

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,

Petitioner,

v.

HEADWATER RESEARCH LLC,

Patent Owner.

Case No. IPR2026-00138

U.S. Patent No. 9,609,544

DECLARATION OF DR. KEVIN BUTLER

TABLE OF CONTENTS

I.	ASSIGNMENT.....	1
II.	QUALIFICATIONS	1
III.	SUMMARY OF CONCLUSIONS FORMED	7
IV.	LEVEL OF ORDINARY SKILL IN THE ART	8
V.	LEGAL STANDARDS.....	9
	A. Claim Construction.....	10
	B. Anticipation Under 35 U.S.C. § 102	11
	C. Obviousness Under 35 U.S.C. § 103.....	12
	D. Secondary Considerations of Non-Obviousness.....	15
VI.	MATERIALS CONSIDERED	17
VII.	TECHNOLOGY OVERVIEW	20
	A. Mobile Devices.....	20
	B. Resource Management in Mobile Devices	24
VIII.	OVERVIEW OF THE '544 PATENT.....	25
	A. Specification.....	25
	B. Claims.....	28
	C. Prosecution History	32
IX.	SUMMARY OF RELEVANT PRIOR ART	33
	A. U.S. Pat. App. Pub. No. 2006/0039354 (“Rao,” EX1005).....	33
	B. U.S. Pat. App. Pub. No. 2009/0217065 (“Araujo,” EX1006).....	39
	C. U.S. Pat. No. 5,987,611 (“Freund,” EX1007).....	44

D.	U.S. Pat. No. 8,381,127 (“Singh,” EX1008).....	47
E.	U.S. Pat. App. Pub. No. 2009/0207817 (“Montemurro,” EX1009)....	48
F.	U.S. Pat. App. Pub. No. 2006/0039364 (“Wright,” EX1010).....	50
G.	U.S. Pat. App. Pub. No. 2003/0172112 (“Vignaud,” EX1011).....	52
X.	GROUND 1A: Rao in view of Araujo renders obvious claims 1-2, 4-8, 12-16, 18, 20 and 22-23.	54
A.	Rao-Araujo Combination	54
B.	Analysis of the Claims	62
XI.	GROUND 1B: Rao in view of Araujo and Freund renders obvious claims 2, 17 and 19-21	111
A.	Rao-Araujo-Freund Combination	111
B.	Analysis of the Claims	116
XII.	GROUND 1C: Rao in view of Araujo and Singh renders obvious claim 3.....	126
A.	Rao-Araujo-Singh Combination	126
B.	Analysis of the claims	129
XIII.	GROUND 1D: Rao in view of Araujo and Montemurro renders obvious claim 11.....	130
A.	Rao-Araujo-Montemurro Combination	130
B.	Analysis of the claims	132
XIV.	GROUND 1E: Rao in view of Araujo and Wright renders obvious claims 9-10, 13 and 18.....	135
A.	Rao-Araujo-Wright Combination.....	135
B.	Analysis of the claims	138

XV. GROUND 1F: Rao in view of Araujo and Vignaud renders obvious claim 5.	
.....	145
A. Rao-Araujo-Vignaud Combination	145
B. Analysis of the claims	149
XVI. CONCLUSION.....	151

I, Kevin R. B. Butler of Gainesville, Florida, declare that:

I. ASSIGNMENT

1. I have been retained on behalf of Google LLC (“Petitioner” or “Google”) to offer technical opinions related to U.S Patent No. 9,609,544 (the “’544 Patent”) (EX1001). I understand that Petitioner requests the Patent Trial and Appeal Board (“PTAB” or “Board”) to institute an *inter partes* review (“IPR”) proceeding of the ’544 Patent.

2. I have been asked to provide my independent analysis of the ’544 Patent based on the prior art publications cited in this declaration.

3. I am not and never have been an employee of Google. I received no compensation for this declaration beyond my normal hourly compensation based on my time spent analyzing the ’544 Patent, the prior art publications cited below, and issues related thereto, and I will not receive any added compensation based on the outcome of any IPR or other proceeding involving the ’544 Patent.

II. QUALIFICATIONS

4. I am over the age of 18 and am competent to write this declaration. I have personal knowledge, or have developed knowledge of these technologies based upon education, training, or experience, of the matters set forth herein.

5. I have summarized in this section my educational background, career history, publications, and other relevant qualifications.

6. I received a B.Sc. degree in Electrical Engineering from Queen's University in 1999, an M.S. degree in Electrical Engineering from Columbia University in 2003, and a Ph.D. in Computer Science and Engineering from the Pennsylvania State University in 2010.

7. I am a Professor with tenure in Computer and Information Science and Engineering and Director of the Florida Institute for Cybersecurity Research at the University of Florida. Before moving to Florida under the Rising to National Preeminence initiative, I founded and directed the Oregon Systems Infrastructure and Information Security (OSIRIS) Lab at the University of Oregon, where I was an assistant professor of computer and information science for four years.

8. I have authored over 115 peer-reviewed publications including book chapters, journal articles, conference proceedings papers, and workshop papers. My research focuses on the area of computer systems security, including embedded systems, mobile devices, and firmware, as well as network security, including the security of Internet routing and security of telecommunications networks.

9. I received a National Science Foundation CAREER award in 2013, an International Educator of the Year award within the Herbert Wertheim College of Engineering at the University of Florida in 2017, a University of Florida Term Professorship for 2018-2021 and 2021-2024, and an Arnold and Lisa Goldberg

Rising Star Endowed Professorship in Computer Science for 2018-2024, which I relinquished in 2021 upon promotion to Full Professor. I also received an Outstanding Community Service Award from the IEEE Technical Committee on Security and Privacy in 2017.

10. I am a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE), and a Senior Member of the Association for Computing Machinery (ACM). I have been involved with international standards-setting bodies; in particular, I was co-chair and leader of the Security Workstream for the International Telecommunications Union (ITU)'s Technology, Innovation, and Competition Working group within the Focus Group on Digital Financial Service from 2015-2016, and from 2017-2022, I served as Co-Chair of the Security, Infrastructure, and Trust Working Group within the ITU's Financial Inclusion Global Initiative.

11. I currently serve on four journal editorial boards, and have served on numerous funding panels for the National Science Foundation and reviewed grant proposals on behalf of science and engineering boards in Austria, Canada, and Israel. I have served on over 115 technical program committees for selecting papers to appear at academic conferences on computer security, and I have served as program committee chair and general conference chair for multiple conferences. I have also given over 100 presentations and invited talks, including invited

lectures at the University of Oxford, ETH Zurich, the Chinese Academy of Sciences, Dartmouth College, Columbia University, and UCLA. My research has been featured in news outlets such as the Wall Street Journal, BBC News, and WIRED.

12. I have experience with networking and power consumption of networked computing systems. At Flarion Technologies in 2003, I implemented packet diversion and IP header modification programs in the FreeBSD operating system for mobile IP packet testing, to be deployed on WiFi devices where power consumption was a factor considered in benchmarking results. In 2004 at AT&T Labs-Research, I led the design and implementation of mechanisms to support the secure delivery of routing information within the Border Gateway Protocol and evaluated their efficacy using routing data. I have also led the development of a survey of security mechanisms for the Border Gateway Protocol that has been cited over 500 times.

13. I have experience with services and implementation in telecommunication networks, particularly telephony networks. As a research assistant at Columbia University in 2001-2002, I incorporated authentication protocols into a Java-based software stack for the Session Initiation Protocol used for Internet telephony. More recently, I led a project that demonstrated the extraction of data from smart phone firmware images and demonstrated that legacy

command sets (i.e., “AT commands” developed for modems in the 1980s) were being used to provide undocumented features on these devices that could be accessed over a USB connection, as well as methods for enabling the transmissions of these commands. I also led the investigation of the processors on smart phones that are used for communicating with the cellular network and developed an analysis framework that found vulnerabilities in the implementation of cellular communication network protocols implemented in these devices.

14. I have experience with the development and analysis of software and firmware. In 1998 at the Royal Bank of Canada, I developed client-server applications, including design of graphical user interfaces on the client side, to port business processes from mainframe environments.

15. In 2006, I compiled and modified OpenEmbedded firmware to support the SlugOS environment to allow experimentation with storage devices, in order to develop a disk prototype for preventing a type of malware called a rootkit from persisting on a system after reboot. Since then, I have led efforts to analyze firmware on embedded devices, particularly firmware from USB flash drives that uses the Intel 8051 microcontroller and demonstrated how such binary firmware could be lifted to an intermediate representation to enable control flow graph recovery and symbolic analysis.

16. I have experience with peripherals and portable devices. In 2009, I developed a USB device capable of attesting the integrity of the host computer it was attached to while at Symantec Research. This work was later patented (U.S. Patent 8,856,918, Host validation mechanism for preserving integrity of portable storage data. Petros Efstathopoulos, Bruce Montague, Dharmesh Shah, Kevin Butler. October 7, 2014.). Since then, I have overseen the development of USB devices that allow for tracking the provenance of data at the block level and the development of mobile device software that automates the collection of USB enumeration data.

17. I have additionally been involved with numerous projects incorporating encryption, such as mechanisms using additive homomorphic encryption to support accounting audits for preserving the confidentiality of wiretap records and cryptographic schemes for assuring the secure time release of data.

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

III. SUMMARY OF CONCLUSIONS FORMED

19. This Declaration explains the conclusions that I have formed based on my analysis. I understand that the following references, including Rao (EX1005), Araujo (EX1006), Freund (EX1007), Singh (EX1008), Montemurro (EX1009), Wright (EX1010), and Vignaud (EX1011), are prior art to the '544 Patent.

20. Based on my review, claims 1-23 ("the Challenged Claims") of the '544 Patent are unpatentable. To summarize those conclusions:

- **Ground 1A:** Based upon my knowledge and experience and my review of the prior art publications in this declaration, I believe that claims 1-2, 4-8, 12-16, 18, 20 and 22-23 are obvious in view of the Rao (EX1005) and Araujo (EX1006) references.
- **Ground 1B:** Based upon my knowledge and experience and my review of the prior art publications in this declaration, I believe that claims 2, 17 and 19-21 are obvious in view of the Rao (EX1005), Araujo (EX1006), and Freund (EX1007) references.
- **Ground 1C:** Based upon my knowledge and experience and my review of the prior art publications in this declaration, I believe that claim 3 is obvious in view of the Rao (EX1005), Araujo (EX1006), and Singh (EX1008) references.

- **Ground 1D:** Based upon my knowledge and experience and my review of the prior art publications in this declaration, I believe that claim 11 is obvious in view of the Rao (EX1005), Araujo (EX1006), and Montemurro (EX1009) references.
- **Ground 1E:** Based upon my knowledge and experience and my review of the prior art publications in this declaration, I believe that claims 9-10, 13 and 18 are obvious in view of the Rao (EX1005), Araujo (EX1006), and Wright (EX1010) references.
- **Ground 1F:** Based upon my knowledge and experience and my review of the prior art publications in this declaration, I believe that claim 5 is obvious in view of the Rao (EX1005), Araujo (EX1006), and Vignaud references (EX1011).

IV. LEVEL OF ORDINARY SKILL IN THE ART

21. I have been informed that a person of ordinary skill in the art (“POSITA”) is a hypothetical person who is presumed to have the skill and experience of an ordinary worker in the field at the time of the alleged invention. The ’544 Patent was filed November 15, 2013, and claims priority to many provisional applications, the earliest of which was filed January 28, 2009. EX1001, Cover. I have assumed January 28, 2009 is the “Critical Date” in this proceeding.

22. Based on my knowledge and experience in the field and my review of the '544 Patent and file history, I believe that a person of ordinary skill in the art in this matter would have had at least (1) a bachelor's degree in computer science, electrical engineering, or a related field, and (2) at least three years of experience with networking, power consumption of networked computing devices, and/or wireless digital communications systems. More education, e.g., a doctorate in an academic area emphasizing electrical engineering, computer engineering, computer science, or a related technical field, would compensate for fewer years of work experience. Based on my experiences, I understand the capabilities of a POSITA as of the Critical Date. Indeed, I have taught, mentored, advised, and collaborated closely with many such individuals over the course of my career.

V. LEGAL STANDARDS

23. In forming my opinions and considering the subject matter of the '544 Patent and its claims in light of the prior art, I am relying on certain legal principles that counsel in this case explained to me. My understanding of these concepts is summarized below.

24. I understand that the claims define the invention. I also understand that an unpatentability analysis is a two-step process. First, the claims of the patent are construed to determine their meaning and scope. Second, after the claims are construed, the content of the prior art is compared to the construed claims.

25. I understand that there are two ways in which prior art may render a patent claim unpatentable. First, I have been informed that the prior art can “anticipate” a claim. Second, I have been informed that the prior art can render a claim “obvious” to a person of ordinary skill in the art. I understand that a claim is patentable if it was not anticipated and would not have been obvious by the prior art at the effective filing date of the patent.

A. Claim Construction

26. I understand that, in this proceeding, the claims are construed according to their ordinary and customary meaning, in light of the specification and prosecution history, as understood by a person of ordinary skill in the art at the time of the invention. I understand that this is the same claim construction approach used in district court litigation.

27. I have been instructed that the “intrinsic record” includes the ’544 Patent itself, including the claims, description, and figures (EX1001), and the ’544 Patent’s prosecution history—i.e., the record of proceedings at the U.S. Patent and Trademark Office (“USPTO”) concerning the patent (EX1002). I understand that, like the claims and written description, the prosecution history provides evidence to a person of ordinary skill in the art of how the inventor intended his patent to be understood, and how the USPTO understood the patent. I understand that the inventor is permitted to apply a special definition to the terms or to limit the scope

of claim terms in his patent claims, which may differ from the term's plain and ordinary meaning. That special definition or limitation on scope may be provided in the patent's written description, the patent's prosecution history, or both.

28. I understand that claim interpretation may also be informed by "extrinsic evidence" (that is, evidence outside of the patent record itself). I have been informed that extrinsic evidence may include dictionaries, technical treatises, and other materials evidencing the meaning of a claim term and the understanding held by a person of ordinary skill in the art in the relevant time period.

29. In my opinion, none of the claim terms in the '544 Patent require an express construction. Instead, the claims should all be given their plain and ordinary meaning as they would have been understood by a person of ordinary skill in the art at the Critical Date of the '544 Patent.

B. Anticipation Under 35 U.S.C. § 102

30. I understand that a patent claim is invalid as anticipated if a single piece of prior art teaches every element of the claims, viewed from the perspective of a person of ordinary skill in the art. I also understand that an anticipatory reference does not have to recite word for word what is in the anticipated claims. Anticipation can also occur when a claimed limitation is inherent in the relevant reference. I have been advised that if the prior art necessarily functions in

accordance with, or includes, the claims limitations, it can anticipate even though the limitation is not expressly disclosed.

C. Obviousness Under 35 U.S.C. § 103

31. I understand that a patent claim is invalid as obvious if the claimed invention would have been obvious to a person of ordinary skill in the art at the time the claimed invention was made. This means that even if all of the elements of the claim cannot be found in a single prior art reference that would anticipate the claim, a person of ordinary skill in the field who knew about all the prior art would have come up with the claimed invention. I understand that in an obviousness determination, the person of ordinary skill in the art is presumed to have knowledge of all prior art. I understand that whether a claim is obvious is based upon the determination of several factual issues.

32. I have been informed that, in an obviousness analysis, prior art must be analogous to the patent being considered. I have been informed that a prior art reference is considered to be analogous, or in the same field of art, if the reference is either (1) in the same field of endeavor as the challenged patent, regardless of the problems the challenged patent and the prior art address, or (2) reasonably pertinent to the particular problem being solved by the challenged patent.

33. In considering obviousness, I understand that one must determine the scope and content of the prior art. I also understand that one must determine what differences, if any, existed between the claimed invention and the prior art.

34. I understand that a patent claim composed of several elements is not proved obvious merely by demonstrating that each of its elements was independently known in the prior art. In evaluating whether such a claim would have been obvious, one may consider whether a reason has been identified that would have prompted a person of ordinary skill in the art to combine the elements or concepts from the prior art in the same way as in the claimed invention. There is no single way to define the line between true inventiveness on the one hand (which is patentable) and the application of common sense and ordinary skill to solve a problem on the other hand (which is not patentable). For example, market forces or other design incentives may be what produced a change, rather than true inventiveness.

35. I also understand that, while there is no requirement that the prior art contain an express suggestion to combine known elements to achieve the claimed invention, and while a suggestion to combine known elements to achieve the claimed invention may come from the prior art as a whole or individually and may consider the inferences and creative steps a person of ordinary skill in the art would employ, as filtered through the knowledge of one skilled in the art,

obviousness grounds cannot be sustained by mere conclusory statements and must include some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. Moreover, I understand that a proper obviousness analysis requires a determination of whether a person of ordinary skill in the art would have a “reasonable expectation of success”—but not “absolute predictability” of success—in achieving the claimed invention by combining prior art references.

36. I understand that one may consider whether (1) the change was merely the predictable result of using prior art elements according to their known functions, or whether it was the result of true inventiveness; (2) there is some teaching or suggestion in the prior art to make the modification or combination of elements claimed in the patent; (3) the innovation applies a known technique that had been used to improve a similar device or method in a similar way; (4) the claimed invention would have been obvious to try, meaning that the claimed innovation was one of a relatively small number of possible approaches to the problem with a reasonable expectation of success by those skilled in the art; (5) the invention merely substituted one known element for another known element in order to obtain predictable results; (6) the invention merely applies a known technique to a known device, method, or product to yield predictable results, or (7) known work in the field may have prompted variations of use of the same

inventions in the same or different fields due to market forces or design incentives that would have been predictable to a person of ordinary skill in the art.

