IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	Gregory G. Raleigh, et al.	
U.S. Patent No.:	9,647,918	Attorney Docket No.: 39843-0182IP1
Issue Date:	May 9, 2017	
Appl. Serial No.:	15/227,814	
Filing Date:	August 3, 2016	
Title:	MOBILE DEVICE AND METHOD ATTRIBUTING MEDIA SERVICES NETWORK USAGE TO REQUESTING APPLICATION	

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: 9 September 2024

By: _____
Patrick Traynor, Ph.D.

SAMSUNG 1003

Table of Contents

I. QUALIFICATIONS AND BACKGROUND INFORMATION.....3

II. LEGAL PRINCIPLES.....8
- A. Anticipation.....8
- B. Obviousness.....9

III. OVERVIEW OF CONCLUSIONS FORMED.....10

IV. BACKGROUND KNOWLEDGE ONE OF SKILL IN THE ART WOULD HAVE HAD PRIOR TO THE PRIORITY DATE OF THE ’918 PATENT11

V. INTERPRETATIONS OF THE ’918 PATENT CLAIMS AT ISSUE.....12

VI. THE ’918 PATENT.....12
- A. Overview of the ’918 Patent.....12
- B. Prosecution History of the ‘918 Patent.....14

VII. OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES..15
- A. Overview of Bennett.....15
- B. Overview of Vadde.....16
- C. The combination of Bennett and Vadde.....17
- D. Overview of Riggs.....23
- E. The combination of Bennett, Vadde, and Riggs.....24
- F. Overview of Hendrickson.....27
- G. The combination of Bennett, Vadde, Riggs, and Hendrickson.....28
- H. Overview of Srikantan.....30
- I. The combination of Bennett, Vadde, Riggs, and Srikantan.....31

VIII. MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE ’918 CLAIMS UNPATENTABLE.....34
- A. Claims 1-3, 8-9, 13-14, and 19 are obvious over Bennett in view of Vadde.....34
- B. Claims 4-6, 11-13, and 15-17 are obvious over Bennett in view of Vadde and Riggs.....74
- C. Claims 7, 12, and 18 are obvious over Bennett in view of Vadde, Riggs, and Hendrickson.....86
- D. Claim 10 is obvious over Bennett in view of Vadde, Riggs, and Srikantan.....94

IX. CONCLUSION.....100

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 Samsung in the matter of Samsung Electronics Co., Ltd. ("Samsung") vs. Headwater Research, LLC. My qualifications for forming these conclusions are summarized below.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14. My curriculum vitae, included with this declaration as SAMSUNG-1003, 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:

- U.S. Patent No 9,647,918 (SAMSUNG-1001), and its accompanying prosecution history (SAMSUNG-1002)
- U.S. Patent Publication No 2006/0149811 ("Bennett") (SAMSUNG-1041)
- U.S. Patent Publication No. 2012/0117478 ("Vadde") (SAMSUNG-1042)
- U.S. Patent No. 8,429,516 ("Riggs") (SAMSUNG-1043)
- EP Patent Publication No. 1 850 575 A1 ("Rybak") (SAMSUNG-1044)
- U.S. Patent Publication No. 2004/0260630 ("Benco") (SAMSUNG-1045)
- U.S. Patent No. 6,578,077 ("Rakoshitz") (SAMSUNG-1046)
- U.S. Patent Publication No. 2006/0223495 ("Cassett") (SAMSUNG-1047)
- U.S. Patent Publication No. 2008/0080458 ("Cole") (SAMSUNG-1048)
- U.S. Patent Publication No. 2008/0209451 ("Michels") (SAMSUNG-1049)
- U.S. Patent Publication No. 2006/0039354 ("Rao") (SAMSUNG-1050)
- U.S. Provisional Application No. 61/435,564 (SAMSUNG-1053)
- U.S. Patent No. 6,754,470 ("Hendrickson") (SAMSUNG-1054)
- U.S. Patent Publication No. 2002/0056126 ("Srikantan") (SAMSUNG-1055)
- Newton's Telecom Dictionary, 24th Edition (SAMSUNG-1056)
- Webster's New World, Telecom Dictionary (SAMSUNG-1057)
- Wiley Electrical and Electronics Engineering (IEEE) Dictionary (SAMSUNG-1058)

- The Authoritative Dictionary of IEEE Standards Terms (SAMSUNG-1059)
- U.S. Patent Publication No. US 2008/0122796 ("Jobs") (SAMSUNG-1062)
- U.S. Patent Publication No. US 2010/0017506 ("Fadell") (SAMSUNG-1063)

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, I have applied a date of January 24, 2011 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 January 24, 2011. Additionally, because I understand the priority date of the '918 Patent is in dispute, my analysis also considers the earliest priority date of January 28, 2009 and my opinions are additionally applicable to that date, except where otherwise noted.

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 1-3, 8-9, 13-14, and 19 of the '918 Patent are obvious over Bennett in view of Vadde.
- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claims 4-6, 11-13, and 15-17 of the '918 Patent are obvious over Bennett in view of Vadde and Riggs.

- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claims 7, 12, and 18 of the ’918 Patent are obvious over Bennett in view of Vadde, Riggs, and Hendrickson.
- Based upon my knowledge and experience and my review of the prior art publications listed above, I believe that claim 10 of the ’918 Patent is obvious over Bennett in view of Vadde, Riggs, and Hendrickson.

IV. BACKGROUND KNOWLEDGE ONE OF SKILL IN THE ART WOULD HAVE HAD PRIOR TO THE PRIORITY DATE OF THE ’918 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 ’918 Patent would have had (1) at least a bachelor’s degree in computer science, computer engineering, electrical engineering, or a related field, and (2) at least two years of industry experience in wireless communication network applications and software. 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 ’918 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 that I should use January 24, 2011 as the point in time for claim interpretation purposes. Additionally, because I understand the priority date of the ’918 Patent is in dispute, my analysis also considers the earliest priority date of January 28, 2009 and my opinions are additionally applicable to that date, except where otherwise noted.

VI. THE ’918 PATENT

A. Overview of the ’918 Patent

24. The ’918 Patent is directed to “a wireless end-user device” that includes a “proxy network service manager” (also referred to as a “proxy”) that facilitates media requests from resident applications. SAMSUNG-1001, Abstract, 71:21-42, 110:12-111:17, 119:49-60, FIGS. 30, 35. In an example embodiment depicted in FIG. 30, the application “utilizes an API to trigger the proxy 3012 which in turn passes through a socket connection at the socket 3016 as traffic.” *Id*., 110:46-53.

FIG. 35 depicts another example embodiment that includes "a proxy service manager 3502," a "proxy/library API 3504," a "stack API 3518," and a "usage/classification reconciliation engine 3526." *Id*., 119:49-60. The '918 Patent describes that example "stack API level … requests" are "socket open/send requests." *Id*., 93:33-36.

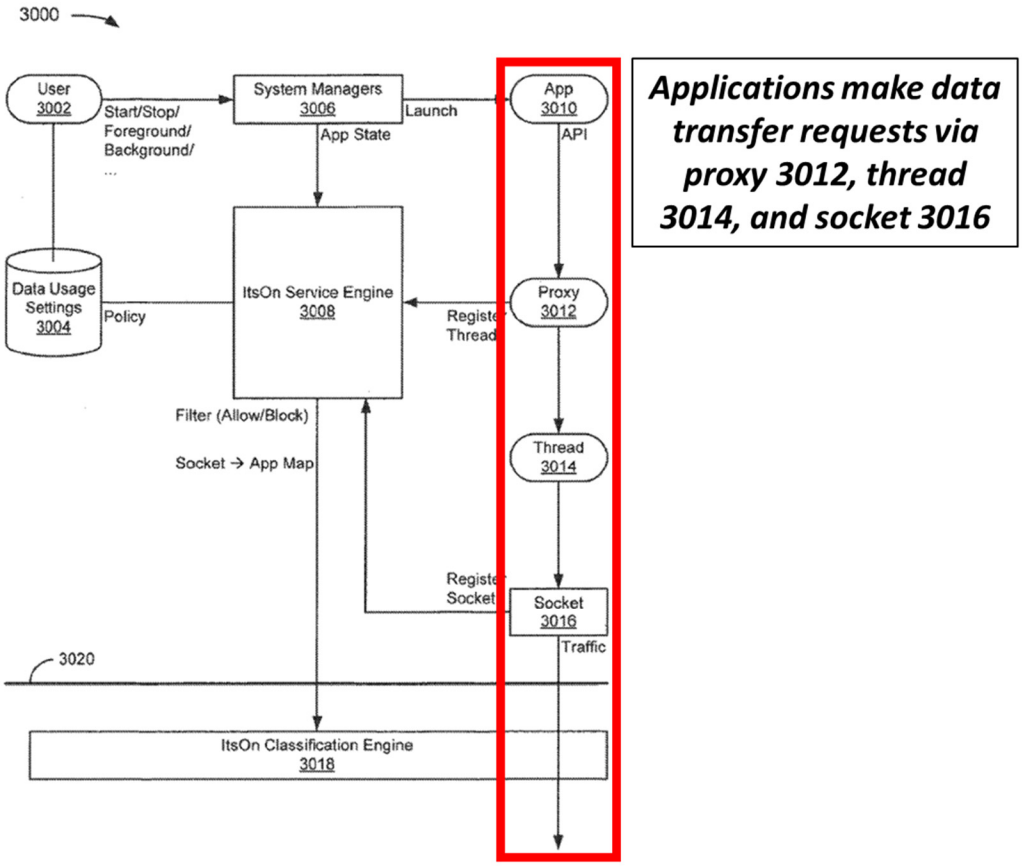


FIG. 30

SAMSUNG-1001, FIG. 30[1].

[1] Annotations to figures are shown in color.

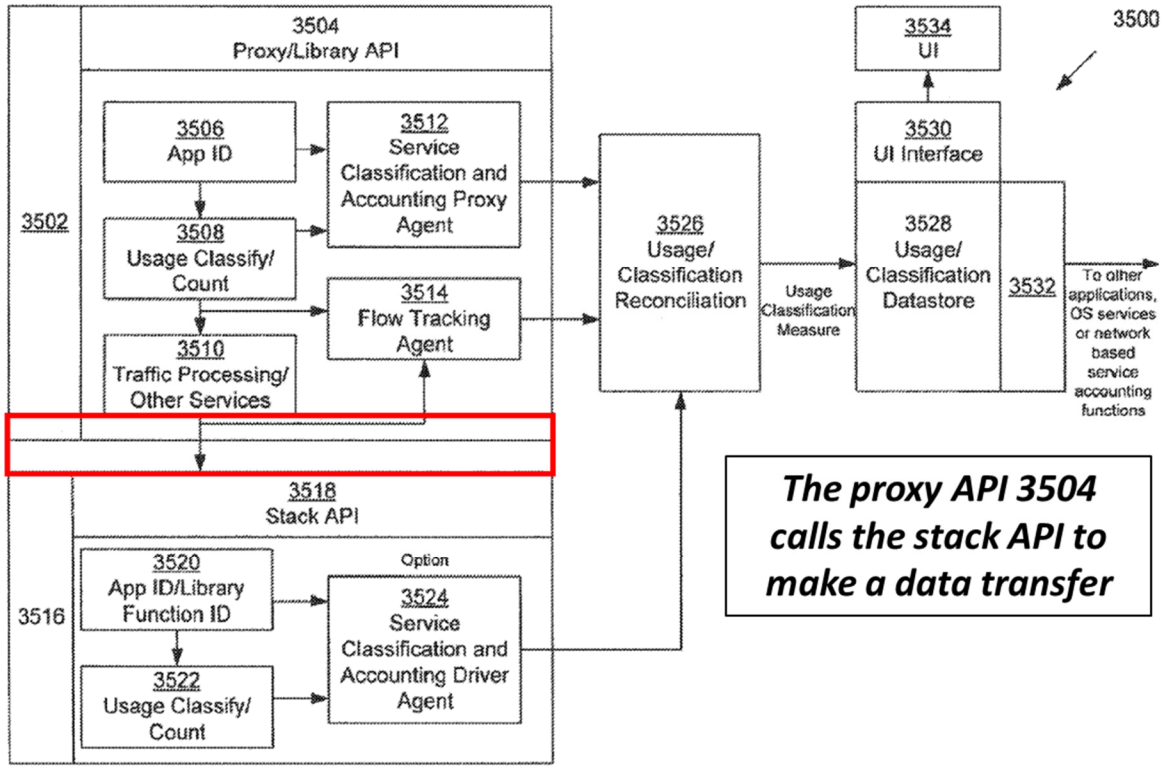


FIG. 35

SAMSUNG-1001, FIG. 35

B. Prosecution History of the '918 Patent

25. The Examiner issued only one office action during the '918 Patent's prosecution, including prior art rejections of claims 2-4, 11, and 13-16 (issued claims 1-2, 9, and 11-14) under §102 over Deu-Ngoc (US 8,402,165), and a rejection of claim 5 (issued claim 3) under §103 over Deu-Ngoc in view of Constantinof (US 2014/0241342). SAMSUNG-1002, 381-390. The Examiner also indicated that claims 6-10 and 12 (issued claims 4-8 and 10) were allowable. *Id*. The applicant amended the claims to overcome the above rejections and added new claims 17-21

(issued claims 15-19). SAMSUNG-1002, 99-112. All claims were then allowed. SAMSUNG-1002, 21-25.

VII. OVERVIEW AND COMBINATIONS OF PRIOR ART REFERENCES

A. Overview of Bennett

26. Bennett discloses a "media client" including a "user agent to communicate with a multimedia application in the networked communication device," a "signaling agent … to establish and maintain communication sessions," and a "media agent" which "performs media operations." SAMSUNG-1041, Abstract, ¶¶[0024]-[0026], [0029]-[0031], FIG. 3. These media operations include "Push-to-Talk over Cellular (PoC), presence and Instant Messaging (IM), video and audio streaming, voice over IP videoconferencing, interactive gaming, white-boarding and content sharing." SAMSUNG-1041, ¶[0024]. Bennett discloses that its media client is implemented in a "mobile device" that includes "a [user agent] 202, [signaling agent] 204 and [media agent] 206." SAMSUNG-1041, ¶¶[0028], [0078]. Bennett's media agent "stream[s]" media to a "media player" on the device, which outputs the media to the user using "a local media rendering device (e.g., speaker and/or display of a mobile terminal 100)." SAMSUNG-1041, ¶¶[0025], [0076], FIG. 3. Additionally, Bennett discloses that media can also be routed directly to the application. ¶[0076], FIG. 10.

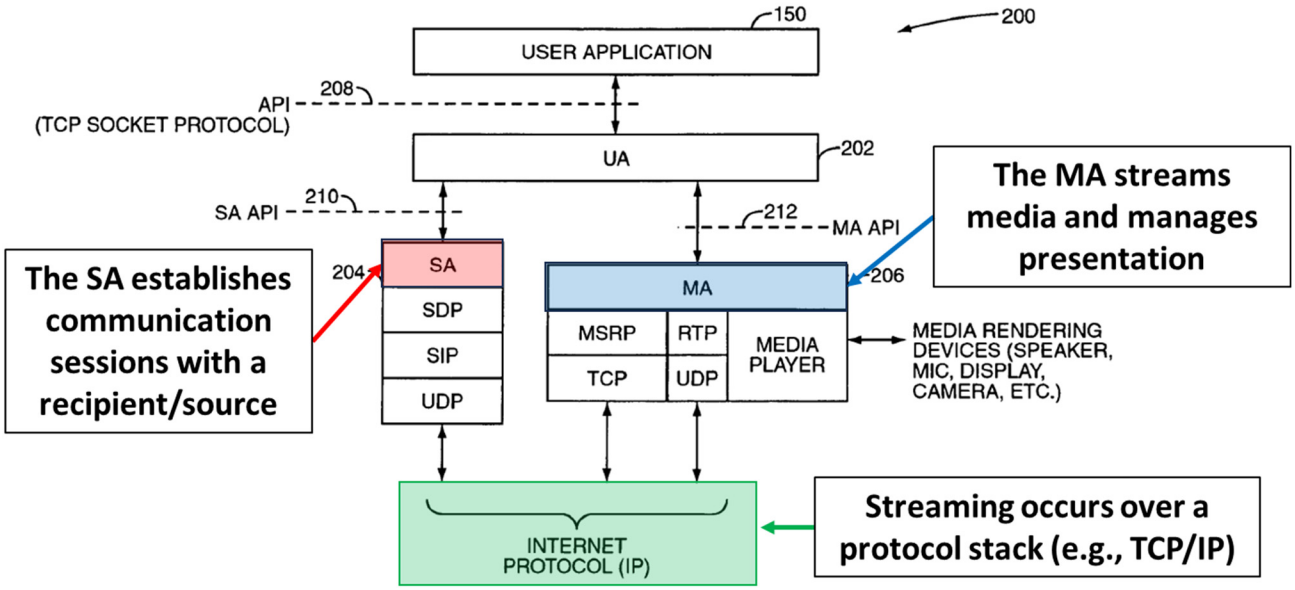


FIG. 3

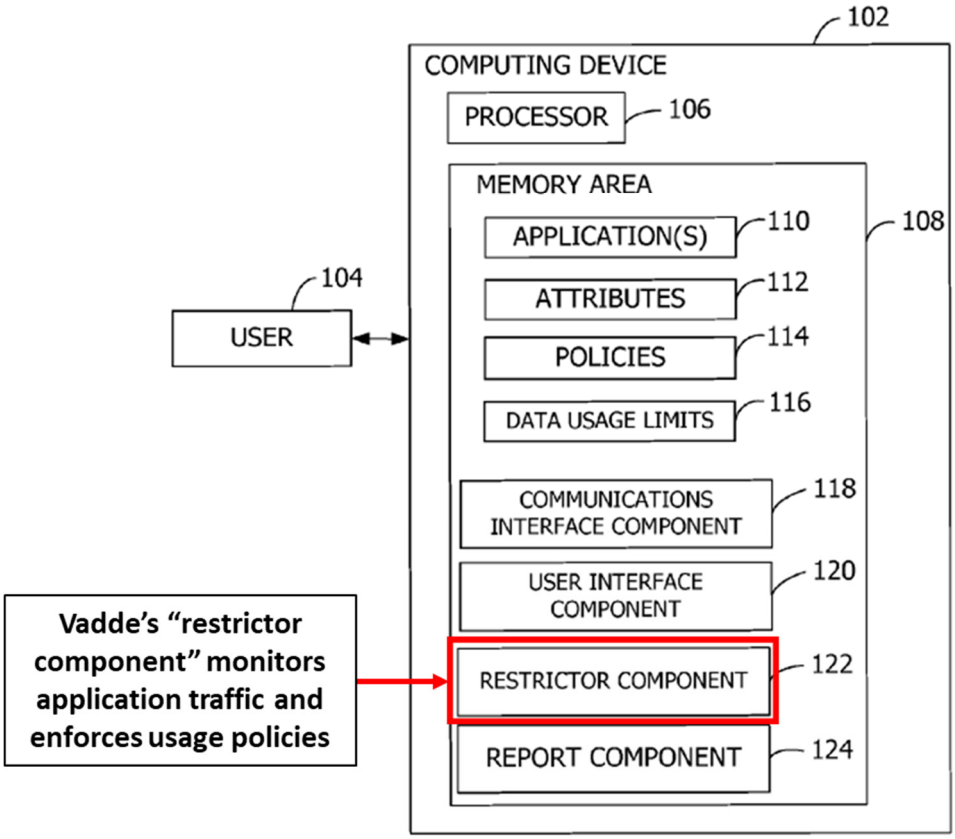
SAMSUNG-1041, FIG. 3.

B. Overview of Vadde

27. Vadde discloses techniques for "managing data traffic" for a plurality of applications operating on a "computing device 102." SAMSUNG-1042, ¶¶[0009]-[0023]. Vadde uses a "policy" based system that enforces restrictions on application data usage based on "attributes" and "usage limits." SAMSUNG-1042, ¶¶[0015]-[0016], [0025]-[0026]. Vadde's techniques are applied for "each" application and are enforced with a "restrictor component 122" which "appl[ies] the data usage policy" and "monitors the data transmitted and/or received by the applications 110 and determines whether the data usage limits 116 corresponding to each of the applications 110 have been exceeded or are about to be exceeded."

SAMSUNG-1042, ¶¶[0016], [0022]. An example computing device is depicted below. SAMSUNG-1042, FIG. 1.

FIG. 1



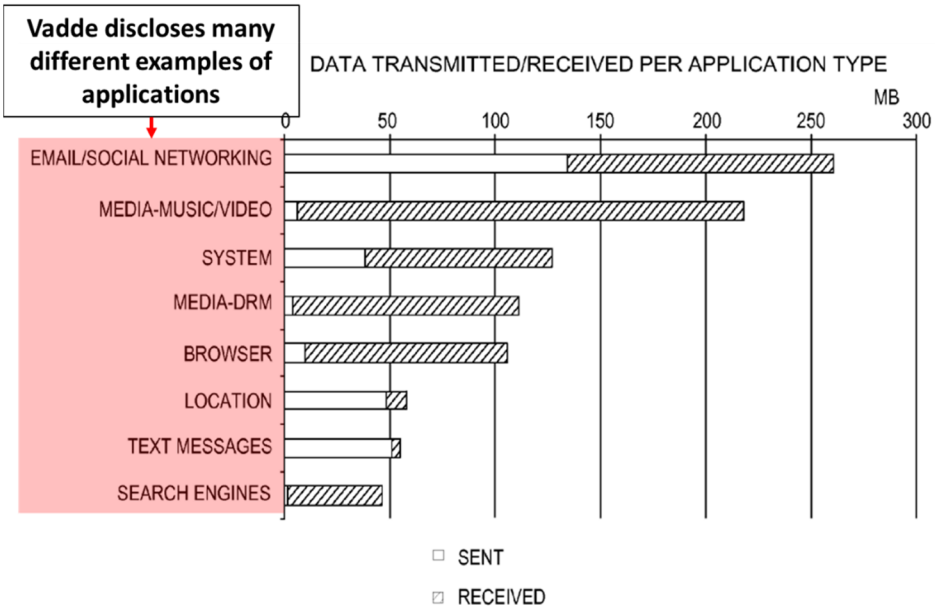
SAMSUNG-1042, FIG. 1.

C. The combination of Bennett and Vadde

28. It would have been obvious for a POSITA to incorporate Vadde's techniques of managing data traffic—to include Vadde's policies and restrictor component—into the media clients of Bennett to monitor data usage for applications making "media object network data transfers" and using "respective data packet

flows." SAMSUNG-1041, ¶[0078]; SAMSUNG-1042, ¶¶[0010], [0022]. A POSITA would have been motivated to make this combination for multiple reasons.

29. First, as Vadde notes, "[t]he cost of mobile operator data plans is often based on usage" and "with existing systems, users are unable to determine the relative costs incurred by different applications executing on a mobile telephone." SAMSUNG-1042, ¶[0001]. Further, Vadde discloses that many various different applications of different types (to include "media-music/video") can be operating on a mobile device. SAMSUNG-1042, ¶[0031], FIG. 4. Incorporating Vadde's data usage monitoring into the Bennett device would have enabled the user of the Bennett device to monitor their data usage and avoid unforeseen expenses. *Id*. The ability to identify and restrict data-intensive applications would have also allowed a user and network provider to "reduce battery usage" caused by these applications, extending operating time between charging. SAMSUNG-1042, ¶¶[0009], [0023]-[0024].



SAMSUNG-1042, FIG. 4.

30. The benefits of data usage monitoring were well-known prior to the '918 Patent and would have been part of a POSITA's general knowledge. For example, Rybak describes the need to monitor data usage and discloses a "method for monitoring resource usage of a mobile communications device" with respect to a "mobile communication plan profile associated with a subscriber." SAMSUNG-1044, ¶¶[0003]-[0004], [0030]-[0042], [0047], FIGS. 2, 7. Like Vadde, Rybak notes that resource usage correlates to a "billing period" or "plan" that would be chargeable to a user. SAMSUNG-1044, ¶¶[0031]-[0034], [0045], [0060], FIGS. 7-8. Benco discloses another example of a "method for providing mobile telephone subscribers with data on accumulated usage" where "[s]ubscribers are warned if their accumulated usage threatens to exceed or exceeds the allowable basic usage of

their billing plan." SAMSUNG-1045, Abstract, ¶¶[0001]-[0020]. Jobs provides yet another example, where a user interface of a mobile device "displays an updated account usage metric for an account associated with usage of the device (e.g., a cellular phone account)." SAMSUNG-1062, ¶[0213]. Finally, Fadell describes "metering" network resource usage on a mobile device to prevent a user from exceeding a "resource allocation." SAMSUNG-1063, ¶¶[0002]-[0007], [0017], [0050]-[0053], [0056]. With this background and knowledge of the benefits of data usage monitoring, a POSITA would have been motivated to consider and include Vadde's data usage monitoring in Bennett's device to achieve similar benefits as described above.

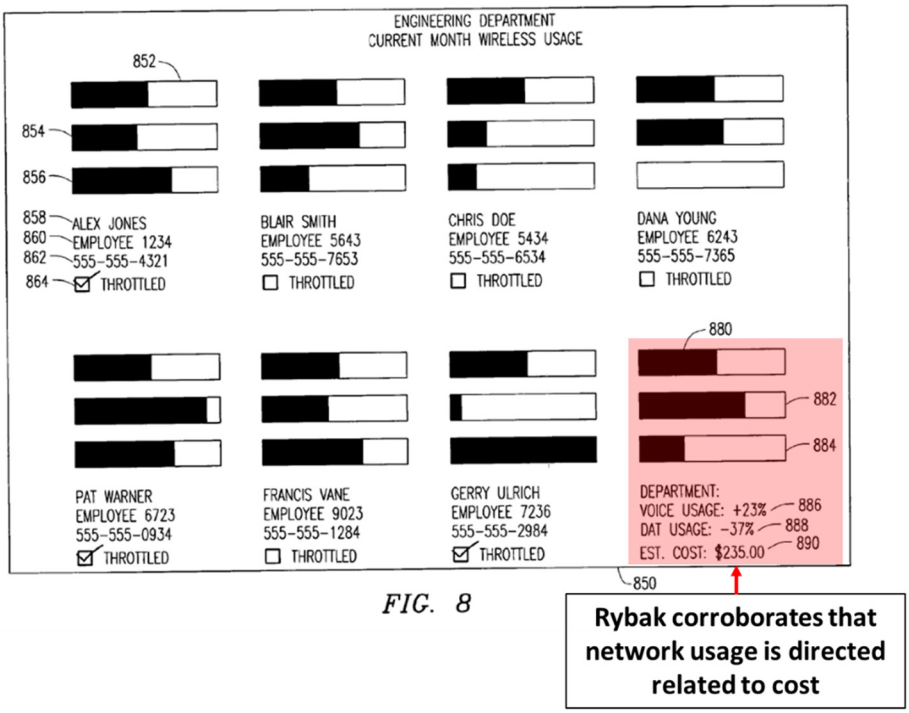


FIG. 8

SAMSUNG-1044, FIG. 8.

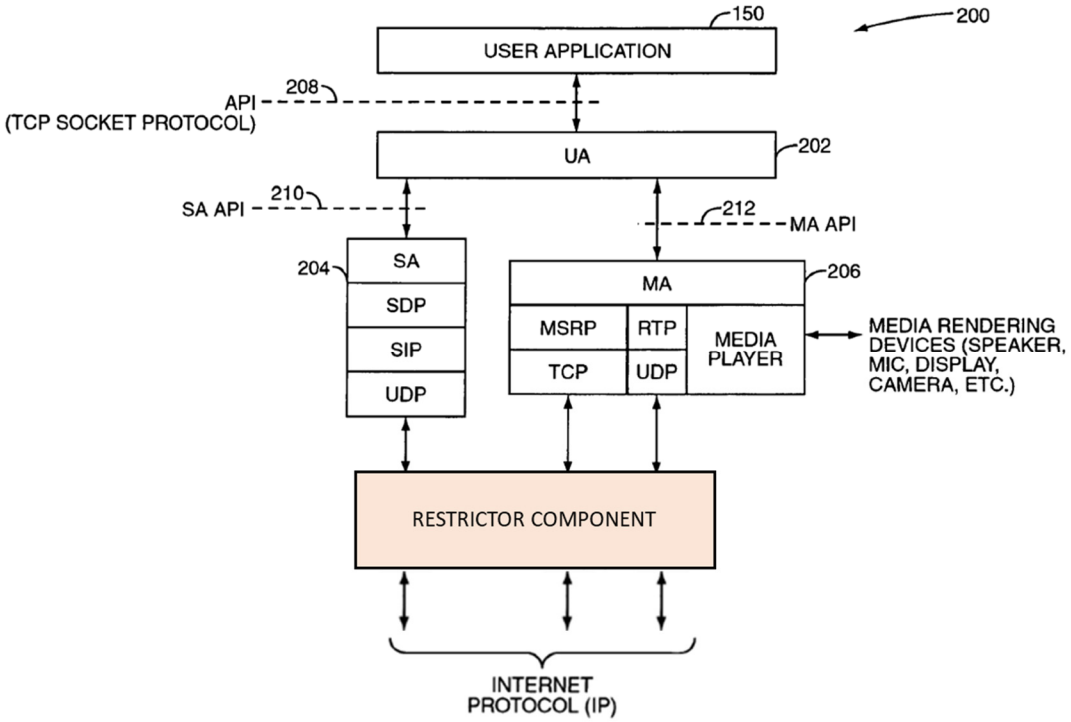
31. Second, because Vadde's policies are applied at an application level, Vadde's techniques would have enabled the Bennett service providers greater control over specific application activity that was data-intensive for the network (e.g., streaming video while roaming). SAMSUNG-1042, ¶¶[0010], [0016], [0018], [0022], [0025], [0029]-[0030], [0032]. These restrictions would have enabled service providers to prevent an aggregation of data-intensive activity from degrading a network's effectiveness. *Id*. For example, Vadde discloses that mobile devices can be an "employer-sponsored mobile telephone," and an employer would typically have great interest in how their company devices were being used at the user level. SAMSUNG-1042, ¶¶[0033]-[0034]. Moreover, "roaming" could also be extremely financially costly for the user, particularly for high-bandwidth activities like streaming, and was typically avoided if possible. SAMSUNG-1042, ¶[0034]; SAMSUNG-1046, 7:40-50, 14:61-67, Table-2 (describing "real-time audio and video" applications as "[h]igh bandwidth" applications).

32. Finally, adding per-application data usage monitoring to the Bennett device would have enabled device manufacturers and service providers to incorporate additional applications and functionality into wireless devices while allowing users to retain control of aggregate device data usage. SAMSUNG-1042, ¶¶[0010], [0016], [0018], [0022], [0025], [0029]-[0030], [0032]. Specifically, Bennett acknowledges that "[t]he convergence of mobile and IP networks will allow

service providers to offer new IP services to mobile subscribers that were previously available only to users in fixed networks, such as the Internet." SAMSUNG-1041, ¶[0002]. Vadde's techniques would have allowed service providers to incorporate the "new IP services" described by Bennett while retaining control of device wireless data usage in higher-cost wireless networks. SAMSUNG-1041, ¶[0002]; SAMSUNG-1042, ¶¶[0010], [0016], [0018], [0022], [0025], [0029]-[0030], [0032].

33. Incorporating Vadde's techniques into the Bennett device would have been nothing more than the application of known techniques (e.g., managing data traffic according to Vadde) to a known structure (e.g., Bennett's devices) to yield predictable results (e.g., the management of the Bennett-Vadde device's data traffic). A POSITA would have expected success in implementing this combination because the monitoring of outgoing API data traffic on a mobile device (such as the UA, SA, and MA APIs of Bennett) was known as of the Critical Date and would have involved only routine programming skill. For example, Rakoshitz discloses a method for "monitoring or profiling quality of service within a network of computers" that includes a "policy engine module" that "interfaces with [an] API" to enforce a "traffic policy [that] defines specific limitations or parameters for the traffic." SAMSUNG-1046, Abstract, 9:18-24, 12:12-58, Claim 1. Michels provides another example of a system for "monitoring and control of access to [an] API" with a processor that "monitors the distribution of the API elements" and "the number of

API requests made by [a] developer client over a period of time, the identity of the developer client, usage trends by the developer client, and usage trends based on IP address." SAMSUNG-1049, ¶¶[0002]-[0015], [0043]-[0063]. Furthermore, as explained above, tracking an aggregate application data usage on a mobile device was also known. SAMSUNG-1044, ¶¶[0003]-[0004], [0030]-[0042], [0047], FIGS. 2, 7; SAMSUNG-1045, Abstract, ¶¶[0001]-[0020].

