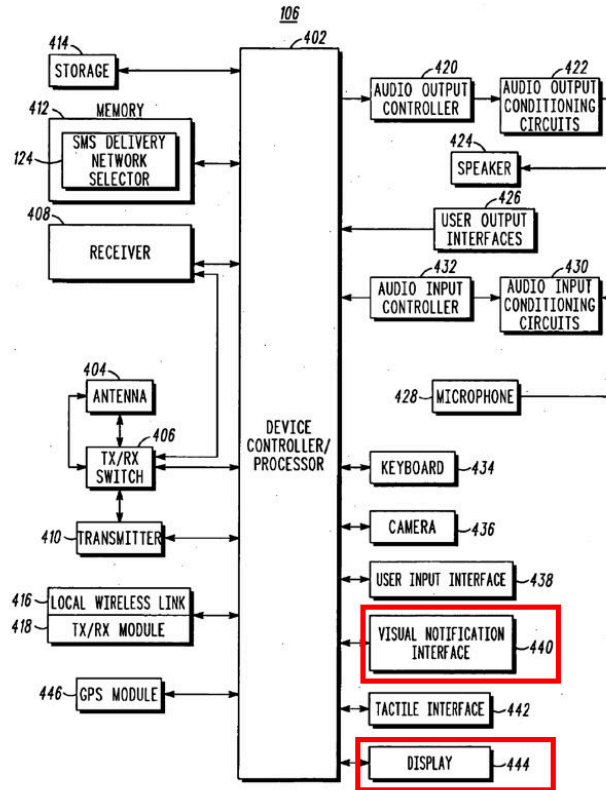


FIG. 4

APPLE-1004, FIG. 4 (Annotated)

184. Also in the combination, Kansal discloses that “an IM icon” displayed in the unified messaging UI “may indicate whether the contact is currently online and available to receive an IM message” (*presence information associated with the wireless device of the addressed recipient*). APPLE-1053, [0062], FIG. 3. A POSITA would have found obvious that the combination’s sending device 106 *receives the presence information associated with the wireless device of the addressed recipient if the wireless device of the addressed recipient corresponds to a subscriber of the service* because subscribers of the IM service like those in Kansal

publish their presence information to allow other subscribers (e.g., on a Buddy list) to know when they are available to receive messages. APPLE-1053, [0062]; APPLE-1007, 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.”); APPLE-1064, 2 (“SIP location services already contain presence information, in the form of registrations”); *supra*, [1g]-[1h] (describing IMS core returning to the sending device presence information in the form of indications of current registration status of other devices).

Claim [12]: The mobile wireless device of claim 1, wherein the message client retrieves information representative of at least one electronic mail (email) address of another wireless device of another recipient; wherein the addressed recipient and the another recipient are each a subscriber of the service.

185. Horvath-Tsampalis-Tumminaro-Kansal renders Claim [12] obvious. For example, Kansal describes a wireless device having a “contacts database” of a message client “arranged to store contact records for individuals or entities specified by the user.” APPLE-1053, [0037]. “The contact record for an individual may comprise identifying information such as first name, last name, ... [and] e-mail address” *Id.* “The contacts database 142 may be used or accessed when receiving and/or sending messages.” *Id.*, [0038]. “For example, the user of the mobile computing device 100 may search for and open the contact record of a particular individual to initiate communication.” *Id.* Accordingly, it would have

been obvious that the Horvath-Tsampalis-Tumminaro-Kansal sending device 106 retrieves an e-mail address (*information representative of at least one electronic mail (email) address of another wireless device of another recipient*) to initiate an e-mail communication with another recipient. *See also supra*, Ground 1A at [1f]. Kansal and Tsampalis also address and render obvious the common situation in which contacts subscribe to different messaging services and some contacts subscribe to the same service (e.g., multiple subscribers of the IM service) (*the addressed recipient and the another recipient are each a subscriber of the service*). APPLE-1005, [0061]-[0063]; APPLE-1053, [0037]-[0038], [0042], [0046], [0062], [0067], FIGs. 2-3 (providing that contacts associated with multiple devices can subscribe to the same services).

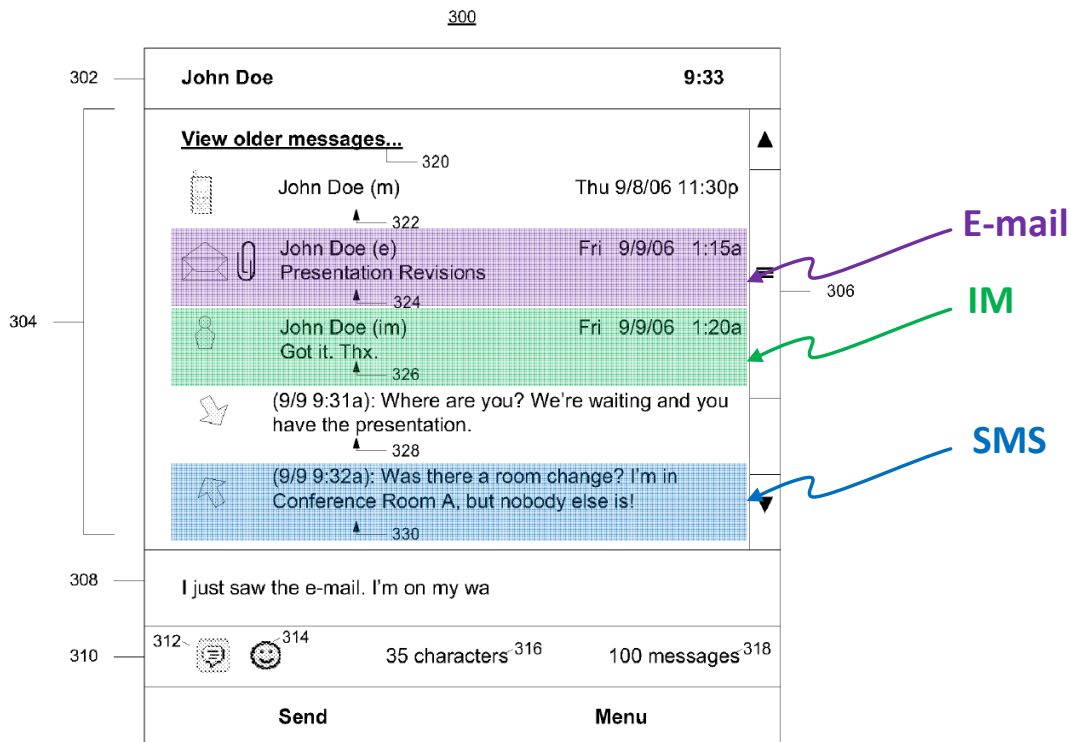
Claim [13]: The mobile wireless device of claim 12, wherein the WLAN transceiver transmits at least one message from the mobile wireless device to the wireless device of the addressed recipient and to the wireless device of the another recipient.

186. Horvath-Tsampalis-Tumminaro-Kansal renders Claim [13] obvious. As I previously discussed in Ground 1A with respect to Elements [1a] and [1i]-[1j], the combination's sending device 106 uses its WLAN transceiver to transmit at least one message from the mobile to the wireless device of the addressed recipient. *Supra*, Ground 1A at [1a], [1i]-[1j]. Tsampalis and Kansal also each describe transmitting messages to multiple recipients. APPLE-1005, [0035] ("multiple recipient IDs are entered"), [0062] ("multiple remote recipients"), [0063]; APPLE-1053, [0073]-

[0078]. A POSITA would have found it obvious that the sending device 106 would also transmit the same or different messages to the wireless device of another recipient (*e.g.*, another recipient subscribed to the IM service) because each recipient can receive messages and the sender may desire to share information with multiple recipients.

Claim [22]: The mobile wireless device of claim 1, further comprising: a single interface for transmission of and reception of both text and multimedia messages; wherein the single interface provides an option to add a voice attachment for subsequent playback by the wireless device of the addressed recipient.

187. Horvath-Tsampalis-Tumminaro-Kansal renders Claim [22] obvious. As discussed above, the combination implements Kansal's unified messaging UI, which provides a single interface for transmission of and reception of both text messages (*e.g.*, SMS messages) and multimedia messages (*e.g.*, MMS messages, IM messages). APPLE-1053, [0046]; *see also id.*, [0009]; [0045]-[0046]; [0054]-[0056]; [0062]-[0064]; [0070]; [0077]-[0078]. FIGs. 2, 3; *supra*, §VII.E. For example, message thread 304 "includes a message 326 comprising a sent IM message" and additional messages of various types. APPLE-1053, [0062]-[0064], [0046].



APPLE-1053, FIG. 3 (Annotated)

188. Also in the combination, Kansal describes that the messaging UI provides a selectable menu item that provides the option of “Record[ing] Sound” to create a voice recording to attach to a message. APPLE-1053, [0073], FIG. 5; *see also id.*, [0074]-[0078] (“add media”), [0060], FIG. 3 (314). A POSITA would have found it obvious that the voice recording may be played back by the addressed recipient upon receipt of the message to which the voice recording was attached because voice recordings are made to allow earlier utterances to be played back later in time. *Id.*; *see also* APPLE-1005, [0062] (“attached/inserted multimedia files”).

Claim [24]: The mobile wireless device of claim 1, wherein the message client provides an option to add one or more attachments based at least in part on the response.

189. Horvath-Tsampalis-Tumminaro-Kansal renders Claim [24] obvious. As I previously discussed in Ground 1A with respect to Elements [1i] and [11]-[1m], the combination's sending device 106 selects either a message format that supports multimedia attachments (*e.g.*, MMS or IM) or an SMS format that does not support multimedia attachments (*e.g.*, SMS) based at least in part on the messaging capabilities of the addressed recipient indicated by the response. *Supra*, Ground 1A at [1i], [11]-[1m]; APPLE-1007, 7 (describing IM support for "file transfer"); APPLE-1008, [0046]-[0047] (describing transmission of multimedia content via an IM client); APPLE-1053, [0075]-[0077] (describing need to convert SMS to another message type in order to add "media objects such as pictures, video, and/or sounds to a message"). Further, as I previously discussed for Claim [22], the message client of the sending device 106 would implement Kansal's technique for providing an option of "Record[ing] Sound" to create a voice attachment to add to a message that supports multimedia attachments. APPLE-1053, [0073], FIG. 5; *see also id.*, [0074]-[0078] ("add media"), [0060], FIG. 3 (314); *supra*, [22].

190. In this context, a POSITA would have found it obvious for the message client to provide an option of adding attachment(s) based at least in part on the response because the response informs the selection of a messaging format, and only

a subset of messaging formats support attachments. The option would predictably be provided, for instance, when messaging a recipient for which the response indicates that the recipient is capable of messaging according to a format that supports attachments (*e.g.*, MMS, IM), but the option would not be provided for SMS. For example, Tsampalis teaches that an MMS may include “attached/inserted multimedia files,” which would need to be discarded if the MMS is transformed into an SMS. APPLE-1005, [0062]. Similarly, Kansal describes that, “after a media object has been added to the message, the [unified] messaging UI 500 may undergo an automatic or seamless conversion” from SMS to MMS. APPLE-1053, [0077]. “In the event that the user adds a media object and then removes the media object, the messaging UI 500 may automatically or seamlessly convert back from an MMS messaging UI to an SMS messaging UI.” *Id.*; *see also* APPLE-1067, [0060] (“the SMS option is greyed out since the message includes media items which are unable to be transmitted by SMS”).