37. I understand that one must be careful not to determine obviousness using the benefit of hindsight; many true inventions might seem obvious after the fact. I understand that the determination should be based on the position of a person of ordinary skill in the field at the time the claimed invention was made and should not consider what is known today or what is learned from the teaching of the patent.

D. Secondary Considerations of Non-Obviousness

38. I understand that certain secondary considerations may be considered in evaluating obviousness in order to prevent hindsight bias. These secondary considerations include commercial success of products that practice the patent, long-felt need for the patented technology, failure by others to solve the problem addressed by the patent, initial skepticism by others in the industry, industry recognition and praise of the patented products, and efforts by others to copy the patented technology. I am not presently aware of any secondary considerations that would apply here.

39. I have been informed that these secondary considerations of non-obviousness must be balanced against the strength of the prima facie case of obviousness. Where the invention represents no more than the predictable use of

prior art elements according to their established functions, secondary considerations are inadequate to establish non-obviousness.

40. I have also been informed that the patentee must establish a nexus between any secondary consideration factors and the claimed invention. Where a secondary consideration factor results from something other than what is both claimed and novel in the patent, there is no nexus to the merits of the claimed invention.

41. I have been informed that, for example, the nexus requirement as it applies to the evidence of commercial success requires that the patentee must show that the sales of a product that allegedly practices the claimed invention must be a direct result of the unique characteristics of the claimed invention, as opposed to other economic and commercial factors that are unrelated to the patented invention. I understand that this means if the commercial success is due to an element that existed in the prior art or that is not claimed by the patent, then no nexus exists.

42. I have been further informed that, for example, the nexus requirement as it applies to the long-felt need element must likewise be supported by evidence. Where the differences between the prior art and the claimed invention are minimal, it cannot be said that any long-felt need was met by the patented invention or that the patent solved any technological problems that were unaddressed by others.

43. I have been informed that evidence of industry praise must also show a nexus with the claimed invention, and that self-serving statements by the patentee regarding the merits of the claimed invention are generally not given weight.

VI. MATERIALS CONSIDERED

44. My analysis and conclusions set forth in this declaration are based on my educational background and experiences in the field (*see* Section II), consideration of the evidence, and the '544 Patent (EX1001) and its file history (EX1002). Based on my knowledge and experience, I believe that I am an expert in the field relevant to the '544 Patent.

45. As part of my independent analysis for this Declaration, I have considered the following: the background knowledge and technologies that were commonly known to POSITAs during the time before the Critical Date of the '544 Patent, my own knowledge and experiences gained from my work experience in the field of the '544 Patent and related disciplines, and my experience working with others involved in this field and related disciplines.

46. I have reviewed the '544 Patent (EX1001) and its file history (EX1002). I have also analyzed, including the materials cited in this Declaration, the following publications and materials:

- EX1002: Excerpts from the Prosecution History of the '544 Patent (“the Prosecution History”)

- EX1005: U.S. Pat. App. Pub. No. 2006/0039354 (“Rao”);
- EX1006: U.S. Pat. App. Pub. No. 2009/0217065 (“Araujo”);
- EX1007: U.S. Pat. No. 5,987,611 (“Freund”);
- EX1008: U.S. Pat. No. 8,381,127 (“Singh”);
- EX1009: U.S. Pat. App. Pub. No. 2009/0207817 (“Montemurro”);
- EX1010: U.S. Pat. App. Pub. No. 2006/0039364 (“Wright”);
- EX1011: U.S. Pat. App. Pub. No. 2003/0172112 (“Vignaud”);
- EX1012: Bajaj, et al., IETF RFC 3198, Web Services Policy 1.2 - Framework (WS-Policy), April 25, 2006, downloaded from the internet at <https://www.w3.org/Submission/WS-Policy/> on August 29, 2023;
- EX1013: Sloman, et. al., "Security and management policy specification." IEEE Network, March/April 2002 pp. 10-19;
- EX1014: Lu, et. al., "Comparing system level power management policies." IEEE Design & Test of Computers, March/April 2001 pp. 10-19;
- EX1015: Davie, et al., IETF RFC 3246, An Expedited Forwarding PHB (Per-Hop Behavior), March 2002, downloaded from the internet at <https://datatracker.ietf.org/doc/html/rfc3246> on September 5, 2023;

- EX1016: Memorandum, Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (USPTO June 21, 2022) (“Director’s Guidance”);
- EX1017: Excerpts, The New Penguin Dictionary of Computing, by Dick Pountain, 2001;
- EX1018: Westerinen, et al., IETF RFC 3198, Terminology for Policy-Based Management, November 2001, downloaded from the internet at <https://www.ietf.org/rfc/rfc3198.txt> on August 15, 2023;
- EX1019: U.S. Pat. No. 7,757,185 (“Paquette”);
- EX1020: U.S. Pat. No. 7,023,909 (“Adams”);
- EX1021: U.S. Pat. No. 9,408,070 (“Altbaum”);
- EX1022: Yavatkar, IETF RFC 2753, A Framework for Policy-based Admission Control, January 2000, downloaded from the internet at <https://datatracker.ietf.org/doc/html/rfc2753> on September 5, 2023;
- EX1023: U.S. Pat. App. Pub. No. 2008/0080458 (“Cole”);
- EX1024: U.S. Pat. No. 8,413,172 (“Sng”);
- EX1025: U.S. Pat. No. 6,754,709 (“Gbadegesin”);
- EX1026: Claim Construction Order, *Headwater Research LLC v. AT&T Serv. ’s, Inc.*, 2:23-cv-00397 (E.D. Tex. Jan. 19, 2025);

- EX1027: U.S. Pat. App. Pub. No. 2008/0080457 (“Cole-2”);
- EX1028: U.S. Pat No. 7,305,562 (“Bianco”);
- EX1029: U.S. Pat. App. Pub. No. 2007/0204154 (“Swander”); and
- EX1030: U.S. Pat. App. Pub. No. 2008/0215718 (“Stolorz”);
- EX1031: ABRAHAM SILBERSCHATZ & PETER BAER GALVIN,
OPERATING SYSTEMS CONCEPTS (5th ed., 1999) (“Silberschatz”).

47. My analysis and conclusions set forth in this declaration are based on the perspective of a POSITA.

VII. TECHNOLOGY OVERVIEW

48. In this section I provide a broad overview of the relevant technology and state of the technical community as of the Critical Date of the ’544 Patent.

This description is not intended to be exhaustive, but to provide sufficient background to support and contextualize my analysis below.

A. Mobile Devices

49. In 2009, use of smart phones experienced a significant surge, marking a pivotal moment in the evolution of mobile technology. The year saw a growing number of consumers transitioning from traditional feature phones (e.g., flip phones) to more capable and versatile smart phones. Key factors driving this uptake included advancements in mobile operating systems such as Apple’s iOS and Google’s Android, offering a user-friendly interface and access to a burgeoning

app ecosystem. Additionally, the earlier introduction of 3G networks enabled faster mobile data speeds, prompting users to embrace smart phones for tasks beyond voice and messaging. As a result, smart phone sales soared, laying the groundwork for the transformative impact they would have on communication, productivity, and entertainment in the years to come.

50. However, smart phones in 2009 were resource-limited compared to the current devices. For example, smart phones of 2009 were equipped with single-core processors, usually running at speeds below 1 GHz. These processors lacked the computing power of today's multi-core CPUs found in modern smart phones. As a result, tasks that required significant processing, such as running complex applications or playing graphically intensive games, were often slow and less efficient. Similarly, (non-transitory¹) memory capacities in smart phones of 2009 were generally limited, typically ranging from 128 MB to 512 MB. Long term storage was also limited, consisting of between 4GB and 16GB of space.

¹ In patents, the term “non-transitory” can refer to computer-readable media (CRM) that stores data for short periods or in the presence of power such as a memory device or Random Access Memory (RAM).

Devices were connected to wireless networks using WWAN (cellular) and WLAN (Wi-Fi) modems.²

51. The networks that were being used in 2009 were also limited in speed and throughput. In 2009 wide-area (WWAN) cellular 3G networks, as implemented by the Global System for Mobile Communications (GSM)³ and Code Division Multiple Access (CDMA) protocols were becoming widespread, but 4G networks were still in the early stages of deployment. This meant slower internet speeds and limited coverage for mobile data, affecting the overall online experience. Wi-Fi technology as implemented in the 802.11 suite of protocols complemented cellular networks. Smart phones, laptops, and other devices could connect to Wi-Fi hotspots in homes, offices, cafes, and public spaces to access the internet at much higher speeds than what 3G networks could offer. Wi-Fi also

² The modems I reference here are *modulators/demodulators*, which are devices to process electrical signals received and sent over a physical media (e.g., copper wire) or over the air. In mobile devices, modems are software supported radios that process specific network access protocols.

³ Note that GSM predates 3G networks (actually, back to 1991), but, for the purposes of this report, I will focus only on those variants of GSM which were classified as 3G.

allowed users to offload data usage from their cellular plans, which was particularly helpful due to the relatively limited data caps on mobile plans during that time. Regardless of the network protocol it was running on, the IP protocol was used to connect each device with the Internet.

52. At the same time, battery technology had not yet seen significant advancements, leading to smart phones with relatively short battery life. The computational requirements and increased user engagement (using the phone for longer periods) led to increased demand for energy. Here, the combination of power-hungry processors, smaller batteries, and less optimized software meant that users often had to charge their phones frequently.

53. While 2009 smart phone displays were already evolving towards touchscreens, they were smaller, less vibrant, and had lower resolutions compared to modern displays. Common screen resolutions were around 320x480 pixels, making it challenging to display content with high visual fidelity. Devices' operating systems provided windowed environments that would generally have a single application being displayed (and prioritized by the operating system) and interacting with the users. These applications were referred to as having focus (of the user interface). Users could switch between applications as needed but could only interact with the one application with focus at a time.

B. Resource Management in Mobile Devices

54. A challenge known well before 2009 was addressing the rapidly increasing needs of mobile users using the resource-limited devices and networks. Solutions to these problems were developed before the Critical Date of the '544 Patent by adapting known techniques in computer systems and networks (e.g., priority queuing), as well as developing new, faster devices and networks.

55. Policy for computational systems has been a part of the technical landscape since the 1970s, with a primary focus on differentiating resource usage in various environments. For example, a policy might specify that data from interactive applications, such as multi-player games, are assigned the highest priority to ensure the best user experience. These policies were implemented to manage and allocate computing resources efficiently in diverse computing environments. For instance, differentiated services emerged as a crucial policy in this context, especially as mobile devices such as phones began to traverse heterogeneous environments, transitioning between Wi-Fi and cellular networks seamlessly. By employing policies like differentiated services, computing systems could optimize resource allocation, ensuring a smooth and reliable user experience while adapting to changing network conditions and device capabilities in these dynamic environments. Such techniques were particularly important to address the challenges faced by early mobile devices.

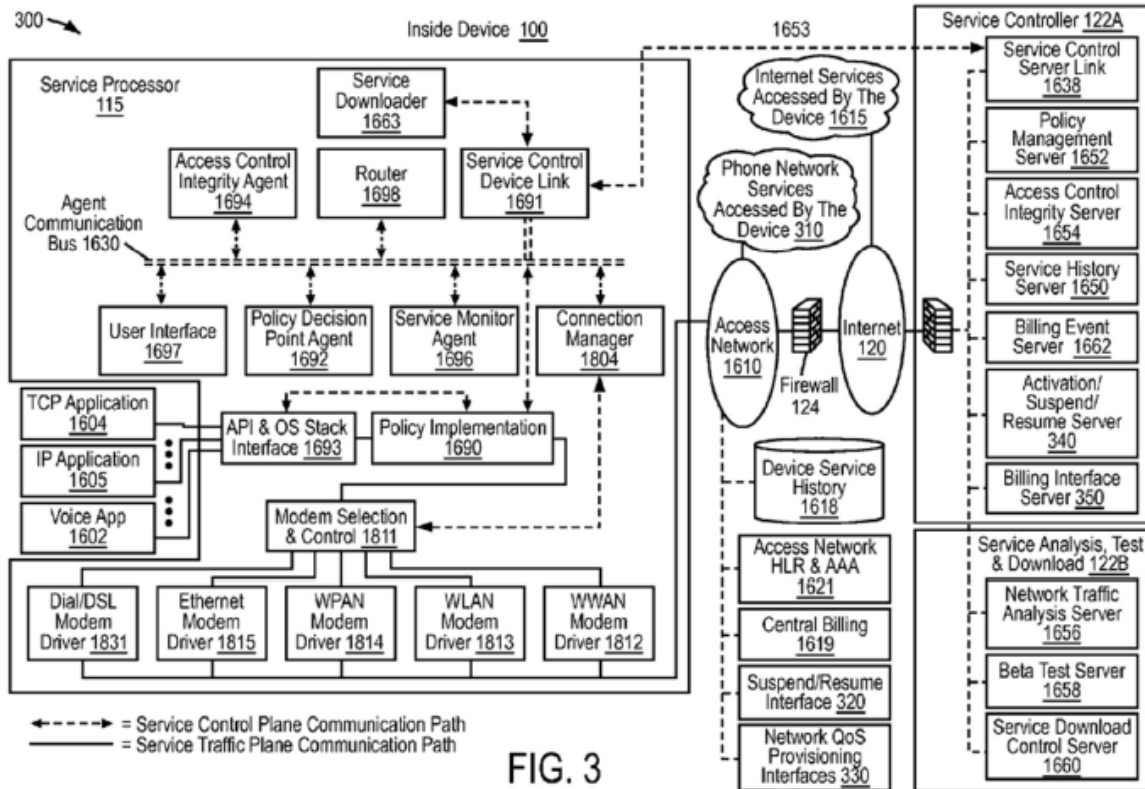
56. A Policy Decision Point (PDP) and Policy Enforcement Point (PEP) are essential components in policy-based systems. A PDP is logical entity that makes policy decisions for itself or for other network elements that request such decisions. EX1010, ¶20. The PDP functions as the determining logic of the system, responsible for evaluating policy rules and making decisions based on the input received from sources. Conversely, the PEP serves to enforce policy. A PEP is a logical entity that enforces policy decisions. EX1010, ¶20. PEPs are located at the point where policies are applied. The PEP communicates with the PDP to obtain the relevant policy decisions and then enacts them by controlling access to resources. In the example given above, the PDP would determine whether data are from an interactive game, and if so, the PEP would assign the highest priority to the data, e.g., by adding the data to a high-priority queue. Again, this would ensure the user does not experience performance problems (e.g., lag).

VIII. OVERVIEW OF THE '544 PATENT

A. Specification

57. The '544 Patent is directed to “device-assisted services for protecting network capacity”. EX1001, Title. The '544 Patent discloses “a wireless end-user device” that has a wireless modem and may support multiple wireless network types, which can include a WWAN and WLAN, as illustrated below. EX1001, Claim 1, FIG. 3. The '544 Patent teaches that “in wireless networks, managing the

wireless access connection capacity and network access connection resources is important to maintain network performance as network resources/capacity demand increases.” EX1001, 5:56-49.



EX1001, FIG. 3

58. To manage capacity, the device can “apply a service usage control policy for the network service usage activities to protect network capacity (e.g., reduce network capacity demand).” EX1001, 13:66-14:2. The device may “assign[] a priority to a network service usage activity and control[] traffic associated with the network services usage activity based on the assigned priority” and can provide a “differentiated and dynamic background services

classification ... as a function of network availability state and/or network busy state.” *Id.*, 14:25-31. The service usage control policy may assist “in network access control of network service usage activities (e.g., deferring some or all of the network capacity demand from these source activities).” *Id.*, 14:33-35. The device may associate “the network service usage activity with a network service usage control policy” based on factors such as “a network busy state, a time of day, ..., an application behavior, ..., a power state of device, a device usage state, a time based criteria, availability of alternative networks, and a set of policy rules.” *Id.*, 89:14-22. When a policy applies to an access request, the device can take various actions including acting to “throttle, delay, priority queue, time window, suspend, quarantine, kill, remove, and other well known traffic control techniques.” 15:48-50.

59. To enforce the controls, the device includes “a policy implementation driver/agent 1690 (e.g., policy enforcement point driver/agent)” and a Policy Decision Point Agent 1692. EX1001, FIG. 3, 61:26-28. A POSITA would have recognized policy decision points (PDPs) and policy enforcement points (PEPs) as terms of the arts describing components that determine whether a policy applies (PDP), and when the policy applies, enforcing the policy decision (PEP). EX1010, ¶20.

B. Claims

60. The table below includes identifiers for the '544 Patent claims and limitations, which are referenced throughout.

Claim	Identifier	Claim Language
1	[1.1]	A wireless end-user device, comprising:
	[1.2]	a wireless modem to communicate data for network service usage activities between the device and a wireless network;
	[1.3]	a processor that executes instructions to associate network service usage activity, on behalf of a first device application, and that occurs when the first device application is not in the foreground of user interaction, with a network service usage control policy,
	[1.4]	set an application state indicating whether the first device application, associated with a particular network service usage activity, is in the foreground of user interaction, and
	[1.5]	dynamically determine whether to apply the network service usage control policy to the particular network service usage activity, based on the application state and based on a power control state; and
	[1.6]	a memory coupled to the processor to provide the processor with the instructions.
2	[2]	The wireless end-user device of claim 1, wherein the processor executing the instructions determines that the first device application is in the foreground of user interaction when the user of the device is directly interacting with that application or perceiving any benefit from that application.
3	[3]	The wireless end-user device of claim 1, wherein the processor executing the instructions determines that the first device application is in the foreground of user interaction based on a state of user interface priority for the application.