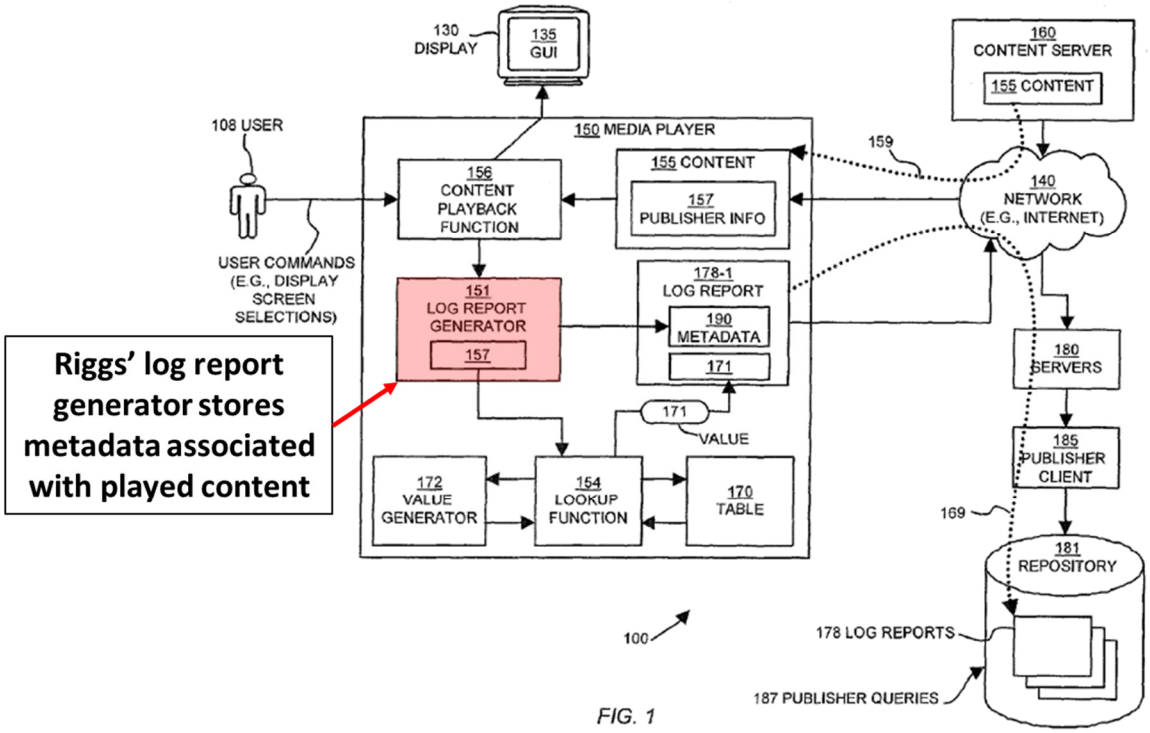


SAMSUNG-1041, FIG. 3 (as modified by Vadde).

D. Overview of Riggs

34. Riggs discloses a "media player" with an integral "log report generator" that generates a "log report" of "metadata" associated with media. SAMSUNG-1043, 5:20-6:45, FIG. 1. Riggs' metadata includes "application name," "URL,"

"publisher information," and other information particular to a content source or publisher. SAMSUNG-1043, 1:58-2:5, 6:32-45, 10:13-23, 11:18-31, 16:28-33, FIG. 2.



SAMSUNG-1043, FIG. 1.

E. The combination of Bennett, Vadde, and Riggs

35. It would have been obvious for a POSITA to incorporate Riggs's techniques of logging metadata associated with media—to include Riggs' log generators and log reports—into the Bennett-Vadde device to log metadata associated with the media played by applications. SAMSUNG-1043, 1:58-2:5, 6:32-45, 10:13-23, 11:18-31, 16:28-33, FIG. 2. Riggs' log reports would have also

provided a convenient way to track and display per application data usage determined by Vadde's restrictor component. SAMSUNG-1041, ¶¶[0002], [0025], [0076], FIGS. 3, 9, 11; SAMSUNG-1042, ¶[0021], FIG. 1; SAMSUNG-1043, 6:25-31. A POSITA would have been motivated to make this combination for multiple reasons, including: (1) increased insight into a user's data usage patterns, (2) convenient tracking and sharing of usage data, and (3) increased granularity of data usage tracking on a per-media player basis. SAMSUNG-1042, ¶¶[0002], [0009], [0018], [0024], [0027]-[0028]; SAMSUNG-1043, 1:58-2:5, 6:32-45, 10:13-23, 11:18-31, 11:54-13:46, 16:28-33, FIG. 2.

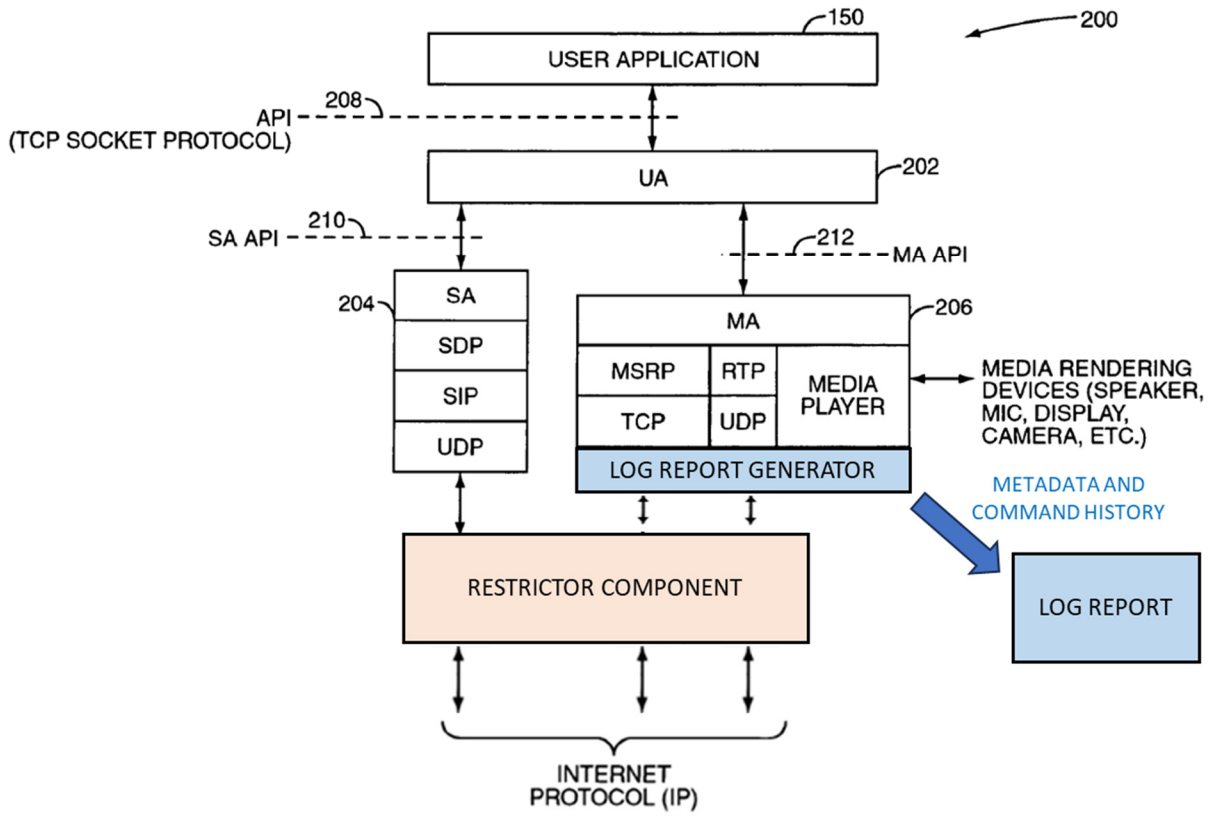
36. Specifically, Riggs discloses that, by "record[ing] events such as occurrence of playback commands and related playback information," a publisher can "identify corresponding portions of such content that are most appealing to a viewer." SAMSUNG-1043, 1:49-57; 14:27-36. Incorporating Riggs' techniques of logging metadata associated with played content would have enhanced the ability of third-party publishers to recommend relevant media to the user of the Bennett-Vadde device (e.g., a song from a music streaming service, or a video from a movie streaming service). SAMSUNG-1041, ¶¶[0024], [0076]; SAMSUNG-1043, 1:49-57, 14:27-36. Additionally, Riggs discloses that, with user consent, this information can be shared between publishers, allowing many such streaming services to gain

insight into a user's preferences without the need for a publisher to collect this data organically. SAMSUNG-1043, 1:49-57, 2:35-40, 14:27-36.

37. Riggs also teaches that a specific media player may be relevant to streamed media, and to that end, data specifying the type of media player that viewed the media can be collected. SAMSUNG-1043, 11:54-14:26, FIG. 3. This is particularly relevant to Bennett, which discloses that "one <u>or more</u> media players" can be included on any given device. SAMSUNG-1041, ¶[0025]. Riggs' techniques allow for the collection of data from multiple media players to be standardized such that this data can be easily correlated and analyzed. SAMSUNG-1043, 11:54-14:26, FIG. 3.

38. Incorporating Riggs' techniques into the Bennett-Vadde device would have been nothing more than the application of known techniques (e.g., logging metadata according to Riggs) to a known structure (e.g., Bennett-Vadde's device) to yield predictable results (e.g., the logging of metadata associated with media played by the Bennett-Vadde device's media players). A POSITA would have expected success in implementing this combination because logging metadata associated with media played by the Bennett-Vadde media players using Riggs' techniques simply applies Riggs' teachings—with little modification—to a device that Riggs explicitly discloses can implement its techniques (e.g., a media player). Further, the

modification would have involved routine programming ability that would have been well within the skill of a POSITA. *Id.*

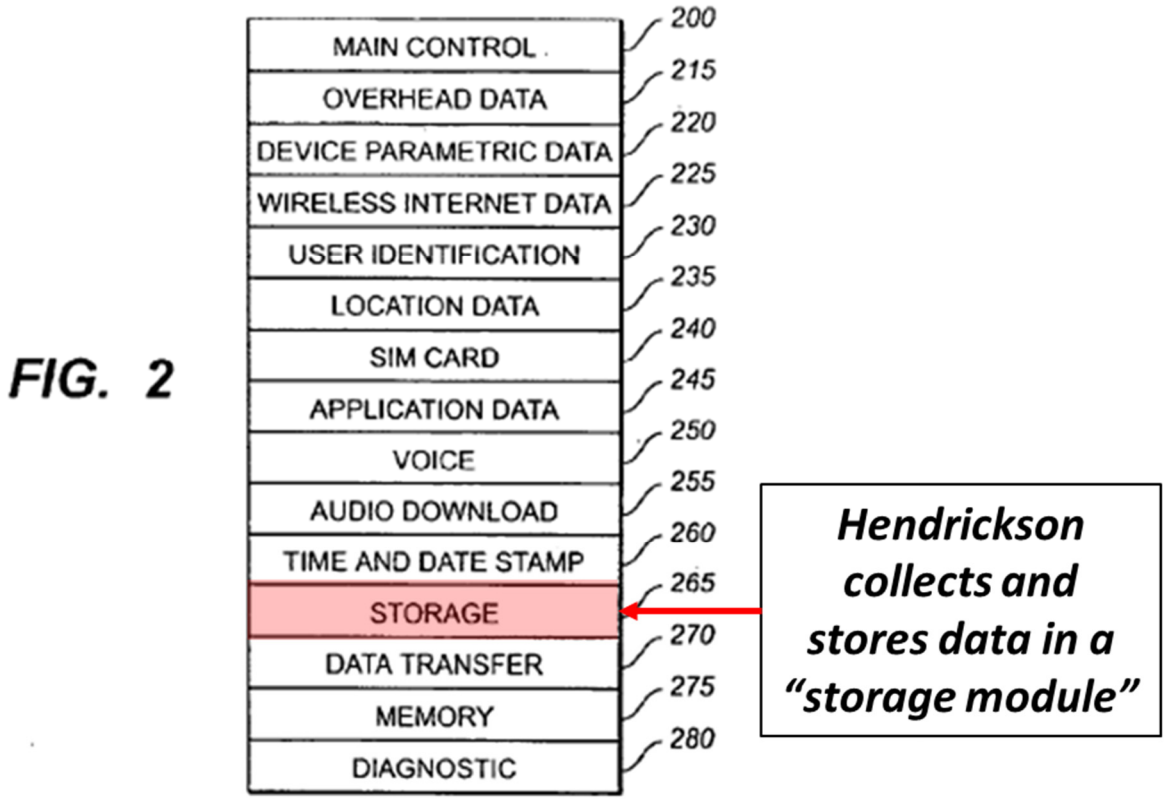


SAMSUNG-1041, FIG. 3 (as modified by Vadde and Riggs).

F. Overview of Hendrickson

39. Hendrickson discloses a system for measuring "wireless device and wireless network usage and performance metrics" which collects "device parametric data" and "transmit[s] the collected data via a wireless communication network to one or more control centers for processing." SAMSUNG-1054, 4:37-5:38, 7:25-8:6, FIGS. 1-2. Hendrickson collects and stores its data into a local "storage module 265"

prior to transmission to the control center because, as Hendrickson notes, there may be "no network connection available to transmit" or "immediate transfer of data [may] result in a poor user experience." SAMSUNG-1054, 12:29-42.



SAMSUNG-1054, FIG. 2.

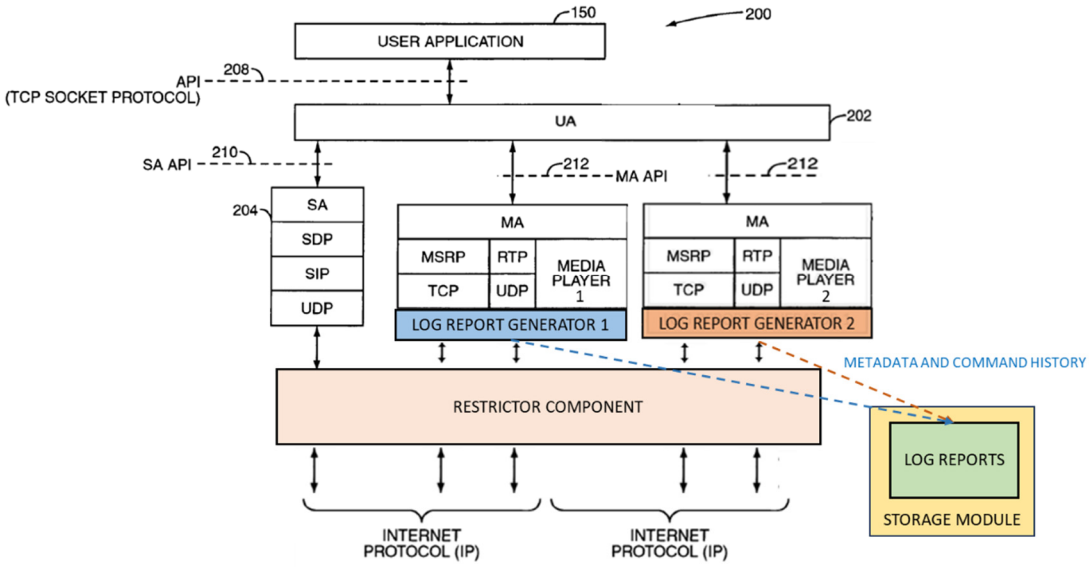
G. The combination of Bennett, Vadde, Riggs, and Hendrickson

40. It would have been obvious for a POSITA to incorporate Hendrickson's techniques of storing data associated with played media content (e.g., using a storage module) into the Bennett-Vadde-Riggs device to store log reports generated by Bennett-Vadde-Riggs' log report generators. SAMSUNG-1043, 1:58-2:5, 6:32-45, 10:13-23, 11:18-31, 16:28-33, FIG. 2; SAMSUNG-1054, 12:29-42; *see below*

§§VIII.B.[4]-[6]. A POSITA would have recognized and found obvious that generated log reports would have needed to have been stored locally on the device at least temporarily, at least to preserve the data across device operating cycles in the absence of a network connection. SAMSUNG-1054, 12:29-42 (noting that storing data is prudent when "there is no network connection available to transmit" or "immediate transfer of data would result in a poor user experience"); *see below* §§VIII.B.[4]-[6].

41. Incorporating Hendrickson's techniques into the Bennett-Vadde-Riggs device would have been nothing more than the application of known techniques (e.g., storing data in the form of log reports) to a known structure (e.g., Bennett-Vadde-Riggs' device) to yield predictable results (e.g., the storing of log reports associated with media played by the Bennett-Vadde-Riggs device). A POSITA would have expected success in implementing this combination because the storing of Bennett-Vadde-Riggs' log reports using Hendrickson's techniques simply applies Hendrickson's teachings—with little modification—to a device that performs the same functions that Hendrickson envisions within its own disclosure (e.g., a system that logs metadata associated with content played by a media player). This modification would have (1) involved routine programming ability that would have been well within the skill of a POSITA, and (2) leveraged the existing infrastructure of the base references in a way that was already well known in the art (e.g., using

the device memory that Bennett, Vadde, and Riggs all individually disclose and render obvious). SAMSUNG-1041, ¶[0029] ("[t]he host device includes memory in which to store code implementing the present invention"); SAMSUNG-1042, ¶¶[0011]-[0014], [0017] (describing a device "memory area 108"); SAMSUNG-1043, 14:37-15:2, FIG. 4 (describing a "computer system" with a "memory system 112").

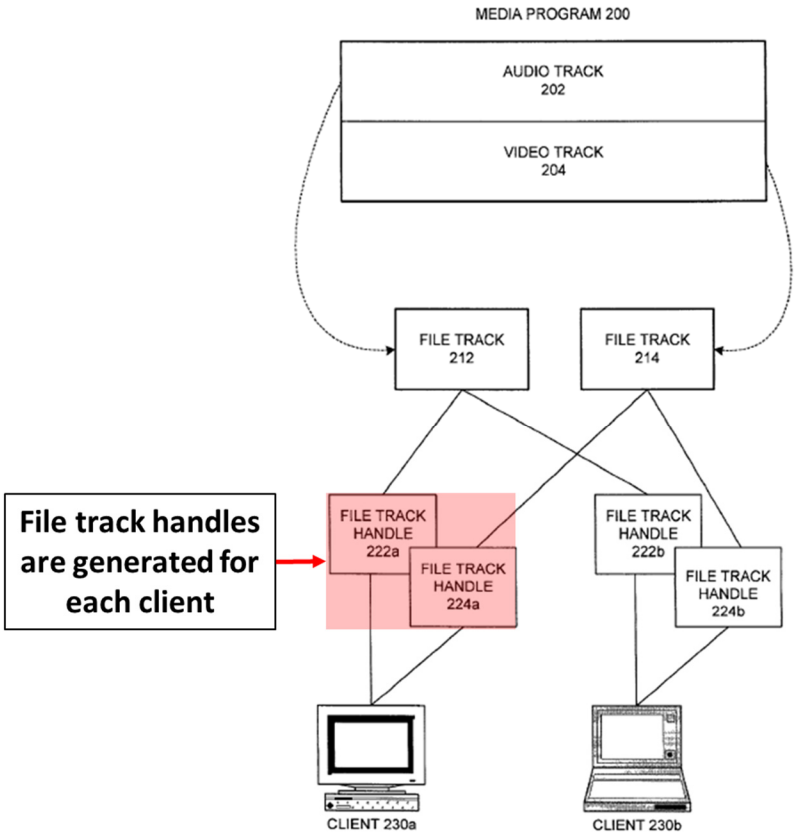


SAMSUNG-1041, FIG. 3 (as modified by Vadde, Riggs, and Hendrickson).

H. Overview of Srikantan

42. Srikantan discloses techniques for "streaming a media track to multiple clients using a single copy of the track's metadata, rather than making separate copies of the metadata for each stream." SAMSUNG-1055, Abstract, ¶¶[0040]-[0047]. To manage the streaming of the track to multiple clients, Srikantan generates a "file track handle" that "acts as an interface between its client stream … and the single

instance of media metadata." SAMSUNG-1055, ¶¶[0008]-[0009], [0044]-[0046], [0051]-[0054], [0059], [0071], FIG. 2. Srikantan also discloses that the receiving client "may issue commands to control the stream—e.g., to rewind or fast forward to locate a particular part of the media, to pause the streaming, etc." SAMSUNG-1055, ¶¶[0024], [0029], [0060], [0073].



SAMSUNG-1055, FIG. 2.

I. The combination of Bennett, Vadde, Riggs, and Srikantan

43. It would have been obvious for a POSITA to incorporate Srikantan's techniques, to include a media streaming server that generates file track handles for media files streamed to the Bennett-Vadde-Riggs device. SAMSUNG-1041,

¶¶[0025], [0076], FIG. 3; SAMSUNG-1055, ¶¶[0008]-[0009], [0044]-[0046], [0051]-[0054], [0059], [0071], FIG. 2. A POSITA would have recognized and found obvious that generating multiple copies of metadata associated with a media file is resource intensive, and Srikantan's techniques would have reduced server-side computing requirements by reducing the need to generate multiple copies of metadata for a streamed media file. SAMSUNG-1055, ¶¶[0004], [0007]-[0009], [0019]-[0020], [0024]-[0026]. Also, as Srikantan notes, sharing a single file handle among multiple clients "can lead to a great deal of contention among the client streams as each one attempts to seek to (i.e., find) and extract a different media segment or sample"—streams that a POSITA knows cost precious bandwidth. SAMSUNG-1055, ¶¶[0005]-[0006]; SAMSUNG-1042, ¶[0034]; SAMSUNG-1046, 7:40-50, 14:61-67, Table-2 (describing "real-time audio and video" applications as "[h]igh bandwidth" applications); *see above*, §VII.C. To that end, a POSITA would have recognized the bandwidth savings that would be gained from eliminating conflicting streaming sessions using Srikantan's techniques. *Id*.

44. Incorporating Srikantan's media streaming server and file track handle generation techniques into the Bennett-Vadde-Riggs device would have been nothing more than the application of known techniques (e.g., generating a file track handle for a media file) to a known structure (e.g., media streamed by the Bennett-Vadde-Riggs device) to yield predictable results (e.g., the Bennett-Vadde-Riggs

device referencing the Srikantan file track handle when streaming a media file). A POSITA would have expected success in implementing this combination because generating and using file handles to reference media streamed on the Bennett-Vadde-Riggs device using Srikantan's techniques simply applies Srikantan's teachings—with little modification—to a system that Srikantan itself envisions within its own disclosure (e.g., a device that streams media accessed from a server). SAMSUNG-1055, ¶¶[0023]-[0033]. This modification would have (1) involved routine programming ability that would have been well within the skill of a POSITA, (2) introduced concepts that were already well known in the industry ("file handles," or "file descriptors") and (3) required little to no modification to Srikantan's envisioned system. SAMSUNG-1055, Cover, ¶¶[0016]-[0018], [0083]. File handles were, and still are, a well-known technique to ensure continuity of a file being shared in a server-client system, as evidenced by Srikantan pre-dating the Critical Date by almost a decade. SAMSUNG-1055, Cover; SAMSUNG-1058, 3 (defining a file handle as "[a] temporary designation an operating system assigns to an opened file during any given session"); SAMSUNG-1059, 3 (defining a file descriptor as "[a] value used to identify an open file for the purpose of file access").

VIII. MANNER IN WHICH THE PRIOR ART REFERENCES RENDER THE '918 CLAIMS UNPATENTABLE

A. Claims 1-3, 8-9, 13-14, and 19 are obvious over Bennett in view of Vadde

[1.pre] A wireless end-user device, comprising:

45. As an initial matter, the '918 Patent does not define a "wireless end-user mobile device," but instead describes various devices that can implement its techniques, to include "**mobile devices**, such as phones, PDAs, computing devices, laptops, net books, tablets, **cameras, music/media players**, GPS devices, networked appliances, and any other networked device." SAMSUNG-1001, 40:28-46[2]. The prior art here discloses similar devices.

46. Bennett discloses that its techniques can be implemented in a "mobile device," "video camera," and "remote video player" (all "***wireless end-user device[s]***" which communicate over wireless networks). SAMSUNG-1041, ¶¶[0078], *see also* ¶¶[0002], [0005], [0025], FIGS. 1, 4, 11.

---

[2] All emphasis is added unless otherwise noted.

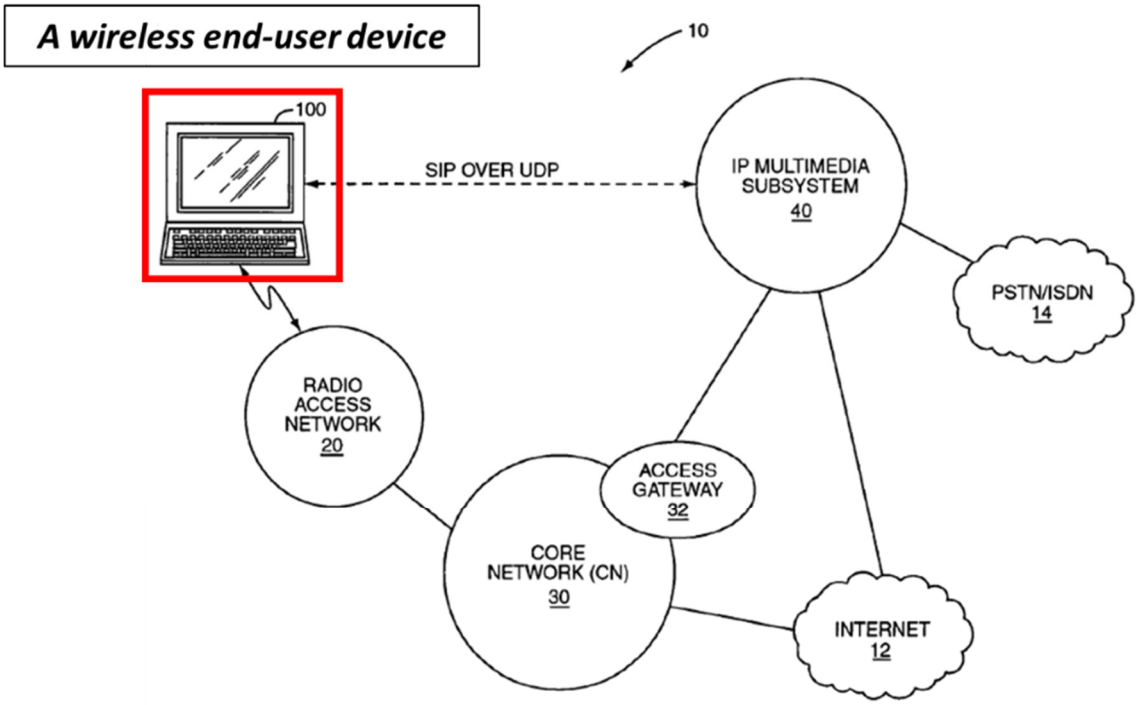


FIG. 1

SAMSUNG-1041, FIG. 1.

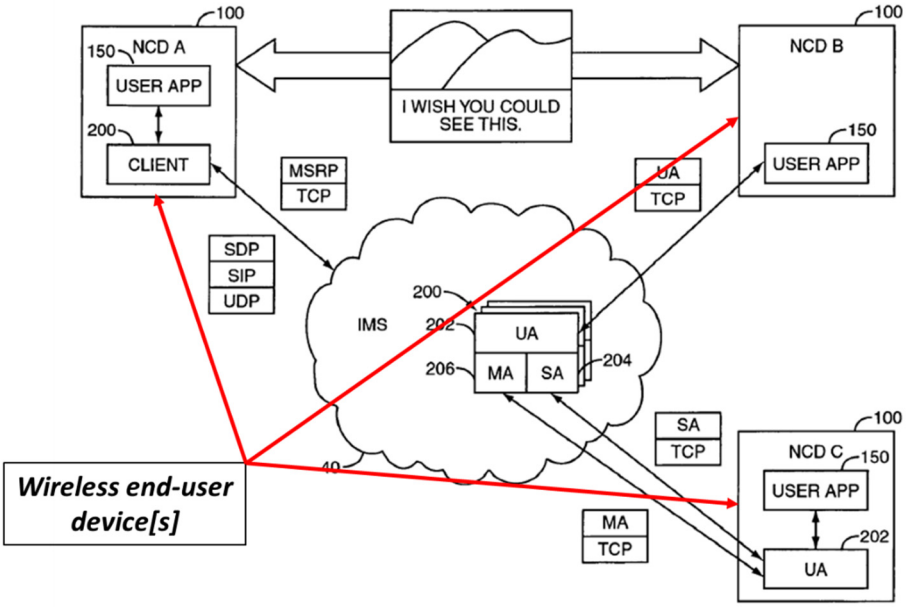


FIG. 4

SAMSUNG-1041, FIG. 4.

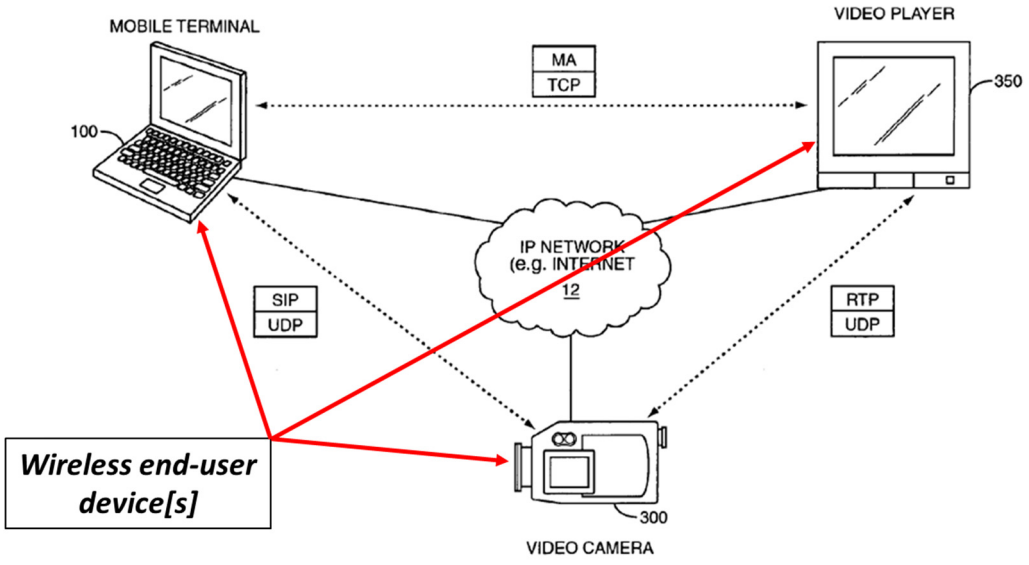


FIG. 11

SAMSUNG-1041, FIG. 11.

47. Bennett discloses a "media client 200" including a "user agent to communicate with a multimedia application in the networked communication device," a "signaling agent … to establish and maintain communication sessions," and a "media agent" which "performs media operations." SAMSUNG-1041, Abstract, ¶¶[0024]-[0026], [0029]-[0031], FIG. 3. Bennett's media client 200 is entirely contained within a "***wireless end-user device***." SAMSUNG-1041, ¶¶[0028], [0078], FIGS. 4, 11.