XI. GROUND 1D: CLAIMS 4-6 ARE OBVIOUS IN VIEW OF THE HORVATH-TSAMPALIS-TUMMINARO-COTTRELL COMBINATION

A. Combining Horvath, Tsampalis, Tumminaro and Cottrell

191. A POSITA would have found it obvious to modify the Horvath-Tsampalis-Tumminaro system of Ground 1A further in view of Cottrell to include a remote proxy server that selectively removes or replaces privacy sensitive

information in communications between a user device (*e.g.*, Horvath’s sending wireless device 106) and a target server (*e.g.*, Tumminaro’s payment server). *Supra*, §VII.F. Cottrell describes how the remote proxy server can be implemented in any of a variety network locations or elements including “networked game systems ..., a router, network-address translation device, switch, firewall, or other network device or appliance” between the user device and the target server. APPLE-1040, [021]. In the context of a system that includes an IMS as in the combination—which already functions as an intermediary that routes information from the sending device 106 to application servers and servers of third-party providers (*e.g.*, Tumminaro’s payment server)—the IMS core or an application server associated with the IM, MMS, or third-party service would have been a natural and obvious location to implement the privacy-protecting functions of Cottrell’s remote proxy server. *Supra*, §VIII.A(ii), Ground 1A at [1n].

192. A POSITA would have been motivated to pursue the combination to better protect the privacy of a user of Horvath’s sending wireless device 106 when messaging with a target server such as the payment server described in Tumminaro or another server. Cottrell explains that the removal or “substitution of personal information related to the user” is beneficial for “identity protection, privacy, and tracking prevention.” APPLE-1040, [051]. A POSITA would have sought to achieve these known benefits in the combination system for the same reasons

expressed in Cottrell. Indeed, Cottrell notes it was common for “businesses and certain individuals [to] attempt to identify and track individual Internet users for numerous purposes,” and explains that “[m]any of these attempts are threats to the individual privacy of users ... because they attempt to gain personal information about the user and the user’s activities online ..., often without the user’s consent or knowledge.” APPLE-1040, [006]. Substituting or otherwise removing sensitive information between the wireless device 106 and a target server would have helped ameliorate these threats. Applying Cottrell’s techniques for improved network security to address known privacy problems in substantially the same types of systems as those described in Horvath, Tsampalis, and Tumminaro also would have been obvious. For example, Cottrell’s suggestion to modify and remove privacy-sensitive packets communicated between devices would have been useful in a variety of contexts, such as to remove the sender’s phone number or other identifying information about the sender when the sender sends a message to be distributed by a mailing list or to other recipients that should not have the sender’s personal information. Similar behavior has long been implemented in phone networks with respect to caller ID being removed before receipt by the final recipient.

193. A POSITA would have reasonably expected success implementing the combination, especially as the messaging and communication protocols involved were all well known before the Critical Date. Further, the techniques integrated from

Cottrell in the combination are fully compatible with Horvath's, Tsampalis's, and Tumminaro's teachings and would not disturb the ability of Horvath's system to transmit or deliver messages over either a packet-based or circuit-switched network, the use of capabilities-based messaging techniques taught by Tsampalis, or Tumminaro's mobile payment transactions. For example, Cottrell explains how its techniques can be adapted for a wide range of applications by allowing adjustments to selectively remove/substitute or retain different information depending on the needs of different services and the user. APPLE-1040, [022], [024]. Cottrell's techniques are also broadly applicable to a wide range of networks and the messaging and protocols involved were all well known before the Critical Date. APPLE-1040, [021] ("Network Device 102 maybe a PC, a PDA, ... an Internet-cell phone or like electronic device."), [019] ("implementations may apply to other networks" and techniques are "capable of implementation using any network protocol").

B. Analysis with Respect to Claims 4-6

Claim [4]: The mobile wireless device of claim 1, wherein the message forwarded to the third party provider is not identical to a message transmitted by the mobile wireless device comprising the message content intended for the third party provider.

194. Horvath-Tsampalis-Tumminaro-Cottrell renders Claim [4] obvious. As I previously discussed in §XI.A, the IMS core or an application server for the the MMS, IM, or payment service in the combination system forwards messages sent

from the sending wireless device 106 and intended for a third-party provider (e.g., Tumminaro's mobile payment service) to a server associated with the third-party provider, and in so doing, substitutes or otherwise removes at least one information element (e.g., a phone number of the sending wireless device 106) from the message before it is forwarded as taught in Cottrell. *Supra*, §§VII.F, XI.A; APPLE-1040, [024] ("replace sensitive information"), [051] ("substitution of personal information related to the user, such as ... phone number"); *see also* APPLE-1060, 6:59-7:5 ("masks the identity of the sender and recipient ... to protect the anonymity of the [] participants"), Abstract, FIGs. 3, 4b; APPLE-1061, Abstract ("A mobile device identifier (such as an MSISDN) that typically accompanies a mobile device request is replaced with an 'enriched' identifier ..."). Accordingly, the forwarded message *is not identical* to the message transmitted by the sending wireless device 106.

Claim [5]: The mobile wireless device of claim 4, wherein the message transmitted by the mobile wireless device comprising the message content intended for the third party provider includes at least one information element which is not included in the message forwarded to the third party provider.

195. *Supra*, [4].

Claim [6]: The mobile wireless device of claim 5, wherein the information element is a phone number of the mobile wireless device.

196. *Supra*, [5].

XII. GROUND 1E: CLAIMS 10, 14-15 ARE OBVIOUS IN VIEW OF THE HORVATH-TSAMPALIS-TUMMINARO-LIN COMBINATION

A. Combining Horvath, Tsampalis, Tumminaro and Lin

197. It would have been obvious to further modify the Horvath-Tsampalis-Tumminaro combination described in Ground 1A by integrating Lin's suggested techniques for establishing IM sessions between mobile devices by sending SMS messages that invite participants to join the IM sessions and that allow devices to authenticate with an IM server. Multiple reasons would have prompted a POSITA to implement this combination.

198. First, a POSITA would have implemented Lin's 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-1041, [0003], [0006].

199. Second, a POSITA would have implemented Lin's techniques in the combination because Lin explains that its server-based architecture for mobile IM provides better efficiency than P2P architectures when more than two devices are involved in a dialog. APPLE-1041, [0005]-[0006]. The server-based architecture and SMS-based invitations also beneficially allow devices to join the IM session from outside a private network.

200. Third, a POSITA would have implemented Lin's techniques in the combination to improve the initiating mobile devices to securely authenticate with a server and be cleared as a moderator for an IM sessions using a commonly available

messaging format (SMS), thereby enhancing security and convenience. APPLE-1041, [0017].

201. Fourth, applying Lin's suggested techniques for establishing IM sessions and authenticating with an IM server through SMS messaging in the context of references like Horvath, Tsampalis, and Tumminaro that describe the same types of messaging services to obtain substantially similar results would have been obvious.

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

B. Analysis with Respect to Claims 10, 14-15

Claim [10]: The mobile wireless device of claim 1, wherein the mobile wireless device receives an over the air (OTA) configuration message which includes at least one parameter for establishing a server connection with the server associated with the service which forwards the message comprising the message content intended for the third party provider.

203. Horvath-Tsampalis-Tumminaro-Lin renders Claim [10] obvious. As an initial matter, it would have been obvious that the combination's sending device 106 would receive a network address of the P-CSCF 206 that it uses to connect to the IMS core (*server associated with the service which forwards the message comprising the message content intended for the third party provider*). *Supra*, Ground 1A at [1pre], [1n]. For example, Horvath explains that "the wireless device 106 locates its respective P-CSCF 206 via a dynamic host configuration protocol ('DHCP'). The wireless device 106 is assigned to a specific P-CSCF 206 for the duration of the device's subscription to the IMS network." APPLE-1004, [0036]. As I previously discussed in Ground 1A with respect to Elements [1c]-[1d], the sending device 106 establishes a *server connection* with the IMS core (*server*). *Supra*, Ground 1A at [1c]-[1d]. Because device 106 is a "wireless" device, it would have been obvious to a POSITA for the sending device 106 to receive the network address and any necessary information for connecting to the IMS core (*at least one parameter*) wirelessly over the air (OTA), and therefore in an *OTA configuration message*. Indeed, OTA configuration messages were well known before the alleged invention. APPLE-1013, 10:8-11 ("the handset 102 may be programmed and/or configured over-the-air, for example from a wireless base station, a wireless access point, or a peer handset 102"); APPLE-1032, [0023] ("The mobile communication device 30 is configured to include the mobile application 40....the service provider

15 can be configured to automatically ‘push’ the application 40 to the mobile communication device 30”), supported by APPLE-1033, page 3, lines 19-26); APPLE-1004, [0004], [0039] (“air interface”).

204. Further, based on Lin’s teachings, to initiate or join an IM session, the sending device 106 in the combination would be configured to receive “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-1041, [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 sending device 106 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 the server.

Claim [14]: The mobile wireless device of claim 1, wherein the wireless device transmits a short message service (SMS) message for authentication to the service.

205. Horvath-Tsampalis-Tumminaro-Lin renders Claim [14] obvious. As discussed above, based on Lin’s teachings, the combination’s sending device 106 initiates an IM session by transmitting an SMS message for authentication to an IM

service such that the first mobile wireless device is authenticated to the IM service via SMS. APPLE-1041, [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.

Claim [15]: The mobile wireless device of claim 1, wherein the mobile wireless device is authenticated to the service via SMS; wherein the server that receives packet-switched messages transmitted via the service to recipient devices that correspond to subscribers of the service is located outside of the cellular network; wherein the server that maintains the subscriber list is located outside of the cellular network.

206. Horvath-Tsampalis-Tumminaro-Lin renders Claim [15] obvious for each of the reasons described above in Ground 1A with respect to Claim [11] and in Ground 1B with respect to Claim [14].

XIII. CONCLUSION

207. For all the reasons I have noted in the foregoing paragraphs, claims 1-30 of the '827 Patent are obvious in view of the references discussed above.