Claim	Identifier	Claim Language
4	[4]	The wireless end-user device of claim 1, wherein when the network service usage control policy is applied it disallows the particular network service usage activity, and wherein the processor executes the instruction further to, when it is determined that the particular network access request is disallowed, queue that particular network service usage activity until a power state change occurs.
5	[5]	The wireless end-user device recited in claim 1, wherein the processor executes the instructions further to: implement the network service usage control policy at least in part via communication with the first device application through an emulated network access API that indicates to the first device application that an available wireless network is unavailable when a dynamic determination applies the network service usage control policy to the particular network service usage activity.
6	[6]	The wireless end-user device of claim 1, wherein the processor further executes the instruction to, for at least a second device application or service, allow network service usage activities without regard to the power control state.
7	[7]	The wireless end-user device of claim 1, wherein the power control state is a power state of the device.
8	[8]	The wireless end-user device recited in claim 1, wherein the processor executes the instructions further to: execute a router for dynamically managing one or more network capacity controlled services and/or QoS sessions for the wireless end-user device.
9	[9.1]	The wireless end-user device recited in claim 1, wherein the processor executes the instructions further to:
	[9.2]	execute a router for dynamically managing one or more network capacity controlled services and/or QoS sessions for the wireless end-user device; and
	[9.3]	send network busy state information to a service controller, wherein the service controller provides a

Claim	Identifier	Claim Language
		policy decision point for management for a plurality of wireless end-user devices in communication with one or more base stations.
10	[10.1]	The wireless end-user device recited in claim 1, wherein the processor executes the instructions further to:
	[10.2]	execute a router for dynamically managing one or more network capacity controlled services and/or QoS sessions for the wireless end-user device;
	[10.3]	send network busy state information to a service controller, wherein the service controller provides a policy decision point for management for a plurality of wireless end-user devices in communication with one or more base stations; and
	[10.4]	receive router traffic control instructions from the service controller, wherein the service controller provides the router traffic control instructions to assist in dynamically managing network capacity usage for the plurality of wireless end-user devices in communication with the one or more base stations.
11	[11]	The wireless end-user device recited in claim 1, wherein dynamically determining whether to apply the network service usage control policy to the particular network service usage activity is further based on a current wireless network and/or the network service usage control policy is based on a current wireless network.
12	[12]	The wireless end-user device recited in claim 1, wherein dynamically determining whether to apply the network service usage control policy to the particular network service usage activity further includes dynamically assigning a network capacity controlled services priority level to the particular network service usage activity based on a network busy state.
13	[13]	The wireless end-user device recited in claim 1, wherein associating includes querying a network element for determining an association of the first

Claim	Identifier	Claim Language
		device application with the network service usage control policy.
14	[14]	The wireless end-user device recited in claim 1, wherein the network service usage control policy includes one or more of the following: block/allow settings, throttle settings, adaptive throttle settings, QoS class settings, packet error rate, jitter and delay settings, queue settings, and tag settings.
15	[15]	The wireless end-user device recited in claim 1, wherein the network service usage control policy includes traffic control policy filters, the filters comprising a first filter specifying applicability of the policy only when the first device application is not in the foreground of user interaction, and a second filter specifying applicability of the policy only in one or more specific power control states.
16	[16]	The wireless end-user device recited in claim 1, wherein the network service usage control policy includes traffic control policy filters implemented as cascading filters.
17	[17]	The wireless end-user device recited in claim 1, wherein the network service usage control policy includes traffic control policy filters using a network busy state and/or a time of day as an index into a traffic control setting.
18	[18]	The wireless end-user device recited in claim 1, wherein the processor executes the instructions further to: differentially control the particular network service usage activity based on the network service usage control policy based on a network busy state.
19	[19]	The wireless end-user device recited in claim 1, wherein the processor executes the instructions further to: differentially control the particular network service usage activity based on the network service usage control policy based on a user input and/or a current wireless network.
20	[20]	The wireless end-user device recited in claim 1, wherein the processor executes the instructions

Claim	Identifier	Claim Language
		further to: modify or replace a network stack interface of the wireless end-user device to provide for intercept or discontinuance of network access messaging for implementing traffic control of the particular network service usage activity.
21	[21]	The wireless end-user device recited in claim 1, wherein the processor executes the instructions further to: store a network capacity controlled service list, wherein the network capacity controlled service list is periodically updated based on monitored network service usage activities.
22	[22]	The wireless end-user device of claim 1, wherein the power control state is a power save state of the device.
23	[23]	The wireless end-user device of claim 1, wherein the power control state is a power state of the wireless modem.

C. Prosecution History

61. The '544 Patent was allowed after one office action rejecting the claims as: (i) directed to unpatentable subject matter under §101, and (ii) unpatentable as being obvious over U.S. Patent No. 8,484,658 ("Rados"). EX1002, 668-672. The applicant amended the claims and asserted priority to provisional application No. 61/348,022, claiming that Rados was not prior art. *Id.*, 109-117. The claims were subsequently allowed. *Id.*, 76-83.

IX. SUMMARY OF RELEVANT PRIOR ART

A. U.S. Pat. App. Pub. No. 2006/0039354 (“Rao,” EX1005)

62. Rao discloses a “remote access architecture” that provides “peer-to-peer communications and remote access connectivity.” EX1005, Abstract. The system includes clients 105 (instances of computing devices 102) that communicate with each other over a network 104 (and optionally through a gateway 340) and with other computing devices, such as servers 102e and server farms 102n. *Id.*, ¶¶86-96.

63. Figure 1A shows an example of the Rao system:

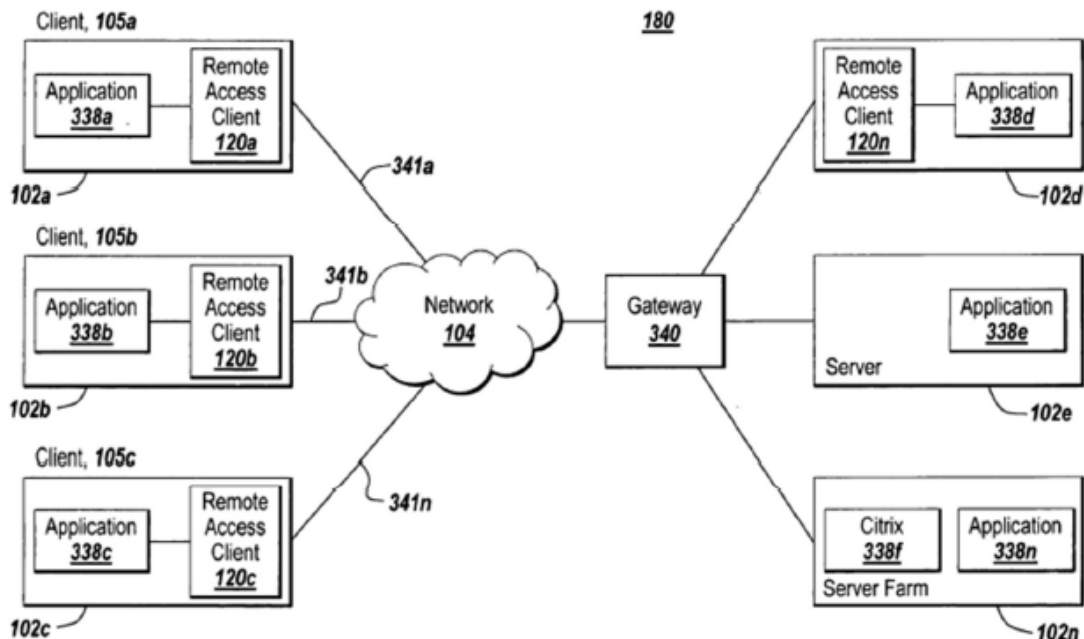


Fig. 1A

EX1005, FIG. 1A

64. Rao addresses inefficient use of network resources when network communications between devices are “processed in the order generated by the activity of a user and applications of the client,” which is not “always desirable” since “a network packet generated or received for an application running in the background may be processed ahead of a network packet generated or received for the application running in the foreground.” EX1005, ¶3. This results in applications suffering from increased latency and reduced quality of voice communication. *Id.* For example, while parties participating in a voice call will immediately notice if the packets carrying voice signals are not delivered promptly, a slight delay in delivering email or uploading a social media post is unlikely to be perceived.

65. Rao contemplates addressing these network inefficiencies through a prioritization scheme that “provide[s] application-aware, client-specific prioritization of packet traffic.” EX1005, ¶3. The prioritization scheme is achieved by augmenting client 105 with a remote access client 120 that interacts with applications 338 and network stack 310. EX1005, ¶¶89, 98-100.

66. Figure 1C shows an example of a system with a remote access client for routing network packets from client 105 to network 104:

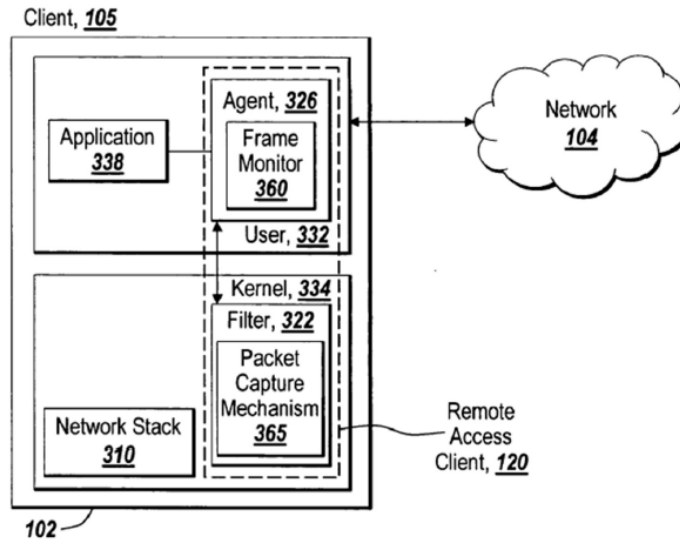


Fig. 1C

EX1005, FIG. 1C

67. The remote access client 120 includes a filter 322 that uses a “filtering table ... to determine what action to take against packets,” including “ensur[ing] that unwanted packets are discarded,” “deny[ing] access to particular protocols,” and/or “prevent[ing] unauthorized access from remote computers by discarding packets to specified destination addresses.” EX1005, ¶102. As noted above, such techniques are helpful in ensuring delivery of real-time network traffic. The remote access client 120 can include an agent 326 with frame monitor 360 that “include[s] policies and logic for applying a policy to a received packet.” *Id.*, ¶108. Frame monitor 360 “transmit[s] a packet to a gateway 340 responsive to a policy-based determination made by the frame monitor 360.” *Id.* The use of policies in remote access client 120 thereby guides efficient use of network

resources and enables Rao's system to address the inefficiencies identified within Rao's disclosure, e.g., as illustrated in the example above where voice packets are prioritized over packets that are not time-critical.

68. Rao's system further enables "intelligent and client centric prioritization of application network communications on a client based on the type and/or priority of an application." EX1005, ¶¶179, 182-84, FIG. 5A. To perform this prioritization, Rao's system "appl[ies] a policy to determine a condition of the client 105, or endpoint, at the time of transmission of the packet." EX1005, ¶109. Further, frame monitor 360 can "identify an application 338 that generated the packet." EX1005, ¶109.

69. Figure 5A shows an environment of a client providing client-side application-aware network communication:

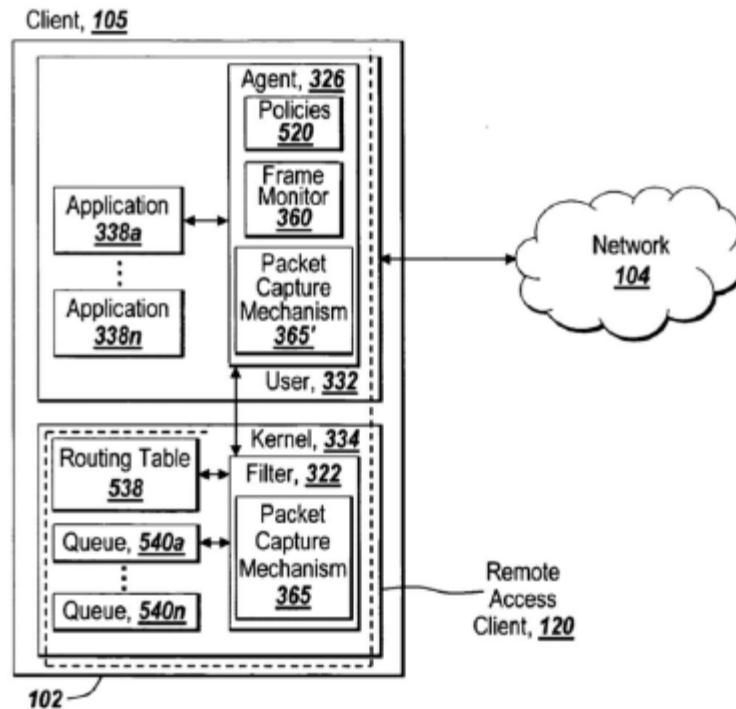


Fig. 5A

EX1005, FIG. 5A

70. Rao offers non-limiting disclosure relating to the specification of policies 520 and how its system leverages each of these policies 520 for prioritization. EX1005, ¶182 (“policies 520 may be specified by any suitable means and/or mechanisms”), ¶¶183-84.

71. By the Critical Date, numerous approaches to policy specification were known. For example, “[t]he Web Services Policy Framework (WS-Policy) provides a general purpose model and corresponding syntax to describe the

policies of a Web Service.” EX1012, 1. Sloman further provides an overview of policy specification. *See, generally*, EX1013.

72. As examples, Rao describes that policies 520 can be specified by “name of the,” “type of application,” or “type of one or more protocols used by the applications.” EX1005, ¶182. Further, policies 520 offer several types of functionality relating to prioritization, such as “defin[ing] prioritization based on whether an application is running in the foreground or the background of the client 105,” “indicat[ing] prioritization based on the destination network address, such as host name or IP address, and/or destination port number,” and being “specified conditionally, such as if one application 338a is running, a second application 338b may have a higher or lower priority.” *Id.* Indeed, “[o]ne ordinarily skilled in the art will recognize and appreciate the multitude of ways to define client-side application priorities.” *Id.* This assertion aligns with numerous teachings in the field, including those of Bajaj and Sloman. *See, generally*, EX1012, EX1013. Thus, policies 520 can “apply a priority to network packets of applications 338a-338n in accordance with the prioritization rules specified or indicated by the policies 520,” which include, for example, “defin[ing] prioritization based on whether an application is running in the foreground or the background of the client 105.” EX1005, ¶¶182, 189.

B. U.S. Pat. App. Pub. No. 2009/0217065 (“Araujo,” EX1006)

73. Araujo explains that electronic devices such as computers and wireless telephones “normally employ some type of power management framework.” EX1006, ¶14. Such power management schemes “govern the use of energy” because “[b]attery-powered machines have a finite amount of energy stored between charges,” so such machines “generally attempt to use the energy in a way that strikes a balance between providing functionality and maintaining longevity of the charge.” EX1006, ¶1. As described above, the use of policy was a well-known technique for systems management, including for power management. *See, generally*, EX1012, EX1013, EX1014.

74. To strike this balance, Araujo teaches that a machine's “power usage may be managed by a power-management policy” and “[w]hen a program makes a request that involves use of one of the machine's power-consuming devices, the policy may take into account factors such as the program's status, where the status indicates the program's relative level of justification to consume power.” *Id.*, Abstract. Araujo explains that power-management policies can consider the status of programs. *Id.*, ¶27. For example, “a program may have a status that reflects its worthiness to consume power” such as a “VIP” status that allows it “to consume power in situations where other programs would not be permitted to consume power.” *Id.* Enabling higher priority application with preferential access to power

enables a device to stretch remaining battery charge while still executing important applications.

75. Araujo further teaches that, in some cases, program activities are permitted without regard to power factors, such as allowing a software update program to perform a software update immediately and “regardless of the power expenditure” when “there is known to be a zero-day attack propagating through the Internet, in which case delaying the update might expose the computer to an attack.” EX1006, ¶16.