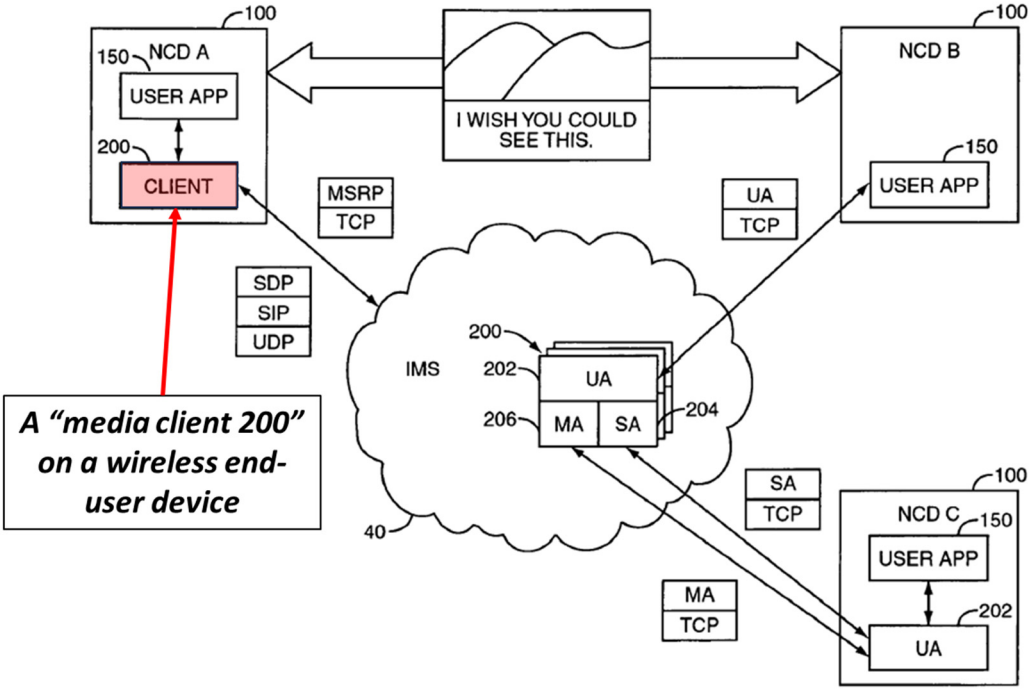


FIG. 4

SAMSUNG-1041, FIG. 4.

[1.1] a wireless modem configurable to connect to a wireless network;

48. Bennett discloses that its mobile devices operate on various "mobile communication network[s]." SAMSUNG-1041, ¶[0017], FIG. 1. Bennett's networks include "General Packet Radio Services (GPRS) network[s]" and Universal Mobile Telecommunications Service ("UMTS") networks ("***wireless network[s]***"). *Id.*

49. A POSITA would have understood and found obvious that to communicate and retrieve media via these networks, Bennett's mobile devices would have had the ability to modulate and demodulate data using a "***wireless modem***." It was well known before the Critical Date that ***wireless modem[s]*** were

used to transmit data from mobile devices operating on wireless networks, including GPRS and UMTS networks, and that these modems were "***configurable to connect to a wireless network***." SAMSUNG-1047, ¶¶[0025], [0068]. For example, Cassett discloses that devices communicating in "GPRS" and "UMTS" networks included "wireless modems." *Id*.

50. Additionally, a POSITA would have understood and found obvious that mobile devices at the time of the Critical Date typically included ***wireless modem[s]*** that were "***configurable to connect to a wireless network***" as evidenced by multiple prior art references. SAMSUNG-1048, ¶¶[0034]-[0035], FIG. 2; SAMSUNG-1013, ¶¶[0125], [0130]. Cole discloses a "mobile device" that includes a plurality of "***wireless modem[s]***," to include a "WWAN modem 230," a "WLAN modem 235," and a "voice band modem 250." SAMSUNG-1048, ¶¶[0034]-[0035], FIG. 2. Rao discloses that "computing device[s] 102" included "network interface[s] 118," for example, a "modem." SAMSUNG-1050, ¶¶[0125], [0130].

[1.2] a network stack configurable to receive and transmit data via the wireless modem and the wireless network;

51. Bennett discloses that the media agent 200 is in communication with several "protocol stack[s]" ("***a network stack***") which are configured to transmit and obtain—or "stream"—"media" ("***configurable to receive and transmit data via the wireless modem and the wireless network").*** SAMSUNG-1041, ¶¶[0018],

[0025], [0060], [0066], [0075]-[0076], FIGS. 3-4, 8-12[3]. As described above, communication over wireless networks on the Bennett mobile end-user device occurs via "***the wireless modem and the wireless network***." *See above*, [1.1].

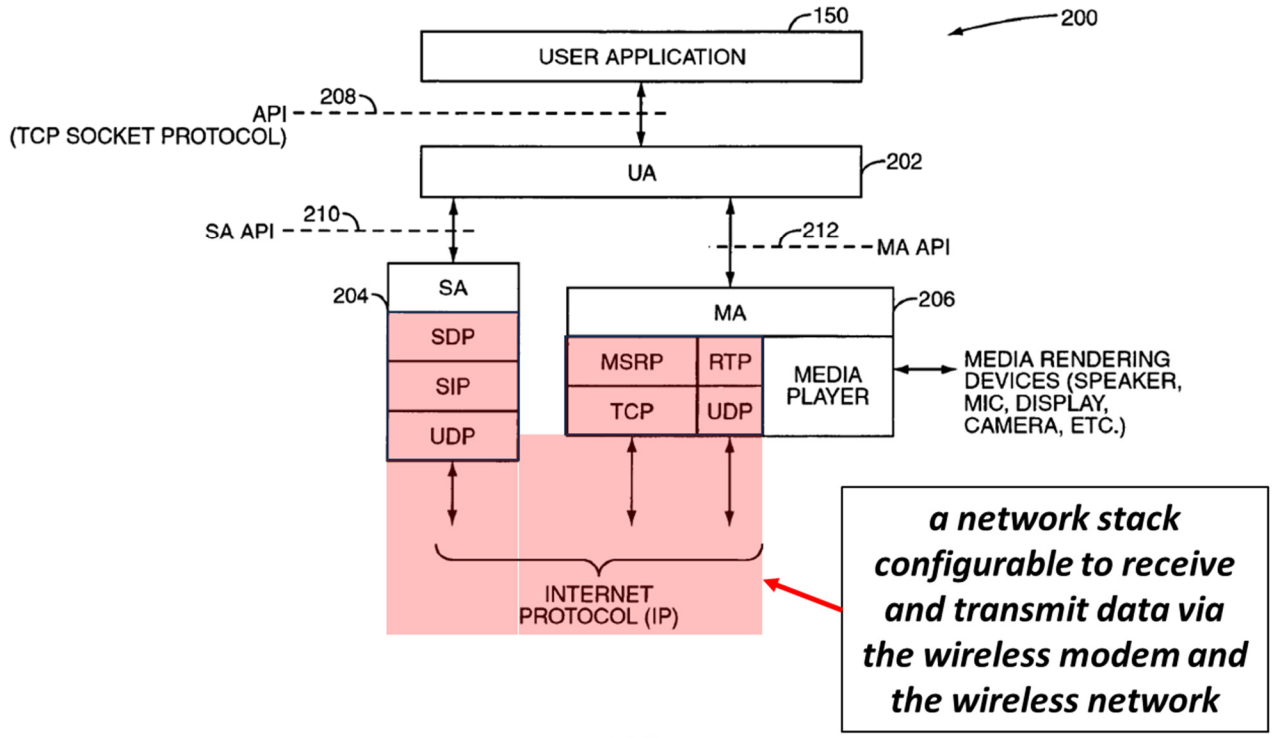


FIG. 3

SAMSUNG-1041, FIG. 3.

[3] Bennett's figures all denote "media client 200," thus indicating the same embodiment. SAMSUNG-1041, FIGS. 3-4, 8-12

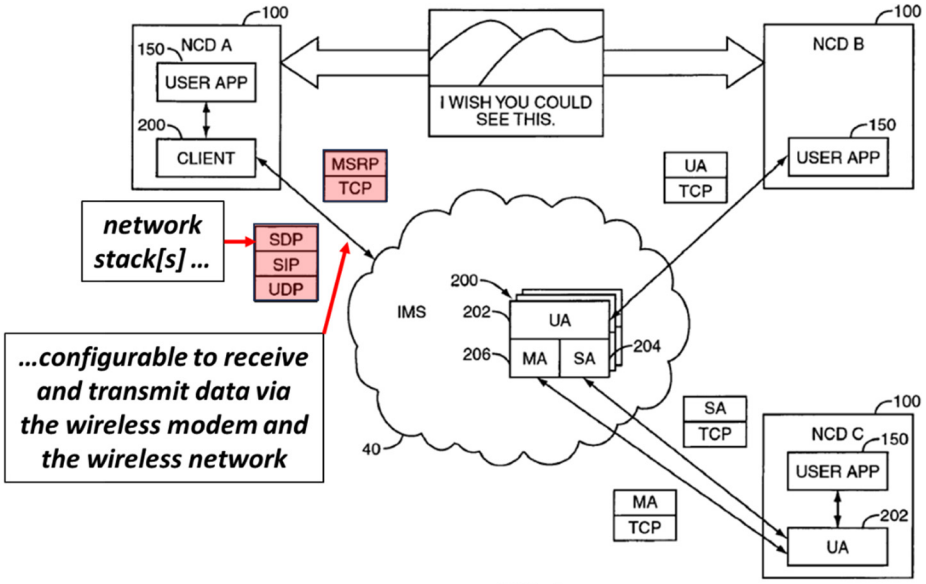


FIG. 4

SAMSUNG-1041, FIG. 4.

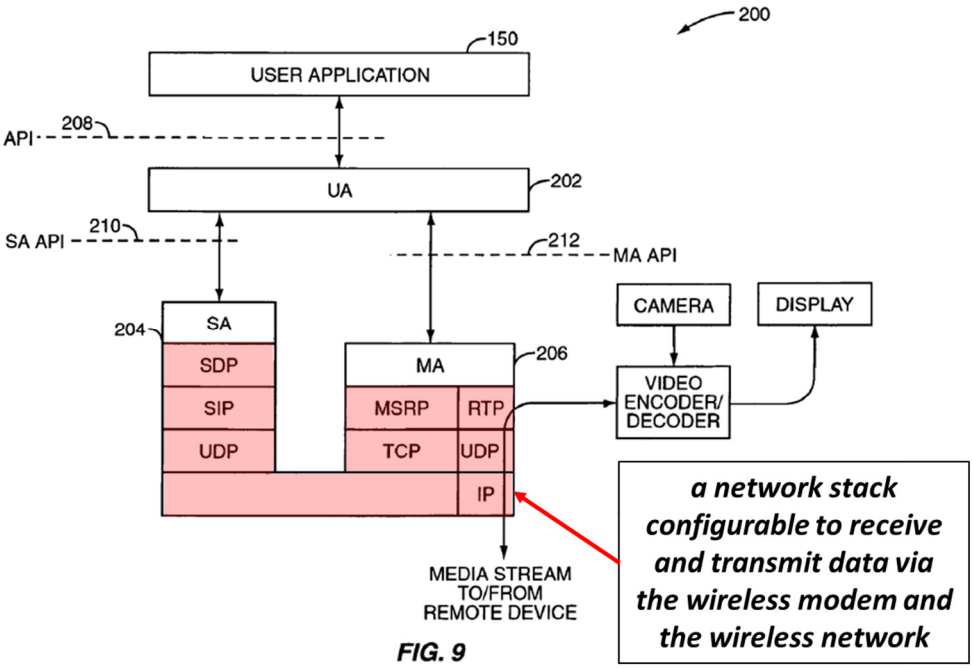


FIG. 9

SAMSUNG-1041, FIG. 9.

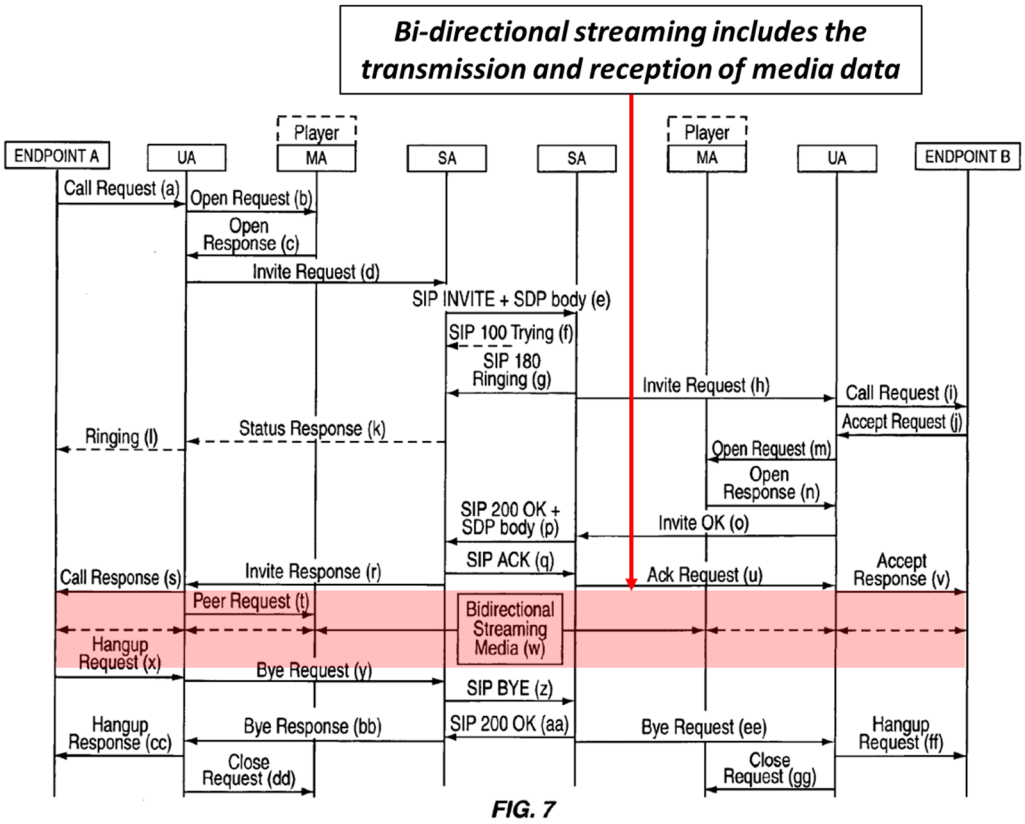


FIG. 7

SAMSUNG-1041, FIG. 7.

52. Similarly, the '918 Patent depicts Internet Protocol ("IP"), Transmission Control Protocol ("TCP"), and User Datagram Protocol ("UDP") as part of a "device stack." SAMSUNG-1001, 2:21-26, FIGS. 12-13. This device stack <u>is</u> a "***network stack***," as this term is known in the industry, as the device stack as pictured and described in the '918 Patent shows and describes similar features as a network stack. *Id*. The '918 Patent also frequently refers to "IP" techniques with respect to the "network stack." SAMSUNG-1001, 61:51-62, 109:22-26, 112:62-113:9.

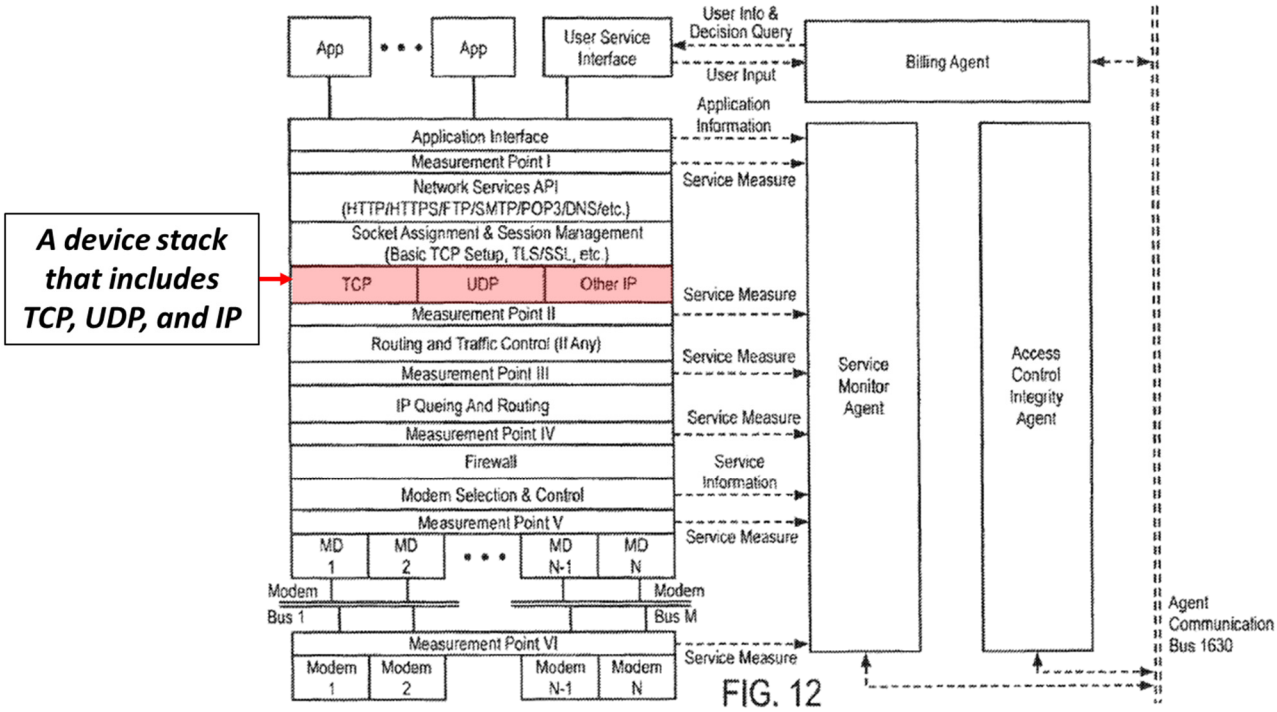


FIG. 12

SAMSUNG-1001, FIG. 12.

[1.3] a first network stack Application Programming Interface (API), containing at least one first call accessible to each of a plurality of device applications, the first network stack API callable by each of the plurality of device applications to open and use data packet flows via the network stack, the wireless modem, and the at least one wireless network;

<u>open and use data packet flows via the network stack, the wireless modem, and the at least one wireless network</u>

53. Bennett discloses the use of "Session Initiation Protocol (SIP)" for "establishing, modifying and terminating communication sessions between one or more participants" ("***open and use data packet flows via the network stack,***

the wireless modem, and the at least one wireless network")[4]. SAMSUNG-1041, ¶¶[0018]-[0022]. Bennett discloses that SIP enables applications residing on the mobile terminal to "establish a communications session." SAMSUNG-1041, ¶[0022]. SIP sessions include "Internet multimedia conferences, Internet telephony calls, and multimedia distributions" that are performed using protocols such as "Real-time Transfer Protocol (RTP)" and "Message Session Relay Protocol (MSRP)." *Id*.

54. A POSITA would have recognized and found obvious that the protocols disclosed in Bennett would have included "***data packet flows***" as these protocols are examples of "packet switched services" that communicate data in a series of data packets. SAMSUNG-1041, ¶[0017]. Additionally, a POSITA would have recognized and found obvious that the communication of these "***data packet flows***" would have been "***via the network stack, the wireless modem, and the at least one wireless network***" as Bennett's media, included in the data packet flow, is retrieved over various wireless networks, described above, that use protocol stacks and wireless modems. *See above* [1.1], [1.2].

---

[4] Bennett discloses that other protocols may be used, for example, "H.323." SAMSUNG-1041, ¶[0018].

a first network stack Application Programming Interface (API), containing at least one first call accessible to each of a plurality of device applications, the first network stack API callable by each of the plurality of device applications

55. Bennett also discloses a "signaling agent (SA) 204" within its "media client 200" that "implements SIP and SDP protocols to handle signaling tasks" which include "setting up, modifying, and tearing down communication sessions, [and] negotiating session parameters" ("***open and use data packet flows via the network stack, the wireless modem, and the at least one wireless network***"). SAMSUNG-1041, ¶¶[0025], [0031], [0033], [0040], [0043]-[0049], Table-2, FIGS. 3-10. The SA 204 is called by the "user agent (UA) 202" of the media client 200 using a "SA API 210" *("**a first network stack Application Programming Interface (API)***") in response to a request from a "user application 150" ***("the first network stack API callable by each of the plurality of device applications***"). *Id*.

56. The SA API 210 includes various "requests" ("***at least one first call accessible to each of a plurality of device applications***") to perform actions in SIP sessions, including "INVITE" requests ("***open and use data packet flows via the network stack, the wireless modem, and the at least one wireless network***") which identify a source of data or a recipient. SAMSUNG-1041, ¶¶[0031], [0033], [0040], [0045]-[0046], FIGS. 6-7, Table-2. Bennett frequently refers to "applications" operating on its devices and says that "any" application 150 can

use its techniques ("***a plurality of device applications***"). SAMSUNG-1041, ¶¶[0018], [0022], [0029], [0075]. Vadde also explicitly describes performing its techniques for "a plurality of applications executing on a computing device" ("***a plurality of device applications***"). SAMSUNG-1042, Abstract, ¶¶[0002], [0043].

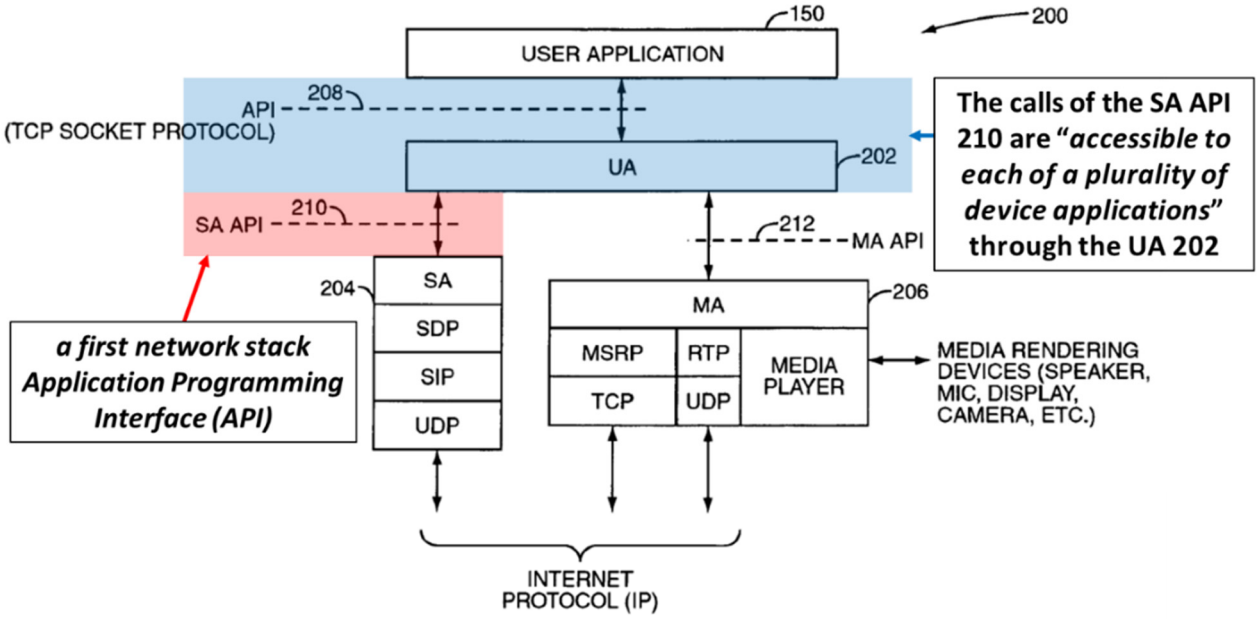


FIG. 3

SAMSUNG-1041, FIG. 3.

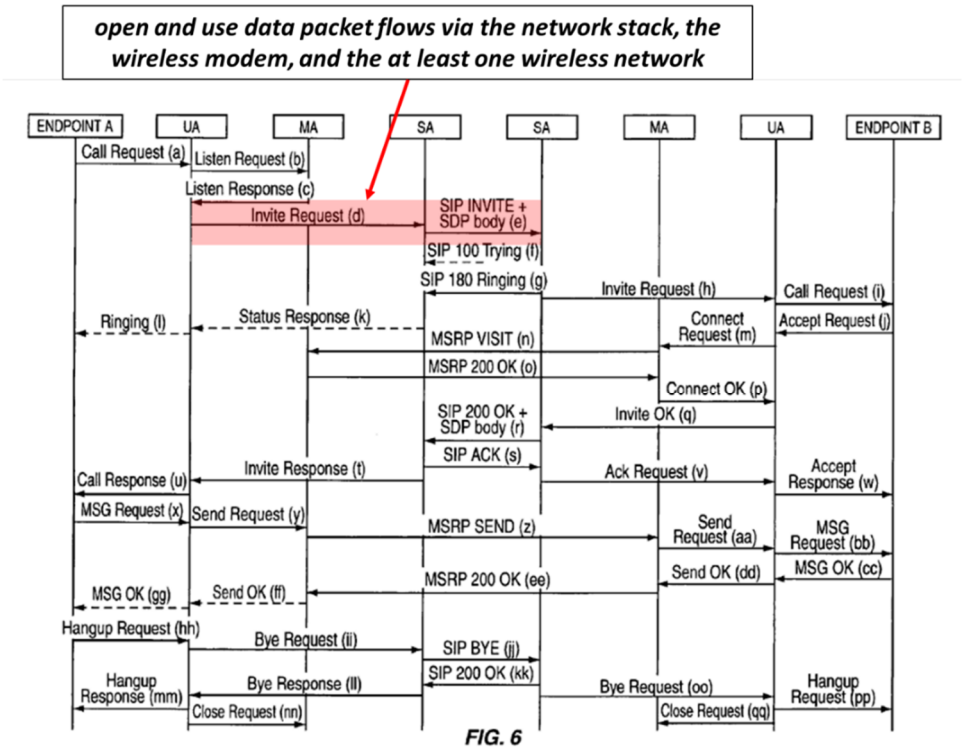


FIG. 6

SAMSUNG-1041, FIG. 6.

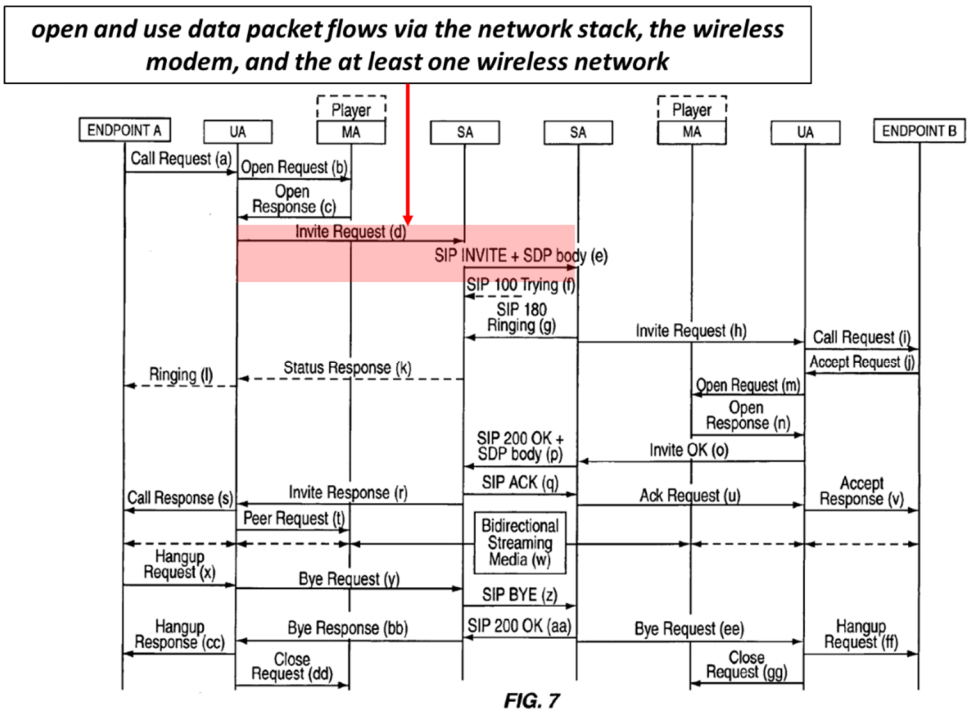


FIG. 7

SAMSUNG-1041, FIG. 7.

57. To the extent it is argued that the calls of the "***first network stack Application Programming Interface (API)***" must be directly "***accessible to each of a plurality of device applications***," or that the application must directly call the "***first***" API, the '918 Patent does not support such a narrow interpretation. On the contrary, the process of applications indirectly calling APIs is depicted in the '918 Patent in multiple embodiments. SAMSUNG-1001, 110:12-111:17, 116:39-58; 119:49-60, FIGS. 30, 32, 35. The '918 Patent depicts multiple embodiments where an API (e.g., a "socket") is called by a program module other than the requesting "application," indicating that such an interpretation is within the scope of the claims. *Id*.

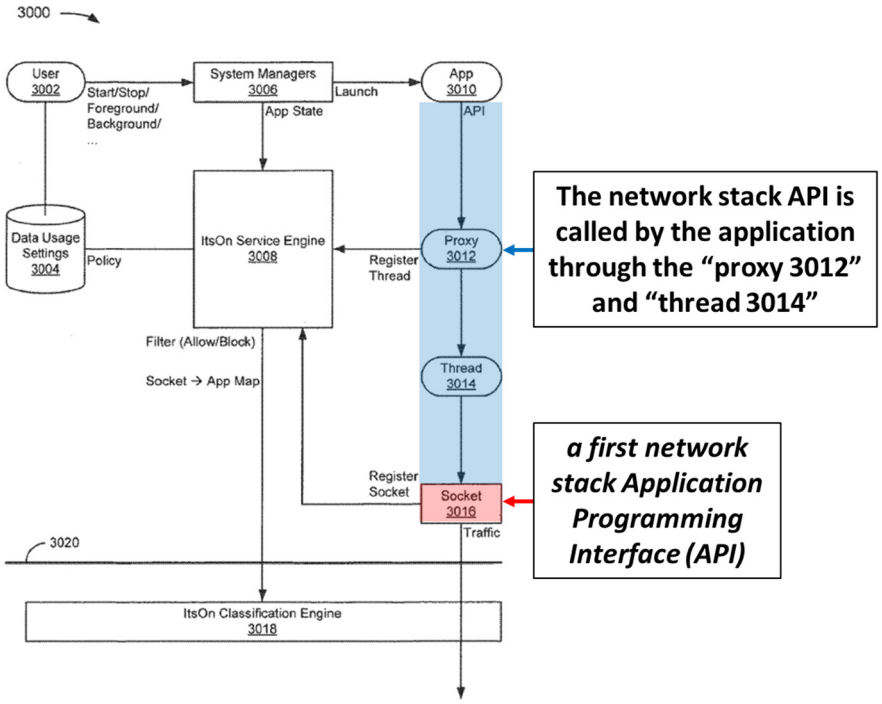


FIG. 30

SAMSUNG-1001, FIG. 30.