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

APPENDIX A

Patrick Gerard Traynor

Professor

Associate Chair for Research in CISE

John and Mary Lou Dasburgh Preeminent Chair in Engineering

Department of Computer & Information Science & Engineering (CISE)

University of Florida

1889 Museum Rd,

Gainesville, FL 32611 USA

traynor@cise.ufl.edu

<http://www.cise.ufl.edu/~traynor>

Table of Contents

EDUCATIONAL BACKGROUND	4
EMPLOYMENT HISTORY	4
CURRENT FIELDS OF INTEREST	4
I. TEACHING	6
A. Courses Taught	6
B. Continuing Education	6
C. Curriculum Development	6
D. Individual Student Guidance	7
E. Teaching Honors and Awards	12
II. RESEARCH AND CREATIVE SCHOLARSHIP	13
A. Thesis	13
B. Published Journal Papers (Refereed)	13
C. Published Books and Parts of Books	15
D. Edited Proceedings	15
E. Conference Presentations	15
E.1. Conference Papers with Proceedings (Refereed)	15
E.2. Conference Presentations with Proceedings (Non-Refereed)	23
E.3. Conference Presentations without Proceedings	23
F. Other	23
F.1. Submitted Journal Papers	23
F.2. Refereed Research Reports	23
F.3. Software	23
F.4. Published Papers (Non-Refereed)	23
F.5. Books in Preparation	23
F.6. Workshops and External Courses	24
G. Research Proposals and Grants (Principal Investigator)	24
H. Research Proposals and Grants (Contributor)	27
I. Research Honors and Awards	28
III. SERVICE	29
A. Professional Activities	29
A.1. Memberships and Activities in Professional Societies	29
A.2. Conference Committee Activities	29
B. On-Campus Committees	30
B.1. University of Florida	30
B.2. Georgia Tech	31
C. Special Assignments	31
D. Ph.D. Examining Committees	31
E. External Member of M.S. Examining Committee	35
F. Consulting and Advisory Appointments	35
G. Civic Activities	35
IV. NATIONAL AND INTERNATIONAL PROFESSIONAL RECOGNITION	36
A. Honors and Awards	36
B. Invited Conference Session Chairmanships	36
C. Professional Registration	36
D. Patents	36
E. Editorial and Reviewer Work for Technical Journals and Publishers	37
F. Expert Witness Services	39
V. OTHER CONTRIBUTIONS	41
A. Seminar Presentations (Invited Papers and Talks at Meetings and Symposia)	41

B. Special Activities	45
---------------------------------	----

EDUCATIONAL BACKGROUND

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

EMPLOYMENT HISTORY

Title	Organization	Years
Interim Department Chair	University of Florida	July 2025–Present
Associate Chair for Research	University of Florida	August 2018–Present
Professor	University of Florida	August 2018–Present
Associate Professor	University of Florida	August 2014–July 2018
Associate Professor	Georgia Institute of Technology	March 2014–August 2014
Assistant Professor	Georgia Institute of Technology	2008–March 2014
Research Assistant	Pennsylvania State University	2004–2008
Teaching Assistant	Pennsylvania State University	2004

CURRENT FIELDS OF INTEREST

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

Recognizing this, my research focuses on three specific themes: (1) developing efficient techniques to allow telephony providers and customers to authenticate the origin of incoming calls; (2) measuring and

improving the security of emerging mobile financial systems and (3) efficient and strong privacy-preserving techniques for mobile devices. Additionally, I have significant expertise in fraud detection, particularly for payment systems.

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

I. TEACHING

A. Courses Taught

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

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

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

B. Continuing Education

None.

C. Curriculum Development

University of Florida

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

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

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

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

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

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

D. Individual Student Guidance

1. Research Scientists Supervised

None.

2. Ph.D. Students Graduated

Hadi Abdullah University of Florida

Fall 2016–Summer 2022

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

Chaitrali Amrutkar Georgia Institute of Technology

Fall 2009–Fall 2013

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

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

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

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

2. Ph.D. Students Supervised

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

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

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

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

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

3. Ph.D. Students - Other

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

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

Ryon Kennedy University of Florida
Fall 2020–Spring 2023
Finding vulnerabilities in cellular core networks via fuzzing. Left to join UFIT.

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

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

Frank Park Georgia Institute of Technology

Fall 2008–Spring 2010

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

Ferdinand Schober Georgia Institute of Technology

Fall 2009–Summer 2010

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

4. M.S. Students Supervised

Chaitrali Amrutkar Georgia Institute of Technology

Fall 2008–Spring 2009

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

Logan Blue University of Florida

Fall 2015–Spring 2016

Investigated problems of cellular and network security.

David Dewey Georgia Institute of Technology

Fall 2009–Spring 2010

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

Christopher Grayson Georgia Institute of Technology

Fall 2012–Fall 2013

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

Young Seuk Kim Georgia Institute of Technology

Fall 2012–Fall 2013

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

Daniel Komaromy Georgia Institute of Technology

Fall 2008–Summer 2009

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

Nigel Lawrence Georgia Institute of Technology

Fall 2011–Spring 2012

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

Philip Marquardt Georgia Institute of Technology

Fall 2009–Present

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

Rishikesh Naik Georgia Institute of Technology

Fall 2008–Spring 2010

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

Ashish Nautiyal University of Florida

Fall 2015–Spring 2016

Research on connecting telephone calls to the larger authentication infrastructure.

Nilesh Nipane Georgia Institute of Technology

Fall 2008–Spring 2010

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

Walter “Nolen” Sciafe Georgia Institute of Technology

Spring 2012–Spring 2014

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

Tyler Tucker University of Florida

Fall 2018–Spring 2021

Evaluating the security of Bluetooth radios.

5. M.S. Special Problems Students

Siddhant Deshmukh University of Florida

Fall 2016–Present

Developed tools for analysis of mobile digital financial services.

Chinmay Gangakhedkar Georgia Institute of Technology

Spring 2009

Research on multi-factor authentication using mobile phones.

Christopher Grayson Georgia Institute of Technology

Spring 2013

Research on continuous authentication using mobile phones.

Aarushi Karnany University of Florida

Fall 2016–Present

Developed tools for analysis of mobile digital financial services.

Rohit Matthews Georgia Institute of Technology

Spring 2011

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

Ashwin Narasimhan Georgia Institute of Technology

Spring 2009

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

Aamir Poonawalla Georgia Institute of Technology

Spring 2010

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

Erin Reddick Georgia Institute of Technology

Fall 2008–Fall 2009

Research on IPTV security with GTRI.

Lalanthika Vasudevan Georgia Institute of Technology

Spring 2009

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

6. Undergraduate Special Problems Students

Ethan Shernan Georgia Institute of Technology

Spring 2014

Developed an infrastructure for detecting billing bypass fraud attacks.

Young Seuk Kim Georgia Institute of Technology

Fall 2011–Spring 2012

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

Dane Van Dyck Georgia Institute of Technology

Summer 2009

Research on virtualization support for mobile phones.

E. Teaching Honors and Awards

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

II. RESEARCH AND CREATIVE SCHOLARSHIP

A. Thesis

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

B. Published Journal Papers (Refereed)

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

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

C. Published Books and Parts of Books

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

D. Edited Proceedings

None.

E. Conference Presentations

E.1. Conference Papers with Proceedings (Refereed)

1. Daniel Olszewski, Tyler Tucker, Kevin Butler, and Patrick Traynor. SoK: Towards a Unified Approach to Applied Replicability for Computer Security. In *Proceedings of the USENIX Security Symposium (Security)*, 2025.
2. Daniel Olszewski, Allison Lu, Anna Crowder, Nathaniel Bennett, Seth Layton, Sri Hrushikesh Varma Bhupathiraju, Tyler Tucker, Siddhant Kalgutkar, Hunter Ver Helst, Carson Stillman, Kevin Butler, Sara Rampazzi, and Patrick Traynor. "Raise Your Hand If You've Been Personally Victimized By A Lack Of Reproducibility": On Reproducibility in Tier 2 Security Conferences. In *Proceedings of ACM Conference on Reproducibility and Replicability (REP)*.
3. Cassidy Gibson and Daniel Olszewski and Natalie Grace Brigham and Anna Crowder and Kevin R. B. Butler and Patrick Traynor and Elissa M. Redmiles and Tadayoshi Kohno. Analyzing the AI Nudification Application Ecosystem. In *Proceedings of the USENIX Security Symposium (Security)*, 2025.
4. Tyler Tucker, Nathaniel Bennett, Martin Kotuliak, Simon Erni, Srdjan Capkun, Kevin Butler, and Patrick Traynor. Detecting IMSI-Catchers by Characterizing Identity Exposing Messages in Cellular Traffic. In *Symposium on Network and Distributed System Security (NDSS)*, 2025. (Acceptance Rate 16.1%).
5. Anna Crowder, Allison Lu, Kevin Childs, Carson Stillman, Patrick Traynor, and Kevin Butler. Data to Infinity and Beyond: Examining Data Sharing and Reuse Practices in the Computer Security Community. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2025.
6. Magdalena Pasternak, Kevin Warren, Daniel Olszewski, Susan Nittroveri, Patrick Traynor, and Kevin Butler. Characterizing the Impact of Audio Deepfakes in the Presence of Cochlear Implant Simulated Audio. In *Symposium on Network and Distributed System Security (NDSS)*, 2025. (Acceptance Rate 16.1%).
7. Anna Crowder, Daniel Olszewski, Patrick Traynor, and Kevin R. B. Butler. I Can Show You the World (of Censorship): Extracting Insights from Censorship Measurement Data Using Statistical Techniques. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, December 2024. (Acceptance Rate 21.8%).

8. Kevin Childs, Cassidy Gibson, Anna Crowder, Kevin Warren, Carson Stillman, Elissa Redmiles, Eakta Jain, Patrick Traynor, and Kevin Butler. "I Had Sort of a Sense that I Was Always Being Watched... Since I Was": Examining Interpersonal Discomfort From Continuous Location-Sharing Applications. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2024. (Acceptance Rate 16.9%).
9. Nathaniel Bennett, Weidong Zhu, Benjamin Simon, Ryon Kennedy, William Enck, Patrick Traynor, and Kevin Butler. RANsacked: A Domain-Informed Approach for Fuzzing LTE and 5G RAN-Core Interfaces. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2024. (Acceptance Rate 16.9%).
10. Kevin Warren, Tyler Tucker, Anna Crowder, Daniel Olszewski, Allison Lu, Caroline Fedele, Magdalena Pasternak, Seth Layton, Kevin Butler, Carrie Gates, and Patrick Traynor. Better Be Computer or I'm Dumb": A Large-Scale Evaluation of Humans as Audio Deepfake Detectors. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2024. (Acceptance Rate 16.9%).
11. K. Virgil English, Nathaniel Bennett, Seaver Thorn, Kevin Butler, William Enck, and Patrick Traynor. Examining Cryptography and Randomness Failures in Open-Source Cellular Cores. In *Proceedings of the ACM Conference on Data and Application Security and Privacy (CODASPY)*, 2024. (Acceptance rate: 21.3%)(Best Paper).
12. Seth Layton, Tyler Tucker, Daniel Olszewski, Kevin Warren, Carrie Gates, Kevin Butler, and Patrick Traynor. SoK: The Good, The Bad, and The Unbalanced: Measuring Structural Limitations of Current Deepfake Datasets. In *Proceedings of the USENIX Security Symposium (Security)*, 2024. (Acceptance Rate 18.3%).
13. Imani Munyaka, Daniel Delgado, Juan Gilbert, Jaime Ruiz, and Patrick Traynor. "I used to live in Florida": Exploring the Impact of Spam Call Warning Accuracy on Callee Decision-Making. In *Symposium on Usable Security and Privacy (USEC)*, 2024.
14. Jianliang Wu, Patrick Traynor, Dongyan Xu, Dave (Jing) Tian, and Antonio Bianchi. Finding Traceability Attacks in the Bluetooth Low Energy Specification and Its Implementations. In *Proceedings of the USENIX Security Symposium (Security)*, 2024. (Acceptance Rate 18.3%).
15. Daniel Olszewski, Allison Lu, Carson Stillman, Kevin Warren, Cole Kitroser, Alejandro Pascual, Divyajyoti Ukirde, Kevin Butler, and Patrick Traynor. "Get in Researchers; We're Measuring Reproducibility": A Reproducibility Study of Machine Learning Papers in Tier 1 Security Conferences. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2023. (Acceptance rate: 19.8%).
16. Christian Peeters, Tyler Tucker, Anushri Jain, Kevin Butler, and Patrick Traynor. LeopardSeal: Detecting Call Interception via Audio Rogue Base Stations. In *Proceedings of the ACM International Conference on Mobile Systems, Applications and Services (MobiSys)*, 2023. (Acceptance rate: 21%).
17. Tyler Tucker, Hunter Searle, Kevin Butler, and Patrick Traynor. Blue's Clues: Practical Discovery of Non-Discoverable Bluetooth Devices. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2023. (Acceptance rate: 14%).
18. Hadi Abdullah, Aditya Karlekar, Saurabh Prasad, Muhammad Sajidur Rahman, Logan Blue, Luke Bauer, Vincent Bindschaedler, and Patrick Traynor. Attacks as Defenses: Designing Robust Audio CAPTCHAs Using Attacks on Automatic Speech Recognition Systems. In *Symposium on Network and Distributed System Security (NDSS)*, 2023. (Acceptance rate: 16%).
19. Daniel Olszewski, Sandeep Sathyanarayana, Weidong Zhu, Kevin Butler, and Patrick Traynor. HallMonitor: A Framework for Identifying Network Policy Violations in Software. In *IEEE Conference on Communications and Network Security (CNS)*, 2022.