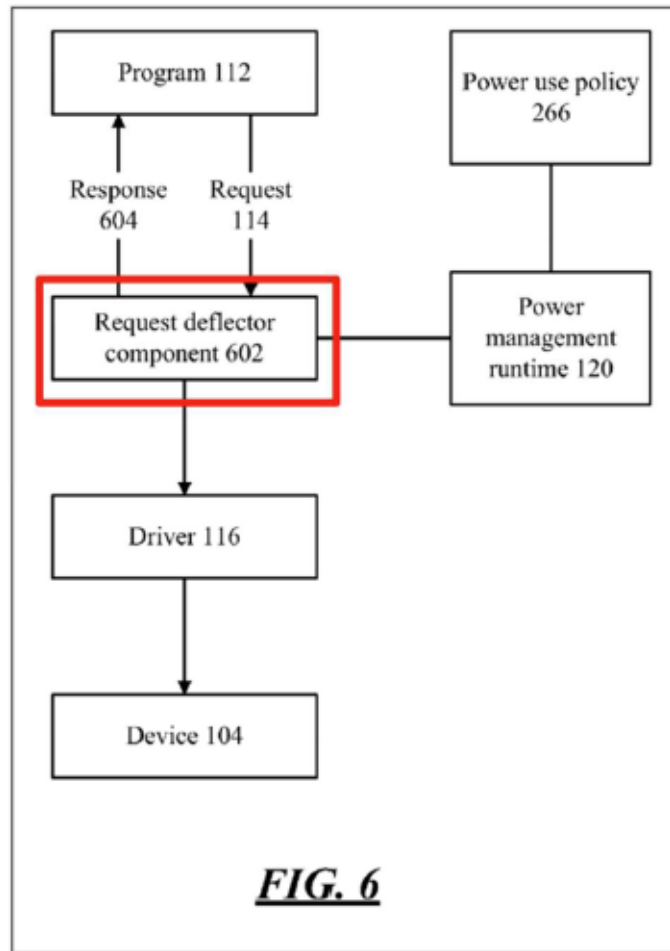
76. Protecting the device from hackers is of prime importance, both to protect the device itself and to stop the device from propagating the attack to other devices on the network. Note that enabling the software update program to operate regardless of power for critical updates does not necessarily mean that the updater can perform more routine functions without regard for power. A POSITA would have understood that some Araujo policies could state, in essence, “if (a zero-day attack remediation is available) then (install the update)” and “if (a non-critical update is available) and (the power state is low-battery) then (defer installation).” Both policies apply to the software update application. The former policy is executed without regard to power state, and the latter does consider power state. Examples of non-critical updates include feature enhancements and minor bug fixes.

77. Araujo's system includes a power manager "that controls the respective power states of devices" and "may cause devices to be turned off, or into a lower power state, based on factors such as timers, the amount of battery power remaining, or any other factor." EX1006, ¶22. Since Araujo teaches the power states of each component device (e.g., processor, network card, etc.) within a computing device, a POSITA would have recognized that the power state of the computing device ("machine 700" in Araujo) is the aggregate power states of the component devices. *Id.*, ¶¶4, 56. For example, a POSITA would have known that the power state of the device could be represented as a vector, such as [1, 1, 0, 1], where "1" represents the "on" state and "0" represents the "off" state. In this example, the components of the vector would represent processor, screen, audio and network. (Other encodings, such as XML and JSON, could have also been used.) A POSITA would have further recognized that the power state of a battery could be represented as a percentage of charge remaining, and that value could have also been included in the device power state vector, e.g., [1, 1, 0, 1, 0.8], adding the battery's 80% power to the prior example vector.

78. Such factors are evaluated by Araujo's power management runtime that "may implement policies that determine when, and under what circumstances, power manager 110 is to turn devices 104-108 on or off, or is to place those devices in a different power state." EX1006, ¶22. For brevity, the collective

functions of Araujo's power manager and power management runtime can be called the "power policy manager" ("PPM").

79. In some cases, the policy decisions are enforced by a "request deflector" component that is "interposed" between a "program" and a "driver" of a "device." EX1006, ¶5. When request deflector component intercepts a request, "it interacts with power management runtime 120 to determine what the ambient policy (e.g., power use policy 266) says about whether the request may be carried out at the expense of power use" and does so "before the request reach[es] a device driver." EX1006, Abstract, ¶¶21, 24, 50. Figure 6 (below) shows an example of the "request deflector component":



EX1006, FIG. 6 (annotated)

80. Araujo contrasts this approach with traditional operation in which, interaction between a program and a power policy would be through a driver, and “the program either learns that the device is off, or issue[s] a request that results in the device being turned on,” thus allowing policy enforcement even with a device that is powered off. EX1006, ¶50. Note that the mention of “device” refers to a component of the mobile device, such as the network interface or display.

EX1006, ¶2 (“A machine may include various devices that draw power, such as a disk, network card, processor, monitor, etc.”).

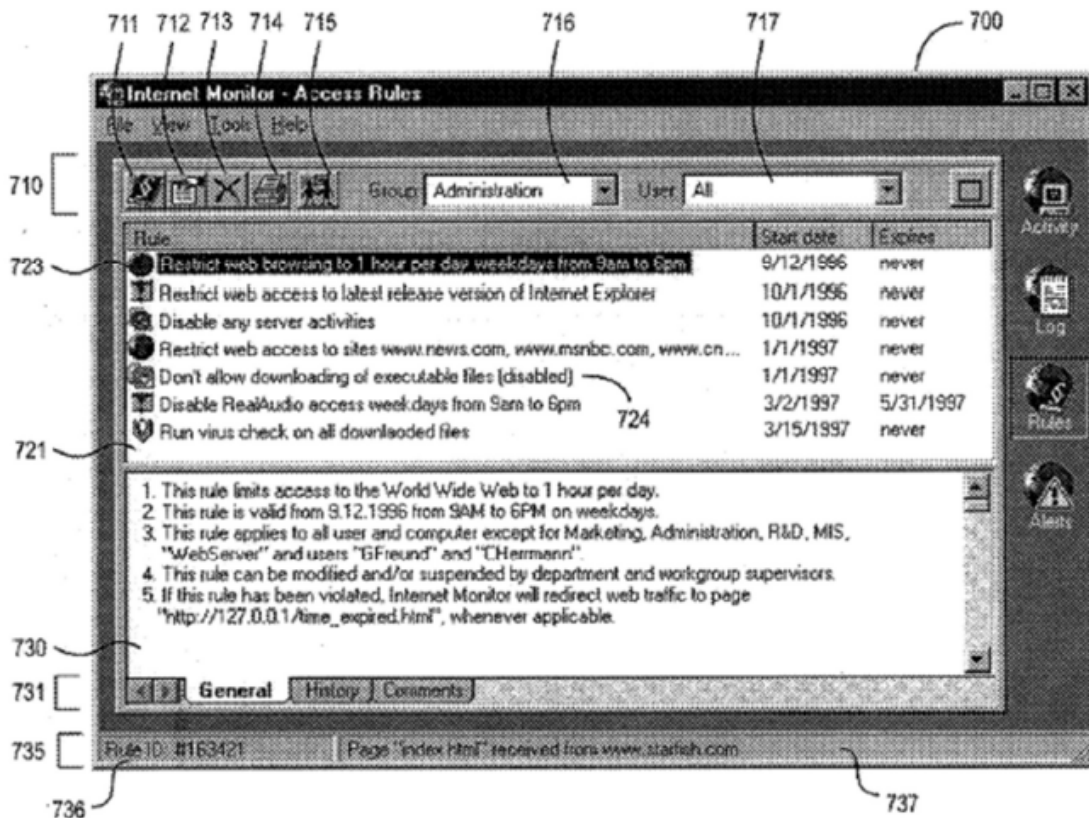
C. U.S. Pat. No. 5,987,611 (“Freund,” EX1007)

81. Freund generally relates to the efficient use of computing resources, and more specifically controlling the use of networks by “set[ting] access rules for the entire LAN for one or more workgroups or individual users, a client-based filter application (installed at each client), and a central supervisor application that maintains the access rules for the client based filter and verifies the existence and proper operation of the client-based filter application.” EX1007, 3:62-67.

82. Freund uses “access rules [that] can include criteria such as total time a user can be connected to the Internet (e.g., per day, week, month, or the like), time a user can interactively use the Internet (e.g., per day, week, month, or the like), a list of applications or application versions that a user can or cannot use in order to access the Internet, a list of URLs (or WAN addresses) that a user application can (or cannot) access, a list of protocols or protocol components (such as Java Script™) that a user application can or cannot use, and rules to determine what events should be logged (including how long are logs to be kept).” EX1007, 4:8-19. To apply the rules, in some cases, Freund classifies whether an application is interacting with the user in the device user interface foreground, e.g., “monitoring of time spent by an employee for ‘actively’ interacting with the

Internet,” which “occurs when a user directly interacts with an Internet application (e.g., Web browser) while that application accesses the Internet.” EX1007, 10:16-20. Freund addresses challenges, including “hording[sic] available network bandwidth through use of bandwidth-intensive applications (e.g., real-time audio programs).” EX1007, 2:12-14.

83. To enable configuration of such rules, Freund includes “a preferred user interface or ‘wizard’ dialogs for configuring rules” that “provides a ‘view’ of rules governing operation of the Internet access monitor, displaying all of the rules which are available for a current configuration” and “allows the user to create a new rule,” “edit an existing rule,” and “delete a rule.” EX1007, 24:16-24. An example of such a user interface (UI) panel is shown in Figure 7A, reproduced below.



EX1007, FIG. 7A.

84. In addition to configuring rules via a UI, Freund teaches that policies can be loaded from a network element, called a “supervisor,” e.g., explaining that “the Supervisor filters rules appropriate for the client (i.e., application, Host, and other rules), and transmits them to the Client Monitor,” and “the Client Monitor confirms successful reception of rules.” EX1007, 28:14-18. “The Client Monitor” then “saves a copy of the rules onto a local hard disk (i.e., to a local storage medium)” where they are ready for use. *Id.*, 28:18-19.

D. U.S. Pat. No. 8,381,127 (“Singh,” EX1008)

85. Singh generally relates to “displaying windows on a graphical user interface based on relative priorities associated with the windows.” EX1008, Abstract. Singh explains that “[c]omputers and other electronic devices are typically operable to execute multiple applications concurrently,” such as “a word processing application, a web browser application, and an e-mail application.” *Id.*, 1:20-25. However, “[o]ne problem with the simultaneous display of multiple windows is the arrangement of the windows on the GUI” because “[t]he display area of the graphical user interface available to windows is limited.” *Id.*, 1:36-40. Singh notes that “it is desirable to position, size, and/or configure the windows on the GUI in order to maximize the benefit of the display area of the GUI for the user.” *Id.*, 1:40-42.

86. To maximize the benefit, Singh teaches determining the “relative priorities of ... windows of a graphical user interface” so that “[t]he windows are automatically arranged on the graphical user interface based on the relative priorities.” *Id.*, Abstract. Since many device interfaces can display multiple windows simultaneously, Singh further explains that a “higher priority window may cover a lower priority portion of a lower priority window to provide for a simultaneous viewing of the higher priority window and a higher priority portion of the lower priority window.” EX1008, Abstract. The “priorities assigned to each

of the windows may be set by the user, the computer system, or by both the user and the computer system.” *Id.*, 4:52-55.

E. U.S. Pat. App. Pub. No. 2009/0207817 (“Montemurro,” EX1009)

87. Montemurro describes communication devices “capable of at least two communication modes (e.g. WLAN, WMAN and WWAN and/or wired modes)” that “can be configured to optimize communications using a policy-based mechanism to configure connections and routes.” EX1009, Abstract. A “rules engine evaluates its policies on a state change (e.g. network availability, time of day, etc.) to configure a routing table” and “provides an appropriate connection to an application for its respective communications.” *Id.* Policies can be responsive to various factors (e.g., bandwidth, cost, time of day, application type, etc.). *Id.* “Rules engine 206A configures the communication operations with a set of rules/policies.” *Id.*, ¶29.

88. Montemurro gives a “natural language example of a policy” in which “the MP3 download application 204D runs on the lowest cost network” available. *Id.* In another example, “the CRM application ... only synchronizes the sales contact database (e.g. 120B) over a WLAN network.” *Id.*

89. Figure 2 (reproduced below) shows a device configured with the system of Montemurro. *Id.*, Figure 2, ¶¶25-37.

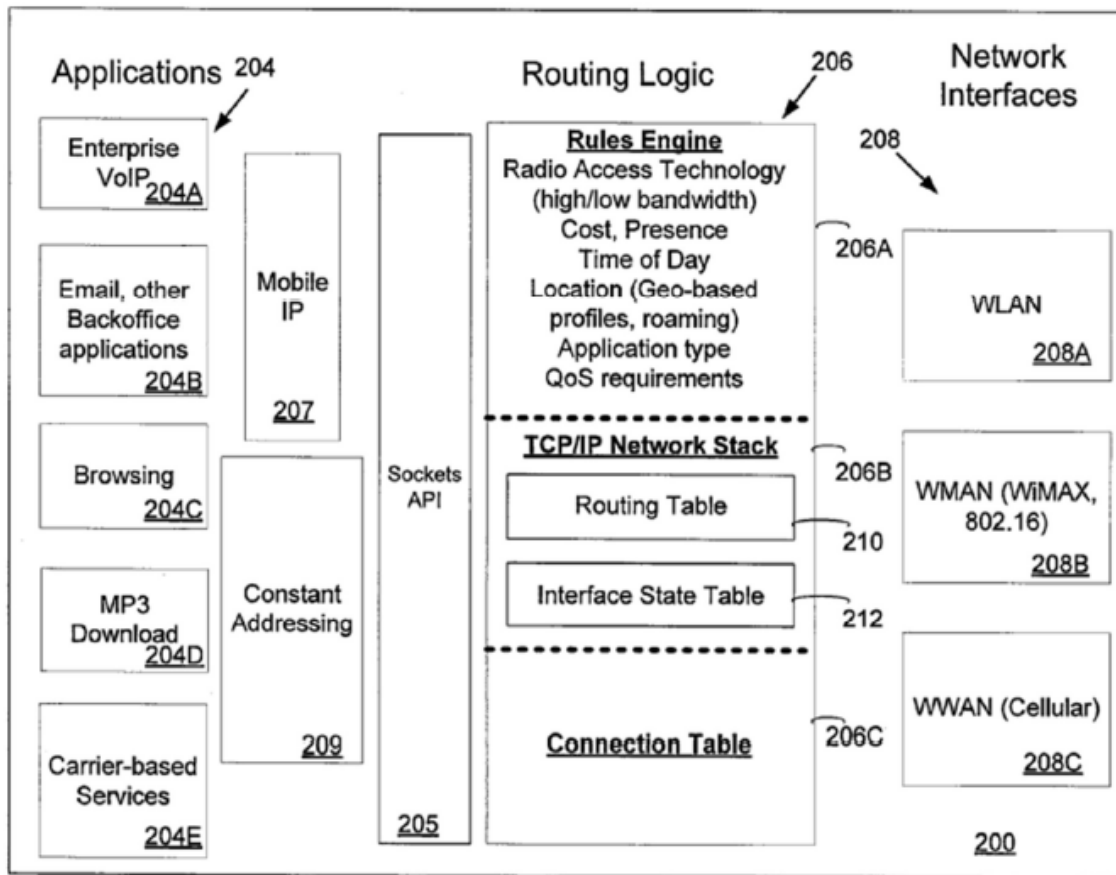


Figure 2

EX1009, FIG. 2

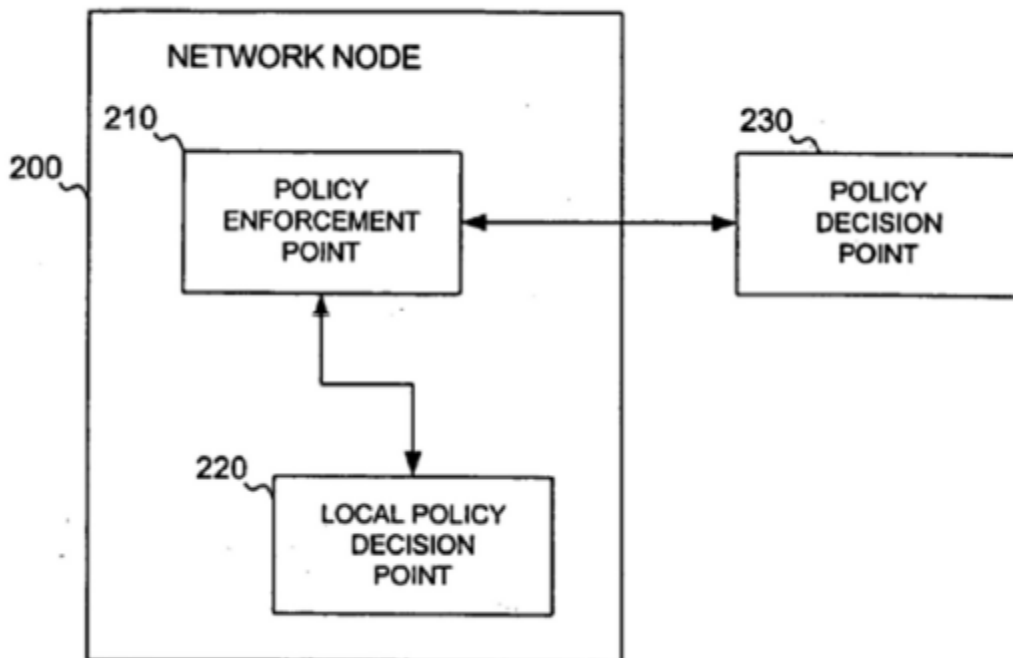
90. Examples of applications that benefit from network selection techniques include “enterprise VoIP application 204A for voice over IP communications in an enterprise data network such as a LAN; email and other back office applications 204B that communicate typically non-voice data; browsing application 204C such as a Web browser, MP3 Download 204D for acquiring audio or other media files and carrier-based services 204E such as SMS and voice communications over a carrier network.” *Id.*, ¶25.