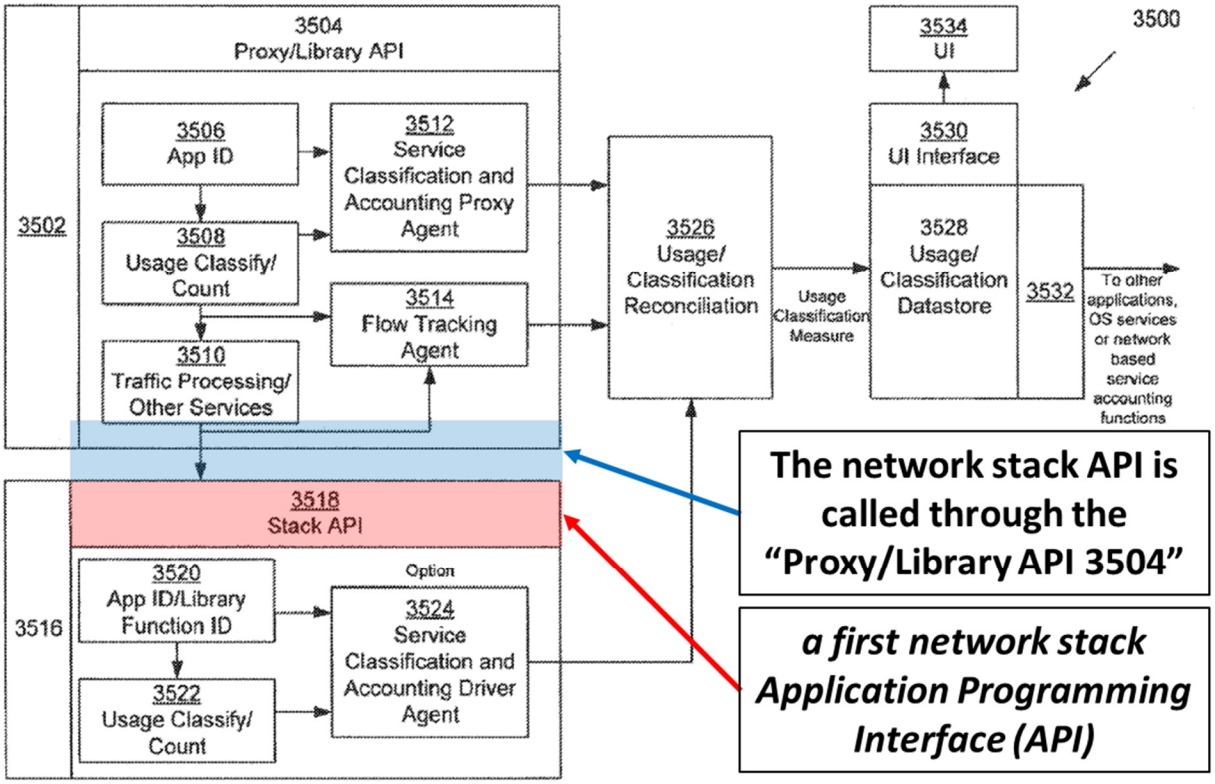
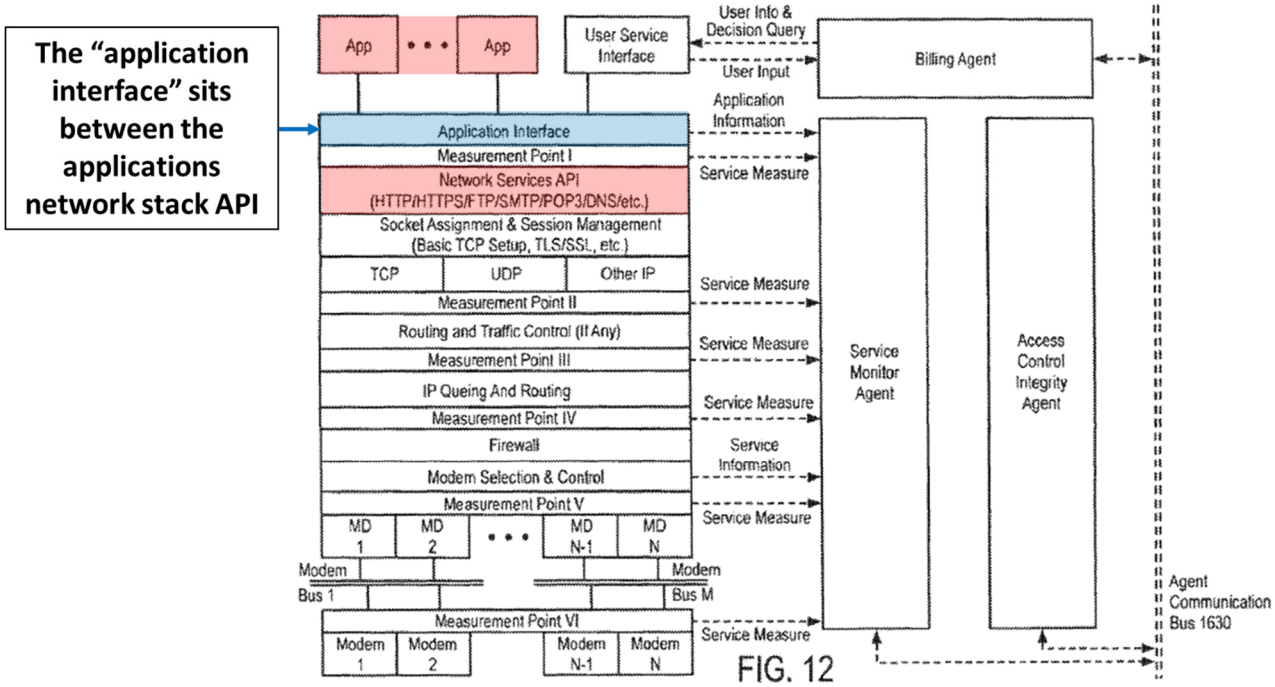


FIG. 35

SAMSUNG-1001, FIG. 35.

58. Moreover, the '918 Patent describes an "application service interface layer" that is "above the standard networking stack API"—positioned between the API and the requesting applications (much like Bennett's UA 202)—further confirming that the APIs need only be "***accessible***" to the applications when called (e.g., capable of being used). SAMSUNG-1001, 62:10-51, FIG. 12-13; SAMSUNG-1041, ¶[0025], FIG. 3. Even further, the '918 Patent describes "network based APIs" that are located "on a network element"—completely separate from the device itself. SAMSUNG-1001, 75:26-37.



SAMSUNG-1001, FIG. 12.

[1.4] a second API containing at least one second call accessible to each of the plurality of device applications, the second API callable by each of the plurality of device applications to make a data transfer request for a media object associated with a network resource identifier supplied by the calling device application;

<u>a data transfer request for a media object</u>

59. The '918 Patent describes "media download[s]," "media streaming," "audio files" played by a "media player," "streaming audio," "video conference[s]," Voice over Internet Protocol ("VoIP"), "multimedia data," and "instant messaging" as example application activities that involve the transfer of media ("a data transfer request for a media object"). SAMSUNG-1001, 72:37-50, 107:34-46, 111:44-112:17. Bennett discloses similar "***media objects***"

retrieved after a "***data transfer request***," for example, "voice over IP (VoIP), video and audio streaming, … videoconferencing, [and] instant messaging." SAMSUNG-1041, ¶¶[0017]-[0018], [0024], [0070], [0076].

a second API containing at least one second call accessible to each of the plurality of device applications, the second API callable by each of the plurality of device applications

60. Bennett discloses that its media client 200 includes a "media agent (MA …) 206" that "manages media connections, routes media according to media type and user settings, and invokes media players to process media as required" ("***make a data transfer request for a media object***"). SAMSUNG-1041, ¶¶[0025], [0050]-[0056], Table-3, FIGS. 3-10. The MA 206 is called by the UA 202 of the media client 200 using a "MA API 212" ("***a second API***") in response to a request from a "user application 150" ("***the second API callable by each of the plurality of device applications***"). SAMSUNG-1041, ¶¶[0031], [0050]-[0056], Table-3, FIGS. 3-10.

61. The MA API 212 includes various "requests" ("***at least one second call accessible to each of the plurality of device applications***") to send and receive media, including "LISTEN," "SEND," and "OPEN" requests ("***make a data transfer request for a media object***"). SAMSUNG-1041, ¶¶[0031], [0033], [0040], [0045]-[0046], FIGS. 6-7, Table-2; *see above* [1.3] (describing a "***plurality of device applications***").

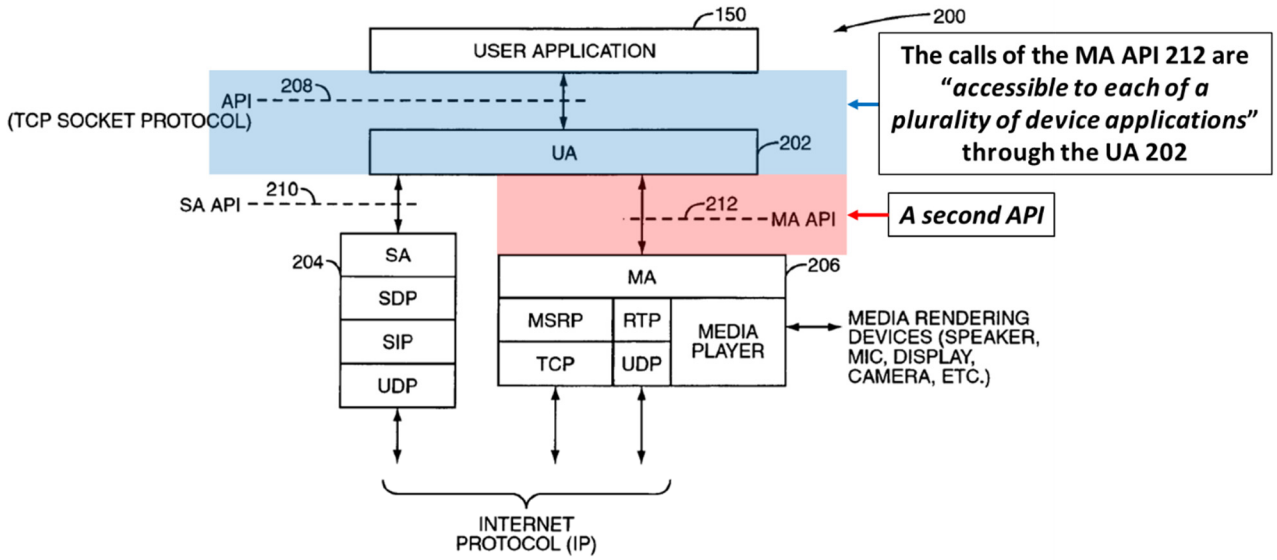


FIG. 3

SAMSUNG-1041, FIG. 3.

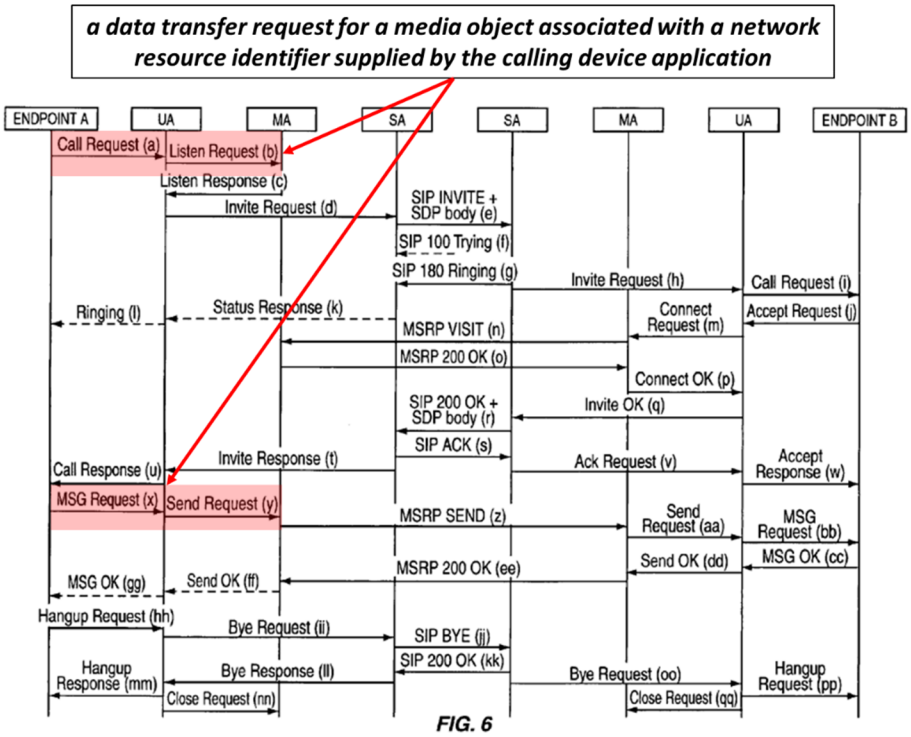


FIG. 6

SAMSUNG-1041, FIG. 6.

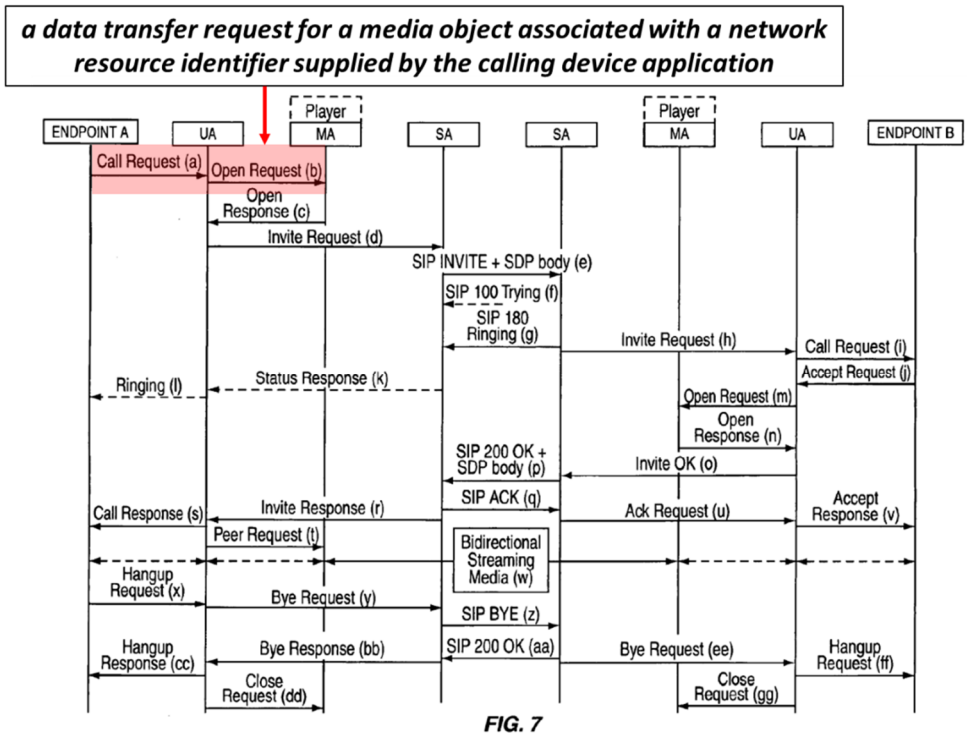


FIG. 7

SAMSUNG-1041, FIG. 7.

62. To the extent it is argued that the calls of the "***second API***" must be directly "***accessible to each of a plurality of device applications***," or that the application must directly call the "***second***" API, the '918 Patent does not support such a narrow interpretation. On the contrary, the process of applications indirectly calling APIs is depicted in the '918 Patent in multiple embodiments. SAMSUNG-1001, 110:12-111:17, 116:39-58; 119:49-60, FIGS. 30, 32, 35; *see above* [1.4].

a network resource identifier supplied by the calling device application

63. The '918 Patent gives examples of "***network resource identifier[s]***" that include: "(e.g., an IP address, a URL, a remote file name or address, a stream

name, an object name, or any combination of these identifiers) that identifies a source (or a proxy to the source) of the data to be transferred or a data object to be transferred." SAMSUNG-1001, 112:43-47.

64. Bennett discloses that its MA API 212 calls, for example the OPEN request, includes "a network address of a remote host from which media connections will be accepted" ("***a network resource identifier***") that is provided by the application when it calls the UA 202 (e.g., via a "CALL" request) ("***supplied by the calling device application***"). SAMSUNG-1041, ¶¶[0034], [0050]-[0056], [0086], Table-3. Applications also provide a "userid" and a "port" to call via the CALL request ("a network resource identifier"). SAMSUNG-1041, ¶[0084], Table-1.

65. Bennett's examples of "***network resource identifier[s]***" are consistent with the '918 Patent, and include: "a userID, alias, or fully qualified network address" ("an IP address" and "remote file … address"). SAMSUNG-1041, ¶[0034]. Bennett also provides example addresses of "call alice@ims.net: 5060 video/h263" and "call 10.0.0.1:5060 video/h263" (a "remote file … address"). *Id*. Additionally, all the aforementioned examples "identif[y] a source (or a proxy to the source) of the data to be transferred or a data object to be transferred." SAMSUNG-1041, ¶[0034]; SAMSUNG-1001, 112:43-47. Bennett also describes content located at Uniform Resource Identifiers ("URIs"),

which a POSITA would have recognized include Uniform Resource Locators (URLs). SAMSUNG-1041, Table-1.

"*network resource identifiers*" supplied by the calling application via the CALL request

TABLE 1-continued

UA API

MESSAGE	USE	SYNTAX	PARAMETERS	PARAMETER DESCRIPTION
Notify Response	Sent by IMS application to UA to acknowledge notify request	notify status_message	status_message	Indicates receipt of notify request, e.g. "OK"
Publish Request	Sent by IMS application to IMS UA to publish change in the user's presence status	publish uri expire_time [autorefresh]	uri expiretime autorefresh	Address. Time before the publish expires in seconds. Optional flag instructing the UA to refresh the publish automatically when it expires. If the application does not want the UA to automatically refresh the publish, the flag is omitted.
Publish Response	Sent by IMS UA to IMS application responsive to Publish request	publish uri expiretime status_message[:status_code]	uri expiretime status_message status_code	Address. Sometimes the server ignores the requested expire time and sets it to another value. This parameter returns the expiretime selected by the server. Status of request indicating success (e.g. "OK") or failure (e.g., "Failed") Optional code indicating status of publish request, 200 if the request was successful or a failure code on failure.
Call Request	Sent between IMS application and IMS UA to initiate MSRP and RTP sessions	call userid [userid@remotehost[:port]] call_type1...call_typeN	userid host:port call_type	At the originating endpoint, the IMS application specifies a userid to call when sending Call request if registered with a proxy. At the terminating endpoint the UA specifies the userid of the calling party. At the originating endpoint, the UA specifies the host address and port to call, if not registered with a proxy. At the terminating endpoint the UA specifies the userid of the network address and port designated by the calling party for the call. Type of call to be established, for example audio/amr or video/h263. Multiple call_types may be listed, e.g., audio/amr and video/h263 for video telephony

SAMSUNG-1041, Table-1.

The OPEN request of the MA API includes the "*network resource identifier*" supplied by the calling application

TABLE 3

MA API

MESSAGE	USE	SYNTAX	PARAMETERS	PARAMETER DESCRIPTION
Listen Request	Sent by UA to MA to initiate a MSRP session. The MA opens a TCP listener in response to the Listen request.	listen [remotehost]	remotehost	Optional parameter specifies address from which connections can be made.
Listen Response	Sent by MA to UA as final response to Listen request. The Listen response includes the address and port of the TCP connection opened for the MSRP session.	listen status_message[:status_code] host:port	status_message	Status of listen request indicating success (e.g. "OK") or failure (e.g., "Failed")
			status_code	Optional code indicating status of Listen request, 200 if the request was successful or an error code on failure.
			host:port	Network address of host and port number for port opened in response to Listen Request. Returned when Listen request is successful. Omitted when Listen request fails.
Open Request	Sent by UA to MA to initiate RTP session. The MA opens a TCP connection in response to the Open request.	open [remotehost]	remotehost	Optional address specifies address from which connections can be made.

SAMSUNG-1041, Table-3.

[1.5] a media service manager prompted by the second call, to manage network data transfers for the media object by interfacing with the network stack to retrieve the media object associated with the network resource identifier via the wireless modem and the wireless network; and

66. Bennett discloses that its media client 200 includes a "media agent (MA …) 206" ("***a media service manager***") that "implements the message session relay protocol (MSRP) and the Real-Time Transport Protocol (RTP)" and "manages media connections, routes media according to media type and user settings, and invokes media players to process media as required" ("***manage network data transfers for the media object by interfacing with the network stack to retrieve the media object***"). SAMSUNG-1041, ¶¶[0025], [0050]-[0056], Table-3, FIGS. 3-10.

67. The MA 206 is called by the UA 202 of the media client 200 using a "MA API 212" ("***prompted by the second call***") in response to a request from a "user application 150." SAMSUNG-1041, ¶¶[0031], [0050]-[0056], Table-3, FIGS. 3-10. Additionally, the MA 206 uses "TCP and/or UDP over IP for transport of RTP and MSRP messages" and retrieves media that "passes up through the IP, UDP and RTP stacks" prior to being played at a media player or decoder ("***interfacing with the network stack to retrieve the media object***"). SAMSUNG-1041, ¶¶[0025], [0076]-[0079]. Additionally, as described above, Bennett's media is retrieved from "remote host[s]" over wireless networks (e.g., "GPRS") through the use of a corresponding wireless modem (such that Bennett's media is retrieved "via the wireless modem and the wireless network"). SAMSUNG-1041, ¶[0017], [0054], FIG. 1; *see above*, [1.1].

68. As described above, requests from applications include a "network resource identifier" that is "associated" with the "media object." *See above*, [1.4].

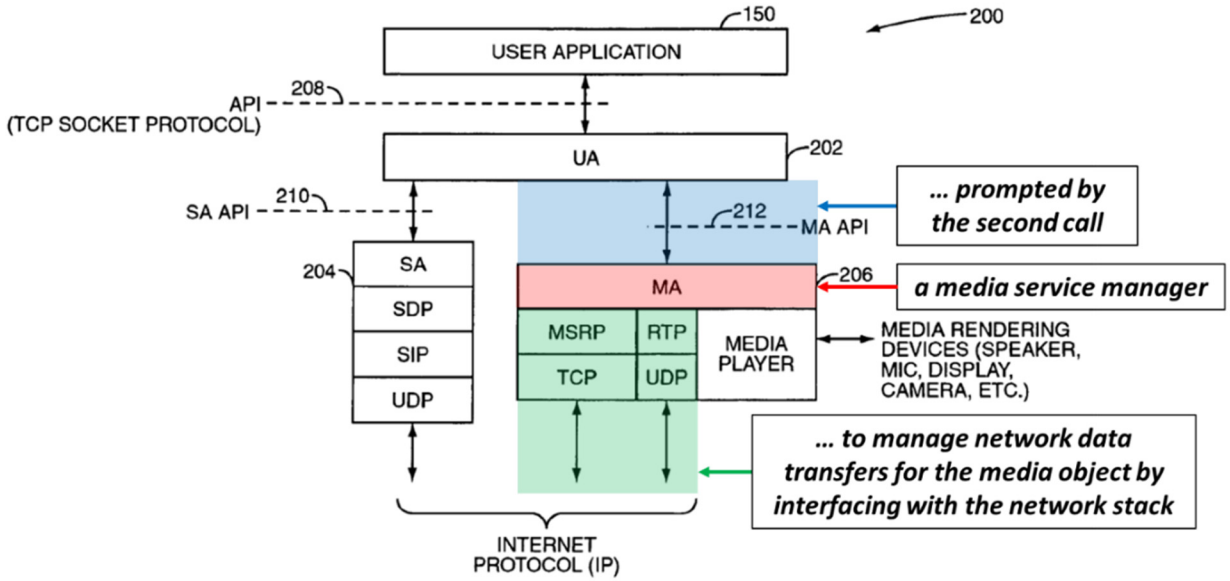


FIG. 3

SAMSUNG-1041, FIG. 3.

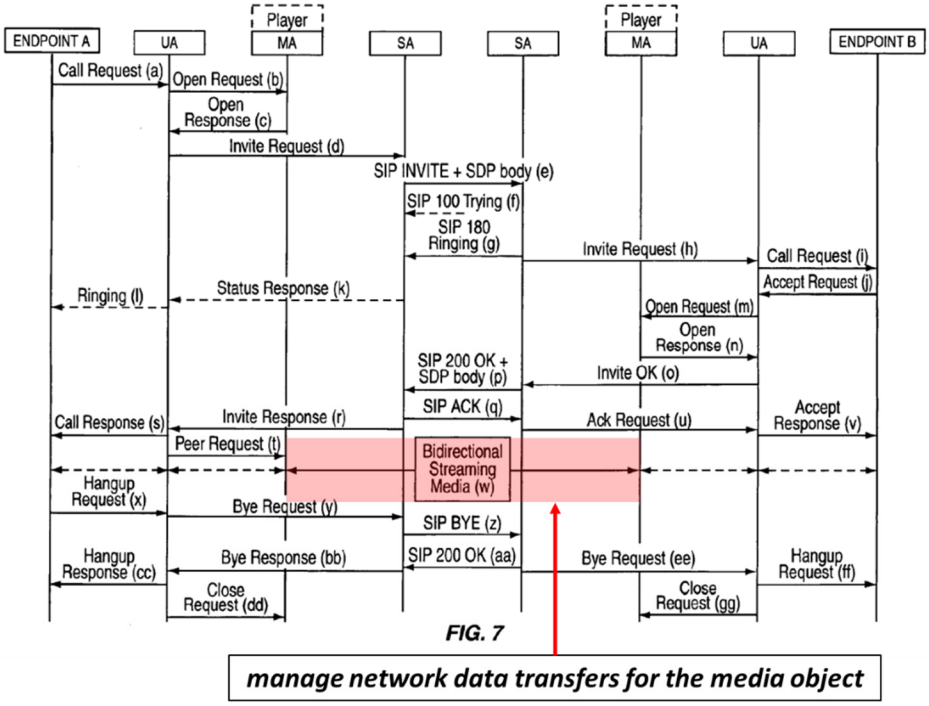


FIG. 7

SAMSUNG-1041, FIG. 7.

[1.6] one or more service classification and measurement agents to associate wireless network data usage for the media object network data transfers with the device application that requests the data transfer for the media object, to associate wireless network data usage for respective data packet flows opened and used via the first network stack API with the device application opening such respective data packet flow, and to reconcile wireless network data usage for each of the plurality of device applications to track an aggregate wireless network data usage attributable to each of the plurality of device applications via both the first network stack API and the second API.

69. Vadde discloses techniques for "managing data traffic" for each of a plurality of applications using a "policy" based system that enforces restrictions based on "attributes" in the transmitted data and corresponding data "usage limits." SAMSUNG-1042, ¶¶[0010], [0015]-[0016], [0025]-[0026].

one or more service classification and measurement agents to associate wireless network data usage for the media object network data transfers with the device application that requests the data transfer for the media object

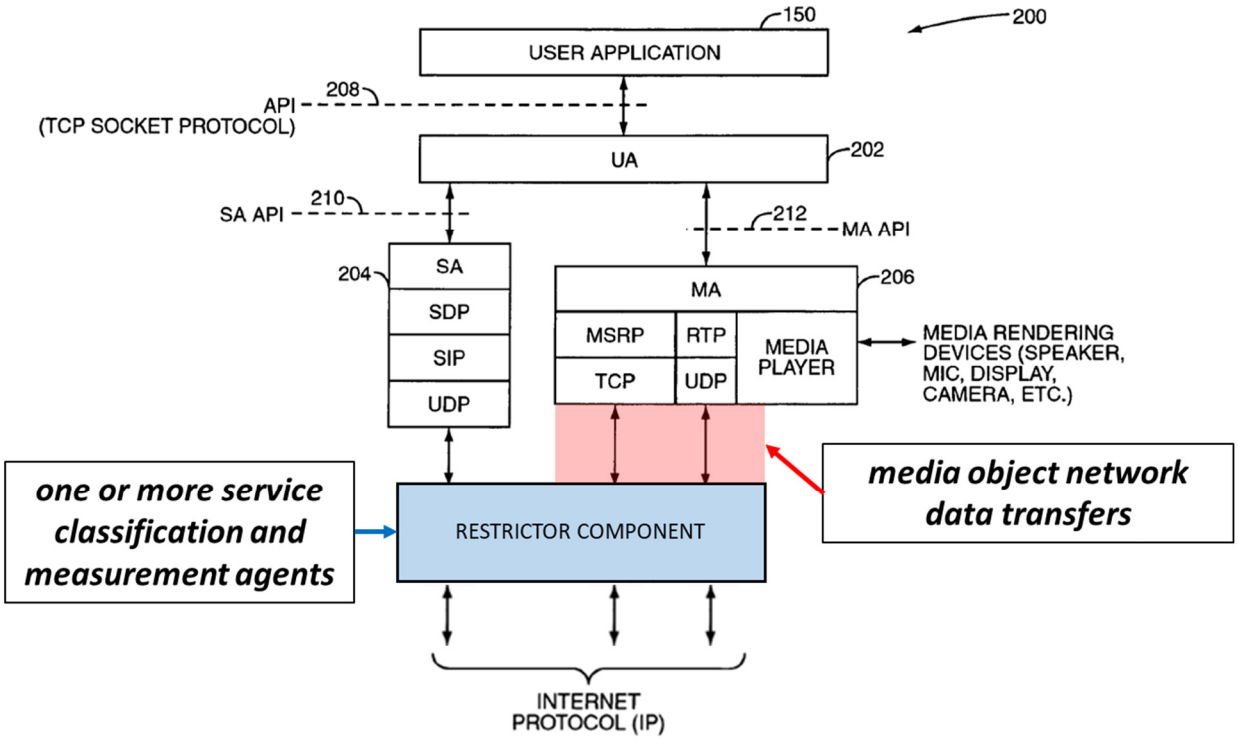
70. Vadde enforces its policies with a "restrictor component 122" ("***one or more service classification and measurement agents***") which "appl[ies] the data usage policy" and "monitors the data transmitted and/or received by the applications 110 and determines whether the data usage limits 116 corresponding to each of the applications 110 have been exceeded or are about to be exceeded." SAMSUNG-1042, ¶¶[0022], [0024]-[0026], [0029]-[0032]. In particular, Vadde's restrictor component 122 monitors transmitted data to determine "attributes 112," which include an "application name" which is given a "Program ID" ("***associate wireless network data usage for … the device application***"). SAMSUNG-1042, ¶¶[0024],

[0032]. Applications also have "a corresponding set of attribute values" that are monitored to produce "usage patterns" ("***associate wireless network data usage for … the device application***"). SAMSUNG-1042, ¶[0024]. In combining Vadde's techniques into Bennett's device, as explained above, a POSITA would have found it obvious to leverage Vadde's monitoring of application data usage to monitor and associate "***media object network data transfers***" performed via the MA API 212 with "***the device application that requests the data transfer for the media object***" as these transfers would have resulted in data usage that would potentially be chargeable to the user of the Bennett-Vadde device. *See above*, §VII.C.

Vadde's policies denote specific applications with a "Program ID"

```
<budget>
    <policy Cellular
        <Program ID=EMAIL, Limit=500MB, Send=100MB,
Roaming=YES>
        <Program ID=SocialNetworkingSiteA, Limit=10MB>
        <Program ID=DEF, Limit=10MB, Roaming=NO>
        <PromptReminder Criteria=Bytes, PercentofBudget=50%>
        <PromptData Criteria=Bytes, PercentofBudget=90%>
        <PromptData Criteria=Roaming, Limit=20MB>
    </policy>
    <policy WiFi>
        <Program ID=XYZ, Limit=5000MB>
        <Program ID=ABC, Limit=5000MB>
    </policy>
</budget>
```

SAMSUNG-1042, ¶[0032].