20. Hadi Abdullah, Aditya Karlekar, Vincent Bindschaedler, and Patrick Traynor. Demystifying Limited Adversarial Transferability in Automatic Speech Recognition Systems. In *Proceedings of the International Conference on Learning Representations (ICLR)*, 2022. (Acceptance rate: 32%).
21. Logan Blue, Kevin Warren, Hadi Abdullah, Cassidy Gibson, Luis Vargas, Jessica O'Dell, Kevin Butler, and Patrick Traynor. Who Are You (I Really Wanna Know)? Detecting Audio DeepFakes Through Vocal Tract Reconstruction. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2022. (Acceptance rate: 17.2%).
22. Grant Hernandez, Marius Muench, Dominik Maier, Alyssa Milburn, Shinjo Park, Tobias Scharnowski, Tyler Tucker, Patrick Traynor, and Kevin R. B. Butler. FirmWire: Transparent Dynamic Analysis for Cellular Baseband Firmware. In *Symposium on Network and Distributed System Security (NDSS)*, 2022. (Acceptance rate: 16.2%).
23. Christian Peeters, Christopher Patton, Imani N. Sherman, Daniel Olszewski, Thomas Shrimpton, and Patrick Traynor. SMS OTP Security (SOS): Hardening SMS-Based Two Factor Authentication. In *ACM Asia Conference on Computer and Communications Security (ASIACCS)*, 2022. (Acceptance rate: 18.2%).
24. Hadi Abdullah, Muhammad Sajidur Rahman, Christian Peeters, Cassidy Gibson, Washington Garcia, Vincent Bindschaedler, Thomas Shrimpton, and Patrick Traynor. Beyond L_p Clipping: Equalization based Psychoacoustic Attacks against ASRs. In *The Asian Conference on Machine Learning (ACML)*, 2021.
25. Imani Sherman and Daniel Delgado and Juan Gilbert and Jaime Ruiz and Patrick Traynor. Characterizing User Comprehension in the STIR/SHAKEN Anti-Robocall Standard. In *Proceedings of the Annual Research Conference on Communications Information and Internet Policy (TPRC 49)*, 2021.
26. Hadi Abdullah, Kevin Warren, Vincent Bindschaedler, Nicolas Papernot, and Patrick Traynor. The Faults in our ASRs: An Overview of Attacks against Automatic Speech Recognition and Speaker Identification Systems. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2021. (Acceptance rate: 12.1%).
27. Hadi Abdullah, Muhammad Sajidur Rahman, Washington Garcia, Logan Blue, Kevin Warren, Anurag Swarnim Yadav, Tom Shrimpton, and Patrick Traynor. Hear “No Evil”, See “Kenansville”: Efficient and Transferable Black-Box Attacks on Speech Recognition and Voice Identification Systems. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2021. (Acceptance rate: 12.1%).
28. Imani Sherman, Jasmine Bowers, Liz-Laure Laborde, Juan E. Gilbert, Jaime Ruiz, and Patrick Traynor. Truly Visual Caller ID? An Analysis of Anti-Robocall Applications and their Accessibility to Visually Impaired Users. In *IEEE International Symposium on Technology and Society (IEEE ISTAS)*, 2020.
29. Imani Sherman, Jasmine Bowers, Keith McNamara, Juan Gilbert, Jaime Ruiz, and Patrick Traynor. Are You Going to Answer That? Measuring User Responses to Anti-Robocall Application Indicators. In *Proceedings of the ISOC Network & Distributed Systems Security Symposium (NDSS)*, 2020. (Acceptance rate: 17.4%).
30. Joseph Choi, Dave Tian, Grant Hernandez, Christopher Patton, Benjamin Mood, Thomas Shrimpton, Patrick Traynor, and Kevin Butler. A Hybrid Approach to Secure Function Evaluation Using SGX. In *Proceedings of the ACM ASIA Conference on Computer and Communications Security (ASIACCS'19)*, 2019. (Acceptance Rate: 17.0% for full papers).
31. Vanessa Frost, Dave Tian, Christie Ruales, Patrick Traynor, and Kevin Butler. Examining DES-based Cipher Suite Support within the TLS Ecosystem. In *Proceedings of the ACM ASIA Conference*

on Computer and Communications Security (ASIACCS'19), 2019. (Acceptance Rate: 22.0% for all papers).

32. Dave Tian, Joseph Choi, Grant Hernandez, Patrick Traynor, and Kevin Butler. A Practical Intel SGX Setting for Linux Containers in the Cloud. In *Proceedings of the ACM Conference on Data and Application Security and Privacy (CODASPY'19)*, 2019. (Acceptance rate: 23.5%).
33. Nolen Scaife, Jasmine Bowers, Christian Peeters, Grant Hernandez, Imani Sherman, Lisa Anthony, and Patrick Traynor. Kiss from a Rogue: Evaluating Detectability of Pay-at-the-Pump Card Skimmers. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2019. (Acceptance rate: 12.0%).
34. Jasmine Bowers, Imani Sherman, Kevin Butler, and Patrick Traynor. Characterizing Security and Privacy Practices in Emerging Digital Credit Applications. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2019. (Acceptance rate: 25.6%).
35. Hadi Abdullah, Washington Garcia, Christian Peeters, P. Traynor, K. Butler, and J. Wilson. Practical Hidden Voice Attacks against Speech and Speaker Recognition Systems. In *Proceedings of the ISOC Network & Distributed Systems Security Symposium (NDSS)*, 2019. (Acceptance Rate: 17.1%).
36. Lius Vargas, Logan Blue, Vanessa Frost, Christopher Patton, N. Scaife, K. Butler, and P. Traynor. Digital Healthcare-Associated Infection Analysis of a Major Multi-Campus Hospital System. In *Proceedings of the ISOC Network & Distributed Systems Security Symposium (NDSS)*, 2019. (Acceptance Rate: 17.1%).
37. Dominik Wermke, Nicolas Huaman, Yasemin Acar, Bradley Reaves, Patrick Traynor, and Sascha Fahl. A Large Scale Investigation of Obfuscation Use in Google Play. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2018. Acceptance Rate: 20.1%.
38. Nolen Scaife, Christian Peeters, and Patrick Traynor. Fear the Reaper: Characterization and Fast Detection of Card Skimmers. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2018. Acceptance Rate: 19.0%.
39. Dave (Jing) Tian, Grant Hernandez, Joseph Choi, Vanessa Frost, Christie Raules, Kevin Butler, Patrick Traynor, Hayawardh Vijayakumar, Lee Harrison, Amir Rahmati, and Mike Grace. Attention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2018. Acceptance Rate: 19.0%.
40. Luis Vargas, Gyan Hazarika, Rachel Culpepper, Kevin Butler, Thomas Shrimpton, Doug Szajda, and Patrick Traynor. Mitigating Risk while Complying with Data Retention Laws. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2018.
41. Logan Blue, Luis Vargas, and Patrick Traynor. Hello, Is It Me You're Looking For? Differentiating Between Human and Electronic Speakers for Voice Interface Security. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2018.
42. Logan Blue, Hadi Abdullah, Luis Vargas, and Patrick Traynor. 2MA: Verifying Voice Commands via Two Microphone Authentication. In *ACM Asia Conference on Computer and Communications Security (ASIACCS)*, 2018. (Acceptance Rate: 20.0%).
43. Nolen Scaife, Christian Peeters, Camilo Velez, Hanqing Zhao, Patrick Traynor, and David Arnold. The Cards Aren't Alright: Detecting Counterfeit Gift Cards Using Encoding Jitter. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2018. (Acceptance Rate: 10.4%).

44. Christian Peeters, Hadi Abdullah, Nolen Scaife, Jasmine Bowers, Patrick Traynor, Bradley Reaves, and Kevin Butler. Sonar: Detecting SS7 Redirection Attacks Via Call Audio-Based Distance Bounding. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2018. (Acceptance Rate: 10.4%).
45. Tyler Ward, Joseph Choi, Kevin Butler, John M. Shea, Patrick Traynor, and Tan Wong. Privacy Preserving Localization Using a Distributed Particle Filtering Protocol. In *IEEE MILCOM*, 2017. (Acceptance Rate: 56%).
46. Bradley Reaves and Logan Blue and Hadi Abdullah and Luis Vargas and Patrick Traynor and Thomas Shrimpton. AuthentiCall: Efficient Identity and Content Authentication for Phone Calls. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2017. (Acceptance Rate: 16.3%).
47. Jasmine Bowers and Bradley Reaves and Imani N. Sherman and Patrick Traynor and Kevin Butler. Regulators, Mount Up! Analysis of Privacy Policies for Mobile Money Applications. In *Proceedings of the USENIX Symposium on Usable Privacy and Security (SOUPS)*, 2017. (Acceptance Rate: 26.5%).
48. Bradley Reaves, Logan Blue, and Patrick Traynor. AuthLoop: End-to-End Cryptographic Authentication for Telephony over Voice Channels. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2016. (Acceptance Rate: 15.5%).
49. Dave Tian, Nolen Scaife, Adam Bates, Kevin Butler, and Patrick Traynor. Making USB Great Again with USBFILTER. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2016. (Acceptance Rate: 15.5%).
50. Bradley Reaves, Dave Tian, Logan Blue, Patrick Traynor, and Kevin Butler. Detecting SMS Spam in the Age of Legitimate Bulk Messaging. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2016. (Acceptance Rate: 35.0%).
51. Nolen Scaife, Henry Carter, Patrick Traynor, and Kevin Butler. CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. In *IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2016. (Acceptance Rate: 17.6%).
52. Bradley Reaves, Nolen Scaife, Dave Tian, Logan Blue, Patrick Traynor, and Kevin Butler. Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2016. (Acceptance Rate: 13.0%).
53. Benjamin Mood, Debayan Gupta, Henry Carter, Kevin Butler, and Patrick Traynor. Frigate: A Validated, Extensible, and Efficient Compiler and Interpreter for Secure Computation. In *Proceedings of the IEEE European Symposium on Security and Privacy*, 2016. (Acceptance Rate: 17.3%).
54. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Outsourcing Secure Two-Party Computation as a Black Box. In *Proceedings of the International Conference on Cryptology and Network Security*, 2015. (Acceptance Rate: 52.9%).
55. Nolen Sciafe, Henry Carter, and Patrick Traynor. OnionDNS: A Seizure-Resistant Top-level Domain. In *Proceedings of the IEEE Conference on Communications and Network Security (CNS)*, 2015. (Acceptance Rate: 28.1%).
56. Bradley Reaves, Nolen Scaife, Adam Bates, Patrick Traynor, and Kevin Butler. Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications in the Developing World. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2015. (Acceptance Rate: 15.7%).
57. Bradley Reaves, Ethan Shernan, Adam Bates, Henry Carter, and Patrick Traynor. Boxed Out: Blocking Cellular Interconnect Bypass Fraud at the Network Edge. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2015. (Acceptance Rate: 15.7%).