F. U.S. Pat. App. Pub. No. 2006/0039364 (“Wright,” EX1010)

91. Wright describes policy-based management of a multiprotocol label switching (MPLS) network using a Policy Decision Point (PDP) and Policy Enforcement Point (PEP). EX1010, Abstract, ¶20. A POSITA would have known that a PDP is a component that makes policy decisions, and a PEP is a component that enforces the decision made by the PDP. For example, Yavatkar defines a Policy Decision Point (PDP) as “[t]he point where policy decisions are made” and a Policy Enforcement Point (PEP) as “[t]he point where the policy decisions are actually enforced.” EX1022, 3.

92. Wright explains that “MPLS can support explicit traffic engineering via a number of specifications that allow [Labelled Switch Paths (LSPs)] to be managed based on Quality-of-Service (‘QoS’) and other constraints.” *Id.*, ¶19. Traffic engineering was commonly understood to include performance optimization of networks such as the Internet and can include establishing appropriate rules to resolve network performance issues.⁴ Wright’s system architecture is illustrated in FIG. 2, reproduced below:

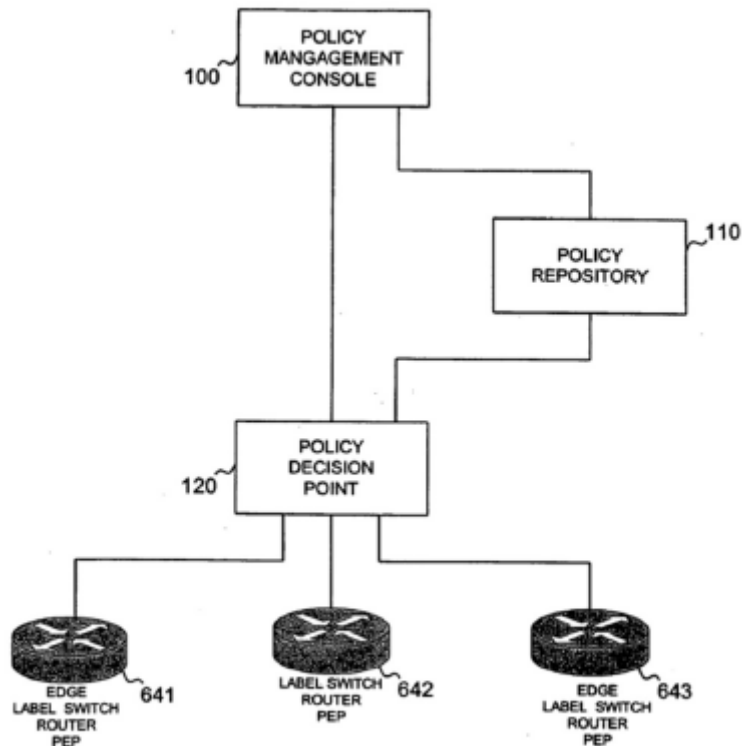
⁴ E.g., see, e.g., “Overview and Principles of Internet Traffic Engineering,” IETF RFC 3272, May 2002.



EX1010, FIG. 2

93. In Wright's architecture, a network node can include a PEP and a Local Policy Decision Point ("LPDP"). EX1010, ¶22. The PEP can use the LPDP to reach a partial decision locally, and the partial decision and the original policy request next can be sent to a PDP that renders a final decision. *Id.* Wright's "policy management system can include feedback from a PEP ... to a PDP," which can include information such as "changes in dynamic state of network resources, link failures and congestion, statistics related to installed policy, etc." *Id.*, ¶23. Wright explains that "information supplied by the PEPs may be used by the PDP to make future policy-based decisions or make changes to current decisions regardless of the implemented policy management model." *Id.* Wright further

explains that “[i]n policy outsourcing, events can occur at the PEPs 130 and require a policy-based decision, and the PEP 130 can request the decision from the PDP 120.” *Id.*, ¶21. In addition, Wright’s PDP provides policy decisions for multiple PEPs, as shown in FIG. 6, reproduced below:



EX1010, FIG. 6

G. U.S. Pat. App. Pub. No. 2003/0172112 (“Vignaud,” EX1011)

94. Vignaud discloses a local proxy that “simulat[es] a service server to make a client application of [a] telephone believe that communication has truly been set up with a service server” to instead “obtain local processing, in the client

apparatus[.]” EX1011, Abstract. Local processing can be used to control network traffic from the device. *Id.*, ¶13. Vignaud’s Figure 2 provides details of the method:

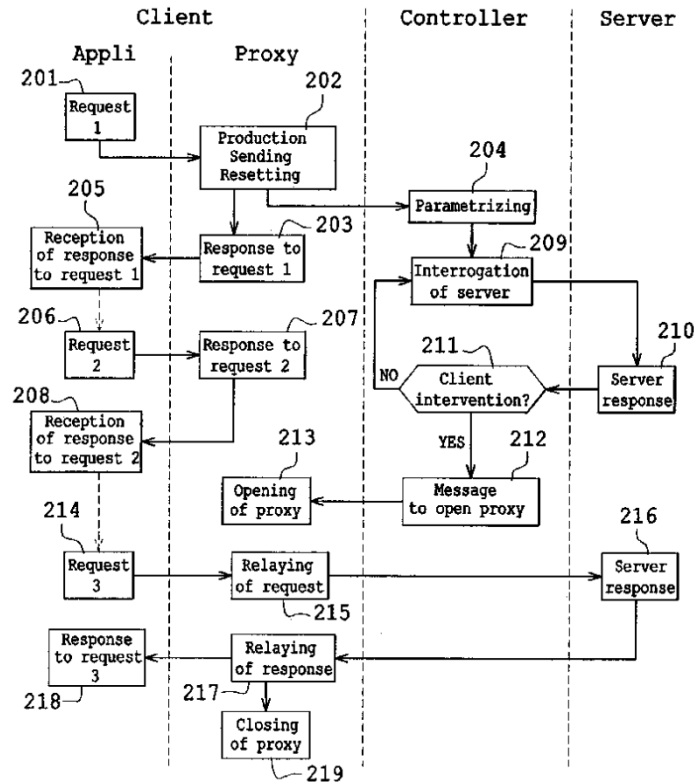


Fig. 2

EX1011, FIG. 2

95. The application of a mobile client sends a request at step 201 and the proxy provides a response at step 203. *Id.*, ¶¶51, 56. The proxy’s response is a “standard response defined by the protocol used” and indicates that the connection to the service server is busy. *Id.*, ¶56. Notably, this response is “aimed at being a decoy for the application 108” to make the application “think that it has set up communication with the service server 115.” *Id.*

X. GROUND 1A: Rao in view of Araujo renders obvious claims 1-2, 4-8, 12-16, 18, 20 and 22-23.

A. Rao-Araujo Combination

96. A POSITA would have found it obvious to combine Rao's remote access client with Araujo's power policy manager and request deflector component to enable a client to control energy usage and "strike[] a balance between providing functionality and maintaining longevity of the charge." EX1006, ¶1. Both techniques for efficient use of device power and for priority-based networking were well-known as of the Critical Date.

97. As discussed in §IX.A, Rao describes policies, which can be specified based on a multitude of factors (e.g., name and type of applications, whether the application is executing in the foreground or background, etc.), and how its system leverages each of these policies for prioritization. EX1005, ¶¶182-84. Rao further provides functionality to control an application's network access by intercepting network packets, determining packet prioritization based on the application, and selectively communicating packets to the network based on the packet prioritization. EX1005, ¶¶184-95. In Rao, these prioritization operations can be performed by one or more "network drivers of a network stack 310" (e.g., by "customiz[ing], modif[y]ing] or adapt[ing]" the network drivers "to provide a custom or modified portion of the network stack 310 in support of any of the techniques"). EX1005, ¶100. For example, the Rao system can include "[a] filter

322 [to] place, arrange, or coordinate network packets into queues 540a-540n in support of the priorities,” and these “queues 540a-540n may be included in a network driver, such as an NDIS driver for the filter 322.” *Id.*, ¶¶143, 180, 191.

98. In implementing such functionality, a POSITA would have sought opportunities for improving the policy management capabilities in Rao to impart additional advantages, such as optimizing power use. As noted above, it was well-known that mobile devices use techniques for optimizing the use of constrained resources, including network bandwidth and battery power. A POSITA would have recognized the importance of power management at least because, in mobile devices, applications cannot execute without sufficient power. EX1006, ¶1 (“Battery-powered machines have a finite amount of energy stored between charges, and these machines generally attempt to use the energy in a way that strikes a balance between providing functionality and maintaining longevity of the charge.”)

99. Consequently, a POSITA would have looked to policy-based power management such as taught in Araujo to serve as one of Rao’s “multitude of ways to define client-side application priorities. EX1005, ¶182. The resulting Rao-Araujo Device (RAD) would both manage power according to the power policy manager techniques of Araujo and manage network use according to the techniques of both Rao and Araujo.

100. In implementing the combined RAD device, a POSITA would have incorporated Araujo's power policy manager and request deflector components in Rao's remote access client. A POSITA would have recognized that both components serve similar roles, specifically in managing network traffic. The enhanced remote access client in RAD would evaluate policies as taught by each of Rao and Araujo – i.e., both power-management policies (as taught by Araujo) and network prioritization policies (as taught by Rao and Araujo). Again, as noted above, such policy-based management techniques were well-known as of the Critical Date. For example, RAD would have determined whether an application has a “relative level of justification to consume power,” which includes determining whether the application is running in the foreground or background. EX1005, ¶182; EX1006, Abstract. A POSITA would have recognized that an application running in the foreground of the interface can interact with a device user, and therefore should be treated as relatively high priority. Applications running in the background often perform non-time-sensitive tasks, and in such cases, can be assigned lower priority.

101. Further, from Rao and Araujo, a POSITA would have understood and found obvious that policy enforcement in the Rao-Araujo Device may be based on application state (foreground, background) and power state (battery/plugged-in). EX1005, ¶182; EX1006, ¶¶4, 11. As one example, when a request to transmit

network packets arrives, a POSITA would have recognized that RAD enforces a particular policy (i) when an application is in the foreground (per Rao) giving it “VIP” status (per Araujo and based on the foreground application state of Rao), and (ii) when the power state of the device indicates the battery is above a threshold charging level. EX1006, ¶22.

102. In such cases, RAD would permit the transmission (since the battery is sufficiently charged) and place the packets in a high-priority queue (for the VIP application). The application is high priority and the battery charge is high, so the application’s activities would typically be permitted.

103. In another example, a POSITA would have recognized that RAD enforces a different policy (i) when an application is in the background (per Rao) not giving it “VIP” status (per Araujo and based on the background application state of Rao), and (ii) when the power state of the device indicates the battery is above a threshold charging level. EX1006, ¶22.

104. In such cases, RAD would permit the transmission (since the battery is sufficiently charged) and place the packets in a lower-priority queue (for the non-VIP application). Note that, if the network is lightly loaded, even packets in a lower-priority queue can be transmitted promptly. Priority queuing tends to differentially impact traffic most dramatically when networks are more heavily loaded much like automotive traffic lanes reserved for high-occupancy vehicles

provide more benefit when traffic is heavy than when traffic is light. A POSITA would be aware that scheduling based on priority is a subject often considered when scheduling jobs within computer operating systems and can entail a risk that lower-priority packets could be subject to indefinite blocking, a term often called “*starvation*.” EX1031 at 134. To ensure that all packets in a queue, even low-priority packets, are eventually serviced, a POSITA would be aware of the concept of “*aging*[,]” which involves gradually increasing the priority of low-priority items to ensure that they are eventually serviced. *Id.* This could mean that in one example, packets would meet a certain priority threshold and be moved into a higher-priority queue if they have been waiting for a long time. *Id.* at 134-35.

105. In still another example, a POSITA would have recognized that RAD enforces yet a different policy (i) when an application is in the foreground (per Rao) giving it “VIP” status (per Araujo and based on the background application state of Rao), and (ii) when the power state of the device indicates the battery is below a threshold charging level. EX1005, ¶3; EX1006, ¶22.

106. In one such case, RAD would place the packets in a high-priority queue (for the VIP application) but would hold the transmission until a more favorable power state existed. Such behavior is advantageous since, when battery power is lower, the transmission can cause the battery to drain completely, disabling the device.

107. In another case (where the application is in the foreground and power state is low), RAD may queue packets and (per Araujo) operate “in a ‘batch’ mode that conserves power by allowing network transmissions to happen in bursts...at specific intervals (e.g., every fifteen minutes). *See* EX1006, ¶43. Whether operating in batch mode or not, a POSITA would have found RAD’s queueing of packets desirable to save power in case packets may be transmitted once the power level increases (e.g., the user plugs in the device and/or charges it above the low power threshold) and/or to improve overall application flow by conserving power to avoid a worse disruption due to unplanned/catastrophic power loss.

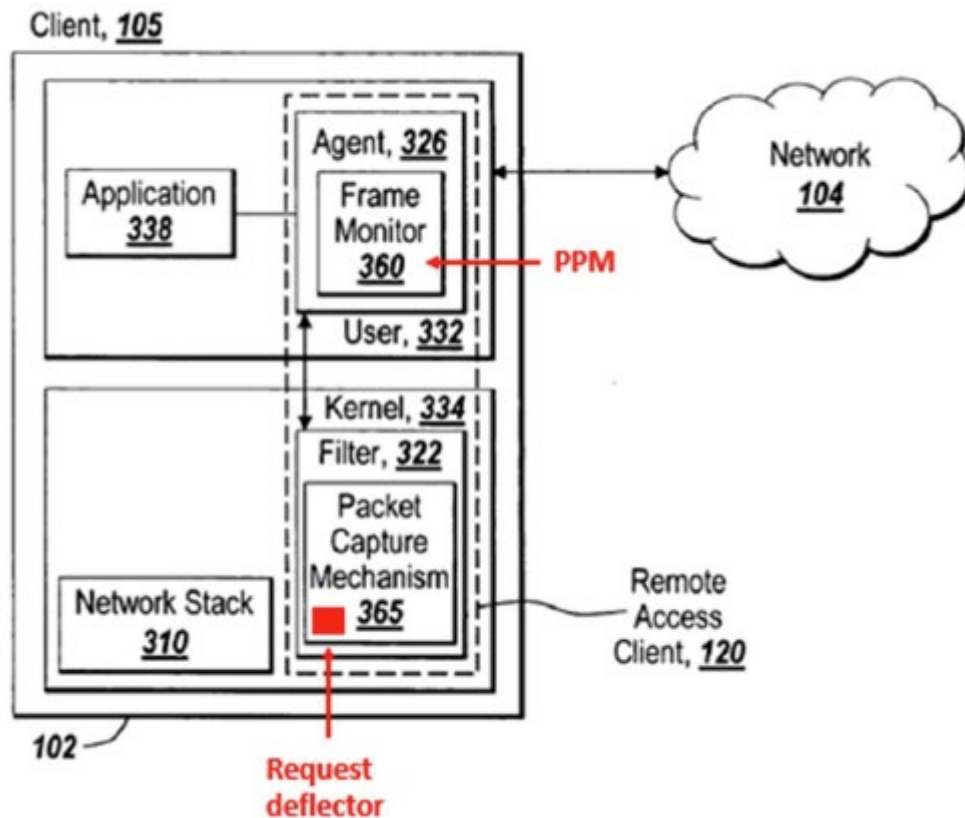
108. In another case (where the application is in the foreground and power state is low), RAD would use Araujo’s prompt-to-continue feature by indicating a low power state and asking the user via dialog box “Would you like to proceed anyway?”, before transmitting any further packets. *See* EX1006, ¶41. A POSITA would have used the prompt-to-continue feature to conserve power by not transmitting packets until the user approves and proceeds through the dialog box (e.g., the user might proceed because they plan to soon charge the device).

109. In yet another example, e.g., when an application is running in the background and the power level is low, RAD can enforce a policy that results in RAD’s request deflector preventing the request from being passed to the device driver, not queuing the packet and further conserving power. EX1006, ¶5. Even

passing data to a driver can consume power, so in certain circumstances, blocking such interactions further conserves power.

110. From these examples, and as Rao describes, a POSITA “will recognize and appreciate the multitude of ways to define client-side application priorities.” EX1005, ¶182. Accordingly, a POSITA would have been motivated to use Araujo’s power-management policy to improve Rao’s network-related prioritization scheme.

111. A POSITA would have expected success integrating a power policy manager and deflector components as taught by Araujo’s into a remote access client as taught by Rao. As described above, the request deflector (Araujo) and packet capture mechanism (Rao) serve similar functions, and the PPM (Araujo) and frame monitor (Rao) both enforce policy. Combining such functions would have required only routine programming skill well within the skill set of a POSITA. An illustration of the combined Rao-Araujo device is shown below.



Rao-Araujo Device (RAD)

112. Since Araujo's request deflector is "interposed between the program and the device driver" and Rao's filter "may include a packet capturing mechanism 365, and the filter 322 and/or packet capturing mechanism 365 may comprise a network driver," RAD's request deflector would reside in the filter interposed between the other packet capture components and network device driver that provides traffic to the network stack, as shown in the figure above. EX1005, ¶101, FIG. 1C (annotated); EX1006, ¶5.