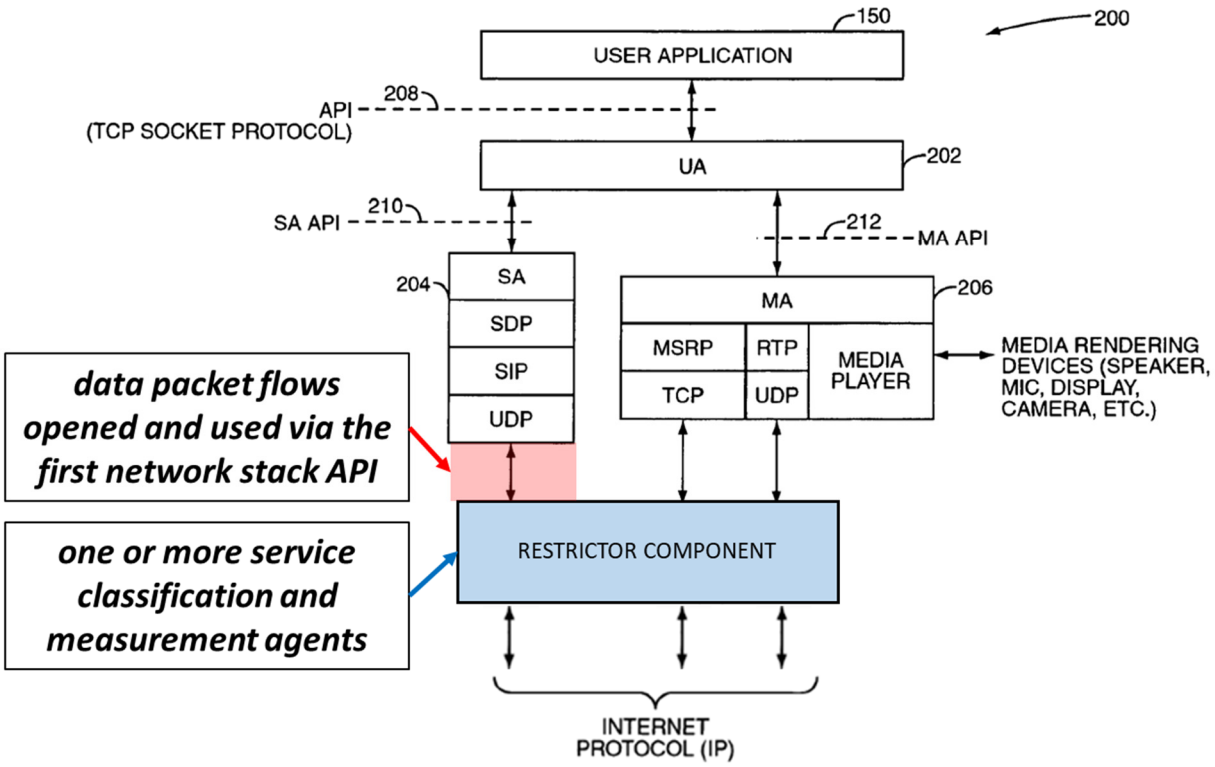
SAMSUNG-1041, FIG. 3 (as modified by Vadde).

<u>to associate wireless network data usage for respective data packet flows opened and used via the first network stack API with the device application opening such respective data packet flow,</u>

71. Additionally, as explained above, a POSITA would have found it obvious to leverage Vadde's monitoring of application data usage to monitor and associate "***respective data packet flows opened and used***" via the SA API 210 with "***the device application opening such respective data packet flow***" as these packet flows would have resulted in data usage that would potentially be chargeable to the user of the Bennett-Vadde device. SAMSUNG-1042, ¶¶[0010], [0015]-[0016], [0025]-[0026]; *see above*, §VII.C.

72. As explained above, a POSITA would have recognized and found obvious that the protocols disclosed in Bennett would have included "***data packet flows***" as these protocols are examples of "packet switched services" that communicate data in a series of data packets. SAMSUNG-1041, ¶[0017]; *see above* [1.3]. For example, Rakoshitz descries that network traffic is "a flow of information or data or packets of information." SAMSUNG-1046, 12:12-58, 15:57-67.

73. In the combination, the restrictor component of the Bennett-Vadde device would have measured data usage associated with the "flow" of information (communication sessions established via the SA 204 and SA API 210—"***respective data packet flows opened and used via the first network stack API***") classified to each application ("***with the device application opening such respective data packet flow***"). SAMSUNG-1042, ¶¶[0010], [0015]-[0016], [0025]-[0026].



SAMSUNG-1041, FIG. 3 (as modified by Vadde).

<u>and to reconcile wireless network data usage for each of the plurality of device applications to track an aggregate wireless network data usage attributable to each of the plurality of device applications via both the first network stack API and the second API.</u>

74. Vadde's restrictor component 122 "monitors the data transmitted and/or received by the applications 110 and determines whether the data usage limits 116 corresponding to each of the applications 110 have been exceeded or are about to be exceeded" ("***reconcile wireless network data usage for each of the plurality of device applications***"). SAMSUNG-1042, ¶¶[0022], [0024]-[0026], [0029]-[0032]. When a data usage limit is exceeded, the application's data usage is "restricted." *Id*.

75. Vadde's "data usage limits 116" are set for "each" application and include "a maximum quantity of data to be transmitted and/or received by a particular application 110" ("***an aggregate wireless network data usage attributable to each of the plurality of device applications***"). SAMSUNG-1042, ¶¶[0010], [0016], [0018], [0022], [0025], [0029]-[0030], [0032]. As described above, this data usage would have been monitored for both the SA API 210 ("***the first network stack API***") and MA API 212 ("***the second API***") in the Bennett-Vadde combination. *See above*, §VII.C.

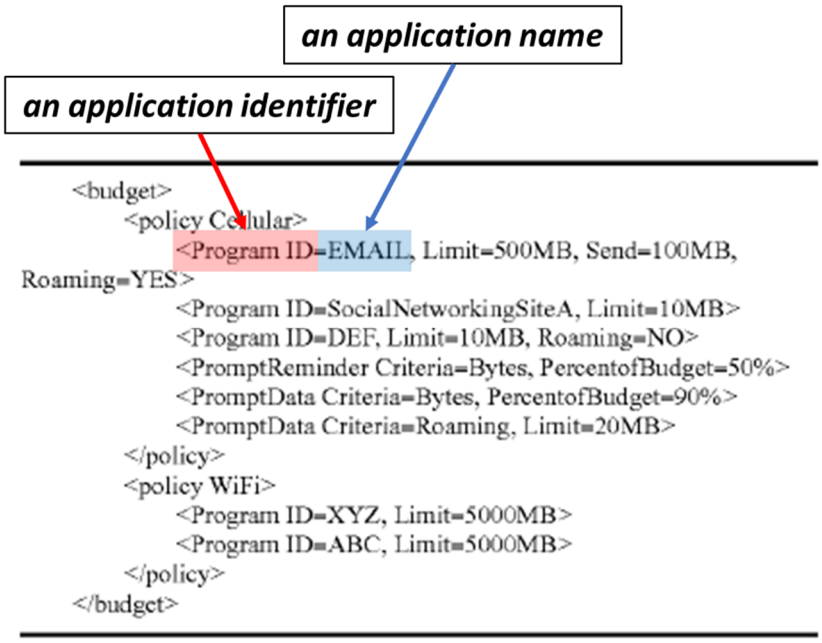
A limit placed on the *"aggregate wireless network data usage"*

```
<budget>
    <policy Cellular>
        <Program ID=EMAIL, Limit=500MB, Send=100MB,
Roaming=YES>
        <Program ID=SocialNetworkingSiteA, Limit=10MB>
        <Program ID=DEF, Limit=10MB, Roaming=NO>
        <PromptReminder Criteria=Bytes, PercentofBudget=50%>
        <PromptData Criteria=Bytes, PercentofBudget=90%>
        <PromptData Criteria=Roaming, Limit=20MB>
    </policy>
    <policy WiFi>
        <Program ID=XYZ, Limit=5000MB>
        <Program ID=ABC, Limit=5000MB>
    </policy>
</budget>
```

SAMSUNG-1042, ¶[0032].

[2] The wireless end-user device of claim 1, wherein to associate wireless network data usage for the media object network data transfers with the device application that makes the data transfer request for the media object comprises to identify at least one of an application name, an application identifier, or a process identifier for the application that makes the data transfer request.

76. As described above, Vadde discloses that each application's usage is tracked by an "application name" ("***an application name")*** that is a "Program ID" ("***an application identifier").*** SAMSUNG-1042, ¶¶[0024], [0032]; *see above* [1.6]. Because Vadde monitors per application usage using these parameters, the Bennett-Vadde device "***associate[s] wireless network data usage for the media object network data transfers with the device application***" by "***identify[ing] … an application name, [and] an application identifier, … for the application that makes the data transfer request***." *Id*.



SAMSUNG-1042, ¶[0032].

[3] The wireless end-user device of claim 2, wherein the data transfer request comprises a network resource identifier that identifies a source of the data to be transferred, a proxy to the source of the data to be transferred, or the media object to be transferred, in particular, wherein the network resource identifier comprises one or more of an Internet Protocol address, a Uniform Resource Locator, a remote file name/address, a stream name, and an object name.

77. As discussed above, Bennett's "requests" ("***the data transfer request***") include "a network address of a remote host from which media connections will be accepted" ("***a network resource identifier that identifies a source of the data to be transferred***") that is provided by the application when it calls the UA 202 (e.g., via a "CALL" request). SAMSUNG-1041, ¶¶[0034], [0050]-[0056], Table-3; *see above* [1.4]. Additionally, the CALL request includes a "host address and port to call" ("@remotehost"—"***a proxy to the source of the data to be transferred***") when the recipient has not previously registered with the proxy. SAMSUNG-1041, ¶¶[0034], [0084], Table-1.

"a proxy to the source of the data to be transferred"

Call Request	Sent between IMS application and IMS UA to initiate MSRP and RTP sessions	call userid [userid@remotehost[:port]] call_type1...call_typeN	userid	At the originating endpoint, the IMS application specifies a userid to call when sending Call request if registered with a proxy. At the terminating endpoint the UA specifies the userid of the calling party.
			host:port	At the originating endpoint, the UA specifies the host address and port to call, if not registered with a proxy. At the terminating endpoint the UA specifies the userid of the network address and port designated by the calling party for the call.
			call_type	Type of call to be established, for example audio/amr or video/h263. Multiple call_types may be listed, e.g., audio/amr and video/h263 for video telephony

SAMSUNG-1041, Table-1.

78. Bennett's examples of "***network resource identifier[s]***" include: "a userID, alias, or fully qualified network address" ("***a remote file name/address***").

SAMSUNG-1041, ¶[0034]. Bennett also provides example addresses of "call alice@ims.net: 5060 video/h263" and "call 10.0.0.1:5060 video/h263" ("***a remote file name/address***"). *Id*. Bennett further describes content located at Uniform Resource Identifiers ("URIs"), which a POSITA would have recognized include "***Uniform Resource Locator[s]***" ("URLs"). SAMSUNG-1041, Table-1; *see above* [1.4]. Further, a POSITA also would have recognized and found obvious that URLs also indicated "***the media object to be transferred, in particular***" as the file name of the media object would typically comprise part of the URL. For example, Riggs discloses that "the global address of content" ("***the media object to be transferred, in particular***") is "typically" provided "in the form of a Uniform Resource Locator (URL)" (e.g., a "feed URL"). SAMSUNG-1043, 1:25-35, 5:54-62, 6:38-43. Riggs also provides an example stream URL for a popular TV show around the time of its filing that shows that a URL includes the file type, thus indicating "***the media object to be transferred, in particular***" ("http://www.nbc.com/heroes/feed.xml). SAMSUNG-1043, 5:54-62.

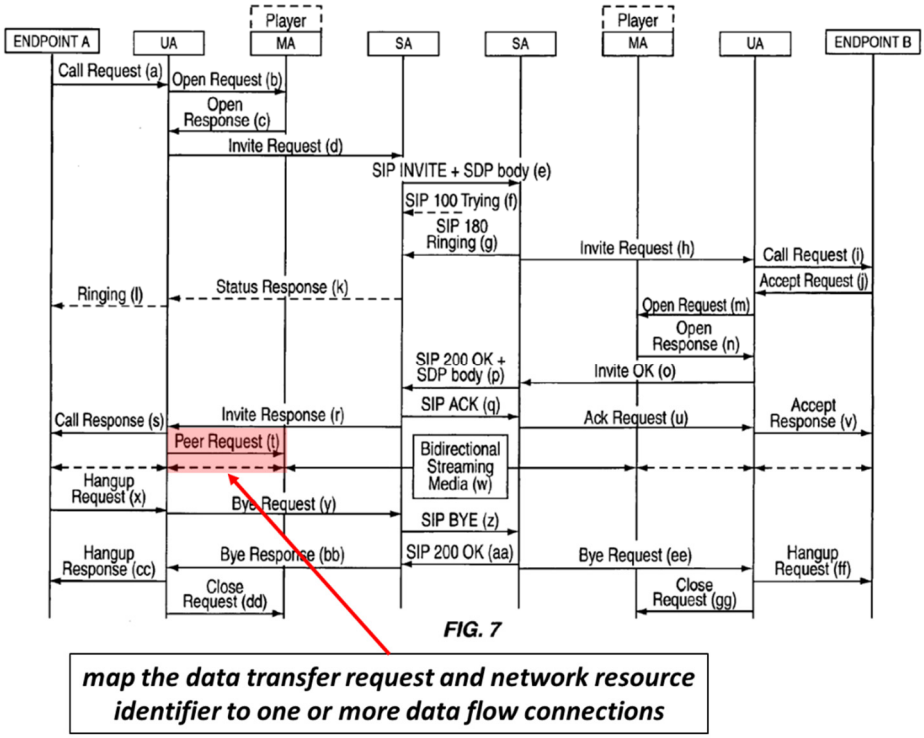
A POSITA would have understood and found obvious that URLs indicate "*media objects*"

One way to identify a publisher associated with content being played back is use of an "authority" section of a feed URL (e.g., a pointer received via media feed **159**) that references the media content. For example, if the user is playing back an episode from NBC's Heroes television show, then the feed URL for the Heroes feed may be something like "http://www.nbc.com/heroes/feed.xml". In this case, the authority (e.g., publisher id information) is "www.nbc.com", which is the publisher identifier.

SAMSUNG-1043, 5:54-62.

[8] The wireless end-user device of claim 3, wherein to manage network data transfers for the media object by interfacing with the at least one network stack comprises to map the data transfer request and network resource identifier to one or more data flow connections communicated through the device network stack.

79. Bennett discloses that, once the SA 204 establishes a communication session (e.g., an "RTP session"—"***one or more data flow connections communicated through the device network stack***"), the UA 202 "sends a PEER request to the MA206 to provide the MA206 with the host address and port opened for the RTP session" ("***map the data transfer request and network resource identifier to one or more data flow connections communicated through the device network stack***"). SAMSUNG-1041, ¶¶[0055], [0073], [0079], FIG. 7. The PEER request includes "the network address and port for the media connection" (the "***network resource identifier***" associated with the "***one or more data flow connections communicated through the device network stack***"). *Id*.



SAMSUNG-1041, FIG. 7.

[9] The wireless end-user device of claim 1, further comprising a media player and a user interface, wherein the media object comprises media data that is, as a result of the media service manager management of network data transfers for the media object, received by the device and played by the media player through the user interface.

80. Bennett discloses that its media client 200 includes "one or more media players" ("***a media player***") to "process and output media to media rendering devices" which include a "speaker and/or display of a mobile terminal 100." SAMSUNG-1041, ¶¶[0002], [0025], [0076], FIGS. 3, 9, 11. As an example, Bennett discloses "media streaming" (a "***media object [that] comprises media data")*** where "the user application 150 … receives the media stream and outputs the media stream to a media player" and, in this situation, the "MA 206 … directly route[s] the

media stream to a media player" ("***that is, as a result of the media service manager management of network data transfers for the media object, received by the device and played by the media player through the user interface***"). SAMSUNG-1041, ¶[0076], FIG. 9. Bennett's FIGS. 3 and 9 depict examples of this process.

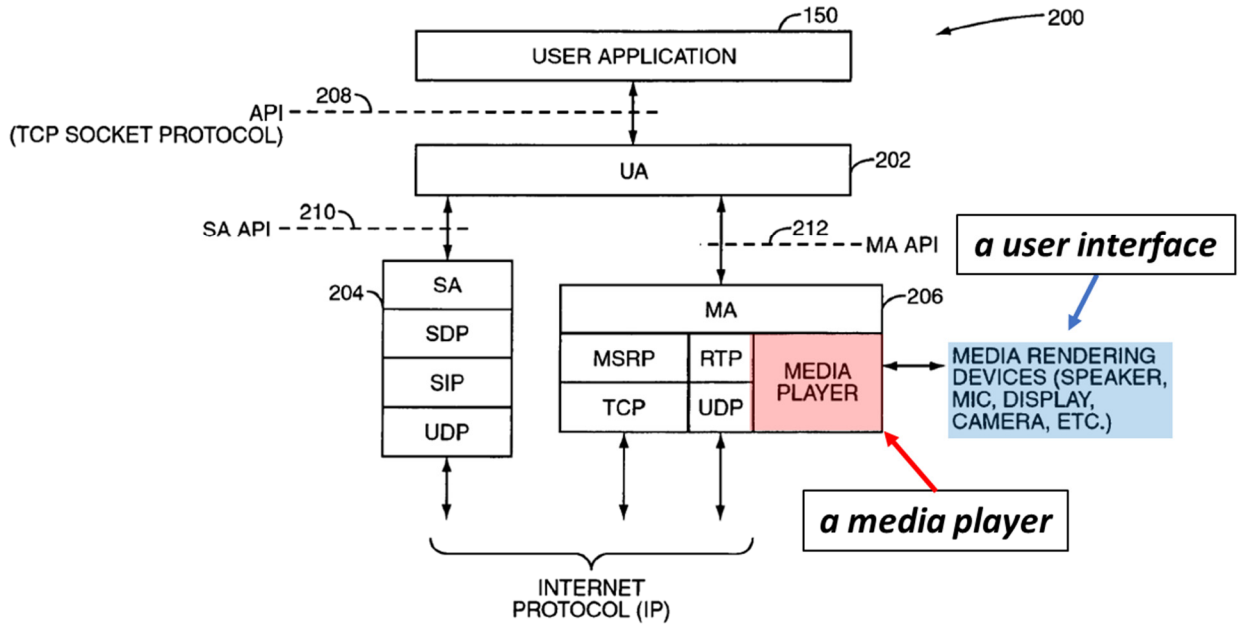


FIG. 3

SAMSUNG-1041, FIG. 3.

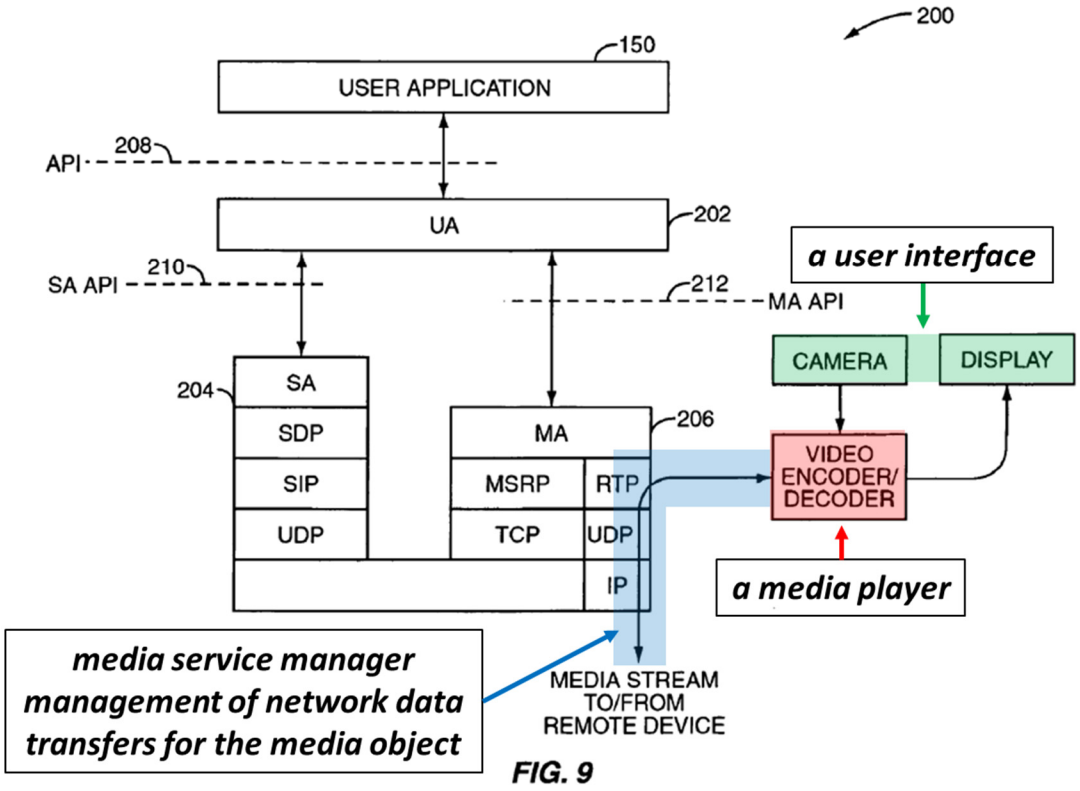


FIG. 9

SAMSUNG-1041, FIG. 9.

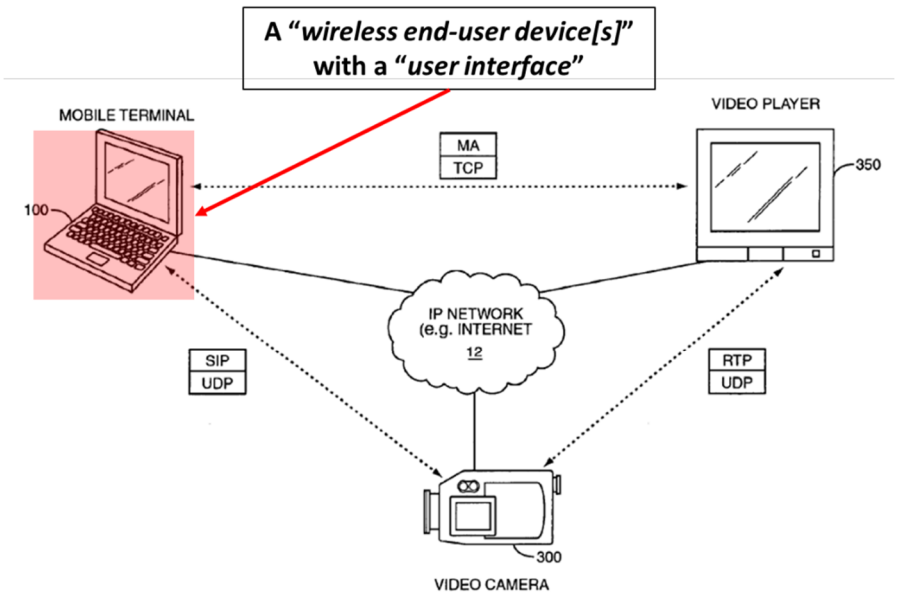
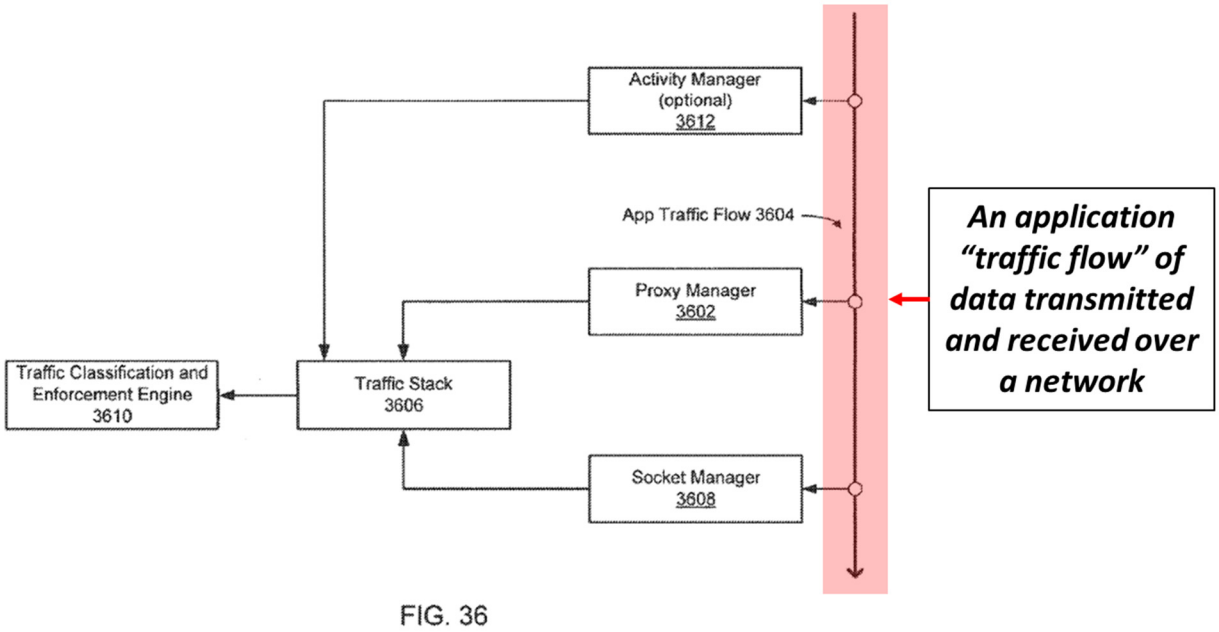


FIG. 11

SAMSUNG-1041, FIG. 11.

[13] The wireless end-user device of claim 1, the one or more service classification and measurement agents to further associate one or more traffic flows, comprising the media object network data transfers, with the device application that makes the data transfer request, the device further comprising an enforcement agent to, based on the association between the one or more traffic flows and the device application, enforce an application-based usage control on network data usage by one or more of the device applications.

81. The '918 patent does not define the feature "***traffic flow***," but generally describes that applications generate "***traffic flows***" (e.g., data transmitted and received when performing activities over a network). SAMSUNG-1001, 62:16-20, 81:36-45, 88:47-53, 89:23-25, 93:42-46, 109:55-59, 120:7-10, FIG. 36.



SAMSUNG-1001, FIG. 36.

82. As described above, Vadde's "policy" based system enforces restrictions on application data usage based on "usage limits" ("***enforce an application-based usage control on network data usage***"). SAMSUNG-1042,

¶¶[0015]-[0016], [0025]-[0026]; *see above* [1.6]. In particular, Vadde's restrictor component 122 ("***one or more service classification and measurement agents***" and an "***enforcement agent***") monitors transmitted data to determine "attributes 112," which include an "application name" which is given a "Program ID" ("***associate one or more traffic flows … with the device application that makes the data transfer request***"). SAMSUNG-1042, ¶¶[0024], [0032]; *see above* [1.6]. Additionally, the data transmitted and received by the Bennett-Vadde device's applications ("***traffic flows***") includes streamed media data ("***one or more traffic flows, comprising the media object network data transfers***"). SAMSUNG-1041, ¶¶[0017]-[0018], [0024], [0070], [0076]; *see above* [1.4].

83. Vadde's restrictor component "monitors the data transmitted and/or received by the applications 110" and applies a "policy" that "prevents the applications 110 from transmitting and/or receiving data in excess of the data usage limits 116" ("***enforce an application-based usage control on network data usage by one or more of the device applications***"). SAMSUNG-1042, ¶[0022]; *see above* [1.6]. Additionally, because Vadde's enforcement of policies is per application, the application of a policy in response to data usage is "***based on the association between the one or more traffic flows and the device application***." *Id*.

Claims 14 and 19

84. The below claims are rendered obvious for similar reasons as discussed in the analysis for the corresponding claim listed in the table below.

Claim	Corresponding Claim
14.pre	1.pre-1.1
14.1	1.2-1.3
14.2	1.4
14.3	1.5
14.4	1.6
19.pre	1.pre
19.1	1.1
19.2	1.2
19.3	1.3
19.4	1.4, 3
19.5	1.5, 8
19.6	1.6, 2

B. Claims 4-6, 11-13, and 15-17 are obvious over Bennett in view of Vadde and Riggs

[4] The wireless end-user device of claim 3, wherein to associate wireless network data usage for the media object network data transfers with the device application that makes the data transfer request for the media object further comprises to store an entry comprising the at least one of the application name, the application identifier, or the process identifier for each of the device applications that makes a data transfer request, each stored entry further comprising information about the corresponding network resource identifier for the data transfer request.

85. Riggs discloses a "media player" with a "log report generator" that generates a "log report" of "playback commands" and "metadata" associated with played media ("***store an entry comprising the at least one of the application name, the application identifier, or the process identifier for each of the device applications that makes a data transfer request***"). SAMSUNG-1043, 1:58-2:5, 6:32-45, 10:13-23, 11:18-31, 16:28-33, FIG. 2. Examples of Riggs "metadata" include an "[a]pplication [n]ame" ("***application name***") and "media feed URL" ("***process identifier***"). *Id.* Riggs' metadata also includes "a URL associated with the content being played back" ("***each stored entry further comprising information about the corresponding network resource identifier for the data transfer request***"). SAMSUNG-1043, 6:32-45, 10:13-23, 11:18-31, 16:28-33.

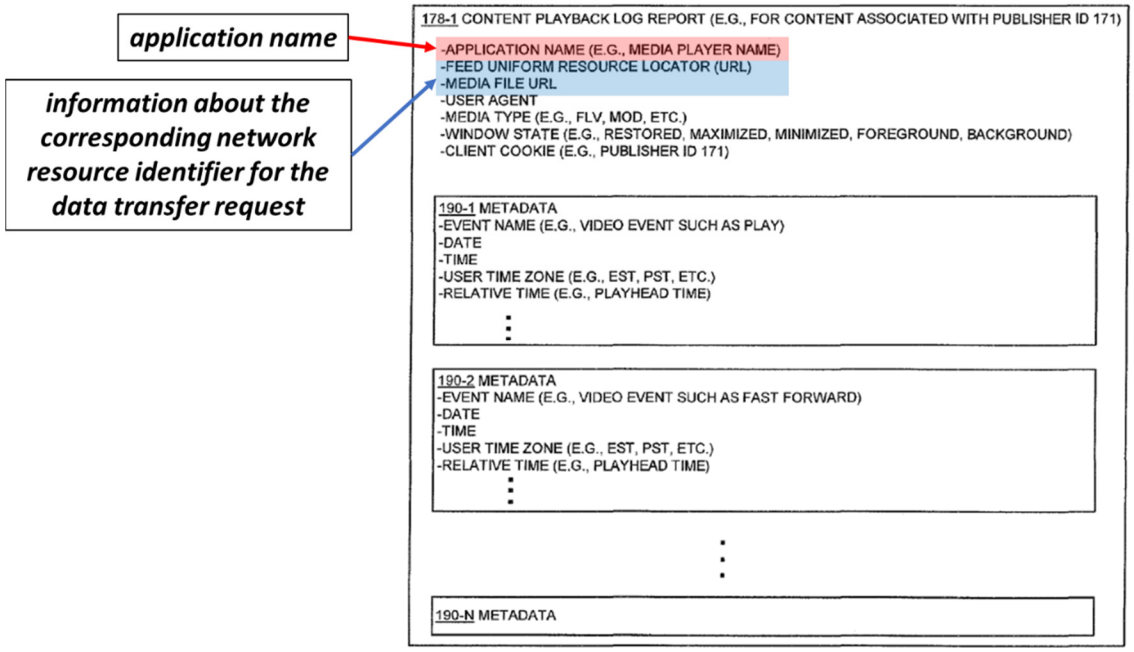


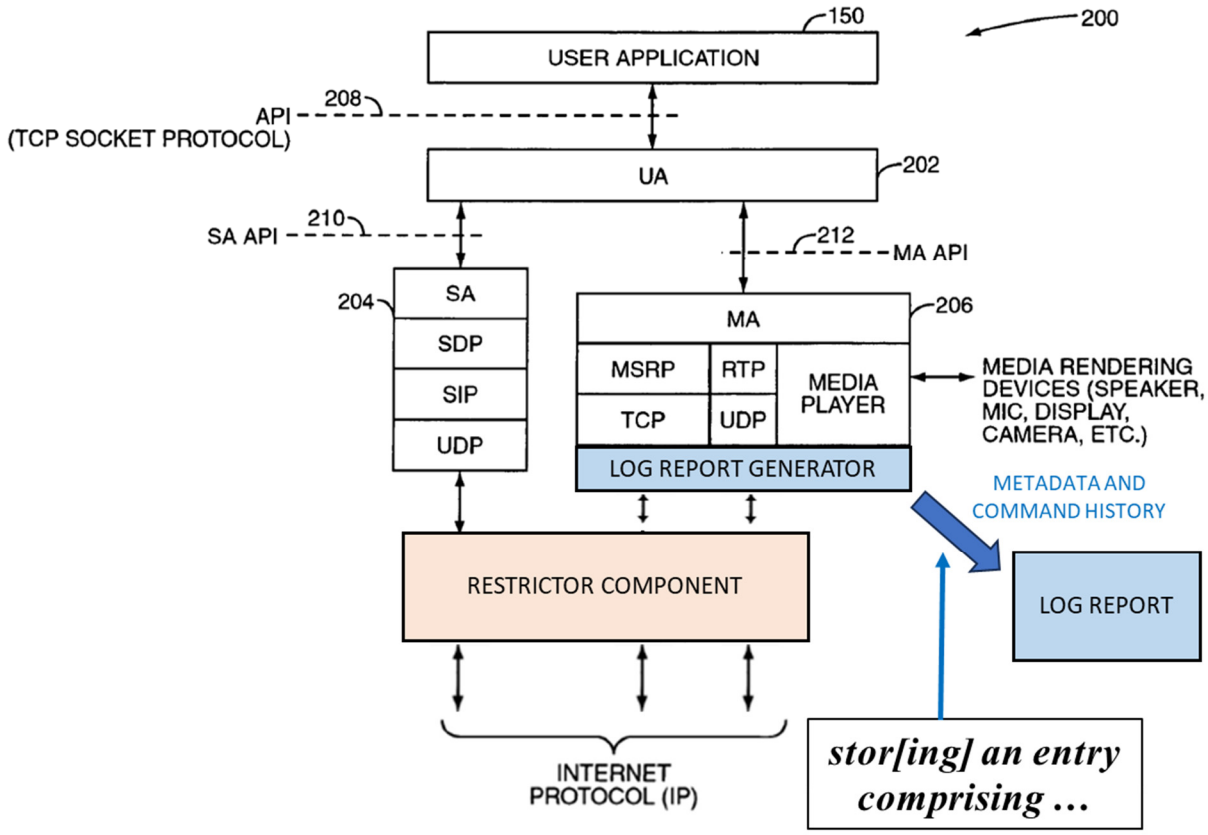
FIG. 2

SAMSUNG-1043, FIG. 2.