58. David Dewey, Bradley Reaves, and Patrick Traynor. Uncovering Use-After-Free Conditions In Compiled Code. In *Proceedings of the International Conference on Availability, Reliability and Security (ARES)*, 2015. (Acceptance Rate: 22%).
59. Ethan Shernan, Henry Carter, Dave Tian, Patrick Traynor, and Kevin Butler. More Guidelines Than Rules: CSRF Vulnerabilities from Noncompliant OAuth 2.0 Implementations. In *Proceedings of the International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA)*, 2015. (Acceptance Rate: 22.7%).
60. Henry Carter, Charles Lever, and Patrick Traynor. Whitewash: Outsourcing Garbled Circuit Generation for Mobile Devices. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2014. (Acceptance Rate: 19.9%).
61. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. Secure Outsourced Garbled Circuit Evaluation for Mobile Devices. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2013. (Acceptance Rate: 16.2%).
62. Chaitrali Amrutkar, Matti Hiltunen, Shobha Venkataraman, Kaustubh Joshi, Patrick Traynor, Trevor Jim, and Oliver Spatscheck. Why is My Smartphone Slow? On The Fly Diagnosis of Poor Performance on the Mobile Internet. In *Proceedings of The 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2013. (Acceptance Rate: 19.6%).
63. Saurabh Chakradeo, Brad Reaves, Patrick Traynor, and William Enck. MAST: Triage for Market-scale Mobile Malware Analysis. In *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2013. (Acceptance Rate: 15.0%)(Best Paper).
64. Charles Lever, Manos Antonakakis, Brad Reaves, Patrick Traynor, and Wenke Lee. The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2013. (Acceptance rate: 18.8%).
65. Chaitrali Amrutkar, Kapil Singh, Arunabh Verma, and Patrick Traynor. VulnerableMe: Measuring Systemic Weaknesses in Mobile Browser Security. In *Proceedings of the International Conference on Information Systems Security (ICISS)*, 2012. (Acceptance rate: 25%) (Best Paper - SAIC Student Paper Competition (GT)) (Finalist - CSAW AT&T Applied Security Research Best Paper Competition 2012).
66. Chaitrali Amrutkar, Patrick Traynor, and Paul van Oorschot. A Measurement Study of SSL Indicators on Mobile Browsers: Extended Life, or End of the Road? In *Proceedings of the Information Security Conference (ISC)*, 2012. (Acceptance rate: 32%) (Best Student Paper).
67. Italo Dacosta, Mustaque Ahamad, and Patrick Traynor. Trust No One Else: Detecting MITM Attacks Against SSL/TLS Without Third-Parties. In *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, 2012. (Acceptance Rate: 20.2%).
68. Adam Bates, Kevin Butler, Micah Sherr, Clay Shields, Patrick Traynor, and Dan Wallach. Accountable Wiretapping -or- I Know They Can Hear You Now. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2012. (Acceptance Rate: 17.8%).
69. Yacin Nadji, Jon Giffin, and Patrick Traynor. Automated Remote Repair for Mobile Malware. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2011. (Acceptance Rate: 18.5%).
70. Nilesh Nipane, Italo Dacosta, and Patrick Traynor. "Mix-In-Place" Anonymous Networking Using Secure Function Evaluation. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2011. (Acceptance Rate: 18.5%).

71. Philip Marquardt, Arunabh Verma, Henry Carter, and Patrick Traynor. (sp)iPhone: Decoding Vibrations From Nearby Keyboards Using Mobile Phone Accelerometers. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2011. (Acceptance Rate: 13.9%).
72. Philip Marquardt, David Dagon, and Patrick Traynor. Impeding Individual User Profiling in Shopper Loyalty Programs. In *Proceedings of the International Conference on Financial Cryptography and Data Security (FC)*, 2011. (Acceptance Rate: 35.1%).
73. David Dewey and Patrick Traynor. No Loitering: Exploiting Lingering Vulnerabilities in Default COM Objects. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2011. (Acceptance Rate: 20.1%).
74. Vijay Balasubramaniyan, Aamir Poonawalla, Mustaque Ahamad, Michael Hunter, and Patrick Traynor. PinDrOp: Using Single-Ended Audio Features to Determine Call Provenance. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2010. (Acceptance Rate: 17.2%).
75. Patrick Traynor, Joshua Schiffman, Thomas La Porta, Patrick McDaniel, Abhrajit Ghosh, and Farooq Anjum. Constructing Secure Localization Systems with Adjustable Granularity. In *IEEE Global Communications Conference (GLOBECOM)*, 2010. (Acceptance Rate: 35.6%).
76. Patrick Traynor. Characterizing the Security Implications of Third-Party EAS Over Cellular Text Messaging Services. In *Proceedings of the Second IEEE International Conference on Security and Privacy in Communication Networks (SecureComm)*, 2010. (Acceptance Rate: 25.0%).
77. Kapil Singh, Samrit Sangal, Nehil Jain, Patrick Traynor, and Wenke Lee. Evaluating Bluetooth as a Medium for Botnet Command and Control. In *Proceedings of the International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA)*, 2010. (Acceptance Rate: 30.7%).
78. Italo Dacosta and Patrick Traynor. Proxychain: Developing a Robust and Efficient Authentication Infrastructure for Carrier-Scale VoIP Networks. In *Proceedings of the USENIX Annual Technical Conference (ATC)*, 2010. (Acceptance Rate: 17.0%).
79. Frank S. Park, Chinmay Gangakhedkar, and Patrick Traynor. Leveraging Cellular Infrastructure to Improve Fraud Prevention. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2009. (Acceptance Rate: 19.0%).
80. Patrick Traynor, Michael Lin, Machigar Ongtang, Vikyath Rao, Trent Jaeger, Thomas La Porta, and Patrick McDaniel. On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2009. (Acceptance Rate: 18.4%).
81. Brendan Dolan-Gavitt, Abhinav Srivastava, Patrick Traynor, and Jonathon Giffin. Robust Signatures for Kernel Data Structures. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2009. (Acceptance Rate: 18.4%).
82. Italo Dacosta, Vijay Balasubramaniyan, Mustaque Ahamad, and Patrick Traynor. Improving Authentication Performance of Distributed SIP Proxies. In *Proceedings of the Conference on Principles, Systems and Applications of IP Telecommunications (IPTComm)*, 2009. (Acceptance Rate: 43.3%).
83. Patrick Traynor, Kevin Butler, William Enck, and Patrick McDaniel. Realizing Massive-Scale Conditional Access Systems Through Attribute-Based Cryptosystems. In *Proceedings of the ISOC Network & Distributed System Security Symposium (NDSS)*, 2008. (Acceptance Rate: 17.7%).
84. Patrick Traynor, Patrick McDaniel, and Thomas La Porta. On Attack Causality in Internet-Connected Cellular Networks. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2007. (Acceptance Rate: 12.3%).

85. Sunam Ryu, Kevin Butler, Patrick Traynor, and Patrick McDaniel. Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems. In *Proceedings of the IEEE International Symposium on Security in Networks and Distributed Systems (SSNDS)*, 2007. (Acceptance Rate: 40%).
86. Luke St. Clair, Lisa Johansen, William Enck, Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Trent Jaeger. Password Exhaustion: Predicting the End of Password Usefulness. In *Proceedings of the International Conference on Information Systems Security (ICISS)*, 2006. (Invited Paper).
87. Kevin Butler, William Enck, Jennifer Plasterr, Patrick Traynor, and P. McDaniel. Privacy-Preserving Web-Based Email. In *Proceedings of the International Conference on Information Systems Security (ICISS)*, December 2006. (Acceptance Rate: 30.4%).
88. Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Brent Waters. Secure Attribute-Based Systems. In *Proceedings of the Thirteenth ACM Conference on Computer and Communications Security (CCS)*, November 2006. (Acceptance Rate: 14.8%).
89. Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta. Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks. In *Proceedings of the Twelfth Annual ACM International Conference on Mobile Computing and Networking (MobiCom)*, September 2006. (Acceptance Rate: 11.7%).
90. Patrick Traynor, Michael Chien, Scott Weaver, Boniface Hicks, and Patrick McDaniel. Non-Invasive Methods for Host Certification. In *Proceedings of the Second IEEE International Conference on Security and Privacy in Communication Networks (SecureComm)*, August 2006. (Acceptance Rate: 25.4%).
91. Patrick Traynor, JaeShung Shin, Barat Madan, Shashi Phoha, and Thomas La Porta. Efficient Group Mobility for Heterogeneous Sensor Networks. In *Proceedings of the IEEE Vehicular Technology Conference (VTC Fall)*, September 2006. (Acceptance Rate: 58%).
92. Patrick Traynor, Raju Kumar, Hussain Bin Saad, Guohong Cao, and Thomas La Porta. LIGER: Implementing Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks. In *Proceedings of the 4th ACM International Conference on Mobile Systems, Applications and Services (MobiSys)*, June 2006. (Acceptance Rate: 15.4%).
93. Patrick Traynor, Guohong Cao, and Thomas La Porta. The Effects of Probabilistic Key Management on Secure Routing in Sensor Networks. In *Proceedings of the 2006 IEEE Wireless Communications and Networking Conference (WCNC)*, April 2006. (Acceptance Rate: 38.8%).
94. Patrick Traynor, Heesook Choi, Guohong Cao, Sencun Zhu, and Thomas La Porta. Establishing Pair-Wise Keys In Heterogeneous Sensor Networks. In *Proceedings of the 25th Annual IEEE Conference on Computer Communications (INFOCOM)*, April 2006. (Acceptance Rate: 18%).
95. William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta. Exploiting Open Functionality in SMS-Capable Cellular Networks. In *Proceedings of the Twelfth ACM Conference on Computer and Communications Security (CCS)*, November 2005. (Acceptance Rate: 15%).
96. Patrick Traynor. Work in Progress Presentations: Fine-Grained Secure Localization for 802.11 Networks. 15th USENIX Security Symposium (SECURITY), August 2006.
97. Patrick Traynor. Work in Progress Presentations: Fundamental Limitations of Sensor Network Security. ACM/USENIX Fourth International Conference on Mobile Systems Applications and Services (MobiSys), June 2006. (Award: Most Entertaining WIP).
98. Patrick Traynor, Heesook Choi, Guohong Cao, and Thomas La Porta. Poster Session: Probabilistic Unbalanced Key Distribution and Its Effects on Distributed Sensor Networks. Workshop on Wireless Security (WiSe), October 2004.