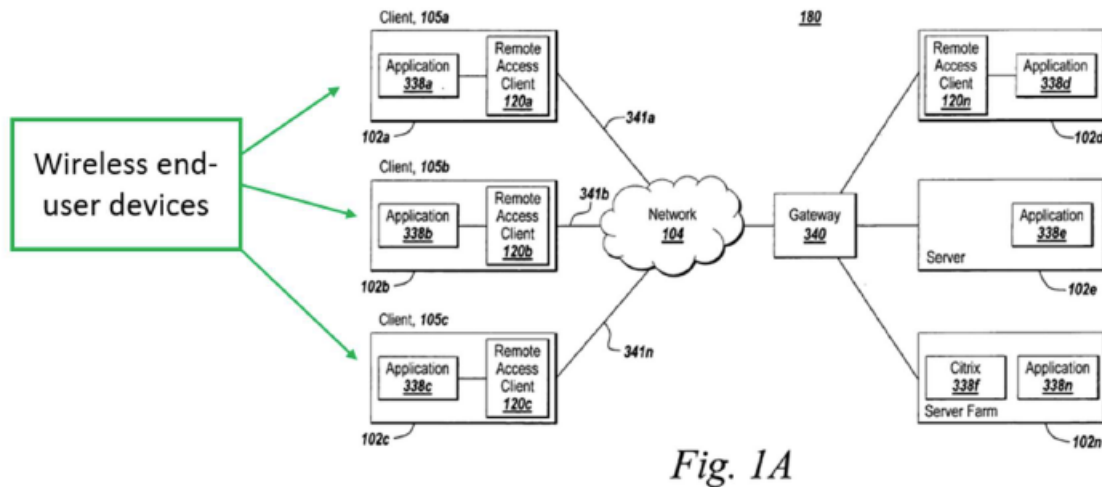
113. Such a combination would have required only routine programming knowledge well within the skill of a POSITA prior to the earliest effective filing date. Indeed, the change would have amounted to nothing more than the use of a known technique to improve similar devices—in each instance a smart phone equipped with network interfaces—in a similar way, and combining prior art elements according to known methods to yield the predictable results described above.

114. For example, both Rao's and Araujo's devices include interfaces between a processor that executes the described functions and network devices that provide communication functions. EX1005, FIGS. 1D-1E, ¶¶118-19, 121-22, 125, 128-30; EX1006, Figure 2, ¶¶34-35. A POSITA would have known that such processors commonly run applications such as Rao's remote access client and Araujo's deflector component. EX1005, ¶114; EX1006, ¶36. Therefore, the combination of the techniques of Araujo into the techniques of Rao in a combined Rao-Araujo device would require only routine programming knowledge.

B. Analysis of the Claims

[1.1] A wireless end-user device, comprising:

115. To the extent the preamble is deemed limiting, RAD (*see* §X.A) renders it obvious. *E.g.*, EX1005, ¶¶30, 86; EX1006, ¶14. Rao teaches a client that is a wireless end-user device, as shown in Fig. 1A:



EX1005, FIG. 1A (annotated)

116. Rao’s “environment 180 includes multiple computing devices 102a-102c [or ‘clients 105a-105c’] connected to a network 104 via one or more network connections 341a-341n.” EX1005, ¶86. “Moreover, the computing device 102 can be any workstation, desktop computer, laptop or notebook computer, server, handheld computer, mobile telephone, any other computer, or other form of computing or telecommunications device that is capable of communication and that has sufficient processor power and memory capacity to perform the operations described” in Rao. EX1005, ¶130. Likewise, Araujo teaches that electronic devices include wireless telephones and “normally employ some type of power management framework.” EX1006, ¶14. A POSITA would have known that these teachings, including a wireless telephone, disclose a wireless end-user device.

[1.2] a wireless modem to communicate data for network service usage activities between the device and a wireless network;

117. The Rao-Araujo combined device renders [1.2] obvious. *See* EX1005, ¶¶172, 198.

118. Specifically, in Rao, a computing device includes a network interface, which can comprise a “**wireless network adapter**,” a “**modem** or any other device suitable for interfacing the computing device 102 to any type of network capable of communication[.]” EX1005, ¶125. Rao also teaches that the network interface of its device “interface[s] to ... wireless connections” and, thus, communicates data between the device and a wireless network. *Id.* Moreover, Rao’s device may be implemented as a “smart phone,” which a POSITA would have understood and found obvious includes a wireless modem. EX1005, ¶198. For example, the iPhone released in 2007 included a wireless modem. Cole further demonstrates that mobile devices commonly included wireless modems, explaining that a “mobile device 110 includes ... a plurality of communication interfaces 225” and “[e]xemplary communication interfaces 225 that may be provided include a WWAN modem 230, a WLAN modem 235...” EX1023, ¶¶34-35.

119. Further, the wireless modem in RAD would have been configured as described in Rao, where a modem communicates data for network service usage using mechanisms for data transfer for Internet network service, such as a

“maximum transmission unit 402*a*-402*b* (MTU) parameter” that “indicate[s] the size of the largest unit of data that can be sent over a type of physical medium in a network, [and] indicates the largest datagram or packet than can be transmitted by an Internet Protocol (IP) layer interface.” EX1005, ¶172.

120. A POSITA would have understood that IP is used by an Internet network, and RAD thereby teaches and/or renders obvious a wireless modem to communicate (e.g., transmit using the MTU parameter) data for network service usage activities between the device and a wireless network. Rao’s client intercepts network packets “associated with an application[.]” EX1005, ¶184. Network packets are “network communications of the client associated with an application of the client” that are, for example, intended to be communicated “via a network stack of the client.” *Id.*, ¶¶38, 40, 43, 82 (describing protocols for network packets), 95 (describing Rao’s network 104 for its network packets), 99 (disclosing that “remote access client 120 ... rout[es] network packets from a client 105 to a network 104.”). A POSITA would have recognized that, in RAD, intercepted packets are examples of network service activities. This corresponds with the ’544 Patent, which discloses network service usage activities as including “network resource requests, network data accesses or other network interaction.” EX1001, 10:60-11:6; *accord* EX1026, 13-15.

[1.3] a processor that executes instructions to associate network service usage activity, on behalf of a first device application, and that occurs when the first device application is not in the foreground of user interaction, with a network service usage control policy,

121. The Rao-Araujo device renders [1.3] obvious. See EX1005, ¶¶118-19, 182, 187.

122. The Rao-Araujo device discloses a processor that executes instructions. For example, Rao Fig. 1D shows a processor (“CPU 121”) to execute instructions. CPU stands for “central processing unit,” which was commonly shortened to “processor.” EX1005, Fig. 1D.

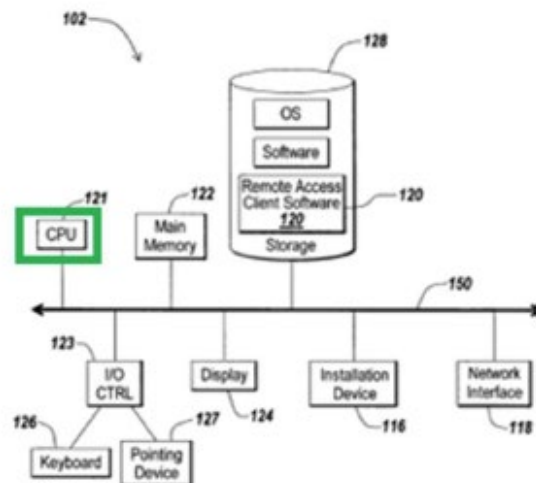


Fig. 1D

EX1005, FIG. 1D (annotated)

123. Rao describes that “in FIGS. 1D and 1E, each computing device 102 includes a central processing unit 102, and a main memory unit 104.” *Id.*, ¶118. Rao discloses, and a POSITA would have understood and found it obvious, that the processor in the Rao-Araujo Device executes instructions since Rao teaches a processor is “any logic circuitry that responds to and processes instructions fetched from the main memory unit 104.” EX1005, ¶119. More generally, processors were known to perform the “instruction cycle,” which consists of fetching an instruction, decoding it and executing the decoded instruction. This sequence is sometimes shortened to fetch- execute. Moreover, processors were conventional features of mobile devices.

124. Rao’s processor executes instructions to associate network service usage activity with control policies “for specifying client-side prioritization of network communications related to applications.” EX1005, ¶182. Rao applies policies when network service usage activity of a first device application *occurs when the first device application is not in the foreground of user interaction*. EX1005, ¶¶182-87. Rao “policies 520 define prioritization based on whether an application is running in the foreground or the background of the client 105.” EX1005, ¶182. Rao further contemplates foreground applications as “currently in active use by the user.” *Id.*, ¶3. A POSITA would have understood and found it obvious that the processor in the Rao-Araujo Device *executes instructions* to

associate network service usage activity, on behalf of a first device application, with a network service usage control policy. EX1005, ¶¶119, 182-87.

125. A POSITA would have understood and found obvious that Rao's applications in the background and not in active use disclose, for example, applications not in the foreground of user interaction. A POSITA would have understood and found obvious that reference to applications "not in the foreground" (quoting the '544 Patent's claim limitation [1.3]) includes, for example, applications in the background and thereby are subject to policies 520. EX1005, ¶182. A POSITA would have understood the applications are either in the foreground or background. For example, Paquette teaches that a foreground application "may refer to an application that is currently configured to receive certain input, such as input from a keyboard," while in contrast, a background application "may refer to an active application that has a corresponding window on the screen 116 but that is not the foreground application." EX1019, 6:31-44.

126. Rao also teaches associating network service usage activity of an application with a network service usage control policy. For example, Rao teaches "one or more policies 520 for specifying client-side prioritization of network communications related to *applications*." EX1005, ¶182. Rao intercepts network packets and queues them "based on the type and/or priority of the application 338a-338n," which a POSITA would have understood teaches associating network

service usage activity, on behalf of a first application, with a network service control policy. EX1005, ¶184. For example, Rao teaches that the remote access client “determines the association of network packets with applications” to “determine priorities and apply any priority based policies” and “can associate network traffic with applications 338a-338n by any suitable means and/or mechanisms.” *Id.*, ¶187. Accordingly, Rao teaches packet interception techniques, which a POSITA would have understood and found obvious to include associating applications with network service activities. EX1005, ¶184.

127. A POSITA would have known that because Rao’s policies can define prioritization based on whether an application is running in the foreground or the background of the client, Rao’s processor executes instructions for its remote access client to associate network packets with applications to determine priorities, and apply priority based policies. Otherwise, without knowing the association of a packet to the application, Rao could not determine whether the application is in the foreground or background. RAD thereby renders obvious associating network service usage activity, on behalf of a first device application, and that occurs when the first device application is not in the foreground of user interaction, with a network service usage control policy. EX1005, ¶¶182, 187. Accordingly, a POSITA would have found that the Rao-Araujo device renders [1.3] obvious.

[1.4] set an application state indicating whether the first device application, associated with a particular network service usage activity, is in the foreground of user interaction, and

128. RAD renders [1.4] obvious. *See* EX1005, ¶¶182, 184.

129. As described in §IX.A, Rao provides non-limiting disclosure of applying policies, which a POSITA would have understood and found obvious to involve setting an application state.

130. A POSITA would have known that to evaluate a policy that involves application state (e.g., foreground or background), the application state must be set in the system. For example, a POSITA would have known that the system would store (set) the application state in a variable and use that variable when evaluating the conditional portions of policies. As one example, Rao explains that policies “define prioritization based on ***whether an application is running in the foreground or the background*** of the client 105.” EX1005, ¶182. Rao further teaches the agent uses characteristics of the application “such as running in the foreground or background, to indicate priority for a network packet of the application.” *Id.*, ¶189. In this example, a POSITA would have understood and found obvious that applying a policy to prioritize network packets for an application involves setting an application’s state (e.g., foreground, background) to permit the evaluation of policies that rely on the application state. As another example, in Rao’s policies “may be specified conditionally” based on application

state (e.g., “if one application 338a is running,” *id.*, ¶182), where a foreground application may be “currently in active use by the user.” *Id.*, ¶3. A POSITA would have similarly understood and found obvious in this example that the policy depends on application state (e.g., “is running”), and thus, use of the policy includes setting an application state so the policy may be applied. A POSITA would have understood that Rao’s specifying a policy to define or indicate prioritization based on whether an application is running in the foreground or background discloses or at least renders obvious “*set[ting] an application state*” indicating whether the application is in the foreground of user interaction. Setting the application state enables Rao to determine whether to apply its policies.

131. Rao further teaches packet interception techniques, which a POSITA would have understood and found obvious to include *associating applications with network service activities*. Rao’s client intercepts network packets “associated with an application” and determines “a priority for the intercepted and queued network packet ... based on the type and/or priority of the application.” Rao, ¶184. As discussed, a POSITA would have recognized that, in the Rao-Araujo Device, intercepted packets are examples of network service usage activities associated with an application (*see* § X.B ([1.2])), and that Rao prioritizes the packets based on an application state (e.g., the associated application being in the foreground or background). In general, in RAD, an application is in the foreground or

background, and based on that application state, packets can be treated differently, e.g., by placing them in different queues.

[1.5] dynamically determine whether to apply the network service usage control policy to the particular network service usage activity, based on the application state and based on a power control state; and

132. RAD renders [1.5] obvious. *See* EX1005, ¶182; EX1006, ¶¶4, 11, 22, 25, 28.

133. For example, Rao teaches policy evaluation based on application state, such that “prioritization [is] based on whether an application is running in the foreground or the background.” EX1005, ¶182. A POSITA would have recognized “foreground” and “background” as examples of application states. *See* § X.B ([1.4]).

134. Araujo teaches that “devices may have various power states” including “‘On’ and ‘Off.’” EX1006, ¶4. Araujo also discloses other exemplary power states, including “different brightness levels” for a display and “different clock speeds” for a processor. *Id.* According to Araujo, “a justification to change a device from one power state to another may be based on at least one factor other than the mere fact that a request to use the device has been made.” *Id.*, ¶25. Araujo discloses that the “current power state of a device may be a factor in determining whether the power state will be changed.” EX1006, ¶28. A POSITA would have recognized that Araujo’s disclosure that “power state of a device” is a power

control state and a “factor in determining whether the power state will be changed” indicates that the power control state is used to determine whether to apply a policy regulating network service usage. For example, power control policies were well-known as of the critical date. *See, generally*, EX1014.

135. As described in §X.B ([1.3]-[1.4]), a POSITA would have understood and found obvious that policy enforcement in RAD may be based on application state (foreground, background) and device power state (battery, plugged-in), and thus, RAD renders obvious dynamically determining whether to apply the network service usage control policy (e.g., Rao’s remote access client’s policies combined with Araujo’s power policy manager) to network service usage activity of an application (e.g., associated to an application based on Rao’s packet interception techniques), based on the application state (foreground/background) and based on a power control state (e.g., power state of a device). EX1005, ¶182; EX1006, ¶¶4, 11. Rao-Araujo’s determination to apply the policy is “dynamic” because, for example, it is based on a power control state and application state that can change based on the power level of the device, battery demand, an application’s activity, and a user’s interaction with an application. EX1006 ¶¶28-30 (disclosing “[c]urrent power state” and “current amount of energy remaining” that are dynamic considerations); EX1005, ¶3 (describing foreground applications as “currently in active use by the user”). This is consistent with the ’544 Patent, which identifies

user input, application behavior, power state of the device, and device usage as exemplary ways policies may be dynamically applied. *See* EX1001, 88:38-56; *see also id.*, 16:4-9.

136. As one example, when a request to transmit network packets arrives, a POSITA would have recognized that RAD enforces a particular policy (i) when an application is in the foreground (per Rao) giving it “VIP” status (per Araujo and based on the foreground application state of Rao), and (ii) when the power state of the device indicates the battery is above a threshold charging level. EX1006, ¶22. In such cases, RAD would permit the transmission (since the battery is sufficiently charged) and place the packets in a high-priority queue (for the VIP application).

137. In another example, POSITA would have recognized that RAD enforces a different policy (i) when an application is in the background (per Rao) not giving it “VIP” status (per Araujo and based on the background application state of Rao), and (ii) when the power state of the device indicates the battery is above a threshold charging level. EX1006, ¶22.

138. In such cases, RAD would permit the transmission (since the battery is sufficiently charged) and place the packets in a lower-priority queue (for the non-VIP application). This technique would yield the expected behavior of prioritizing VIP packets over non-VIP packets. Since the power level is high in both cases, both high-priority and low-priority network packets can be transmitted.

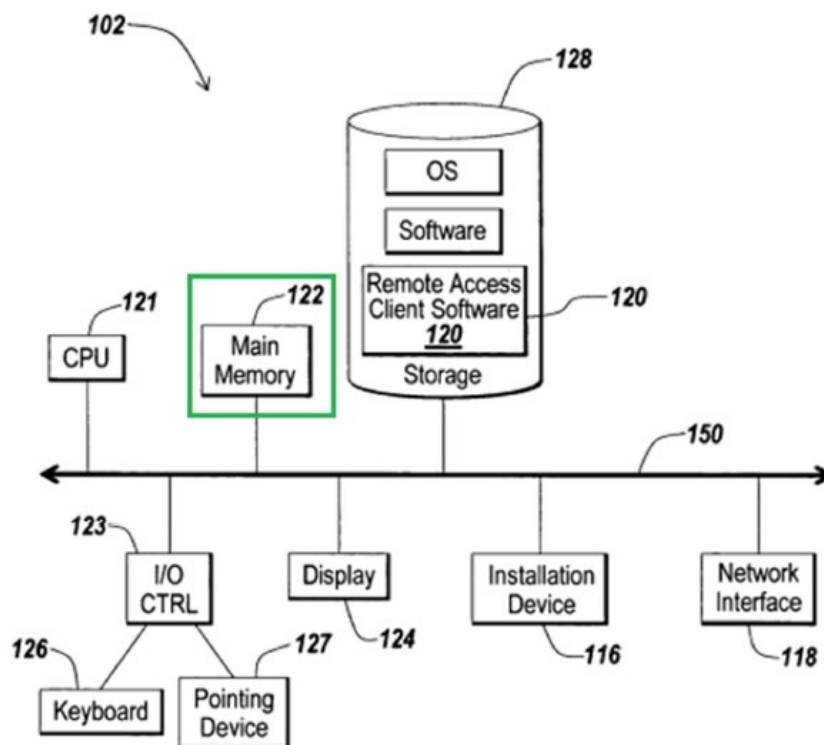
Beyond these particular examples, a POSITA would have recognized and appreciated “the multitude of ways to define client-side application priorities.”
EX1005, ¶182.