86. Additionally, in implementing the Bennett-Vadde-Riggs combination, a POSITA would have recognized and found obvious that other information, as described in Bennett and Vadde, would have been included in the metadata stored in a log report, for example, the Program ID disclosed in Vadde (an "***application name***" and "***identifier***"). *See above*, [2]. This would have allowed a POSITA to leverage the existing features of Bennett and Vadde and adapt them to perform Riggs' techniques in a predictable way that achieves the benefits of Riggs' logging in the context of the media transfers of Bennett-Vadde.

87. As described above, in the combination, when monitoring data usage for each of the applications, the Bennett-Vadde-Riggs device would have

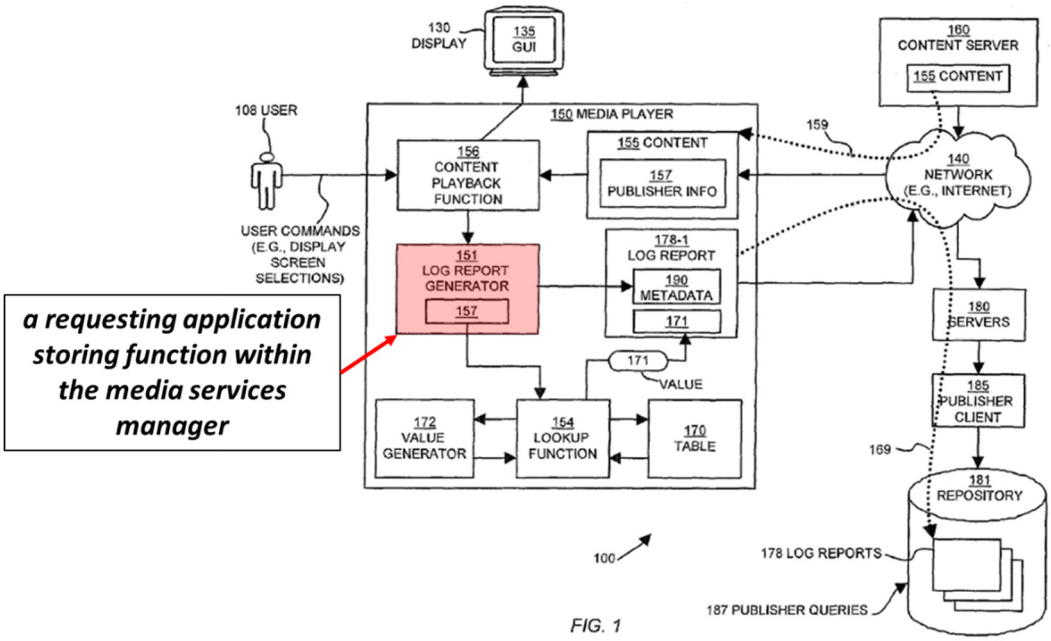
additionally logged "playback commands" and "metadata" describing the retrieved media objects in a "log report," as described in Riggs ("***to associate wireless network data usage for the media object network data transfers with the device application that makes the data transfer request for the media object further comprises to store an entry comprising …***"). *See above*, § VII.E. Doing so would have provided the benefits described above, including gaining increased insight into a user's data usage patterns. *See above*, § VII.E.



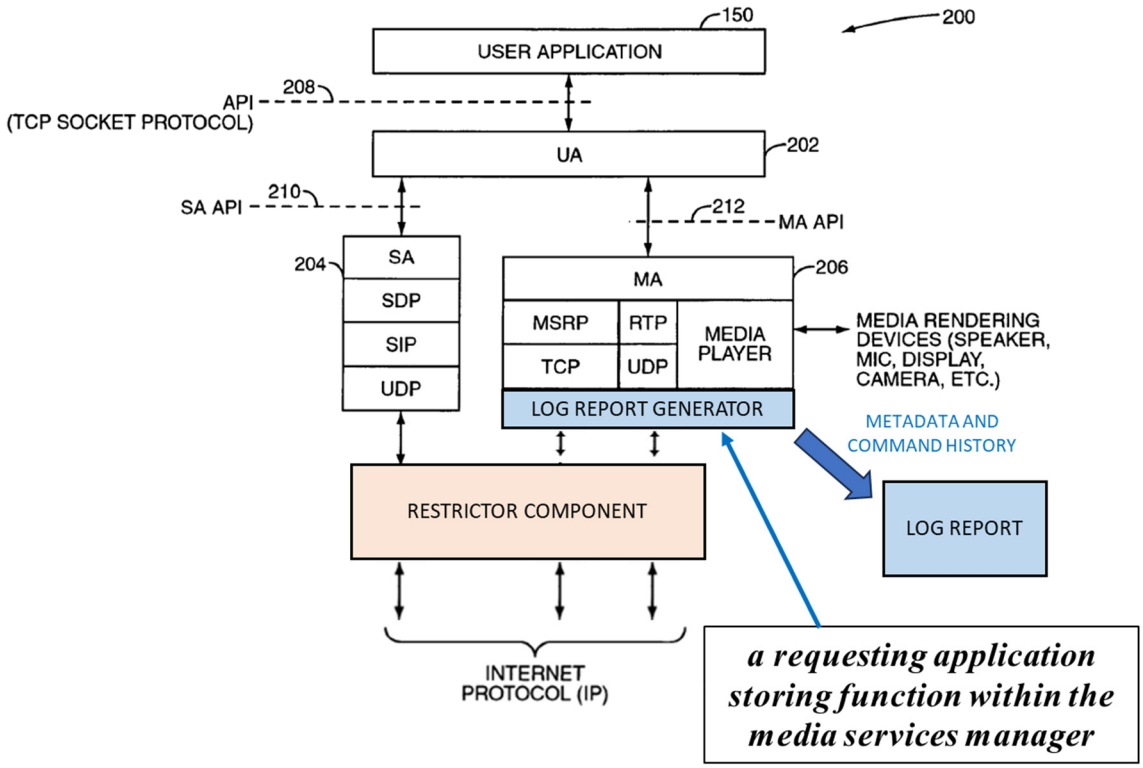
SAMSUNG-1041, FIG. 3 (as modified by Vadde and Riggs).

[5] The wireless end-user device of claim 4, wherein the one or more service classification and measurement agents includes a requesting application storing function within the media services manager.

88. As described above, Riggs discloses a "log report generator" ("***a requesting application storing function***") within the "media player" ("***within the media services manager***") that generates a log report of metadata associated with played content. SAMSUNG-1043, 5:23-32, 6:32-45, 11:45-49, FIG. 1; SAMSUNG-1001, 112:53-61, 114:27-34 (describing the "requesting-application storing function"); *see above* [4] (describing "log reports").



SAMSUNG-1043, FIG. 1.

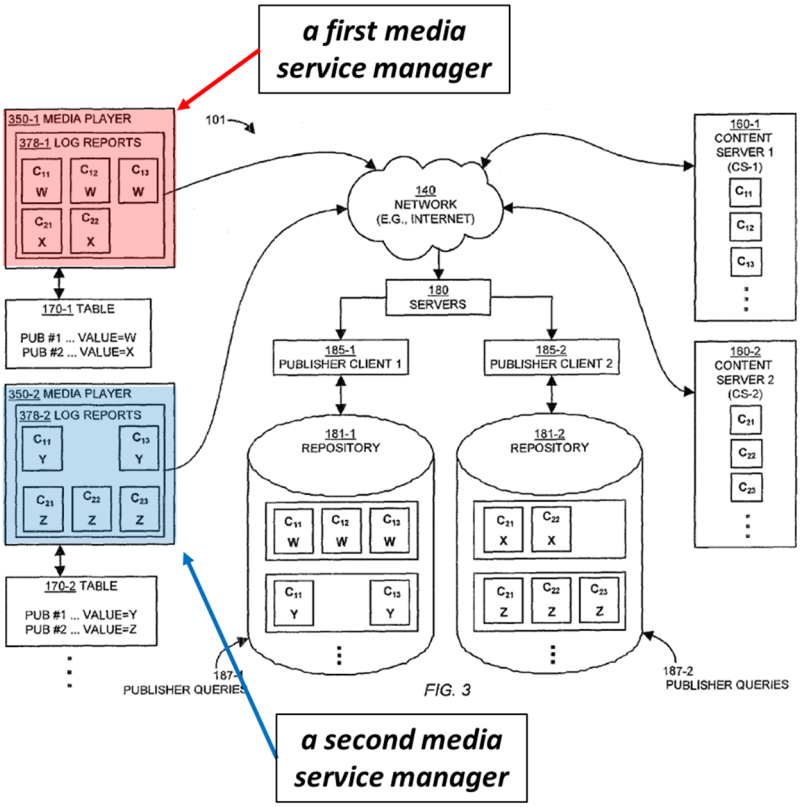


SAMSUNG-1041, FIG. 3 (as modified by Vadde and Riggs).

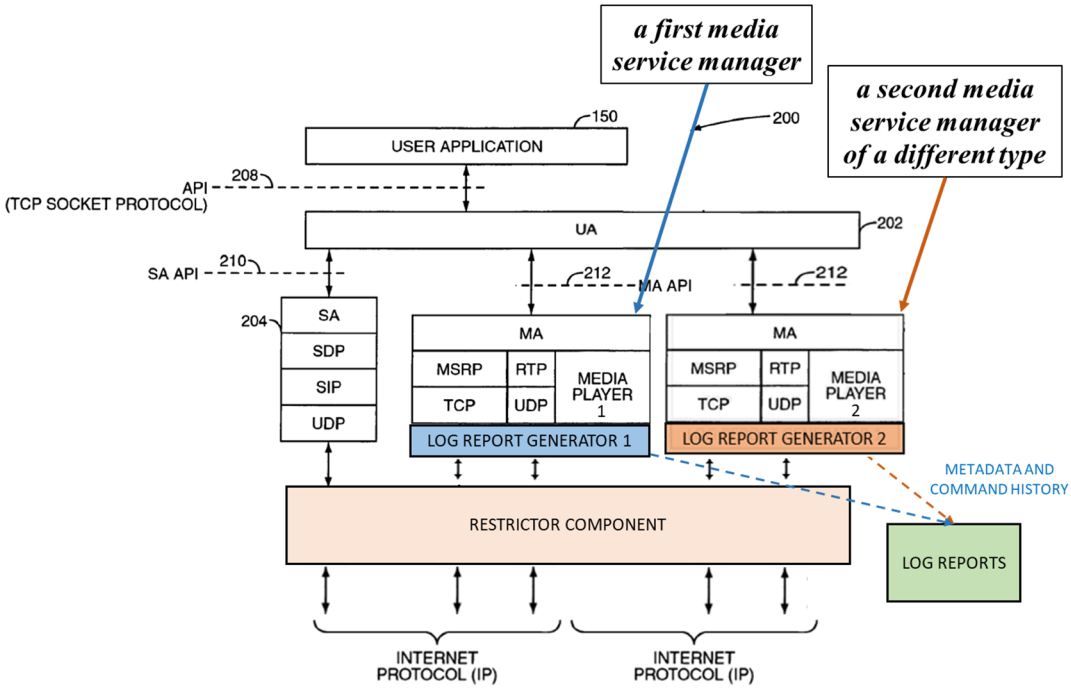
[6] The wireless end-user device of claim 5, wherein the media service manager is a first media service manager and the requesting application storing function is a first requesting application storing function, the device further comprising a second media service manager of a different type than the first media service manager, the service classification agent including a second requesting application storing function within the second media service manager.

89. Riggs discloses that its techniques can be implemented on multiple media players "350-1" and "350-2" ("***a first media service manager [and] … a second media service manager of a different type than the first media service manager***") that each include "log reports" from a respective "log report generator" ("***a first requesting application storing function [and] … a second requesting***

application storing function within the second media service manager"). SAMSUNG-1043, 11:54-13:46. Additionally, Riggs demonstrates that these two media players are "***of a different type***," at least because each of media players 350-1 and 350-2 generate log reports using different "unique values." *Id*.



SAMSUNG-1043, FIG. 3.



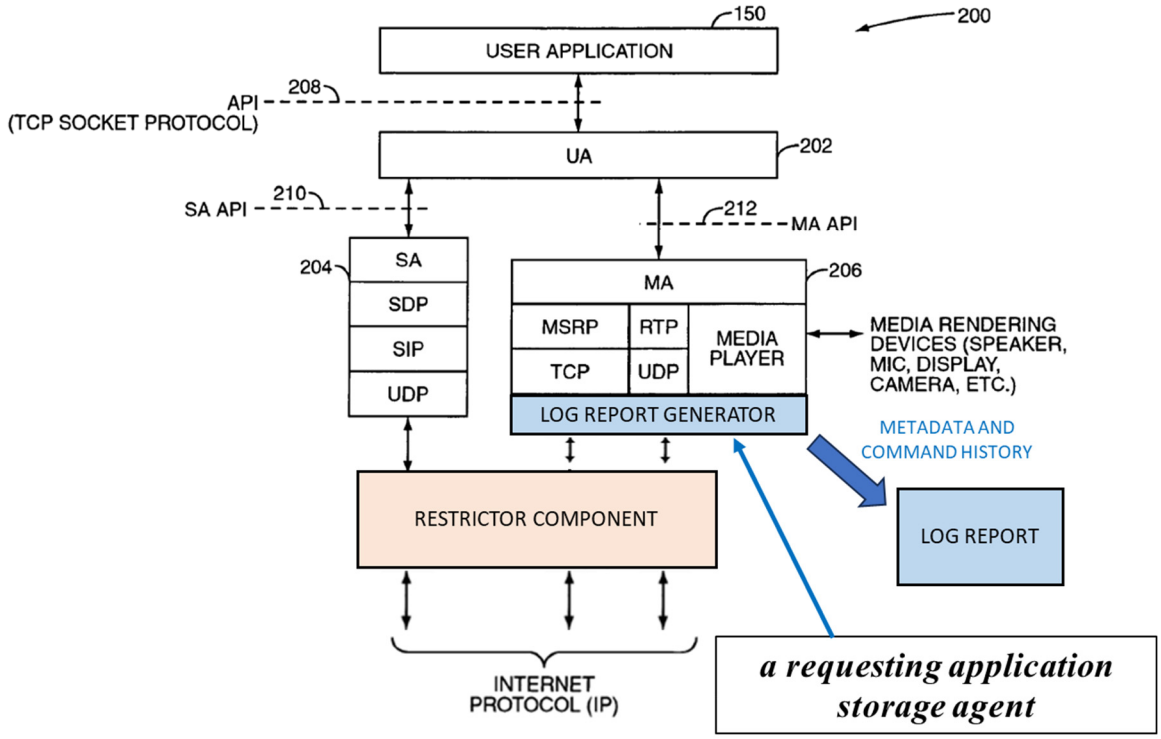
SAMSUNG-1041, FIG. 3 (as modified by Vadde and Riggs).

90. Although Riggs does not explicitly disclose that media players 350-1 and 350-2 are operating on the same device, Riggs does not otherwise exclude or disparage this arrangement. *See generally*, SAMSUNG-1043. Additionally, Bennett describes that its media client includes "one <u>or more</u> media players," and a POSITA would have understood and found obvious that the Bennett-Vadde-Riggs device would have included multiple media players, at least because Riggs describes that media players can be embodied in "browsers" (a plurality of which can operate on the same device simultaneously). SAMSUNG-1041, ¶[0025]; SAMSUNG-1043, 1:13-24, 1:58-62, 5:33-38. Further, the use of two or more media agents in the Bennett device would have enabled simultaneous transmission and reception of media over different protocols, for example, "MSRP" and "RTP" (e.g., MSRP text

communications during an active RTP stream). SAMSUNG-1041, ¶¶[0053]-[0054], [0066], [0072].

[11.1]The wireless end-user device of claim 1, wherein the one or more service classification and measurement agents comprise: a requesting application storage agent to, for each device application that makes a data transfer request using the second API, store application identification information and network resource identification information;

91. *See above*, [4], [5]. As described above, Riggs's "log report generator" ("***a requesting application storing agent***") generates a "log report" of metadata associated with played content ("***store application identification information and network resource identification information***"). SAMSUNG-1043, 1:58-2:5, 6:32-45, 10:13-23, 11:18-31, 16:28-33, FIG. 2. In the combination, metadata and data usage data is stored for "***each device application that makes a data transfer request using the second API,***" at least because Vadde's techniques of data monitoring are performed for each application. SAMSUNG-1042, ¶¶[0022], [0024]-[0026], [0029]-[0032]; *see above* §VIII.A.[1.6].



SAMSUNG-1041, FIG. 3 (as modified by Vadde and Riggs).

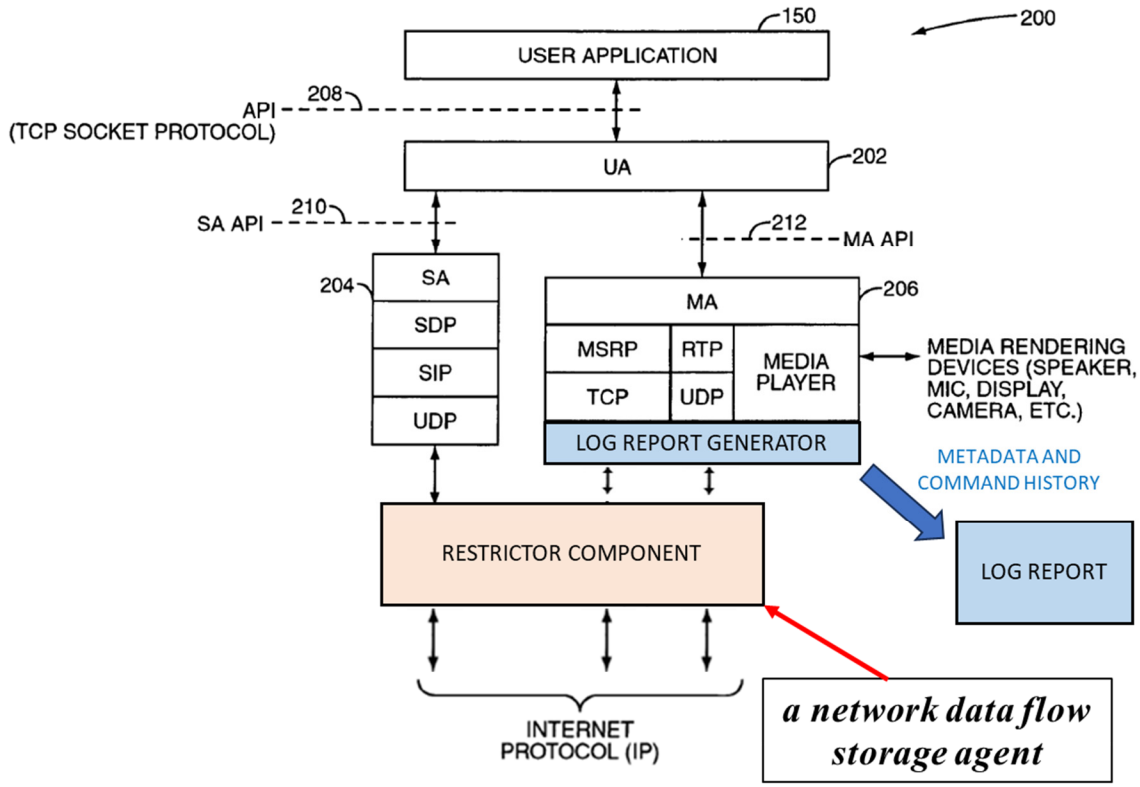
[11.2]a network data flow storage agent to, for each network data flow associated with the media service manager, identify network data flow identification information; and

92. The '918 Patent describes that "network data flow identifiers" include "a data flow tag, an IP address, a TCP-IP identifier, a layer 7 identifier, a socket tuple, etc." SAMSUNG-1001, 113:3-9.

93. As described above, Vadde's "restrictor component" ("***a network data flow storage agent***") "monitors the data transmitted and/or received by the applications 110" for "attributes 112" ("***identify network data flow identification information***") that include, among other things, a "network destination" and "port" ("***network data flow identification information***"). SAMSUNG-1042, ¶¶[0022],

[0024]. Additionally, Bennett's requests include "a network address of a remote host from which media connections will be accepted," for example, a "fully qualified network address" (e.g., an IP address—"***network data flow identification information***"). SAMSUNG-1041, ¶¶[0034], [0050]-[0056], Table-3; *see above* §VIII.A.[1.4].

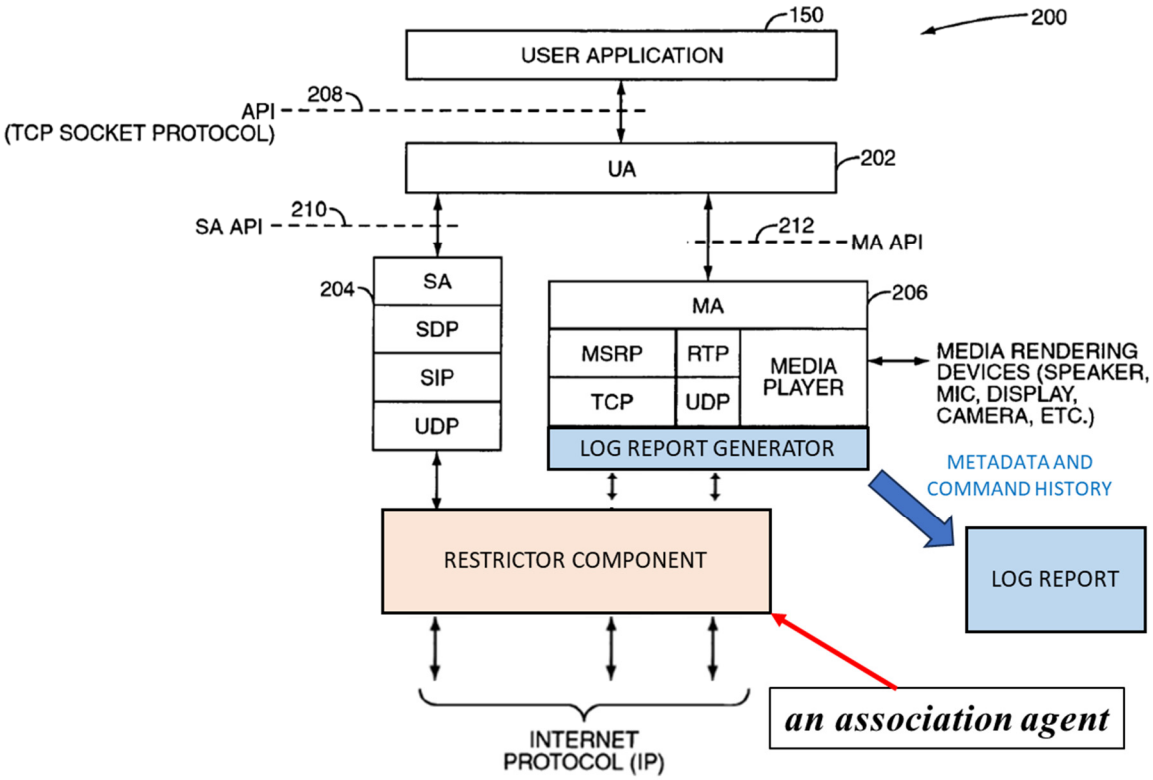
94. Additionally, as described above, because the restrictor component monitors data transmitted for each application, it monitors "***each network data flow associated with the media service manager***." SAMSUNG-1042, ¶[0016]; *see above* §VIII.A.[1.6].



SAMSUNG-1041, FIG. 3 (as modified by Vadde and Riggs).

[11.3]an association agent to match the network data flow identification information for a network data flow with application identification information for the network data transfer associated with the network data flow.

95. As described above, Vadde's "restrictor component" ("***an association agent")*** "monitors the data transmitted and/or received by the applications 110" for "attributes 112." SAMSUNG-1042, ¶¶[0022], [0024]; *see above* §VIII.A.[1.6]. A POSITA would have recognized and found obvious that Vadde's restrictor component would have "***match[ed] the network data flow identification information for a network data flow***" to "***application identification information associated with [that] network data flow***," at least because Vadde's restrictor component is already capable of distinguishing per-application usage and this matching would have been needed to produce useful data usage and metadata patterns for each application. SAMSUNG-1042, ¶¶[0016], [0022]. Specifically, Vadde's policies are intended to control the usage of a <u>particular</u> application based on that <u>particular</u> application's data usage, and therefore, "***data flow[s]***" and "***application identification information"*** would have been obvious to have been "***match[ed]***" to the corresponding application. *Id*.



SAMSUNG-1041, FIG. 3 (as modified by Vadde and Riggs).

Claims 15-17

96. The below claims are rendered obvious for similar reasons as discussed in the analysis for the corresponding claim listed in the table below.

Claim	Corresponding Claim
15.pre	1.pre
15.1	1.1
15.2	1.2
15.3	1.3
15.4	1.4, 3

Claim	Corresponding Claim
15.5	1.5
15.6	1.6, 2, 4
16	5
17	6

C. Claims 7, 12, and 18 are obvious over Bennett in view of Vadde, Riggs, and Hendrickson.

[7] The wireless end-user device of claim 6, further comprising a usage and classification database, the one or more service classification and measurement agents to receive application association information stored by the first and second requesting application storing functions, and to maintain the usage and classification database based in part on the received application association information.

97. The '918 Patent does not define a "***usage and classification database***" but rather describes that "the results of the service usage classification or accounting can be stored in a local device (or operating system) database" and that the stored information "can be provided to other applications, operating system service functions, other device software functions, or network-based service classification or accounting functions." SAMSUNG-1001, 113:46-55.

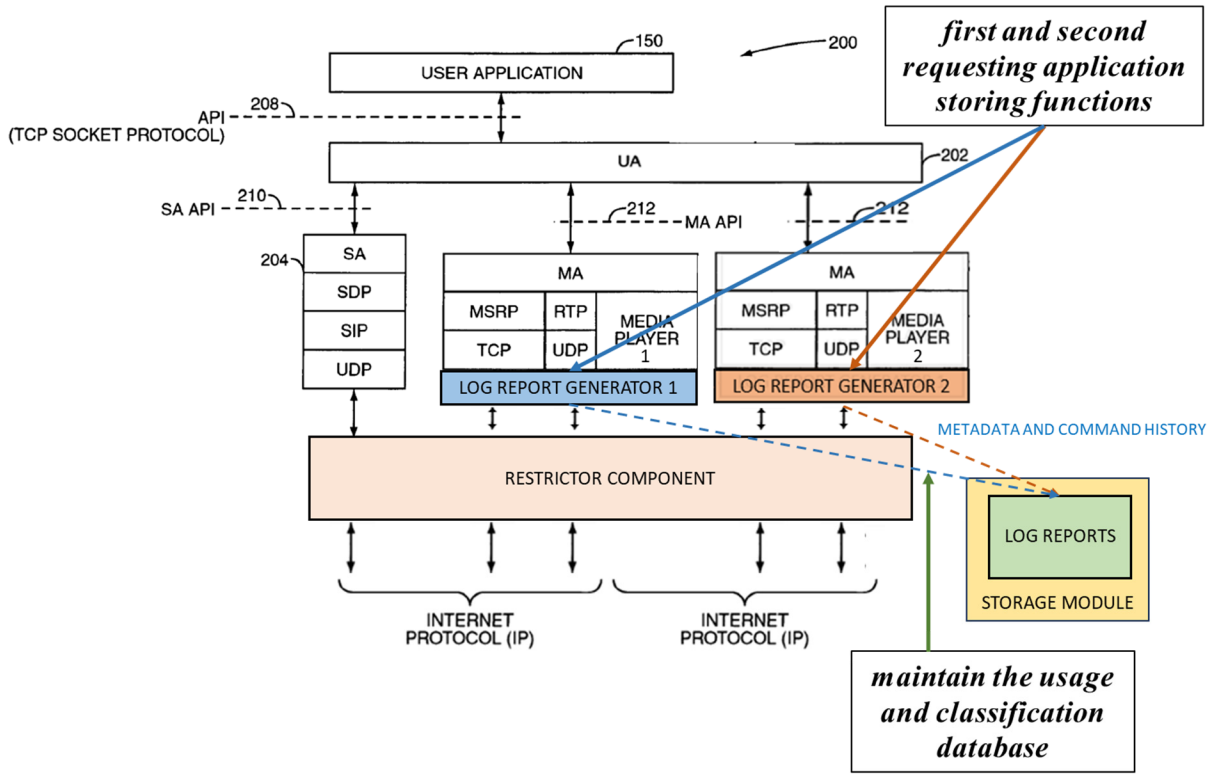
98. As described above, Riggs' "log report generators" ("***first and second requesting application storing functions***") generate "log reports" of "metadata" associated with content played on a media player ("***application association information***"). SAMSUNG-1043, 1:58-2:5, 6:32-45, 10:13-23, 11:18-31, 16:28-33,

FIG. 2; *see above* [4], [6]. As described above, Riggs' log report generators are "***one or more service classification and measurement agents***" and thus "***receive application association information stored by the first and second requesting application storing functions***." *See above*, §§VIII.B.[5].

99. A POSITA would have recognized and found obvious that the generated log reports would have been stored in a local repository on the device ("***usage and classification database***"), at least because this storage would have been needed to preserve the data across device operating cycles in the absence of a network connection. SAMSUNG-1054, 12:29-42. Moreover, the Bennet-Vadde-Riggs device would have included a means for electronic storage of files, like log reports. SAMSUNG-1041, ¶[0029] ("[t]he host device includes memory in which to store code implementing the present invention"); SAMSUNG-1042, ¶¶[0011]-[0014], [0017] (describing a device "memory area 108"); SAMSUNG-1043, 14:37-15:2, FIG. 4 (describing a "computer system" with a "memory system 112").