Removed for external version.

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

None.

E.3. Conference Presentations without Proceedings

1. Patrick Traynor. Characterizing the Limitations of Third-Party EAS Over Cellular Text Messaging Services. Technical report, 3G Americas Whitepaper, 2008.
2. Lisa Johansen, Kevin Butler, William Enck, Patrick Traynor, and Patrick McDaniel. Grains of SANs: Building Storage Area Networks from Memory Spots. Technical Report NAS-TR-0060-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, 2007.
3. Luis Vargas, Patrick Emami, and Patrick Traynor. On the Detection of Disinformation Campaign Activity with Network Analysis. In *Proceedings of the 2020 ACM SIGSAC Cloud Computing Security Workshop, CCSW '20*, 2020.

F. Other

F.1. Submitted Journal Papers

None.

F.2. Refereed Research Reports

None.

F.3. Software

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

F.4. Published Papers (Non-Refereed)

1. Siddhant Deshmukh, Henry Carter, Grant Hernandez, Patrick Traynor, and Kevin Butler. Efficient and Secure Template Blinding for Biometric Authentication. In *IEEE Workshop on Security and Privacy in the Cloud (SPC)*, 2016.
2. Debayan Gupta, Benjamin Mood, Joan Feigenbaum, Kevin Butler, and Patrick Traynor. Using Intel Software Guard Extensions for Efficient Two-Party Secure Function Evaluation. In *Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC)*, 2016.

F.5. Books in Preparation

None.

F.6. Workshops and External Courses

1. Chaitrali Amrutkar and Patrick Traynor. Rethinking Permissions for Mobile Web Apps: Barriers and the Road Ahead. In *Proceedings of the ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, 2012.
2. Nigel Lawrence and Patrick Traynor. Under New Management: Practical Attacks on SNMPv3. In *Proceedings of the USENIX Workshop on Offensive Technologies (WOOT)*, 2012.
3. Andrew Harris, Frank S. Park, Seymour Goodman, and Patrick Traynor. Emerging Privacy Concerns for Digital Wallet Deployment. In *Proceedings of the Workshop on Making Privacy in America*, 2009.
4. Patrick Traynor. Privacy and Security Concerns for Personal and Mobile Health Devices. In *Proceedings of the Workshop to Set A Research Agenda for Privacy and Security of Healthcare Technologies*, 2009.
5. Kevin Butler, William Enck, Harri Hursti, Stephen McLaughlin, Patrick Traynor, and Patrick McDaniel. Systemic Issues in the Hart InterCivic and Premier Voting System: Reflections Following Project EVEREST. In *Proceedings of the USENIX/ACCURATE Electronic Voting Technology (EVT) Workshop*, 2008.
6. Keynote: Well, It Worked on My Computer: Reproducibility in Computer Security Research. Learning from Authoritative Security Experiment Results (LASER) Workshop, December 2024. École Polytechnique Fédérale de Lausanne (EPFL, Switzerland).
7. Social Engineering and Two-Factor Authentication. Cyber Security Training Eastern Indonesia, August 2024. Financial Innovation Lab (EIFIL) (Denpasar, Bali, Indonesia).
8. DFS Security and Mobile Money Analysis. Cyber Security Training Eastern Indonesia, August 2024. Financial Innovation Lab (EIFIL) (Denpasar, Bali, Indonesia).

G. Research Proposals and Grants (Principal Investigator)

1. Approved and Funded

1. **Artus Protocol STTR Phase II - Extension**
Sponsor: Office of Naval Research
Investigator(s): Patrick Traynor (PI), Kevin Butler
Amount: \$300,000 over 2 years
Awarded: August 2023
2. **Testing Audio Deep Fake Detectors**
Sponsor: Bank of America
Investigator(s): Patrick Traynor (PI), Kevin Butler
Amount: \$150,000 over 1 year
Awarded: August 2023
3. **Testing Audio Deep Fake Detectors**
Sponsor: Bank of America
Investigator(s): Patrick Traynor (PI), Kevin Butler
Amount: \$274,000 over 2 years
Awarded: August 2021
4. **Deploying Defenses for Cellular Networks Using the AWARE Testbed**
Sponsor: Department of Homeland Security: CISA:
Investigator(s): Patrick Traynor (PI), Kevin Butler, Guofei Gu, Radu Stoleru, Walter Magnussen, P.

R. Kumar

Amount: \$3,100,000 over 4 years

Awarded: October 2019

5. **SaTC:CORE:Medium: Securing the Voice Processing Pipeline Against Adversarial Audio**

Sponsor: NSF Secure and Trustworthy Cyberspace

Investigator(s): Patrick Traynor (PI), Thomas Shrimpton, Vincent Bindschaedler

Amount: \$1,199,999 over 4 years

Awarded: October 2019

6. **Artus Protocol STTR Phase II**

Sponsor: Office of Naval Research

Investigator(s): Patrick Traynor (PI), Kevin Butler

Amount: \$800,000 over 4 years

Awarded: August 2019

7. **Evaluating the Security of QR Code-Based Payments**

Sponsor: Discover Financial

Investigator(s): Patrick Traynor (PI)

Amount: \$50,000 over 1 year

Awarded: September 2018

8. **Workshop: Addressing the Technical Security Challenges of Emerging Digital Financial Services**

Sponsor: NSF Secure and Trustworthy Cyberspace

Investigator(s): Patrick Traynor (PI), Kevin Butler

Amount: \$50,000 over 1 year

Awarded: September 2017

9. **Designing Strong End-to-End Authentication Mechanisms for Modern Telephony Systems**

Sponsor: NSF Secure and Trustworthy Cyberspace

Investigator(s): Patrick Traynor (PI)

Amount: \$500,000 over 3 years

Awarded: July 2016

10. **Digital Healthcare-Associated Infection: Measurement, Defense and Prevention in a Modern Digital Healthcare Ecosystem**

Sponsor: National Science Foundation

Investigator(s): Patrick Traynor (PI), Kevin Butler, Shigang Chen

Amount: \$1,200,000 over 4 years

Awarded: June 2016

11. **Evaluating and Improving Security in Emerging Branchless Banking Systems**

Sponsor: NSF Secure and Trustworthy Cyberspace

Investigator(s): Patrick Traynor (PI)

Amount: \$500,000 over 3 years

Awarded July 2015

12. **Prevention and Detection of Disallowed Connections in Mobile and Pervasive Systems**

Sponsor: CISE-ECE Harris Endowed Seed Fund Program

Investigator(s): Patrick Traynor (PI), Renato Figueiredo (PI)

Amount: \$40,000 over 1 year

Awarded December 2014

13. **Mobile Excursion Study Support**

Sponsor: Hanscom AFB Electronic Systems Command Development Planning Division (ESC/XR)

Investigator(s): Patrick Traynor (PI), Mustaque Ahamad, Jeff Evans, Chuck Bokath
Amount: \$280,000 over 3 months
Awarded July 2012

14. **Characterizing the Security Limitations of Accessing the Mobile Web**

Sponsor: NSF Secure and Trustworthy Cyberspace
Investigator(s): Patrick Traynor (PI) and William Enck (NC State)
Amount: \$334,000 over 3 years
Awarded July 2012

15. **Mitigating Attacks on Mobile Devices and Critical Cellular Infrastructure**

Sponsor: US Department of Defense - Defense University Research Instrumentation Program (DURIP)
Investigator(s): Patrick Traynor (PI), Jon Giffin, Mustaque Ahamad
Amount: \$210,081 over 1 year
Awarded June 2011

16. **Characterizing and Implementing Efficient Primitives for Privacy-Preserving Computation**

Sponsor: DARPA PROgramming Computation on EncryptEd Data (PROCEED) – Broad Agency Announcement
Investigator(s): Patrick Traynor (PI) and Kevin Butler (UOregon)
Amount: \$580,000 over 4 years
Awarded May 2011

17. **Security for Converged IMS Networks**

Sponsor: US Department of Defense
Investigator(s): Patrick Traynor (PI), Mustaque Ahamad and Russ Clark
Amount: \$242,401 over 1 year
Awarded August 2010

18. **CAREER: Protecting User Data on Lost, Stolen and Damaged Mobile Phones**

Sponsor: NSF Trustworthy Computing
Investigator(s): Patrick Traynor (PI)
Amount: \$400,000 over 5 years
Awarded: May 2010

19. **Provably Anonymous Networking Through Secure Function Evaluation**

Sponsor: NSF Trustworthy Computing
Investigator(s): Patrick Traynor (PI)
Amount: \$200,000 over 2 years
Awarded: July 2009

20. **Characterizing and Mitigating Device-Based Attacks in Cellular Telecommunications Networks**

Sponsor: NSF Trustworthy Computing
Investigator(s): Patrick Traynor (PI) and Jonathon Giffin
Amount: \$450,000 over 3 years
Awarded: July 2009

2. Pending

Removed for external version.

H. Research Proposals and Grants (Contributor)

1. Approved and Funded

1. **SaTC: Frontier: Securing the Future of Computing for Marginalized and Vulnerable Populations**
Sponsor: NSF SaTC
Investigator(s): Kevin Butler (PI), Patrick Traynor, Tadayoshi Kohno, Franzi Roesner, Apu Kapadia, Eakta Jain.
Amount: \$7,500,000 for 5 years
Awarded October 2022
2. **ROCKY: Reliable Obfuscated Communications Kit for everYone**
Sponsor: DARPA Resilient Anonymous Communication for Everyone (RACE) – Broad Agency Announcement
Investigator(s): Thomas Shrimpton (PI), Patrick Traynor, Kevin Butler, Vincent Bindschaedler, Nadia Heninger
Amount: \$1,600,000 over 4 years
Awarded May 2019
3. **WiFiUS: Collaborative Research: SELIOT: Securing Lifecycle of Internet-of-Things**
Sponsor: NSF CNS WiFiUS
Investigator(s): Gene Tsudik (PI), Patrick Traynor
Amount: \$300,000 for 2 years
Submitted December 2016
4. **Cloud-based Oblivious Spectrum Mapping and Allocation**
Sponsor: NSF CNS EARS
Investigator(s): John Shea (PI), Tan Wong, Patrick Traynor
Amount: \$532,952 for 2 years
Submitted May 2016
5. **DURIP: Developing Research Capability in Cyber-Physical Systems at the University of Florida**
Sponsor: Small
Investigator(s): Kevin Butler (PI), Patrick Traynor, My Thai
Amount: \$200,000 for 2 years
Submitted: June 2015
6. **Securing the New Converged Telephony Landscape**
Sponsor: NSF TWC: Small
Investigator(s): Mustaque Ahamad (PI) and Patrick Traynor
Amount: \$500,000 for 3 years
Submitted: December 2012
7. **Facilitating Free and Open Access to Information on the Internet**
Sponsor: NSF Trustworthy Computing
Investigator(s): Nick Feamster (PI), Wenke Lee, Patrick Traynor, Hans Klein, Roger Dingledine, Michael Freedman and Edward W. Felten
Amount: \$1,500,000 for 4 years
Awarded: June 2011
8. **Monitoring Free and Open Access to Information on the Internet**
Sponsor: Google Focus Program
Investigator(s): Nick Feamster (PI), Wenke Lee, Mustaque Ahamad, Patrick Traynor, Henry Owen, Ellen Zegura, Zvi Galil

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

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

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

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

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

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

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

2. Pending

Removed for external version.