139. In one example, if the power level was somewhat lower, a policy would state that VIP packets can flow, but non-VIP packets are held. If the power level was still lower, no transmissions would occur, except for system-critical packets, such as updating anti-virus in response to an imminent threat.

[1.6] a memory coupled to the processor to provide the processor with the instructions.

140. RAD renders [1.6] obvious. See EX1005, ¶¶119-20, FIG. 1D

141. For example, Rao’s Figure 1D shows a main memory 122:



EX1005, FIG. 1D (annotated)

142. The main memory 122 is connected to bus 150 which delivers instructions to CPU (processor) 121.

143. Rao further teaches that the processor (CPU) “is any logic circuitry that responds to and processes instructions fetched from the main memory unit 104” and “the processor 100 communicates with main memory 104 via a system bus.” EX1005, ¶119-20. A POSITA would have recognized that Rao’s system bus couples the processor to the memory, and the memory provides instructions fetched by the processor. This was—and still is—a common architecture for computing systems.

[2] The wireless end-user device of claim 1, wherein the processor executing the instructions determines that the first device application is in the foreground of user interaction when the user of the device is directly interacting with that application or perceiving any benefit from that application.

144. Rao-Araujo renders [2] obvious. *See* EX1005, ¶¶3, 180, 182-83.

145. Rao determines whether an application is in the foreground or background e.g., “the policies 520 define prioritization based on whether an application is running in the foreground or the background of the client.” EX1005, ¶182; *see also id.*, ¶188. Examples of Rao’s applications include VoIP, email, collaboration, etc. EX1005, ¶179.

146. As discussed in [1.3] and [1.4], Rao applies policies based on applications being in the foreground or background, and contemplates exemplary foreground applications as “*currently in active use by the user.*” EX1005, ¶3; *see also id.*, ¶¶182, 188. Rao teaches that some foreground applications are in active use, e.g., explaining that, “although *an application is running in the foreground and currently in active use by the user*, a network packet generated or received for an application running in the background may be processed ahead of a network packet generated or received for the application running in the foreground.” EX1005, ¶3. Rao teaches that current active use by the user indicates that the application is in the foreground of user interaction when the user is directly interacting with that application. Note that a lack of active use does not necessarily indicate that the application is not in the foreground. For example, a user might have placed down the mobile device, and therefore not be actively using it, but the application can remain in the foreground. Rao thus teaches or renders obvious determining whether to apply its policy based on determining that the application is in the foreground of user interaction and when the user is directly interacting with that application (e.g., when it is currently in active use by the user).

[4] The wireless end-user device of claim 1, wherein when the network service usage control policy is applied it disallows the particular network service usage activity, and wherein the processor executes the instruction further to, when it is determined that the particular network access request is disallowed, queue that particular network service usage activity until a power state change occurs.

147. Rao-Araujo renders [4] obvious. *See* EX1005, ¶¶192, 194; EX1006, ¶39.

148. For example, Araujo teaches “various example actions that may be performed if the power state change is not allowable under the policy” such as disallowing and queuing “a program’s request to be processed at some later time.” EX1006, ¶¶38-39. Araujo’s “request[s]” include, for example, “a request to send data over a wireless network.” *Id.*, ¶20. Rao similarly teaches the queuing of requests, explaining that “network packets for an application” are placed in a queue associated with the application and “communicated from the queues ... according to the determined priorities for the network packets.” EX1005, ¶¶192, 194.

149. Araujo discloses that, if a program requests to use a device (e.g., a network card) that is turned off, and the power management policy does not allow the device to be turned on at the time of the request, the request may be queued. EX1006, ¶39. (“if a program requests to use a device that is turned off (e.g., a disk, a network card, etc.), and the power management policy does not allow the device to be turned on at the time of the request, the request may be queued so that it can

be serviced at some later.”); *see also id.*, ¶¶20-21 (discussing requests to a “network card”). Then “at some later time the power management policy allows the device to be turned on, then the program's request may be dequeued and processed (although a request could stay in a queue indefinitely while waiting to be processed, or could be denied asynchronously at a later time).” EX1006, ¶39, FIG. 4 (element 404), *see also id.* ¶¶35-36 (describing handling “requests” when the policy does not allow a change in power state, “the request may be processed in the manner shown in FIG. 4 (at 212)”), 39 (“One such action is to queue a program’s request to be processed at some later time (block 404).”), FIGs. 2, 4.

150. A POSITA would have understood this to disclose queuing network requests until a power state change occurs and/or a more favorable power state is reached. Because Araujo lists a network card as an example of a device that can be turned off to disallow a particular network service usage activity, a POSITA would have understood that Araujo’s teachings of queuing requests for network activity apply to particular network service usage activity. *See* §X.B ([1.2]) It would have therefore been obvious to a POSITA that the Rao-Araujo Device’s processor executes instructions to queue network activity requests (as Rao teaches by queueing network packets and Araujo teaches in queuing requests for network activity via a network card) when they are disallowed until a power state change occurs (as Araujo teaches) because queuing requests until they can be serviced

was common in the field. In an alternative example, it would have been obvious in the Rao-Araujo Device to queue packets by operating in Araujo's "batch" mode that conserves power by allowing network transmissions to happen in bursts ... at specific intervals (e.g., every fifteen minutes). EX1006, ¶43. As Araujo discloses, "the request may be delayed until the next time that the network card is scheduled to be powered on, at which time the request could be allowed." EX1006, ¶43, FIG. 4 (element 414). A POSITA would have understood this to disclose that the Rao-Araujo Device's processor executes instructions to disallow-and-queue a request for particular network service usage activity until a power state change occurs (e.g., "until the next time that the network card is scheduled to be powered on").

[5] The wireless end-user device of claim 1, wherein when the network service usage control policy is applied it disallows the particular network service usage activity, and wherein the processor executes the instruction further to, when it is determined that the particular network access request is disallowed, queue that particular network service usage activity until a power state change occurs.

151. The Rao-Araujo device renders [5] obvious.

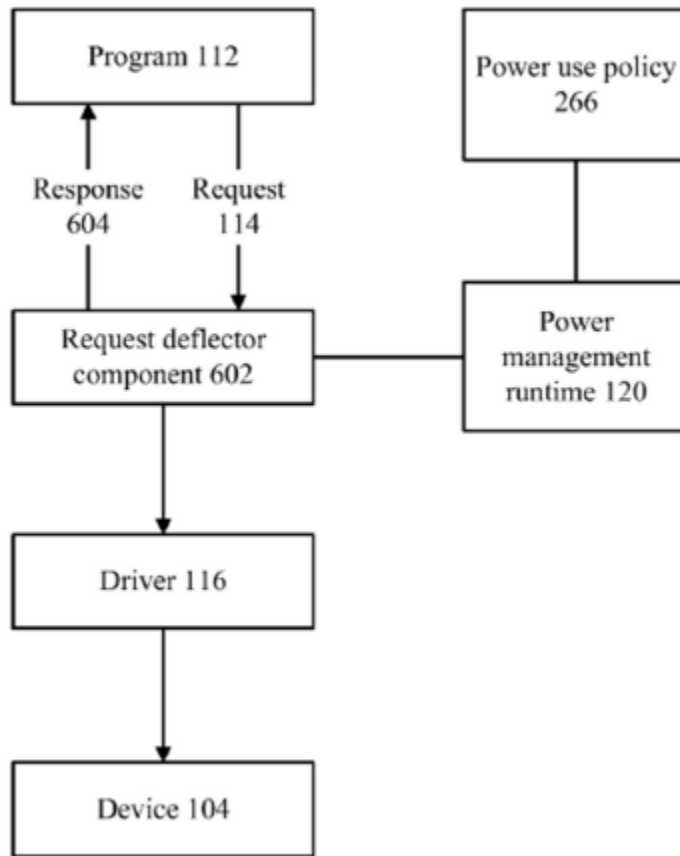
152. An "emulated network access API" is an API that emulates network access. A POSITA would have understood "emulate" to mean "the process by which one system or device mimics the operation of another."

153. For example, “emulation” may include the “process by which one system or device mimics the operation of another, most typically by a computer running suitable software.” EX1017 at 3.

154. The prior art also describes an emulation module for a “socket API 220” that performs “socket API call emulation.” EX1024, Abstract, FIG. 2. Like Araujo’s “request deflector component” being “interposed” between applications and drivers, Sng’s socket API 220 is similarly interposed between applications (e.g., application 210) and drivers (e.g., non-networked I/O device driver 240, networked I/O device driver 250). See *id.*, 3:46-5:10; *see also* EX1006, ¶50.

155. Therefore, a POSITA would have understood that a first API emulates a second API by providing the same interface. In one simple example, a computer system can include a “send” API call that accepts as a parameter the data to be sent, and when the “send” API is invoked, the data are sent. A second API can emulate the first API by also providing a “send” API call. Typically, the second API would provide additional function beyond the function provided by the first API, e.g., by logging all messages, ensuring guaranteed delivery, providing QoS support, etc.

156. Araujo’s request deflector component 602 teaches and/or renders obvious an “emulated network API,” as shown in Araujo FIG. 6, reproduced below.



EX1006, FIG. 6

157. Araujo explains that “a component may be interposed between the program and the device driver to deflect requests based on power management policy,” which Araujo calls a request deflector. EX1006, ¶¶48, 50. A POSITA would have recognized that the request deflector implements the Rao-Araujo policy via communication with an application through an emulated network access API, as the request deflector accepts requests from the application and provides responses to it, as illustrated in FIG. 6. EX1006, FIG. 6. In a non-emulated case, the requests 114 and responses 604 would flow directly from the program 112 to the driver 116, bypassing the emulation layer (request deflector component 602).

158. Araujo explains that the “driver inform[s] a program that use of a device is denied because the device is off.” EX1006, ¶ 48. Such responses from a called function to a caller are common across most computer systems and programming languages and enable programs to function more effectively. For example, upon receiving such a failure notice, the program can log the error or provide a message to a systems administrator. Absent such a response, the administrators would have little understanding of the system operation. For example, the issue could have been a malfunction (a bug in the program, a hardware failure, etc.) instead of proper system operation that results in denying the operation.

159. Araujo explains that “the existence of a rich power management policy means that a program might be denied use of a device for power-related reasons that are separate from the question of whether the device is powered on or off at the time of the request” and the “existence of a component between the program and the driver helps to decouple the question of whether a device is on or off from the question of whether a program is allowed to use the device under the ambient power management policy.” EX1006, ¶48. As described above, there are situations in which a program is not allowed to use a functioning device, e.g., to save power.

160. Therefore, a POSITA would have understood or found obvious that Araujo discloses cases where the device is powered on and there is an available wireless network, but the application is still denied access by a dynamic determination of Araujo's power management policy to the particular network service usage activity (request) that indicates to the application that the available wireless network is nevertheless unavailable (e.g., "decoupl[ing] the question of whether a device is on or off" from "whether a program is allowed to use the device under the ambient power management policy"). *Id.*

161. Thus, the Rao-Araujo device renders obvious [5], including because it discloses a processor that executes instructions to implement a network service usage control policy at least in part via communication with the first device application through an emulated network access API that indicates to the first device application (e.g., program 112 in EX1006, FIG. 6) that an available wireless network is unavailable (e.g., that the device is powered on but the program is denied access) when a dynamic determination applies the network service usage control policy (e.g., the power management policy) to the particular network service usage activity (e.g., request). EX1006, ¶ 48.

[6] The wireless end-user device of claim 1, wherein when the network service usage control policy is applied it disallows the particular network service usage activity, and wherein the processor executes the instruction further to, when it is determined that the particular network access request is disallowed, queue that particular network service usage activity until a power state change occurs.

162. Rao-Araujo renders [6] obvious. *E.g.*, EX1005, ¶¶182-83, 187, 189, 194-95; EX1006, ¶¶16, 39, 43.

163. As discussed for [1.4], Rao teaches prioritization of network traffic for applications based on policy specifications by assigning packets from applications to priority-based queues. *See* EX1005, ¶¶182-83, 187, 189. For example, Rao teaches that the remote access client “may have one or more policies 520 for specifying client-side prioritization of network communications related to applications.” *Id.*, ¶182.

164. Rao’s teachings apply to multiple applications, such as VoIP, email, collaboration, etc. *Id.*, ¶179. In fact, nothing in Rao limits its teachings, so a POSITA would have understood that Rao’s techniques apply to all applications that run on a mobile device. In Rao, communicating “network packets from the queue” is typically “based on the respective priorities of the applications,” although Rao also “considers other network factors in determining what network packets to communicate from what queue.” EX1005, ¶¶194-95.

165. A POSITA would have recognized that communicating network packets is an example of network service usage activity, and that Rao considers factors such as application priority when allowing network service usage activity, but allows or disallows such network service usage activity for applications without regard to power control state. Rao's techniques do not explicitly mention power at all, focusing instead on application priority and network conditions (e.g., "the remote access client 120 of the present invention considers other network factors in determining what network packets to communicate from what queue." EX1005, ¶195). Rao's only substantive mention of power is in the definition of a computing device, "is capable of communication and that *has sufficient processor power* and memory capacity to perform the operations described herein." EX1005, ¶130. However, Rao does not identify power as a factor to be used when specifying, evaluating and enforcing policy.

166. Moreover, Araujo applies policies with and without regard to power control state. EX1006, ¶¶16, 39, 43.

167. First, as described in §IX.B, §X.B ([1.2–1.5]), Araujo teaches applying policies based on power control state. *See, e.g.*, EX1006, ¶¶39, 43. For example, Araujo provides an example in which "a program requests to use a device that is turned off (e.g., a disk, a network card, etc.), and the power management policy does not allow the device to be turned on at the time of the request, [so] the

request may be queued so that it can be serviced at some later.” EX1006, ¶39.

More generally, Araujo primarily describes techniques relating to power, e.g., stating that a “machine’s power usage may be managed by a power-management policy.” EX1006, Abstract.

168. Next, Araujo also describes the application of these policies as permissive, EX1006 ¶34 (“may”), and also teaches that network services can be allowed *without* regard to power state. For example, Araujo explains that “security conditions may be such that there is a reason to perform the software update at that moment regardless of the power expenditure,” such as “if there is known to be a zero-day attack propagating through the Internet, in which case delaying the update might expose the computer to an attack.” EX1006, ¶16. Such immediate response to an imminent threat is necessary to ensure proper device operation and reduce the likelihood that an infected device propagates a threat. In fact, from an administrator’s perspective, a device with a drained battery is strongly preferable to a malware-infected device. The former case can be addressed by simply charging the device; the latter case requires the malware to be removed, which can be time-consuming.

169. A POSITA would have further recognized that software updates are performed by a software update application running on the device. Therefore, a POSITA would have recognized that Araujo teaches allowing or disallowing

network service usage activities *with* regard to the power control state for most applications, and allowing network service usage activity *without* regard to power control state, including for a limited set of applications (e.g., a second device application), such as allowing a software updater to perform network service usage activity when “delaying the update might expose the computer to an attack.”

EX1006, ¶16.

[7] The wireless end-user device of claim 1, wherein when the network service usage control policy is applied it disallows the particular network service usage activity, and wherein the processor executes the instruction further to, when it is determined that the particular network access request is disallowed, queue that particular network service usage activity until a power state change occurs.

170. Rao-Araujo renders [7] obvious. *See* EX1006, ¶¶14, 22, 30, 32, 57.

171. For example, Araujo teaches that a “machine may comprise various devices” and each of these devices may have various power states” such as “on,” “off”, monitor brightness level and processor clock speed. EX1006, ¶¶4, 19. As explained in §IX.B, a POSITA would have understood that the power control state of the device (e.g., the “machine” in Araujo) is the aggregate state of the devices comprising the machine. §IX.B. The state of such component devices (whether they are on or off, and how much power is being used by each component device, e.g., the display brightness level) is important to the power state of the device,

especially when the device is running on battery or is charging (since heavy use can increase the time required to charge a battery).

172. In addition, Araujo teaches that the machine itself can have power states, such as battery level and whether it is plugged in. For example, Araujo includes several relevant teachings, such as: “a power management scheme may run a device in a lower-power- consumption mode, such as when a computer turns down the monitor brightness and processor speed when its remaining battery power drops below a certain threshold;” “if the system is, say, running on battery power, it may be possible to wait for the update until the system is plugged in so that energy can be saved to allow the user to work longer before running out of battery power;” and to “preserve battery power, power-use policy blocks this action while the system is unplugged.” EX1006, ¶¶14, 16, 41; *see, also, Id.*, ¶¶22, 30, 32, 57.