100. To the extent that a POSITA would not have found it obvious that Rigg's log reports are stored locally on the device prior to transmission, Hendrickson discloses a "storage module 265" ("***usage and classification database***") on a mobile device as part of a system for measuring "usage and performance metrics" for applications operated on the mobile device. SAMSUNG-1054, 6:40-7:11, 12:29-42, FIG. 2. The storage module 265 is responsible for "collecting information from each

data module and encrypting, compressing, and storing the data in log file format in the non-volatile memory locations of the wireless device" and "temporarily stor[ing] data before being handled by the Data Transfer Module" which transmits the collected data (a "***usage and classification database***" that stores data "local[ly]" such that data "can be provided to other applications, operating system service functions, other device software functions, or network-based service classification or accounting functions"). SAMSUNG-1054, 12:29-42; SAMSUNG-1001, 113:46-55. In the combination, the storage module 265 would have stored log reports generated by the Bennett-Vadde-Riggs log report generators, prior to these reports being transmitted for external consumption ("***maintain the usage and classification database based in part on the received application association information***"). SAMSUNG-1043, 1:58-2:5, 6:32-45, 10:13-23, 11:18-31, 16:28-33, FIG. 2; SAMSUNG-1054, 12:29-42 (noting that storing data is prudent when "there is no network connection available to transmit" or "immediate transfer of data would result in a poor user experience"); *see above* §§VII.B.[4]-[6].

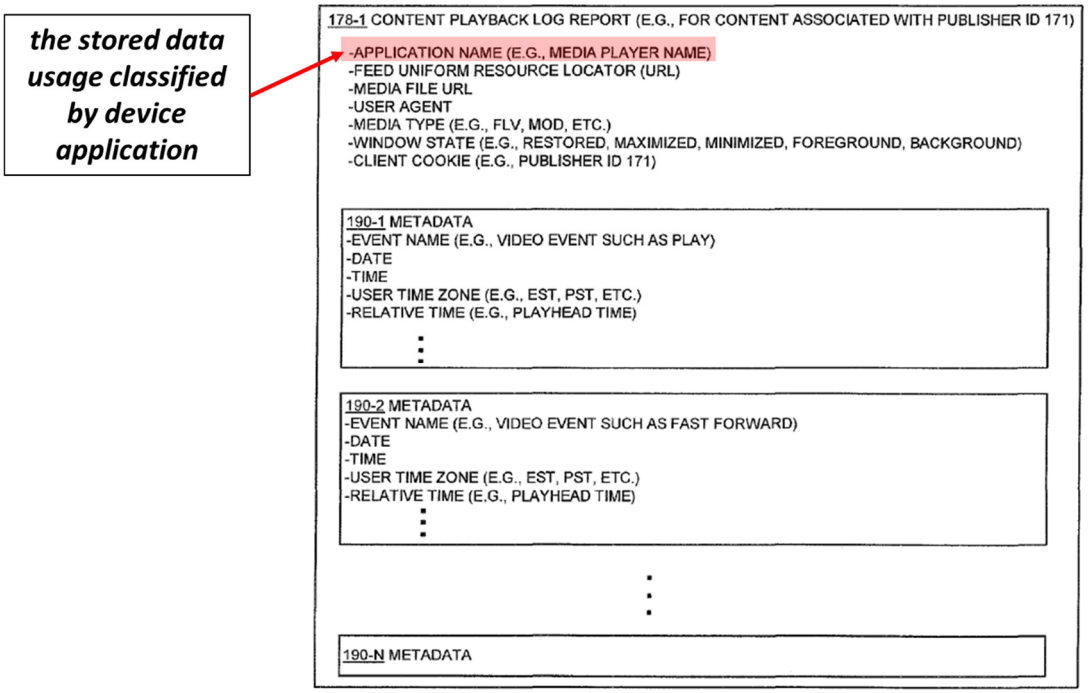


SAMSUNG-1041, FIG. 3 (as modified by Vadde, Riggs, and Hendrickson).

[12.1] The wireless end-user device of claim 1, further comprising: a local database to store data usage, including data usage for network data transfers managed by the media service manager on behalf of a device application, the stored data usage classified by device application;

101. As described above, a POSITA implementing the Bennett-Vadde-Riggs combination would have recognized and found obvious that Rigg's log reports would have been a convenient way to log data usage determined from Vadde's restrictor component. *See above*, §VII.E. In the combination, Riggs' log report generators generate log reports which are then stored in Hendrickson's "storage module 265" ("***a local database to store data usage***") which stores a record of

metadata and data usage associated with played content for each application ("***data usage for network data transfers managed by the media service manager on behalf of a device application***"). SAMSUNG-1043, 1:58-2:5, 6:32-45, 10:13-23, 11:18-31, 16:28-33, FIG. 2; *see above* [7]. Additionally, both Vadde and Riggs disclose that this information is "***classified by device application***" (particularly, using an application name or Program ID). SAMSUNG-1042, ¶[0014]; SAMSUNG-1043, 11:18-31.



SAMSUNG-1043, FIG. 2.

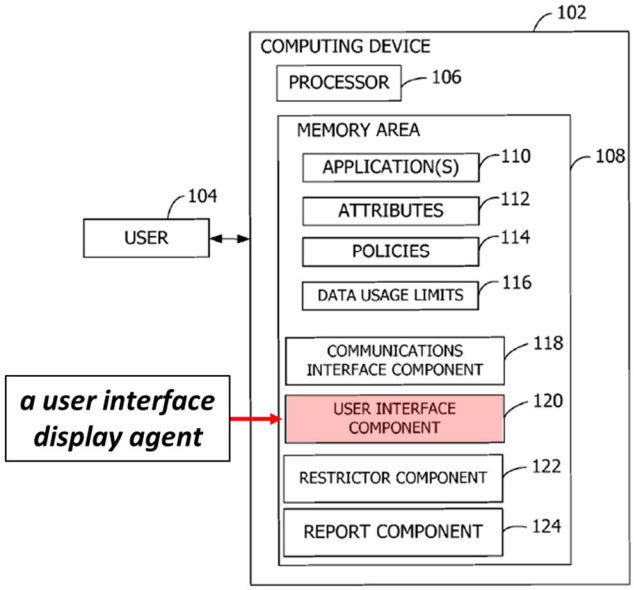
[12.2]a user interface; and

102. This claim limitation is obvious for the reasons discussed above. *See above*, §VIII.A.[9].

[12.3]a user interface display agent to display the data usage classified by application to a user.

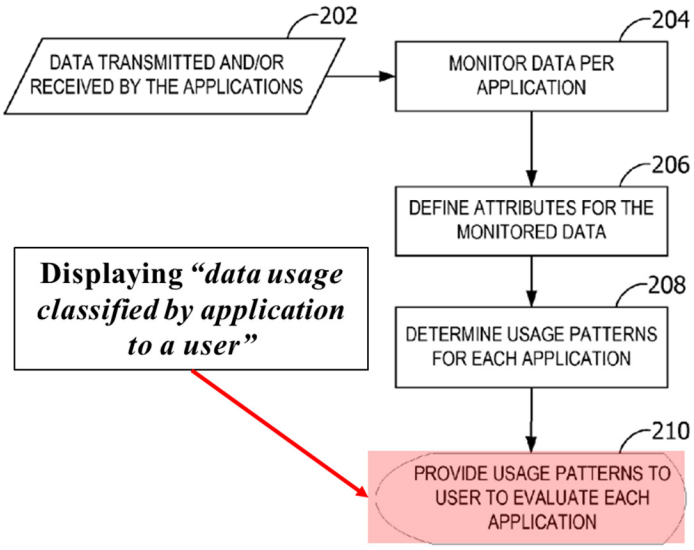
103. Vadde discloses a "user interface component 120" ("***a user interface display agent***") that is used for "displaying data to the user" ("***display the data usage classified by application to a user***"). SAMSUNG-1042, ¶[0021], FIG. 1. In the Bennett-Vadde-Riggs-Hendrickson combination, generated log reports for each application—including metadata and data usage—would have been displayed to the user via the "user interface component 120" and a "user interface" ("***the data usage classified by application to a user***"). Displaying log reports to the user would have enabled the user to monitor their per-application data usage and Vadde specifically notes that "usage patterns" (including data usage) are provided to the user "to evaluate each application" ("***the data usage classified by application to a user***"). SAMSUNG-1042, FIG. 2. Displaying log reports to the user would have also been a convenient way for the user to verify what information was being shared with publishers (particularly because Riggs discloses the need to obtain a user's "consent" before sharing data). SAMSUNG-1043, 1:39-48, 14:27-36.

FIG. 1



SAMSUNG-1042, FIG. 1.

FIG. 2



SAMSUNG-1042, FIG. 2.

[18] The wireless end-user device of claim 17, further comprising a usage and classification reconciliation agent and usage and classification database, the usage and classification reconciliation agent to receive application association information stored by the first and second requesting application storing functions, and to maintain the usage and classification database based in part on the received application association information.

104. Claim 17 repeats the same features recited in claim 7 above, with the substitution of a "***usage and classification reconciliation agent***" for "***the one or more service classification and measurement agents***." *See above*, [7]. The '918 Patent does not define a "***usage and classification reconciliation agent***," but instead describes a "usage/classification reconciliation engine 3216" that "can track usage of [an] app, classify the app, and to the extent there is disagreement at different system locations, reconcile usage in accordance with rules." SAMSUNG-1001, 117:12-24.

105. As described above, Riggs' "log report generators" ("***first and second requesting application storing functions***") generate "log reports" which are then stored in Hendrickson's "storage module 265" ("***a usage and classification database***") which stores a record of "metadata" associated with played content ("***maintain the usage and classification database based in part on the received application association information***"). SAMSUNG-1043, 1:58-2:5, 6:32-45, 10:13-23, 11:18-31, 16:28-33, FIG. 2; *see above*, [7].

106. Vadde's restrictor component 122 "monitors the data transmitted and/or received by the applications 110 and determines whether the data usage limits

116 corresponding to each of the applications 110 have been exceeded or are about to be exceeded." SAMSUNG-1042, ¶¶[0022], [0024]-[0026], [0029]-[0032]. As described above, in the combination, log reports are generated based on metadata determined from Riggs' log report generators and usage data determined by Vadde's restrictor component, both of which determine this information for each application. *See above*, §§VIII.A.[1.6], VIII.A.[2], VIII.B.[4]. Accordingly, Riggs' log report generators, in combination with Vadde's restrictor component, are also a "***a usage and classification reconciliation agent***" that "***receive[s] application association information stored by the first and second requesting application storing functions***" and ***"maintain[s] the usage and classification database based in part on the received application association information***" at least because Riggs' log report generators receive data regarding application data usage for each application from Vadde's restrictor component. *See above*, §§VIII.A.[1.6], VIII.A.[2], VIII.B.[4]; SAMSUNG-1001, 117:12-24.

D. Claim 10 is obvious over Bennett in view of Vadde, Riggs, and Srikantan.

[10.1] The wireless end-user device of claim 9, the media service manager to receive, from the application launching the data transfer request, a network resource indicator that identifies the media object,

107. As described above, Bennett's "CALL requests," sent by the application ("***from the application launching the data transfer request***") to the UA 202 include "a network address of a remote host from which media

connections will be accepted" ("***a network resource identifier***"), and this information is forwarded to the MA 206 via an "OPEN request" ("the media service manager to receive"). SAMSUNG-1041, ¶¶[0034], [0050]-[0056], Table-3; *see above* §VIII.A.[1.4]. As discussed above, Riggs discloses that "the global address of content" ("***a network resource indicator that identifies the media object***") is "typically" provided "in the form of a Uniform Resource Locator (URL)" (e.g., a "feed URL"—"***the media object***"—provided by the requesting application). SAMSUNG-1043, 1:25-35, 5:54-62, 6:38-43; *see above* § VIII.A.[3].

[10.2]return to the application a media object handle descriptor,

108. Srikantan discloses that a "file track handle" ("***a media object handle descriptor***") is created when a client requests a media file (a "stream") stored on a server. SAMSUNG-1055, ¶¶[0008]-[0009], [0044]-[0046], [0051]-[0054], [0059], [0071], FIG. 2; SAMSUNG-1058, 3; SAMSUNG-1059, 3. In the Bennett-Vadde-Riggs-Srikantan combination, a POSITA would have recognized and found obvious that in response to the "OPEN request" of the UA 202, the MA 206 ("***the media service manager***") would have retrieved Srikantan's "file track handle" ("***a media object handle descriptor***") for the stream referenced in the network address of the OPEN request. SAMSUNG-1041, ¶¶[0034]-[0035], [0050]-[0056], [0086], Table-3. Once retrieved, the MA 206 would have

returned the file track handle ("***a media object handle descriptor***") to the UA 202 via the "OPEN response," which would then return the file track handle to the application via the "CALL response" ("***return to the application a media object handle descriptor***"). *Id*.

109. A POSITA would have leveraged the MA 206 to return the file handle of Srikantan to the application because this arrangement is consistent with the responsibilities of the MA 206, as disclosed in Bennett. For example, Bennett describes that the MA 206 "manages media connections" to include "Real-Time Transport Protocol (RTP)" sessions. SAMSUNG-1041, ¶¶[0025], [0034], [0054]-[0055]. Specifically, the OPEN request sent to the MA 206 is an instruction "to initiate an RTP session," and in response, the MA 206 retrieves information from the host ("the network address of the host and port opened for the RTP connection"). SAMSUNG-1055, ¶[0054]. Similarly, Srikantan describes that its media servers use "RTP (Real-Time Transport Protocol) to deliver the stream to the client." SAMSUNG-1055, ¶¶[0027], [0046], [0072]. A POSITA would have recognized that when establishing an RTP session with a host server, the MA 206 ("***the media service manager***") would have retrieved a file handle ("***media object handle descriptor***") for the requested stream, along with the "network address of the host and port," to share with the application streaming the file in the RTP session, such that the application could manipulate

the stream in the session while informing the hosting server of the applied commands (e.g., "pause," "rewind," or "fast-forward"). SAMSUNG-1041, ¶¶[0077], [0080], [0086], Table-3; SAMSUNG-1055, ¶¶[0024], [0029], [0060], [0073].

110. Further, this file handle would have been specifically "***return[ed] to the application***" because, as Bennett notes, "the user application 150 may want to receive the media stream" and, further, "the user application 150 can direct how media or messages are routed," to include specifying commands like "PAUSE" or "RESUME." SAMSUNG-1041, ¶¶[0076]-[0077].

[10.3]call a proxy service to perform one or more network data transfers comprising the media object,

111. Srikantan discloses a "media streaming server" ("***a proxy service***") that "is configured to stream QuickTime media and/or other forms of media, in a unicast or multicast mode, over a proprietary or publicly accessible network such as the Internet" ("***one or more network data transfers comprising the media object***"). SAMSUNG-1055, ¶¶[0027]-[0033], FIG. 1. Additionally, because Bennett's MA 206 "manages media connections" to include "Real-Time Transport Protocol (RTP)" sessions—the same RTP sessions Srikantan discloses its media streaming server maintains for streaming media—the MA 206 would "call" the media streaming server hosting the stream ("***a proxy service***") to "***perform one or more network data transfers comprising the media object***"

using an RTP session. SAMSUNG-1041, ¶¶[0025], [0034], [0054]-[0055]; SAMSUNG-1055, ¶¶[0027], [0046], [0072]; *see above* [10.2].

112. Additionally, a POSITA would have recognized and found obvious that Srikantan's "media streaming server" is "***a proxy service***" (such that the Bennett-Vadde-Riggs-Srikantan device "***calls a proxy service to perform one or more network data transfers comprising the media object***"), at least because Srikantan discloses that the media streaming server can "redirect to clients media that it receives from another entity, such as a live event, a video camera, a broadcast from another server (e.g., server 130)." SAMSUNG-1055, ¶¶[0025], [0032], [0039], FIG. 1. Srikantan discloses that in this mode, the media streaming server "acts as a client" when it receives content from another server to send to the requesting device, which is a mode of operation consistent with a "proxy," as this term is known in the industry. SAMSUNG-1056, 3-4 (describing a "proxy" as "an intermediate application program that acts as both a client and a server"); SAMSUNG-1057, 3 (describing that a "proxy" is "a device or program empowered to act for another").

[10.4]accept, from the application, commands associated with the media object handle descriptor, and

113. Bennett discloses that the MA 206 receives "requests to control the media stream, such as a PAUSE request to pause an active media stream, and a RESUME request to resume a paused media stream" ("***accept … commands***").

SAMSUNG-1041, ¶[0076]; SAMSUNG-1055, ¶¶[0024], [0029], [0060], [0073] (describing other examples of commands). A POSITA would have recognized and found obvious that these commands are issued "***from the application***" because Bennett describes, in the same paragraph discussing the above commands, that "the user application 150 can direct how media or messages are routed." SAMSUNG-1041, ¶[0077]. Generally speaking, the application is the interface between the user and the stream and, given that streaming commands like "pause" and "stop" are typically in response to user action, these commands would have typically originated "from the application" as a result of the user interacting with the application (e.g., a user wishing to pause a stream to step away from their device would have typically used application controls to do so). *See, e.g.*, SAMSUNG-1041, ¶¶[0024] (describing a "user application 150"), [0077].

114. Additionally, the "PAUSE" and "RESUME" commands of Bennett are "***associated with the media object handle descriptor***" at least because these commands are applied to the stream described by the "***media object handle descriptor***." SAMSUNG-1041, ¶¶[0034]-[0035], [0050]-[0056], [0086], Table-3; SAMSUNG-1055, ¶¶[0008]-[0009], [0044]-[0046], [0051]-[0054], [0059], [0071], FIG. 2; *see above* [10.2] (describing that a file track handle is created and shared for a stream once the stream is requested). Specifically, Srikantan discloses that, once a handle is created, each handle "includes methods to start, stop, pause

and otherwise control a media stream (e.g., in response to client commands)" (such that these "methods" are "***associated with the media object handle descriptor***"). SAMSUNG-1055, ¶[0073], FIG. 5.

[10.5]control playback of the media data by the media player based on the commands.

115. Bennett's PAUSE and RESUME commands control the media stream played by the MA 206's media player, and thus the MA 206 "***control[s] playback of the media data by the media player based on the commands***." SAMSUNG-1041, ¶¶[0077], [0080], Table-3. Srikantan similarly describes that commands are applied to retrieved streams to manipulate the content. SAMSUNG-1055, ¶¶[0024], [0029], [0060], [0073].

IX. CONCLUSION

116. For all the reasons I have noted in the foregoing paragraphs, claims 1-19 of the '918 Patent are obvious in view of the references discussed above.

117. 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
E301 CSE Building, PO Box 116120
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 . . . 11

II. RESEARCH AND CREATIVE SCHOLARSHIP **12**
- A. Thesis . . . 12
- B. Published Journal Papers (Refereed) . . . 12
- C. Published Books and Parts of Books . . . 14
- D. Edited Proceedings . . . 14
- E. Conference Presentations . . . 14
  - E.1. Conference Presentations with Proceedings (Refereed) . . . 14
  - E.2. Conference Presentations with Proceedings (Non-Refereed) . . . 20
  - E.3. Conference Presentations without Proceedings . . . 20
- F. Other . . . 20
  - F.1. Submitted Journal Papers . . . 20
  - F.2. Refereed Research Reports . . . 20
  - F.3. Software . . . 20
  - F.4. Published Papers (Non-Refereed) . . . 21
  - F.5. Books in Preparation . . . 21
  - F.6. Workshops and External Courses . . . 21
- G. Research Proposals and Grants (Principal Investigator) . . . 22
- H. Research Proposals and Grants (Contributor) . . . 24
- I. Research Honors and Awards . . . 25

III. SERVICE **27**
- A. Professional Activities . . . 27
  - A.1. Memberships and Activities in Professional Societies . . . 27
  - A.2. Conference Committee Activities . . . 27
- B. On-Campus Committees . . . 28
  - B.1. University of Florida . . . 28
  - B.2. Georgia Tech . . . 29
- C. Special Assignments . . . 29
- D. Ph.D. Examining Committees . . . 29
- E. External Member of M.S. Examining Committee . . . 33
- F. Consulting and Advisory Appointments . . . 33
- G. Civic Activities . . . 33

IV. NATIONAL AND INTERNATIONAL PROFESSIONAL RECOGNITION **34**
- A. Honors and Awards . . . 34
- B. Invited Conference Session Chairmanships . . . 34
- C. Professional Registration . . . 34
- D. Patents . . . 34
- E. Editorial and Reviewer Work for Technical Journals and Publishers . . . 35
- F. Expert Witness Services . . . 37

V. OTHER CONTRIBUTIONS **39**
- A. Seminar Presentations (Invited Papers and Talks at Meetings and Symposia) . . . 39

B. Special Activities 43

EDUCATIONAL BACKGROUND

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

EMPLOYMENT HISTORY

Title	Organization	Years
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 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

CS 8803 Cellular and Mobile Network Security: *Fall 2010.* 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 (GSM, 3G), 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 and receive a non-8803 number. 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.

CS 6262 Network Security: *Fall 2009.* 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.

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

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.

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.

Brad Reaves University of Florida
Fall 2014–Spring 2017
Develop strong authentication techniques for cellular networks. Now: Assistant Professor at North Carolina State University.

Nolen Scaife University of Florida
Fall 2014–Spring 2019
Developed techniques to detect credit card skimming. First: Assistant Professor at the University of Colorado Boulder. Now: Director, Global Cyber Intelligence at Walmart

Imani Sherman University of Florida
Fall 2018–Summer 2021
Developing usable interfaces against robocalls. Co-advised with Juan Gilbert. Now: Assistant Professor at the University of California, San Diego

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

Hadi Abdullah University of Florida
Fall 2016–Summer 2022
Evaluating the security of ML-driven voice interfaces. Now: Research Scientist at Visa Research

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

2. Ph.D. Students Supervised

Logan Blue University of Florida
Fall 2016–Present
Investigating facial feature reconstruction from voice recordings.

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

Cassidy Gibson University of Florida
Fall 2019–Present
Investigating weaknesses in web software.

Ryon Kennedy University of Florida
Fall 2020–Present
Finding vulnerabilities in cellular core networks via fuzzing.

Seth Layton University of Florida
Fall 2020–Present
Detecting deepfakes in audio samples.

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

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

Tyler Tucker University of Florida
Fall 2021–Present
Evaluating the security of Bluetooth/cellular radios.

Kevin Warren University of Florida
Fall 2019–Present
Detecting deepfake audio through linguistic information.

3. Ph.D. Students - Other

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

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

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

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

Frank Park Georgia Institute of Technology
Fall 2008–Spring 2010
Research on multi-factor authentication using cellular phones. Left program after failing comprehensive exam to join startup.

Ferdinand Schober Georgia Institute of Technology
Fall 2009–Summer 2010
Developed mechanisms for smart networks and smart mobile devices to fight infection and provide remote remediation. Returned to Microsoft.

4. M.S. Students Supervised

Chaitrali Amrutkar Georgia Institute of Technology
Fall 2008–Spring 2009
Research on improving performance of security critical functions in IMS cellular core. Completed her Ph.D with me at GT.

Logan Blue University of Florida
Fall 2015–Spring 2016
Investigated problems of cellular and network security.

David Dewey Georgia Institute of Technology
Fall 2009–Spring 2010
Research on security issues caused by transitive trust assumptions in the Windows COM infrastructure. Completed his Ph.D. with me at GT.

Christopher Grayson Georgia Institute of Technology
Fall 2012–Fall 2013
Developed continuous authentication mechanisms using the multitude of sensors available on a mobile phone. Now at Bishop Fox Consulting (industry).

Young Seuk Kim Georgia Institute of Technology
Fall 2012–Fall 2013
Performed research that compared the security vulnerabilities found in the traditional and mobile web.

Daniel Komaromy Georgia Institute of Technology
Fall 2008–Summer 2009
Research on building a real-time streaming audio system using attribute-based crypto for broadcast encryption.

Nigel Lawrence Georgia Institute of Technology
Fall 2011–Spring 2012
Discovered hijacking attacks in SNMPv3, a widely used and thought to be secure network management protocol. Now at Solute (industry).

Philip Marquardt Georgia Institute of Technology
Fall 2009–Present
Research on developing an iPhone application to prevent individuals from being profiled by Shopper Loyalty Programs. First with MIT Lincoln Labs, now Raytheon

Rishikesh Naik Georgia Institute of Technology
Fall 2008–Spring 2010
Research on converting expensive cryptographic primitives (e.g., Secure Function Evaluation) into efficient applications for mobile phones. Now with Cisco Systems.

Ashish Nautiyal CISE
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.

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 Scurity Challenges of Digital Financial Services. *IEEE S&P Magazine*, 15(5):85–89, 2017.

4. Nolen Sciafe, 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 Seurity (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 Presentations with Proceedings (Refereed)

1. 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.

2. 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.

3. 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.

4. 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.

5. 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%).

6. 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%).

7. 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%).

8. 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%).

9. 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.

10. 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 Comunications Information and Internet Policy (TPRC 49)*, 2021.

11. 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%).

12. 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%).

13. 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.

14. 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%).

15. 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 *Procedings of the ACM ASIA Conference on Computer and Communications Security (ASIACCS'19)*, 2019. (Acceptance Rate: 17.0% for full papers).

16. 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).

17. 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%).

18. 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%).

19. 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%).

20. 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%).

21. 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%).

22. 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%.

23. 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%.

24. 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%.

25. 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%).

26. 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%).

27. 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%).

28. 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%).

29. 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%).

30. 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%).

31. 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%).

32. 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%).

33. 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%).

34. 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%).

35. 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%).

36. 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%).

37. 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%).

38. 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%).

39. 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%).

40. 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%).

41. 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%).

42. 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%).

43. 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%).

44. 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%).

45. 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%).

46. 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).

47. 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%).

48. 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).

49. 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).

50. 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%).

51. 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%).

52. 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%).

53. 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%).

54. 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%).

55. 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%).

56. 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%).

57. Vijay Balasubramaniyan, Aamir Poonawalla, Mustaque Ahamad, Michael Hunter, and Patrick Traynor. PinDr0p: 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%).

58. 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%).

59. 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%).

60. 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%).

61. 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%).

62. 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%).

63. 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%).

64. 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%).

65. 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%).

66. 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%).

67. 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%).

68. 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%).

69. 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).

70. 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%).

71. 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%).

72. 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%).

73. 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%).

74. 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%).

75. 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%).

76. 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%).

77. 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%).

78. William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta. Exploiting Open Functionality in SMS-Capable Cellular Networks. In *Proceedings of the Twelfth ACM Conference on Computer and Communications Security (CCS)*, November 2005. (Acceptance Rate: 15%).

Removed for external version.

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

None.

E.3. Conference Presentations without Proceedings

1. Patrick Traynor. Work in Progress Presentations: Fine-Grained Secure Localization for 802.11 Networks. 15th USENIX Security Symposium (SECURITY), August 2006.

2. Patrick Traynor. Work in Progress Presentations: Fundamental Limitations of Sensor Network Security. ACM/USENIX Fourth International Conference on Mobile Systems Applications and Services (MobiSys), June 2006. (Award: Most Entertaining WIP).

3. Patrick Traynor, Heesook Choi, Guohong Cao, and Thomas La Porta. Poster Session: Probabilistic Unbalanced Key Distribution and Its Effects on Distributed Sensor Networks. Workshop on Wireless Security (WiSe), October 2004.

F. Other

F.1. Submitted Journal Papers

None.

F.2. Refereed Research Reports

None.

F.3. Software

1. *GSM Air Interface Simulator:* Developed a full voice, data and SMS capable simulator for the wireless portion of a GSM network. Models communications down to the timeslot for highest possible accuracy. Used in the majority of our work on cellular security.

2. *Malicious Telephony Load Tester:* Built a system on top of the TM1 Telecom Database testing suite to allow for a comparison of malicious traffic of varying composition.

F.4. Published Papers (Non-Refereed)

1. Patrick Traynor. Characterizing the Limitations of Third-Party EAS Over Cellular Text Messaging Services. Technical report, 3G Americas Whitepaper, 2008.

2. Lisa Johansen, Kevin Butler, William Enck, Patrick Traynor, and Patrick McDaniel. Grains of SANs: Building Storage Area Networks from Memory Spots. Technical Report NAS-TR-0060-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, 2007.

F.5. Books in Preparation

None.

F.6. Workshops and External Courses

1. Luis Vargas, Patrick Emami, and Patrick Traynor. On the Detection of Disinformation Campaign Activity with Network Analysis. In *Proceedings of the 2020 ACM SIGSAC Cloud Computing Security Workshop*, CCSW '20, 2020.

2. Siddhant Deshmukh, Henry Carter, Grant Hernandez, Patrick Traynor, and Kevin Butler. Efficient and Secure Template Blinding for Biometric Authentication. In *IEEE Workshop on Security and Privacy in the Cloud (SPC)*, 2016.

3. Debayan Gupta, Benjamin Mood, Joan Feigenbaum, Kevin Butler, and Patrick Traynor. Using Intel Software Guard Extensions for Efficient Two-Party Secure Function Evaluation. In *Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC)*, 2016.

4. Chaitrali Amrutkar and Patrick Traynor. Rethinking Permissions for Mobile Web Apps: Barriers and the Road Ahead. In *Proceedings of the ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, 2012.

5. Nigel Lawrence and Patrick Traynor. Under New Management: Practical Attacks on SNMPv3. In *Proceedings of the USENIX Workshop on Offensive Technologies (WOOT)*, 2012.

6. Andrew Harris, Frank S. Park, Seymour Goodman, and Patrick Traynor. Emerging Privacy Concerns for Digital Wallet Deployment. In *Proceedings of the Workshop on Making Privacy in America*, 2009.

7. Patrick Traynor. Privacy and Security Concerns for Personal and Mobile Health Devices. In *Proceedings of the Workshop to Set A Research Agenda for Privacy and Security of Healthcare Technologies*, 2009.

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

G. Research Proposals and Grants (Principal Investigator)

1. Approved and Funded

1. **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

2. **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

3. **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

4. **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

5. **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

6. **Workshop: Addressing the Technical Security Challenges of Emerging Digital Financal Services**
   Sponsor: NSF Secure and Trustworthy Cyberspace
   Investigator(s): Patrick Traynor (PI), Kevin Butler
   Amount: *$50,000 over 1 year*
   Awarded: September 2017

7. **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

8. **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

9. **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

10. **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

11. **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

12. **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

13. **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

14. **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

15. **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

16. **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

17. **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

18. **Characterizing and Mitigating Device-Based Attacks in Cellular Telecommunications Networks**
Sponsor: NSF Trustworthy Computing
Investigator(s): Patrick Traynor (PI) and Jonathon Giffin
Amount: *$450,000 over 3 years*
Awarded: July 2009

2. Pending

Removed for external version.