I. Research Honors and Awards

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

III. SERVICE

A. Professional Activities

A.1. Memberships and Activities in Professional Societies

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

A.2. Conference Committee Activities

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

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

B. On-Campus Committees

B.1. University of Florida

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

B.2. Georgia Tech

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

C. Special Assignments

None.

D. Ph.D. Examining Committees

Ph.D. Examining Committees

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

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

External Member of Ph.D. Research Committee

None.

External Member of Ph.D. Examining Committee

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

Ph.D. Thesis Proposal Committees

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

Ph.D. Qualifying Exam Committees—Georgia Tech

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

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

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

E. External Member of M.S. Examining Committee

M.S. Thesis Defense Committees None.

F. Consulting and Advisory Appointments

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

G. Civic Activities

None.

IV. NATIONAL AND INTERNATIONAL PROFESSIONAL RECOGNITION

A. Honors and Awards

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

B. Invited Conference Session Chairmanships

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

C. Professional Registration

None.

D. Patents

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

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

E. Editorial and Reviewer Work for Technical Journals and Publishers

Associate Editor:

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

Guest Editor:

Journals

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

Reviewer for:

Journals

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

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

Conferences and Workshops

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

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

F. Expert Witness Services

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

13. *Advanced Coding Technologies LLC v. ByteDance PTE. Ltd., and TikTok PTE. Ltd.*: Expert witness for the Defense for Non-Infringement (via Fish & Richardson, LLP). July 2023 - September 2023.
14. *Epic Games, Inc. & Anor v Google LLC & Ors - Federal Court of Australia Proceeding NSD 190 of 2021*: Expert witness for the Defendant (via Corrs Chambers Westgarth). January 2023 - Present.
15. *Rubin vs KAHOOT! ASA and KAHOOT! EDU*: Expert witness for the Defendant for Inter Partes Review (via Vasquez Benisek & Lindgren, LLP). December 2022 - June 2024.
16. *Telefonaktiebolaget LM Ericsson vs Apple, Inc.*: Expert witness for the Defendant, Non-Infringement and Invalidity (via WilmerHale LLP). February 2022 - December 2022.
17. *Wepay Global Payments, LLC v. Bank of America N. A.*: Expert Witness for the Defendant (via WilmerHale LLP) September 2022 - November 2022.
18. *Apple vs. R.N Nehushtan Trust Ltd.*: Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). August 2022 - June 2023.
19. *Apple/Microsoft vs. Zipit Wireless*: Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). May 2021 - November 2022.
20. *Blackberry Inc v MobileIron, Inc.*: Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). January 2021 - March 2021.
21. *Apple Inc v Seven Networks, LLC*: Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). August 2019 - November 2020.
22. *mSIGNIA, Inc. v. InAuth, Inc.*: Expert Witness for the Defendant for Inter Partes Review, Non-Infringement and Invalidity, Trade Secrets (via Quinn Emanuel Urquhart and Sullivan, LLP). October 2017 - December 2018.
23. *Huawei v. T-Mobile*: Expert Witness for the Defendant for Non-Infringement (via WilmerHale LLP, Alston & Bird LLP) June 2016 - December 2017.
24. *Telefonaktiebolaget LM Ericsson v Apple*: Expert Witness for the Defendant for Non-Infringement, Invalidity (via WilmerHale LLP). June 2015 - December 2015.
25. *Mayfonk v Nike*: Expert Witness for the Plaintiff for Infringement/Trade Secrets (via Paul Hastings). June 2015 - November 2015.
26. *Maxim Integrated Products v Bank of the West*: Expert Witness for the Defendant for Non-Infringement (via Paul Hastings LLP). January 2014 - August 2014.
27. *Maxim Integrated Products v Comerica Inc, et al.*: Expert Witness for the Defendant for Non-Infringement (via McKenna, Long & Aldridge LLP). June 2014 - August 2014.
28. *William Grecia v. Apple Inc. et al.*: Expert Consultant for the Defendant for Invalidity (via Kirkland & Ellis LLP). July 2014 - August 2014.
29. *Intertrust Technologies Corp. v. Apple Inc.*: Expert Consultant for Defendant for Invalidity and Non-Infringement (via Kirkland & Ellis LLP). October 2013 - February 2014.
30. *Maxim Integrated Products v KeyCorp Bank*: Expert Witness for the Defendant for Non-Infringement (via Calfee, Halter & Griswold LLP) April 2013 - June 2013.
31. *Intellectual Ventures LLC vs. Check Point; et al.*: Expert Consultant for the Plaintiff for Infringement (via Susman Godfrey LLP), October 2012 - February 2015.

V. OTHER CONTRIBUTIONS

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

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

16. Responsible Finance for the Digital Client. Foromic Conference, October 2018. Barranquilla, Colombia.
17. Panel: Authentication Challenges for New Interfaces, Devices, and Wireless Networks. ACM Conference on Security and Privacy in Wireless and Mobile Networks, June 2018. Stockholm, Sweden.
18. Sonar: Detecting SS7 Redirection Attacks Via Call Audio-Based Distance Bounding. CyberSecurity@KAIST Workshop - KAIST, June 2018. Daejeon, South Korea.
19. Why Caller-ID Spoofing Is So Easy (and Why End-To-End Solutions Are the Way Forward). IEEE Workshop on Technology and Consumer Protection (ConPro'18), May 2018. San Francisco, CA.
20. Panel: The Future of Cybersecurity. SEC Academic Conference - Auburn University, May 2018. Auburn, AL.
21. Sound Principles: Verifying Voice Commands in an IoT World. IoT Security Workshop - Aalto University, September 2017. Helsinki, Finland.
22. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Eurecom Institute, September 2017. Sophia Antipolis, France.
23. Panel: Infrastructure Stability. ITU-T Focus Group Digital Financial Services, December 2016. Geneva, Switzerland.
24. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. ETH Zurich, December 2016. Zurich, Switzerland.
25. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. University of Richmond, October 2016. Richmond, Virginia.
26. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Indiana University, September 2016. Bloomington, Indiana.
27. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Aalto University Computer Science Department Forum, August 2016. Helsinki, Finland.
28. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. KAIST Information Security Seminar - Korean Advanced Institute of Science and Technology, June 2016. Daejeon, South Korea.
29. Updated Mobile Money Vulnerability Report. International Telecommunications Union Digital Financial Services Working Group Workshop, May 2016. Washington, DC.
30. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. UF Eye Opener Discovery Breakfast - University of Florida, May 2016. Gainesville, FL.
31. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Illinois Science of Security (SoS) Lablet Speaker Series - University of Illinois, Urbana-Champaign, April 2016. Urbana-Champaign, Illinois.
32. New Trends in Cybersecurity: Vulnerabilities in Branchless Banking Systems. United States Departments of State and Justice - Cybersecurity and Cybercrime Workshop for Lusophone Africa, September 2015. Maputo, Mozambique.
33. New Trends in Cybersecurity: Vulnerabilities in Branchless Banking Systems. United States Departments of State and Justice - ECCAS Cybersecurity and Cybercrime Workshop, August 2015. Kinshasa, Democratic Republic of Congo.

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

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

74. Trends in Security: Critical Engineering in the Large. Schlumberger Innovate IT! Workshop, May 2006. Cambridge, MA.
75. Exploiting Open Functionality in SMS-Capable Cellular Networks. InfraGard Pittsburgh Chapter General Meeting, September 2006. Pittsburgh, PA.
76. Exploiting Open Functionality in SMS-Capable Cellular Networks. InfraGard Pittsburgh Chapter General Meeting, September 2006. Pittsburgh, PA.
77. How technology can fight digital fakery. The Babbage Podcast/The Economist <https://shows.acast.com/theeconomistbabbage/episodes/babbage-how-to-detect-a-deepfake/>, January 2023.
78. Deepfake audio has a tell and researchers can spot it. Ars Technica <https://arstechnica.com/information-technology/2022/09/researchers-use-fluid-dynamics-to-spot-deepfake-voices/>, September 2022.
79. This security tool could help stop the problem of ransomware in its tracks. TheJournal.ie <https://www.thejournal.ie/ransomware-researchers-stop-2875032-Jul2016/>, July 2016.

B. Special Activities

Presentations to Lay Media

1. Researchers Unleash Ransomware Annihilation. BankInfoSecurity - <http://www.bankinfosecurity.com/researchers-unleash-ransomware-annihilation-a-9255/>, July 2016.
2. CryptoDrop Stops Ransomware by Stopping its Encryption. Security Intelligence - https://securityintelligence.com/news/cryptodrop-stops-ransomware-by-stopping-its-encryption/?utm_source=tfeed&utm_medium=twitter, July 2016.
3. Ransomware 'stopped' by new software. BBC - <http://www.bbc.com/news/technology-36772461>, July 2016.
4. Researchers create effective anti-ransomware solution. Help Net Security - <https://www.helpnetsecurity.com/2016/07/12/anti-ransomware-solution/>, July 2016.
5. Florida U boffins think they've defeated all ransomware. http://www.theregister.co.uk/2016/07/12/ransomware_defeated/, July 2016.
6. This Anti-Ransomware Tool Could Save You Hundreds of Pounds. Huffington Post - http://www.huffingtonpost.co.uk/entry/anti-ransomware-tool-save-hundreds-pounds_uk_57838beee4b0935d4b4b30ba, July 2016.
7. Researchers develop method to stop 100% of ransomware before it encrypts all files. Myce - <http://www.myce.com/news/researchers-develop-method-stop-100-ransomware-encrypts-files-79873/>, July 2016.
8. Desarrollan una solución para detener el ransomware. ComputerHoy - <http://computerhoy.com/noticias/software/desarrollan-solucion-detener-ransomware-47972>, July 2016.

9. Why your antivirus software can't stop ransomware. Futurity - <http://www.futurity.org/ransomware-computer-files-1198242-2/>, July 2016.
10. CryptoDrop Gives Users Hope to Prevent Ransomware Infections in the Future. Softpedia - <http://news.softpedia.com/news/cryptodrop-gives-users-hope-to-prevent-ransomware-infections-in-the-future-506187.shtml>, July 2016.
11. Could this be the answer to the ransomware threat?, Consumer Affairs. Consumer Affairs - <https://www.consumeraffairs.com/news/could-this-be-the-answer-to-the-ransomware-threat-071116.html>, July 2016.
12. Extortion extinction: Researchers develop a way to stop ransomware. Phys.org - <http://phys.org/news/2016-07-extortion-extinction-ransomware.html>, July 2016.
13. Researchers Develop A Way To Stop Ransomware By Watching The Filesystem. Slashdot - <https://yro.slashdot.org/story/16/07/08/2242244/researchers-develop-a-way-to-stop-ransomware-by-watching-the-filesystem>, July 2016.
14. Mohul Ghosh. Trak.in - Digital Money Apps In India Are Unsafe and Unsecured - Researchers. <http://trak.in/tags/business/2015/08/17/digital-money-apps-india-unsafe-unsecured/>, August 2015.
15. Richard Handford. Mobile World Live - Survey finds security holes in mobile money apps. <http://www.mobileworldlive.com/money/news-money/survey-finds-security-holes-in-mobile-money-apps/#.Vc27Y-QTmsQ.twitter>, August 2015.
16. JENNIFER VALENTINO-DEVRIES. Wall Street Journal - Researchers Find Security Flaws in Developing-World Money Apps. <http://blogs.wsj.com/digits/2015/08/11/researchers-find-security-flaws-in-developing-world-money-apps/>, August 2015.
17. Jonathon Cheng. Wall Street Journal - Samsung Phone Studied for Possible Security Gap. <http://online.wsj.com/news/articles/SB10001424052702304244904579276191788427198>, December 2013.
18. N. V. The Economist - The Threat in the Pocket. <http://www.economist.com/blogs/babbage/2013/10/difference-engine-0?fsrc=scn/fb/wl/bl/thethreatinthepocket>, October 2013.
19. Antone Gonsalves. ComputerWorld - Let's Dump Anti-Virus and Move On:. <http://blogs.computerworld.com/mobile-security/22969/lets-dump-av-and-move>, October 2013.
20. Mathew J. Schwartz. InformationWeek - Google: Don't Fear Android Malware. <http://www.informationweek.com/security/mobile/google-dont-fear-android-malware/240162399>, October 2013.
21. Kirsten Doyle. ITWeb - Android Threat Exaggerated, or is it? http://www.itweb.co.za/index.php?option=com_content&view=article&id=68055, October 2013.
22. Danielle Walker. SC Magazine - Mobile malware prevalence expands, but privacy-abusing apps should be top of mind. <http://www.scmagazine.com/mobile-malware-prevalence-expands-but-privacy-abusing-apps-should-be-top-of-mind/article/300597/>, June 2013.

23. Jim Burrell. WABE NPR - Mobile Web Browsers Full of Security Risks, Tech Professor Finds. <http://wabe.org/post/mobile-web-browsers-full-security-risks-tech-professor-finds>, December 2012.
24. Mark Huffman. Consumer Affairs - Georgia Tech: mobile browsers fail safety test. <http://www.consumeraffairs.com/news/georgia-tech-mobile-browsers-fail-safety-test-120612.html>, December 2012.
25. Matthew J. Schwartz. Information Week - Blame Screen Size: Mobile Browsers Flunk Security Tests. <http://www.informationweek.com/security/mobile/blame-screen-size-mobile-browsers-flunk/240143999>, December 2012.
26. Jon Gold. Network World - Ga. Tech researchers: Mobile Browsers need better HTTPS indicators. <http://www.networkworld.com/news/2012/120512-mobile-browsers-264846.html>, December 2012.
27. United Press International. Study: Most mobile Web browsers unsafe. http://www.upi.com/Science_News/Technology/2012/12/05/Study-Most-mobile-Web-browsers-unsafe/UPI-73431354743353/#ixzz2EGtQsuLd, December 2012.
28. Suzanne Choney. Mobile browser woes can fool even experts: report. <http://www.nbcnews.com/technology/mobile-browser-woes-can-fool-even-experts-report-1C7451203>, December 2012.
29. Meghan Kelly. VentureBeat - 3 hot security startups to watch. <http://venturebeat.com/2012/02/27/3-security-startups-to-watch-at-the-2012-rsa-conference/>, February 2012.
30. Jacob Goodwin. Government Security News - RSA 2012 – Pindrop Security can distinguish a fraudulent phone call from a real one. <http://www.gsnmagazine.com/node/25721?c=communications>, February 2012.
31. Matt Liebowitz. Phone hack logs keystrokes from nearby computers. MSNBC.com - http://www.msnbc.msn.com/id/44993238/ns/technology_and_science-security/#.TqU5MNSjPh4, October 2011.
32. Jacob Aron. iPhone keylogger can snoop on desktop typing. New Scientist - <http://www.newscientist.com/article/dn21059-iphone-keylogger-can-snoop-on-desktop-typing.html>, October 2011.
33. iPhone Keylogger Can Snoop on Desktop Typing. Slashdot - <http://mobile.slashdot.org/story/11/10/18/2346222/iphone-keylogger-can-snoop-on-desktop-typing>, October 2011.
34. Robert Lemos. Smart Phones Could Hear Your Password. Technology Review - <http://www.technologyreview.com/computing/38913/?p1=A2>, October 2011.
35. Kevin McCaney. Bad vibrations: How smart phones could steal PC passwords. Government Computer News - <http://gcn.com/articles/2011/10/18/smart-phone-sensors-steal-keystrokes.aspx>, October 2011.
36. PhysOrg. Turning iPhone into spiPhone: Smartphones' accelerometer can track strokes on nearby keyboards. PhysOrg.com - <http://www.physorg.com/news/2011-10-iphone-spiphone-smartphones-accelerometer-track.html>, October 2011.

37. Brid-Aine Parnell. Securo-boffins call for 'self-aware' defensive technologies. The Register - http://www.theregister.co.uk/2011/09/14/self_aware_cyber_security_technologies_should_be_a_top_priority/, September 2011.
38. Clay Dillow. 'PinDr0p' Tech Uses Unique Noise Fingerprints to Trace Calls. Popular Science - <http://www.popsoci.com/technology/article/2010-10/pindr0p-tech-tags-phone-calls-unique-fingerprints-trace-call-paths-across-networks>, October 2010.
39. Lewis Page. Voice-routing call fingerprint system fights vishing. The Register - http://www.theregister.co.uk/2010/10/06/voice_fingerprints, October 2010.
40. Science Daily. Voice Phishing: System to Trace Telephone Call Paths Across Multiple Networks Developed. <http://www.sciencedaily.com/releases/2010/10/101005121820.htm>, October 2010.
41. Brian Kalish. To Text or Not to Text During Emergencies. NextGov.com - http://www.nextgov.com/nextgov/ng_20100914_5986.php?oref=topnews, September 2010.
42. Ki Mae Heussner. 'Operation Chokehold': Fake Steve Jobs Rallies iPhone Users to Cripple AT&T Network. ABC News - <http://abcnews.go.com/Technology/GadgetGuide/fake-steve-jobs-rallies-iphone-users-cripple-att/story?id=9355447>, December 2009.
43. Bob Brown. Researchers Set Their Sights on iPhones, Mobile Malware. PC World Magazine - http://www.pcworld.com/article/182005/iphone_worms_mobile_malware.html?tk=rss, November 2009.
44. MacGregor Campbell. Botnets show their disruptive potential. New Scientist Magazine - <http://www.newscientist.com/article/mg20427347.000-mobile-botnets-show-their-disruptive-potential.html>, November 2009.
45. Angela Moscaritolo. Remote repair for infected phones in development. SC Magazine - <http://www.scmagazineus.com/remote-repair-for-infected-phones-in-development/article/157504/>, November 2009.
46. Bob Brown. iPhone worms, other smartphone malware in researchers' sights. Network World - <http://www.networkworld.com/news/2009/111109-smartphone-security-georgia-tech.html?hpg1=bn>, November 2009.
47. Urvaksh Karkaria. GT researchers work to secure cellphones. Atlanta Business Chronicle - <http://atlanta.bizjournals.com/atlanta/blog/atlantech/2009/11/cellphone.html>, November 2009.
48. Making Carriers Shoulder Smartphone Security. http://mobile.slashdot.org/story/09/11/11/2318247/Making-Carriers-Shoulder-Smartphone-Security?art_pos=31, November 2009.
49. Ben Meyer. Georgia Tech to Lead Fight Against Cell Phone Hackers. NBC 11 Atlanta - <http://www.11alive.com/news/local/story.aspx?storyid=132505&catid=3>, July 2009.
50. Illena Armstrong. Safeguarding your mobile networks. SC Magazine - <http://www.scmagazineus.com/Safeguarding-your-mobile-networks/article/138289/>, June 2009.
51. Kelli B. Grant. Four Free Cellphone Apps to Help Manage Your Money. SmartMoney Magazine - <http://www.smartmoney.com/Spending/Deals/4-Great-Free-Finance-Apps-for-Cellphones/>, June 2009.

52. Amanda Hoffstrom. Technology's limitations in alerting campus danger. UWire Magazine - <http://www.uwire.com/Article.aspx?id=3738798>, February 2009.
53. Laura Sydel. Compromise Allows Obama To Keep BlackBerry. National Public Radio - <http://www.npr.org/templates/story/story.php?storyId=99790788>, January 2009.
54. Dennis Carter. Questions abound as emergency alert flops Virginia Tech's text-message alert system failed when the sound of gunfire was heard on campus; officials scramble to understand why. eSchool News - http://www.eschoolnews.com/iphone/top-story/index.cfm?i=56122#_56122, November 2008.
55. Jessica Bauer. Study: Text alerts may fail in real emergency. Diamondback Online - <http://media.www.diamondbackonline.com/media/storage/paper873/news/2008/10/14/News/Study.Text.Alerts.May.Fail.In.Real.Emergency-3485509.shtml>, October 2008.
56. Associated Press. Hackers Expected To Start Targeting Cell Phones. <http://cbs5.com/watercooler/Cell.Phones.Hackers.2.840909.html>, 2008.
57. Associated Press. College alert systems unreliable, study says. http://www.ajc.com/search/content/metro/stories/2008/09/25/college_campus_alerts.html, 2008.
58. Lee Shearer. Study: Campus alerts unreliable. Athens Banner Herald http://www.onlineathens.com/stories/092508/uga_336494829.shtml, 2008.
59. Bill Ray. 3G Americas warns against text warning systems. The Register - http://www.theregister.co.uk/2008/09/18/emergency_text/, 2008.
60. 3G Americas. 3G Americas Highlights New Research Report on Use of Cellular Text Messaging for Emergency Alert Services. 3G Americas http://www.3gamericas.org/English/news_room/DisplayPressRelease.cfm?id=3400&s=ENG, 2008.
61. Evan Koblentz. Web Exclusive: From Messaging to Management Duty. Wireless Week - <http://www.wirelessweek.com/Messaging-to-Management-Duty.aspx>, 2008.
62. Christopher Beam. How Do You Intercept a Text Message? Turn your cell phone into a spy gadget. Slate Magazine <http://www.slate.com/id/2161402/>, 2007.
63. Jamming Cellphones with Text Messages. Slashdot <http://it.slashdot.org/it/05/10/05/1839217.shtml?tid=215&tid=172>, 2005.
64. Cell phone networks at risk? CNN http://money.cnn.com/2005/10/05/technology/hacker_cellphones/, 2005.
65. John Schwartz. Text Hackers Could Jam Cellphones, a Paper Says. The New York Times <http://www.nytimes.com/2005/10/05/technology/05phone.html?ex=1286164800&en=d917b9cd43dfaa31&ei=5090&partner=rssuserland&emc=rss>, 2005.
- 66.
- 67.
- 68.