H. Research Proposals and Grants (Contributor)

1. Approved and Funded

1. **SaTC: Frontier: Securing the Future of Computing for Marginalized and Vulnerable Populations**
Sponsor: NSF SaTC
Investigator(s): Kevin Butler (PI), Patrick Traynor, Tadayoshi Kohno, Franzi Roesner, Apu Kapadia, Eakta Jain.
Amount: *$7,500,000 for 5 years*
Awarded October 2022

2. **ROCKY: Reliable Obfuscated Communications Kit for everYone**
Sponsor: DARPA Resilient Anonymous Communication for Everyone (RACE) – Broad Agency Announcement
Investigator(s): Thomas Shrimpton (PI), Patrick Traynor, Kevin Butler, Vincent Bindschaedler, Nadia Heninger
Amount: *$1,600,000 over 4 years*
Awarded May 2019

3. **WiFiUS: Collaborative Research: SELIOT: Securing Lifecycle of Internet-of-Things**
Sponsor: NSF CNS WiFiUS
Investigator(s): Gene Tsudik (PI), Patrick Traynor
Amount: *$300,000 for 2 years*
Submitted December 2016

4. **Cloud-based Oblivious Spectrum Mapping and Allocation**
Sponsor: NSF CNS EARS
Investigator(s): John Shea (PI), Tan Wong, Patrick Traynor
Amount: *$532,952 for 2 years*
Submitted May 2016

5. **DURIP: Developing Research Capability in Cyber-Physical Systems at the University of Florida**
Sponsor: Small
Investigator(s): Kevin Butler (PI), Patrick Traynor, My Thai
Amount: *$200,000 for 2 years*
Submitted: June 2015

6. **Securing the New Converged Telephony Landscape**
Sponsor: NSF TWC: Small
Investigator(s): Mustaque Ahamad (PI) and Patrick Traynor
Amount: *$500,000 for 3 years*
Submitted: December 2012

7. **Facilitating Free and Open Access to Information on the Internet**
   Sponsor: NSF Trustworthy Computing
   Investigator(s): Nick Feamster (PI), Wenke Lee, Patrick Traynor, Hans Klein, Roger Dingledine, Michael Freedman and Edward W. Felten
   Amount: *$1,500,000 for 4 years*
   Awarded: June 2011

8. **Monitoring Free and Open Access to Information on the Internet**
   Sponsor: Google Focus Program
   Investigator(s): Nick Feamster (PI), Wenke Lee, Mustaque Ahamad, Patrick Traynor, Henry Owen, Ellen Zegura, Zvi Galil
   Amount: *$1,000,000 for 2 years*
   Awarded: November 2011

9. **Dynamic-attribute-based Disclosure of Health Information in Emergency Care Scenarios**
   Sponsor: Health Systems Institute (HSI) Seed Grant Program
   Investigator(s): Doug Blough (PI), Mustaque Ahamad, Patrick Traynor and Jim Jose
   Amount: *$50,000 over 1 year*
   Awarded: August 2009

10. **Federal Cyber Service Scholarships at Georgia Tech**
    Sponsor: NSF SFS Scholarships
    Investigator(s): Seymour Goodman (PI), Patrick Traynor
    Amount: *$1,250,682 over 5 years*
    Awarded: June 2009

11. **Security for IMS-Enabled Converged Applications**
    Sponsor: US Department of Defense
    Investigator(s): Mustaque Ahamad (PI), Patrick Traynor (PI), Michael Hunter, Russ Clark
    Amount: *$146,121 for 1 year*
    Awarded: August 2008

2. Pending

Removed for external version.

I. Research Honors and Awards

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

9. Pennsylvania State University Alumni Association Dissertation Award, 2007
10. Pennsylvania State University CSE Graduate Research Assistant Award, 2007
11. AT&T Wireless Fellowship, 2005

III. SERVICE

A. Professional Activities

A.1. Memberships and Activities in Professional Societies

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

A.2. Conference Committee Activities

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

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

B. On-Campus Committees

B.1. University of Florida

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

B.2. Georgia Tech

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

C. Special Assignments

None.

D. Ph.D. Examining Committees

Ph.D. Examining Committees

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

9. Manos Antonakakis, College of Computing, Georgia Tech, Summer 2012.
   Advisor: Professor Wenke Lee.

10. Junjie Zhang, College of Computing, Georgia Tech, Summer 2012.
    Advisor: Professor Wenke Lee.

11. Italo Dacosta, College of Computing, Georgia Tech, Summer 2012.
    Advisor: Professor Patrick Traynor.

12. Virendra Kumar, College of Computing, Georgia Tech, Summer 2012.
    Advisor: Professor Alexandra Boldyreva.

13. Anirudh Ramachandran, College of Computing, Georgia Tech, Summer 2011.
    Advisor: Professor Nick Feamster.

14. Vijay Balasubramaniyan, College of Computing, Georgia Tech, Summer 2011.
    Advisor: Professor Mustaque Ahamad.

15. Kapil Singh, College of Computing, Georgia Tech, Summer 2011.
    Advisor: Professor Wenke Lee.

16. Abhinav Srivastava, College of Computing, Georgia Tech, Summer 2011.
    Advisor: Professor Jon Giffin.

17. Adam O'Neill, College of Computing, Georgia Tech, Summer 2010.
    Advisor: Professor Alexandra Boldyreva.

18. David Cash, College of Computing, Georgia Tech, Fall 2009.
    Advisor: Professor Alexandra Boldyreva.

External Member of Ph.D. Research Committee

None.

External Member of Ph.D. Examining Committee

1. Shannon Eggers, Department of Materials Sciences and Engineering - Nuclear Engineering Program, University of Florida, Fall 2016.
   Advisor: Professor Kelly Jordan.

2. Ed Carlisle, Department of Electrical and Computer Engineering, University of Florida, Summer 2016.
   Advisor: Professor Alan George.

3. Claudio Marforio, Department of Computer Science, Swiss Federal Institute of Technology Zurich (ETH Zurich), Fall 2015.
   Advisor: Professor Srdjan Capkun.

4. Nils Ole Tippenhauer, Department of Computer Science, Swiss Federal Institute of Technology Zurich (ETH Zurich), Spring 2012.
   Advisor: Professor Srdjan Capkun.

5. Bongkyoung Kwon, School of Electrical and Computer Engineering, Georgia Tech, Summer 2009.
   Advisor: Professor John Copeland.

Ph.D. Thesis Proposal Committees

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

Ph.D. Qualifying Exam Committees—Georgia Tech

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

3. Xinyu Xing, College of Computing, Georgia Tech, Spring 2013.
   Advisor: Professor Wenke Lee.

4. Brad Reaves, College of Computing, Georgia Tech, Spring 2013.
   Advisor: Professor Patrick Traynor.

5. Chaz Lever, College of Computing, Georgia Tech, Spring 2013.
   Advisor: Professor Patrick Traynor.

6. Terry Nelms, College of Computing, Georgia Tech, Spring 2012.
   Advisor: Professors Mustaque Ahamad and Roberto Perdesci.

7. Saurabh Chakradeo, College of Computing, Georgia Tech, Spring 2012.
   Advisor: Professor Patrick Traynor.

8. Henry Carter, College of Computing, Georgia Tech, Spring 2012.
   Advisor: Professor Patrick Traynor.

9. David Dewey, College of Computing, Georgia Tech, Spring 2012.
   Advisor: Professor Jon Giffin.

10. Chaitrali Amrutkar, College of Computing, Georgia Tech, Fall 2011.
    Advisor: Professor Patrick Traynor.

11. Yacin Nadji, College of Computing, Georgia Tech, Fall 2011.
    Advisor: Professor Wenke Lee.

12. Yogesh Mundada, College of Computing, Georgia Tech, Fall 2011.
    Advisor: Professor Nick Feamster.

13. Hyojoon Kim, College of Computing, Georgia Tech, Fall 2011.
    Advisor: Professor Nick Feamster.

14. Ikpeme Erete, College of Computing, Georgia Tech, Spring 2011.
    Advisor: Professor Alex Orso.

15. Chaitrali Amrutkar, College of Computing, Georgia Tech, Spring 2011.
    Advisor: Professor Patrick Traynor.

16. Brendan Dolan-Gavitt, College of Computing, Georgia Tech, Spring 2011.
    Advisor: Professor Wenke Lee and Professor Jon Giffin.

17. Sam Burnett, College of Computing, Georgia Tech, Fall 2010.
    Advisor: Professor Nick Feamster.

18. Cong Shi, College of Computing, Georgia Tech, Fall 2010.
    Advisor: Professor Mostafa Ammar and Professor Ellen Zegura.

19. Partha Kanuparthy, 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. *Epic Games, Inc. & Anor v Google LLC & Ors - Federal Court of Australia Proceeding NSD 190 of 2021:* Expert witness for the Defense (via Corrs Chambers Westgarth). Status: Ongoing. *January 2023 - Present*.
2. *Telefonaktiebolaget LM Ericsson vs Apple, Inc:* Expert witness for the Defendant, Non-Infringement and Invalidity (via WilmerHale LLP). Status: Settled. *February 2022 - December 2022*.
3. *Wepay Global Payments, LLC v. Bank of America N. A.,:* Expert Witness for the Defendant (via WilmerHale LLP) Status: Dismissed. *September 2022 - November 2022*.
4. *Apple vs. R.N Nehushtan Trust Ltd.:* Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Status: Submitted to PTAB. *August 2022 - Ongoing*.
5. *Apple/Microsoft vs. Zipit Wireless:* Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Status: Settled. *May 2021 - November 2022*.
6. *Blackberry Inc v MobileIron, Inc:* Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Verdict: Settled. *January 2021 - March 2021*.
7. *Apple Inc v Seven Networks, LLC:* Expert Witness for the Plaintiff for Inter Partes Review (via Fish & Richardson, LLP). Verdict: Three of four petitions instituted by PTAB. Fourth rejected via discretion, case settled. *August 2019 - November 2020*.
8. *mSIGNIA, Inc. v. InAuth, Inc.:* Expert Witness for the Defendant for Inter Partes Review, Non-Infringement and Invalidity (via Quinn Emanuel Urquhart and Sullivan, LLP). Verdict: Dismissed with prejudice. *October 2017 - December 2018*.
9. *Huawei v. T-Mobile:* Expert Witness for the Defendant for Non-Infringement (via WilmerHale LLP, Alston & Bird LLP) Verdict: Settled *June 2016 - December 2017*.
10. *Telefonaktiebolaget LM Ericsson v Apple:* Expert Witness for the Defendant for Non-Infringement, Invalidity (via WilmerHale LLP). Verdict: Settled *June 2015 - December 2015*.
11. *Mayfonk v Nike:* Expert Witness for the Plaintiff for Infringement (via Paul Hastings). Verdict: Settled. *June 2015 - November 2015*.

12. *Maxim Integrated Products v Bank of the West:* Expert Witness for the Defendant for Non-Infringement (via Paul Hastings LLP). Verdict: Dismissed with prejudice. *January 2014 - August 2014.*

13. *Maxim Integrated Products v Comerica Inc, et al:* Expert Witness for the Defendant for Non-Infringement (via McKenna, Long & Aldridge LLP). Verdict: Settled. *June 2014 - August 2014.*

14. *William Grecia v. Apple Inc. et al:* Expert Consultant for the Defendant for Invalidity (via Kirkland & Ellis LLP). Verdict: Closed in initial pleadings, dismissed with prejudice. *July 2014 - August 2014.*

15. *Intertrust Technologies Corp. v. Apple Inc.:* Expert Consultant for Defendant for Invalidity and Non-Infringement (via Kirkland & Ellis LLP). Verdict: Settled. *October 2013 - February 2014.*

16. *Maxim Integrated Products v KeyCorp Bank:* Expert Witness for the Defendant for Non-Infringement (via Calfee, Halter & Griswold LLP) Verdict: Settled. *April 2013 - June 2013.*

17. *Intellectual Ventures LLC vs. Check Point; et al.:* Expert Consultant for the Plantiff for Infringement (via Susman Godfrey LLP), Verdict: Infringement on 2 of 4 patents. *October 2012 - February 2015.*

V. OTHER CONTRIBUTIONS

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

1. Keynote: Well, It Worked on My Computer: Reproducibility, 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.

2. 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.

3. 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.

4. The State of Voice Cloning Technology. Federal Trade Commission (FTC) Workshop on Voice Cloning Technologies, January 2020. Washington, DC.

5. 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.

6. 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.

7. 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.

8. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. Bank of America - Colloquium Series, March 2019. Charlotte, NC.

9. 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.

10. Because That's Where the Money Is: Designing Defenses for Entrenched Legacy Payment Systems. University of Maryland - Distinguished Colloquium, February 2019. College Park, MD.

11. Responsible Finance for the Digital Client. Foromic Conference, October 2018. Barranquilla, Colombia.

12. Panel: Authentication Challenges for New Interfaces, Devices, and Wireless Networks. ACM Conference on Security and Privacy in Wireless and Mobile Networks, June 2018. Stockholm, Sweeden.

13. Sonar: Detecting SS7 Redirection Attacks Via Call Audio-Based Distance Bounding. CyberSecurity@KAIST Workshop - KAIST, June 2018. Daejon, South Korea.

14. 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.

15. Panel: The Future of Cybersecurity. SEC Academic Conference - Auburn University, May 2018. Auburn, AL.

16. Sound Principles: Verifying Voice Commands in an IoT World. IoT Security Workshop - Aalto University, September 2017. Helsinki, Finland.

17. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Eurecom Institute, September 2017. Sophia Antipolis, France.

18. Panel: Infrastructure Stability. ITU-T Focus Group Digital Financial Services, December 2016. Geneva, Switzerland.

19. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. ETH Zurich, December 2016. Zurich, Switzerland.

20. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. University of Richmond, October 2016. Richmond, Virginia.

21. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Indiana University, September 2016. Bloomington, Indiana.

22. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. Aalto University Computer Science Department Forum, August 2016. Helsinki, Finland.

23. 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.

24. Updated Mobile Money Vulnerability Report. International Telecommunications Union Digital Financial Services Working Group Workshop, May 2016. Washington, DC.

25. Who Do I Think You Are? Challenges and Opportunities in Telephony Authentication. UF Eye Opener Discovery Breakfast - University of Florida, May 2016. Gainesville, FL.

26. 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.

27. 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.

28. 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.

29. Chasing Telephony Security: Where the Wild Things... Are? University of Florida - Department Colloquium, January 2014. Gainesville, FL.

30. Chasing Telephony Security: Where the Wild Things... Are? Verizon Wireless RNC/Data Center, October 2013. Alpharetta, GA.

31. Chasing Telephony Security: Where the Wild Things... Are? University of Waterloo - CrySP Speaker Series on Privacy, October 2013. Waterloo, ON, Canada.

32. Analyzing Malicious Traffic in Cellular Networks. GSM Association's (GSMA) Mobile Malware Community Workshop, July 2013. Mountain View, CA.

33. Threats to Mobile Devices. US Federal Trade Commission (FTC) Public Forum - Invited Speaker, June 2013. Washington, D.C.

34. Chasing Telephony Security: Where the Wild Things... Are? University of Wisconsin - Madison, Security Seminar, March 2013. Madison, WI.

35. 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.

36. Chasing Telephony Security: Where the Wild Things... Are? Stanford Security Seminar, March 2013. Stanford, CA.

37. Chasing Telephony Security: Where the Wild Things... Are? University of California, Berkeley, Security Group, March 2013. Berkeley, CA.

38. Chasing Telephony Security: Where the Wild Things... Are? Carnegie Mellon University CyLab Seminar, February 2013. Pittsburgh, PA.

39. Chasing Telephony Security: Where the Wild Things... Are? University of Oregon Department of Computer Science Colloquium, November 2012. Eugene, OR.

40. 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.

41. Needles and Haystacks: Digging for Ground Truth on Mobile Malware. ZISC Workshop on Secure Mobile and Cloud Computing, ETH Zurich, June 2012. Zurich, Switzerland.

42. Panel: Advice for Early Career Faculty. CRA Career Mentoring Workshop, February 2012. Washington, D.C.

43. Research Challenges in Cellular and Mobile Network Security. US-China Software Workshop (Co-Sponsored by NSF and NSFC), September 2011. Beijing, China.

44. Mobile Security: Understanding Risks to Critical Infrastructure. Invited Talk: US Department of State East African Workshop on Cyberspace Security, July 2011. Nairobi, Kenya.

45. Tomorrow's Issues: Solving the Mobile Security Threat. Invited Talk: Centre for Secure Information Technologies (CSIT) Queen's University, March 2011. Belfast, Northern Ireland.

46. PinDr0p: Using Single-Ended Audio Features to Determine Call Provenance. Invited Talk: MITRE Corporation, March 2011. Burlington, MA.

47. Defeating Session Hijacking Attacks with Disposable Web Credentials. Invited Talk: Facebook, February 2011. Palo Alto, CA.

48. Understanding the Disruptive Potential of Malware in Cellular Networks. Invited Talk: RSA Conference, February 2011. San Francisco, CA.

49. Panel: Voice Security – Now Just a False Sense of Security and Privacy. Invited Panelist: Mobile Security Symposium, February 2011. San Francisco, CA.

50. Understanding the Disruptive Potential of Malware in Cellular Networks. Invited Talk: Concordia University, May 2010. Montreal, QC, Canada.

51. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Qualcomm Research, March 2010. San Diego, CA.

52. 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.

53. Considerations for EAS Over Cellular Text Messaging Services. 3G Americas Webinar, July 2009.

54. University Telephony Research Panel. Conference on Principles, Systems and Applications of IP Telecommunications (IPTCOMM), July 2009.

55. The Evolving Mobile Landscape: Emerging Security Threats. Mobile Security eConference, SC Magazine, June 2008.

56. Characterizing the Impact of Rigidity on the Security of Cellular Networks. University of Washington, February 2009. Seattle, WA.

57. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Microsoft Research, February 2009. Redmond, WA.

58. Next Year's Problems. Secure Computing (SC) Magazine Webinar, November 2008.

59. Panel: Embedded Systems and their Increasing Impact on Infrastructure Security. Workshop on Embedded Systems Security (WESS), October 2008.

60. Can you DoS me now? Security Issues in Cellular Networks. Georgia Institute of Technology, September 2008. Atlanta, GA.

61. Characterizing the Impact of Rigidity on the Security of Cellular Networks. Georgia Institute of Technology, April 2008. Atlanta, GA.

62. Characterizing the Impact of Rigidity on the Security of Cellular Networks. AT&T Research Labs, April 2008. Florham Park, NJ.

63. Characterizing the Impact of Rigidity on the Security of Cellular Networks. University of Arizona, March 2008. Tucson, AZ.

64. Cellular Networks Security Panel. USENIX Security Symposium, August 2007. Boston, MA.

65. malnets:Large-Scale Malicious Networks via Compromised Access Points. The Pennsylvania State University - ACM Club Invited Speaker, October 2006. State College, PA.

66. malnets:Large-Scale Malicious Networks via Compromised Access Points. The University of Michigan, October 2006. Ann Arbor, MI.

67. Exploiting Open Functionality in SMS-Capable Cellular Networks. The University of Michigan, October 2006. Ann Arbor, MI.

68. Exploiting Open Functionality in SMS-Capable Cellular Networks. High Technology Crime Investigation Association (HTCIA), September 2006. Pittsburgh, PA.

69. Trends in Security: Critical Engineering in the Large. Schlumberger Innovate IT! Workshop, May 2006. Cambridge, MA.

70. Exploiting Open Functionality in SMS-Capable Cellular Networks. InfraGard Pittsburgh Chapter General Meeting, September 2006. Pittsburgh, PA.

71. Exploiting Open Functionality in SMS-Capable Cellular Networks. InfraGard Pittsburgh Chapter General Meeting, September 2006. Pittsburgh, PA.

B. Special Activities

Presentations to Lay Media

1. How technology can fight digital fakery. The Babbage Podcast/The Economist https://shows.acast.com/theeconomistbabbage/episodes/babbage-how-to-detect-a-deepfake, January 2023.
2. Deepfake audio has a tell and researchers can spot it. Ars Technica https://arstechnica.com/information-technology/2022/09/researchers-use-fluid-dynamics-to-spot-deepfake-voices/, September 2022.
3. This security tool could help stop the problem of ransomware in its tracks. TheJournal.ie https://www.thejournal.ie/ransomware-researchers-stop-2875032-Jul2016/, July 2016.
4. Researchers Unleash Ransomware Annihilation. BankInfoSecurity - http://www.bankinfosecurity.com/researchers-unleash-ransomware-annihilation-a-9255, July 2016.
5. CryptoDrop Stops Ransomware by Stopping its Encryption. Security Intelligence - https://securityintelligence.com/news/cryptodrop-stops-ransomware-by-stopping-its-encryption/?utm_source=tfeed&utm_medium=twitter, July 2016.
6. Ransomware 'stopped' by new software. BBC - http://www.bbc.com/news/technology-36772461, July 2016.
7. Researchers create effective anti-ransomware solution. Help Net Security - https://www.helpnetsecurity.com/2016/07/12/anti-ransomware-solution/, July 2016.
8. Florida U boffins think they've defeated all ransomware. http://www.theregister.co.uk/2016/07/12/ransomware_defeated/, July 2016.
9. This Anti-Ransomware Tool Could Save You Hundreds of Pounds. Huffington Post - http://www.huffingtonpost.co.uk/entry/anti-ransomware-tool-save-hundreds-pounds_uk_57838beee4b0935d4b4b30ba, July 2016.
10. Researchers develop method to stop 100% of ransomware before it encrypts all files. Myce - http://www.myce.com/news/researchers-develop-method-stop-100-ransomware-encrypts-files-79873/, July 2016.
11. Desarrollan una solución para detener el ransomware. ComputerHoy - http://computerhoy.com/noticias/software/desarrollan-solucion-detener-ransomware-47972, July 2016.
12. Why your antivirus software can't stop ransomware. Futurity - http://www.futurity.org/ransomware-computer-files-1198242-2/, July 2016.
13. CryptoDrop Gives Users Hope to Prevent Ransomware Infections in the Future. Softpedia - http://news.softpedia.com/news/cryptodrop-gives-users-hope-to-prevent-ransomware-infections-in-the-future-506187.shtml, July 2016.

14. Could this be the answer to the ransomware threat?, Consumer Affairs. Consumer Affairs - https://www.consumeraffairs.com/news/could-this-be-the-answer-to-the-ransomeware-threat-071116.html, July 2016.

15. Extortion extinction: Researchers develop a way to stop ransomware. Phys.org - http://phys.org/news/2016-07-extortion-extinction-ransomware.html, July 2016.

16. Researchers Develop A Way To Stop Ransomware By Watching The Filesystem. Slashdot - https://yro.slashdot.org/story/16/07/08/2242244/researchers-develop-a-way-to-stop-ransomware-by-watching-the-filesystem, July 2016.

17. Mohul Ghosh. Trak.in - Digital Money Apps In India Are Unsafe and Unsecured – Researchers. http://trak.in/tags/business/2015/08/17/digital-money-apps-india-unsafe-unsecured/, August 2015.

18. Richard Handford. Mobile World Live - Survey finds security holes in mobile money apps. http://www.mobileworldlive.com/money/news-money/survey-finds-security-holes-in-mobile-money-apps/#.Vc27Y-QTmSQ.twitter, August 2015.

19. JENNIFER VALENTINO-DEVRIES. Wall Street Journal - Researchers Find Security Flaws in Developing-World Money Apps. http://blogs.wsj.com/digits/2015/08/11/researchers-find-security-flaws-in-developing-world-money-apps/, August 2015.

20. Jonathon Cheng. Wall Street Journal - Samsung Phone Studied for Possible Security Gap. http://online.wsj.com/news/articles/SB10001424052702304244904579276191788427198, December 2013.

21. N. V. The Economist - The Threat in the Pocket. http://www.economist.com/blogs/babbage/2013/10/difference-engine-0?fsrc=scn/fb/wl/bl/thethreatinthepocket, October 2013.

22. Antone Gonsalves. ComputerWorld - Let's Dump Anti-Virus and Move On:. http://blogs.computerworld.com/mobile-security/22969/lets-dump-av-and-move, October 2013.

23. Mathew J. Schwartz. InformationWeek - Google: Don't Fear Android Malware. http://www.informationweek.com/security/mobile/google-dont-fear-android-malware/240162399, October 2013.

24. Kirsten Doyle. ITWeb - Android Threat Exaggerated, or is it? http://www.itweb.co.za/index.php?option=com_content&view=article&id=68055, October 2013.

25. Danielle Walker. SC Magazine - Mobile malware prevalence expands, but privacy-abusing apps should be top of mind. http://www.scmagazine.com/mobile-malware-prevalence-expands-but-privacy-abusing-apps-should-be-top-of-mind/article/300597/, June 2013.

26. Jim Burress. WABE NPR - Mobile Web Browsers Full of Security Risks, Tech Professor Finds. http://wabe.org/post/mobile-web-browsers-full-security-risks-tech-professor-finds, December 2012.

27. Mark Huffman. Consumer Affairs - Georgia Tech: mobile browsers fail safety test. http://www.consumeraffairs.com/news/georgia-tech-mobile-browsers-fail-safety-test-120612.html, December 2012.

28. Matthew J. Schwartz. Information Week - Blame Screen Size: Mobile Browsers Flunk Security Tests. http://www.informationweek.com/security/mobile/blame-screen-size-mobile-browsers-flunk/240143999, December 2012.

29. Jon Gold. Network World - Ga. Tech researchers: Mobile Browsers need better HTTPS indicators. http://www.networkworld.com/news/2012/120512-mobile-browsers-264846.html, December 2012.

30. United Press International. Study: Most mobile Web browsers unsafe. http://www.upi.com/Science_News/Technology/2012/12/05/Study-Most-mobile-Web-browsers-unsafe/UPI-73431354743353/#ixzz2EGtQsuLd, December 2012.

31. Suzanne Choney. Mobile browser woes can fool even experts: report . http://www.nbcnews.com/technology/mobile-browser-woes-can-fool-even-experts-report-1C7451203, December 2012.

32. Meghan Kelly. VentureBeat - 3 hot security startups to watch. http://venturebeat.com/2012/02/27/3-security-startups-to-watch-at-the-2012-rsa-conference/, February 2012.

33. Jacob Goodwin. Government Security News - RSA 2012 – Pindrop Security can distinguish a fraudulent phone call from a real one. http://www.gsnmagazine.com/node/25721?c=communications, February 2012.

34. Matt Liebowitz. Phone hack logs keystrokes from nearby computers. MSNBC.com - http://www.msnbc.msn.com/id/44993238/ns/technology_and_science-security/#.TqU5MNSjPh4, October 2011.

35. Jacob Aron. iPhone keylogger can snoop on desktop typing. New Scientist - http://www.newscientist.com/article/dn21059-iphone-keylogger-can-snoop-on-desktop-typing.html, October 2011.

36. iPhone Keylogger Can Snoop on Desktop Typing. Slashdot - http://mobile.slashdot.org/story/11/10/18/2346222/iphone-keylogger-can-snoop-on-desktop-typing, October 2011.

37. Robert Lemos. Smart Phones Could Hear Your Password. Technology Review - http://www.technologyreview.com/computing/38913/?p1=A2, October 2011.

38. Kevin McCaney. Bad vibrations: How smart phones could steal PC passwords. Government Computer News - http://gcn.com/articles/2011/10/18/smart-phone-sensors-steal-keystrokes.aspx, October 2011.

39. PhysOrg. Turning iPhone into spiPhone: Smartphones' accelerometer can track strokes on nearby keyboards. PhysOrg.com - http://www.physorg.com/news/2011-10-iphone-spiphone-smartphones-accelerometer-track.html, October 2011.

40. Brid-Aine Parnell. Securo-boffins call for 'self-aware' defensive technologies. The Register - http://www.theregister.co.uk/2011/09/14/self_aware_cyber_security_technologies_should_be_a_top_priority/, September 2011.

41. Clay Dillow. 'PinDr0p' Tech Uses Unique Noise Fingerprints to Trace Calls. Popular Science - http://www.popsci.com/technology/article/2010-10/pindr0p-tech-tags-phone-calls-unique-fingerprints-trace-call-paths-across-networks, October 2010.

42. Lewis Page. Voice-routing call fingerprint system fights vishing. The Register - http://www.theregister.co.uk/2010/10/06/voice_fingerprints, October 2010.

43. Science Daily. Voice Phishing: System to Trace Telephone Call Paths Across Multiple Networks Developed. http://www.sciencedaily.com/releases/2010/10/101005121820.htm, October 2010.

44. Brian Kalish. To Text or Not to Text During Emergencies. NextGov.com - http://www.nextgov.com/nextgov/ng_20100914_5986.php?oref=topnews, September 2010.

45. Ki Mae Heussner. 'Operation Chokehold': Fake Steve Jobs Rallies iPhone Users to Cripple AT&T Network. ABC News - http://abcnews.go.com/Technology/GadgetGuide/fake-steve-jobs-rallies- iphone-users-cripple-att/story?id=9355447, December 2009.

46. Bob Brown. Researchers Set Their Sights on iPhones, Mobile Malware. PC World Magazine - ihttp://www.pcworld.com/article/182005/iphone_worms_mobile_malware.html?tk=rss, November 2009.

47. MacGregor Campbell. Botnets show their disruptive potential. New Scientist Magazine - http://www.newscientist.com/article/mg20427347.000-mobile-botnets-show-their-disruptive-potential.html, November 2009.

48. Angela Moscaritolo. Remote repair for infected phones in development. SC Magazine - http://www.scmagazineus.com/remote-repair-for-infected-phones-in- development/article/157504/, November 2009.

49. Bob Brown. iPhone worms, other smartphone malware in researchers' sights. Network World - http://www.networkworld.com/news/2009/111109-smartphone-security-georgia -tech.html?hpg1=bn, November 2009.

50. Urvaksh Karkaria. GT researchers work to secure cellphones. Atlanta Business Chronicle - http://atlanta.bizjournals.com/atlanta/blog/atlantech/2009/11/cellphone.html, November 2009.

51. Making Carriers Shoulder Smartphone Security. http://mobile.slashdot.org/story/09/11/11 /2318247/Making-Carriers-Shoulder-Smartphone-Security?art_pos=31, November 2009.

52. Ben Meyer. Georgia Tech to Lead Fight Against Cell Phone Hackers. NBC 11 Atlanta - http://www.11alive.com/news/local/story.aspx?storyid=132505&catid=3, July 2009.

53. Illena Armstrong. Safeguarding your mobile networks. SC Magazine - http://www.scmagazineus.com/Safeguarding-your-mobile-networks/article/138289/, June 2009.

54. Kelli B. Grant. Four Free Cellphone Apps to Help Manage Your Money. SmartMoney Magazine - http://www.smartmoney.com/Spending/Deals/4-Great-Free-Finance-Apps-for-Cellphones/, June 2009.

55. Amanda Hoffstrom. Technology's limitations in alerting campus danger. UWire Magazine - http://www.uwire.com/Article.aspx?id=3738798, February 2009.

56. Laura Sydell. Compromise Allows Obama To Keep BlackBerry. National Public Radio - http://www.npr.org/templates/story/story.php?storyId=99790788, January 2009.

57. Dennis Carter. Questions abound as emergency alert flops Virginia Tech's text-message alert system failed when the sound of gunfire was heard on campus; officials scramble to understand why. eSchool News - http://www.eschoolnews.com/iphone/top-story/index.cfm?i=56122#_56122, November 2008.

58. Jessica Bauer. Study: Text alerts may fail in real emergency. Diamondback Online - http://media.www.diamondbackonline.com/media/storage/paper873/news/2008/10/14/News/Study.Text.Alerts.May.Fail.In.Real.Emergency-3485509.shtml, October 2008.

59. Associated Press. Hackers Expected To Start Targeting Cell Phones. http://cbs5.com/watercooler/Cell.Phones.Hackers.2.840909.html, 2008.

60. Associated Press. College alert systems unreliable, study says. http://www.ajc.com/search/content/metro/stories/2008/09/25/college_campus_alerts.html, 2008.

61. Lee Shearer. Study: Campus alerts unreliable. Athens Banner Herald http://www.onlineathens.com/stories/092508/uga_336494829.shtml, 2008.

62. Bill Ray. 3G Americas warns against text warning systems. The Register - http://www.theregister.co.uk/2008/09/18/emergency_text/, 2008.

63. 3G Americas. 3G Americas Highlights New Research Report on Use of Cellular Text Messaging for Emergency Alert Services. 3G Americas http://www.3gamericas.org/English/news_room/DisplayPressRelease.cfm?id=3400&s=ENG, 2008.

64. Evan Koblentz. Web Exclusive: From Messaging to Management Duty. Wireless Week - http://www.wirelessweek.com/Messaging-to-Management-Duty.aspx, 2008.

65. Christopher Beam. How Do You Intercept a Text Message? Turn your cell phone into a spy gadget. Slate Magazine http://www.slate.com/id/2161402/, 2007.

66. Jamming Cellphones with Text Messages. Slashdot http://it.slashdot.org/it/05/10/05/1839217.shtml?tid=215&tid=172, 2005.

67. Cell phone networks at risk? CNN http://money.cnn.com/2005/10/05/technology/hacker_cellphones/, 2005.

68. John Schwartz. Text Hackers Could Jam Cellphones, a Paper Says. The New York Times http://www.nytimes.com/2005/10/05/technology/05phone.html?ex=1286164800&en=d917b9cd43dfaa31&ei=5090&partner=rssuserland&emc=rss, 2005.