173. As another example, a POSITA would have known that when the power state of the device (e.g., the “machine” in Araujo) is low, it would have been obvious to implement Rao-Araujo’s power management policy. For example, if the power state of the device is low (e.g., the overall battery level of Araujo’s machine is low), it would have been obvious to implement Rao-Araujo’s power management policy to exercise power control and turn off its network card. EX1006, ¶¶1-2, 56-57. Accordingly, a POSITA would have found it obvious that

the power state of the device (e.g., overall battery level of Araujo's machine)

would serve as the power control state. *Id.* Araujo thus teaches that the power state can be the power state of the device (machine).

[8] The wireless end-user device recited in claim 1, wherein the processor executes the instructions further to: execute a router for dynamically managing one or more network capacity controlled services and/or QoS sessions for the wireless end- user device.

174. The Rao-Araujo device renders [8] obvious. *See* EX1005, ¶¶38, 180, 184.

175. RAD includes a processor that executes instructions to execute a router for dynamically managing network capacity-controlled services and/or QoS sessions for the device, e.g., by using priority queues. EX1005, ¶¶38, 180, 184; EX1001, 25:32-35, 25:50-51.

176. For example, Rao teaches client-based QoS using priority queues, and specifically, a client that prioritizes “network communications of the client associated with an application of the client.” EX1005, ¶38. To control capacity, Rao teaches that the client intercepts network packets “associated with an application” on the client, and “the network packets are stored to a queue 540a-540n.” EX1005, ¶184. The queues can be “organized by levels of priority, such as high, medium, low, or numerically such as priority 1 ... 10.” *Id.*, ¶180. “[A] priority for the intercepted and queued network packet is determined based on the

type and/or priority of the application” where “the network packets are communicated according to the determined priority.” *Id.*, ¶184. As a result, Rao can manage network capacity controlled services and/or QoS sessions, e.g., by prioritizing “the real-time data communications of application 338a ahead of other applications, such as non-real-time data communication applications.” EX1005, ¶184. This management is “dynamic” because, for example, it is based “application behavior” (e.g., the presence of real-time data applications). *See* EX1001, 88:38 56; *see also id.*, 16:4-9, 16:61-17:4. Such priority-based queuing, especially to enforce QoS guarantees was well-known in the art. In fact, with the increasing popularity of the Internet, numerous QoS techniques were developed to support video of demand.⁵

177. RAD also renders this claim obvious because Rao’s client performs capacity control as described in the ’544 Patent as being performed by a “QoS router.” *See* EX1001, 25:32-35, 25:50-51. As described in the ’544 Patent specification, once a “set of logical QoS channels is thus established, the service

⁵ One example is explained in Fernandez, J.C., Taleb, T., Guizani, M. and Kato, N., *Bandwidth aggregation-aware dynamic QoS negotiation for real-time video streaming in next-generation wireless networks*, 11(6) IEEE TRANSACTIONS ON MULTIMEDIA, 1082-1093 (2009). *See also* U.S. Patent No. 7,450,514.

processor (e.g., **QoS router** agent/function) routes the traffic associated with each QoS service activity to the appropriate RAB” and “the **QoS router** prioritizes traffic on the device.” EX1001, 23:32-35, 26:50-51.

178. A POSITA would have known that capacity control was commonly implemented using the priority queues described in Rao, where higher-priority packets are placed in higher- priority queues, and traffic from the higher-priority queues are given preferential access to the network. In one of many examples, IETF RFC 2746 includes a “priority queue [that] is widely considered as the canonical example of an implementation of EF” and “[a]nother example of an implementation of EF is a weighted round robin scheduler.” EX1015 at 12. IETF RFC 2745, “An Architecture for Differentiated Services” (December 1998), also describes QoS and priority queuing. A POSITA would have known that Rao’s priority queues would allow for dynamic managing of network capacity control would have allowed for dynamic managing the

179. Thus, RAD renders [11] obvious, including rendering obvious “a router for dynamically managing ... capacity controlled services for the wireless end-user device.”

[12] The wireless end-user device recited in claim 1, wherein the processor executes the instructions further to: execute a router for dynamically managing one or more network capacity controlled services and/or QoS sessions for the wireless end- user device.

180. The Rao-Araujo device renders [12] obvious, including dynamically assigning a network capacity controlled services priority level to a network service usage activity based on a network busy state. *See*, EX1005, ¶182, ¶¶194-95.

181. Rao includes two complementary teachings regarding dynamically assigning a network capacity controlled services priority level to a network service usage activity based on a network busy state.

182. First, in Rao, network packets are assigned to a priority-based queue based on factors such as the name of the application, the protocol, whether an application is running in the foreground or background, etc. EX1005, ¶182. Rao's assignment of a priority-based queue renders obvious dynamically assigning a network capacity controlled services priority level to a network service usage activity. EX1005, ¶¶182, 194. RAD's network packets from applications subject to Rao's policies are assigned to a priority-based queue based on various factors, where "network packets are communicated from the queues ... according to the determined priorities for the network packets." *Id.* A POSITA would have known that an application can run as a service. *See* EX1005, ¶116. The '544 Patent explains that "device assisted traffic control is provided for managing network

congestion” including by device processors being “instructed to reduce the traffic control priority for one or more classes of network capacity controlled services traffic, reducing the queuing priority, throttling rate, delay and/or access allowance for some or all of one or more classes of such traffic.” EX1001, 27:61-62, 28:6-12. Accordingly, a POSITA would have understood that Rao renders obvious device assisted traffic control, including dynamically assigning a network capacity controlled services priority level to a network service usage activity, by assigning a priority level to a network packet that determines the order in which it is transmitted from a queue. Also, Rao teaches a classic priority-based queuing mechanism, for example, as explained in [8].

183. Second, Rao discloses considering “network factors in determining what network packets to communicate from what queue,” including “receiv[ing] an indication of *network congestion*, such as receiving a window size of zero for a TCP connection related to an application.” EX1005, ¶195. Rao’s priority level (as determined by send order) therefore considers network congestion, which a POSITA would have understood to teach or render obvious dynamically assigning a priority level (e.g., queuing) to network service usage activity *based on a network busy state*. EX1005, ¶195.

184. A POSITA would have known that the actual priority level assigned to a network packet is determined not by the queue to which a packet is assigned, but

the order in which it is transmitted from a queue. Whether a queue is designated high or low priority matters only to the extent that such designations influence the order in which packets are transmitted as the priority perceived by an application depends on how quickly its packets are transmitted. As explained in Rao, the actual priority level (as determined by the order in which packets are sent) considers network congestion, which a POSITA would have understood to include busy state. EX1005, ¶195.

185. Consider a scenario in which certain links in a network are congested, and other links are not as the scenario relates to Rao's teaching that "the remote access client 120 may throttle back or not communicate network packets related to other networks factors, such as congestion, even though the network packets may have a higher priority than other network packets in a queue." EX1005, ¶195. A POSITA would have understood that if certain high-priority packets will travel over the congested link, adding packets can exacerbate the congestion problem, degrading performance for all network users.

186. Conversely, lower-priority packets designated for an uncongested link are less likely to disrupt the network. Therefore, Rao's teaching of considering network congestion, not merely packet priority, is an important technique for network congestion management. In such cases, Rao is actually giving priority to

the lower-priority packets by transmitting them first, as doing so encourages overall network stability.

187. Therefore, a POSITA would have understood Rao to teach assigning a network capacity-controlled services priority level (the order in which packets are transmitted) based on a network busy state (network congestion), especially at times when congestion is present.

[13] The wireless end-user device recited in claim 1, wherein associating includes querying a network element for determining an association of the first device application with the network service usage control policy.

188. RAD renders [13] obvious. See EX1005, ¶¶182-183.

189. Rao teaches policies “may be ... downloaded via a gateway.” EX1005, ¶183. A POSITA would have known a gateway is a network element, and downloading content (e.g., a policy) commonly occurred in response to a query. Rao further teaches that policies are associated with applications (e.g., a first device application). EX1005, ¶182. The downloaded policies “specify[] client-side prioritization of network communications related to applications” and may “be specified by the name of the application ... and/or the type of application” in Rao (e.g., are associated with a first device application). EX1005, ¶182.

190. By querying and downloading an application priority policy and applying the policy to an application, Rao determines an association of a first device application with the network service usage control policy. EX1003, ¶190.

Therefore, a POSITA would have recognized that Rao teaches [13], including teaching querying a network element to determine an association of a policy with an application.

[14] The wireless end-user device recited in claim 1, wherein associating includes querying a network element for determining an association of the first device application with the network service usage control policy.

191. RAD renders [14] obvious. *See* EX1005, ¶¶38, 180, 182, 184, 195; EX1006, ¶¶38, 40.

192. As described above, a POSITA would have known that QoS was commonly implemented using priority queuing, where higher-priority packets are placed in higher-priority queues, and traffic from the higher-priority queues are typically given preferential access to the network. *See* §X.B [8]. Rao's client has policies "for specifying client-side prioritization of network communications related to applications." EX1005, ¶182. Rao further explains that the client intercepts one or more network packets "associated with an application" and "the network packets are stored to a queue" where the "priority for the intercepted and queued network packet is determined based on the type and/or priority of the application." Rao, ¶184. The packets are then "communicated according to the determined priority." *Id.*

193. Rao teaches client-based QoS using priority queues, and specifically, a client that prioritizes network communication "associated with an application of

the client.” EX1005, ¶38. Rao further teaches that a client “prioritize[s] network communications of the client associated with an application of the client” by “determin[ing] [that] the queued ... network packets [are] associated with a first application of the client” and “indicat[ing] a priority for the ... packets.” EX1005, ¶38. The client then places the determined “packets ahead of at least one network packet in the queue associated with a second application of the client” and “provides the prioritized one or more network packets for communications via a network stack of the client.” *Id.* Rao’s queues “may be organized by levels of priority, such as high, medium, low, or numerically such as priority 1 . . . 10.” *Id.*, ¶180. A POSITA would have recognized such prioritized queues as QoS classes and thus that Rao teaches network service usage control policies that include QoS class settings.

194. Rao further teaches network service usage control policies that can include packet error rate, queue settings and throttling. *Id.*, ¶195, For example, regarding packet error rates, Rao teaches “the remote access client 120 may recognize a high number of retransmits to a particular destination.” *Id.*

195. Regarding queue settings, Rao teaches, “the remote access client 120 may receive an indication of network congestion, such as receiving a window size of zero for a TCP connection related to an application 338a-338n.” *Id.*; *see also* [4]. A POSITA would have known that a window size is a queue setting. Regarding

throttling, Rao teaches, the client “may throttle back or not communicate network packets.” *Id.*

196. In addition, Araujo teaches that when “a power state change is not allowable under the policy,” one action “is to block the request,” which a POSITA would have recognized as a block/allow setting. EX1006, ¶¶38, 40.

[15] The wireless end-user device recited in claim 1, wherein the network service usage control policy includes traffic control policy filters, the filters comprising a first filter specifying applicability of the policy only when the first device application is not in the foreground of user interaction, and a second filter specifying applicability of the policy only in one or more specific power control states.

197. A POSITA would have understood that filters were common mechanisms for determining whether a group of policies should be applied or “filtered out” from consideration and therefore RAD renders [15] obvious. *E.g.*, EX1005, ¶¶182, 184.

198. In one example, an administrator would designate that one set of policies applies only to foreground application and another set of policies applies only to background application. Depending on whether the application is in the foreground or background, RAD’s policy evaluation mechanism would filter from consideration irrelevant policies, improving the efficiency of evaluation (since only a subset of policies need be evaluated).

199. Rao teaches the first filter specifying applicability of the policy only when the first device application is not in the foreground of user interaction. EX1005, ¶182. For example, Rao teaches policy control filters that apply when an application is in the background (i.e., not in the foreground of user interaction), stating that the client may apply policies “for specifying client-side prioritization of network communications related to applications” which can be “based on whether an application is running in the foreground or the background of the client.” *Id.* Based on the determination, “the network packets are stored to a queue” and a priority for the “queued network packet is determined based on the ... priority of the application.” EX1005, ¶184. Therefore, the policy determines the priority, and the priority determines the queue.

200. Araujo teaches the second filter specifying applicability of the policy only in one or more specific power control states. EX1006, ¶28. For example, in Araujo, the “current power state of a device may be a factor in determining whether the power state will be changed,” e.g., because “a device may use a considerable amount of power to turn from off to on.” EX1006, ¶28; *see also id.* ¶25 (disclosing power states that include on, off, and “intermediate” power states). Araujo further teaches that “if a program requests to use a device that is turned off (e.g., a disk, a **network card**, etc.), and the power management policy does not allow the device to be turned on at the time of the request, the request may be

queued so that it can be serviced at some later.” *Id.*, ¶39. A POSITA would have recognized that queuing network traffic, including according to priority, is an example of network service usage control since queuing traffic is controlling how the network is used.

201. A POSITA would have found it obvious for the RAD to include both filters to account for a variety of traffic control policies that can be applied to optimize device operation. For example, a first filter would specify that packets from applications not in the foreground of user interaction are added to a lower priority queue, while a second filter would state that in a low power state (e.g., low battery and not plugged in), packets in a lower priority queue are held instead of transmitted. Because the first filter applies regardless of power state, and the second filter applies regardless of why a packet was added to a low priority queue, it would have been obvious for a POSITA to try using both filters, including based on a limited number of possibilities to try, and arrive at the predictable results that using both filters is complementary and beneficial, and including multiple filters further improves the efficiency of policy evaluation.

202. Therefore, RAD renders obvious [15], including rendering obvious a filter specifying applicability of the policy (e.g., traffic queuing) only when the first device application is in the background (i.e., not in the foreground), and a

second filter specifying applicability of the policy based on power control state (e.g., network card is powered on or off).

[16] The wireless end-user device recited in claim 1, wherein the network service usage control policy includes traffic control policy filters, the filters comprising a first filter specifying applicability of the policy only when the first device application is not in the foreground of user interaction, and a second filter specifying applicability of the policy only in one or more specific power control states.

203. RAD renders [16] obvious. See EX1005, ¶182.

204. As discussed for [15], Rao-Araujo renders obvious traffic control policy filters. See discussion of [15]. Moreover, Rao teaches that “the policies 520 may be specified hierarchically to account for multiple applications 338a-338n and/or multiple protocols that may be executed on the client 105.” EX1005, ¶182. A POSITA would have recognized that in a hierarchical rules structure, rules cascade from higher levels of the hierarchy to lower levels. It would have been obvious to a POSITA to specify the traffic control policy filters of the Rao-Araujo Device hierarchically to “account for multiple applications ... that may be executed on the client.” *Id.*; EX1005, ¶182.

[18] The wireless end-user device recited in claim 1, wherein the processor executes the instructions further to: differentially control the particular network service usage activity based on the network service usage control policy based on a network busy state.

205. RAD renders [18] obvious. EX1005, ¶¶182, 189, 194, 195; *see* § X.B [12].

206. Rao teaches determining whether a policy applies to particular usage activity based on different factors (e.g., foreground/background, application name) and using policies when assigning packets (usage activities) to priority-based queues. EX1005, ¶¶182, 189. Rao further teaches using priority of the queues when controlling network service use activity (sending packets from queue). *Id.*, ¶194. For example, Rao explains that “the network packets are communicated from the queues 540a-540n according to the determined priorities for the network packets”. *Id.* In addition, Rao teaches techniques that “consider[] other network factors in determining what network packets to communicate from what queue.” *Id.*, ¶195 (e.g., explaining that Rao’s “remote access client 120 may receive an indication of network congestion, such as receiving a window size of zero for a TCP connection related to an application.”).

207. A POSITA would have understood that a network that is congested is a network in a busy state. A POSITA would have further understood that determining which queue’s packet to prioritize and transmit over the network is an

example of differentially controlling the network service usage, including because transmitting packets from queues results in using the network. Rao's network service usage control policy is a differential control policy because it distinguishes a first application's network service usage activity from other applications. For example, Rao explains "policies 520 may be specified hierarchically to account for multiple applications 338*a*-338*n* and/or multiple protocols that may be executed on the client 105 at any point." EX1005, ¶182. "Furthermore, the policies 520 may be specified conditionally, such as if one application 338*a* is running, a second application 338*b* may have a higher or lower priority." *Id.*

208. A POSITA also would have understood that Rao's network service usage control policy can be made up of multiple rules to allow for differential control because, in the context of distinguishing network service usage activity across different applications, Rao discloses that "[o]ne ordinarily skilled in the art [would] recognize and appreciate the multitude of ways to define client-side application priorities." EX1005, ¶182.

209. Interpretations of another term—"differential traffic control policy"—in other proceedings do not undermine Rao-Araujo's disclosure. *See* EX1026 at 21-22 (construing "differential traffic control policy" in litigation to mean a "rule for controlling network traffic that distinguishes between two or more things.").

For example, even if the Board applies this construction here⁶, Rao-Araujo teaches a network service usage control policy with power control state rules that control an application's network traffic based on a network busy state and distinguish between an application's foreground and background activity, as well as those of different applications.

210. Accordingly, Rao-Araujo renders [18] obvious, including rendering obvious differentially controlling network service usage activity (choosing the queue from which to send) based on a network busy state. *See also*, § X.B ([12]).

[20] The wireless end-user device recited in claim 1, wherein the processor executes the instructions further to: differentially control the particular network service usage activity based on the network service usage control policy based on a network busy state.

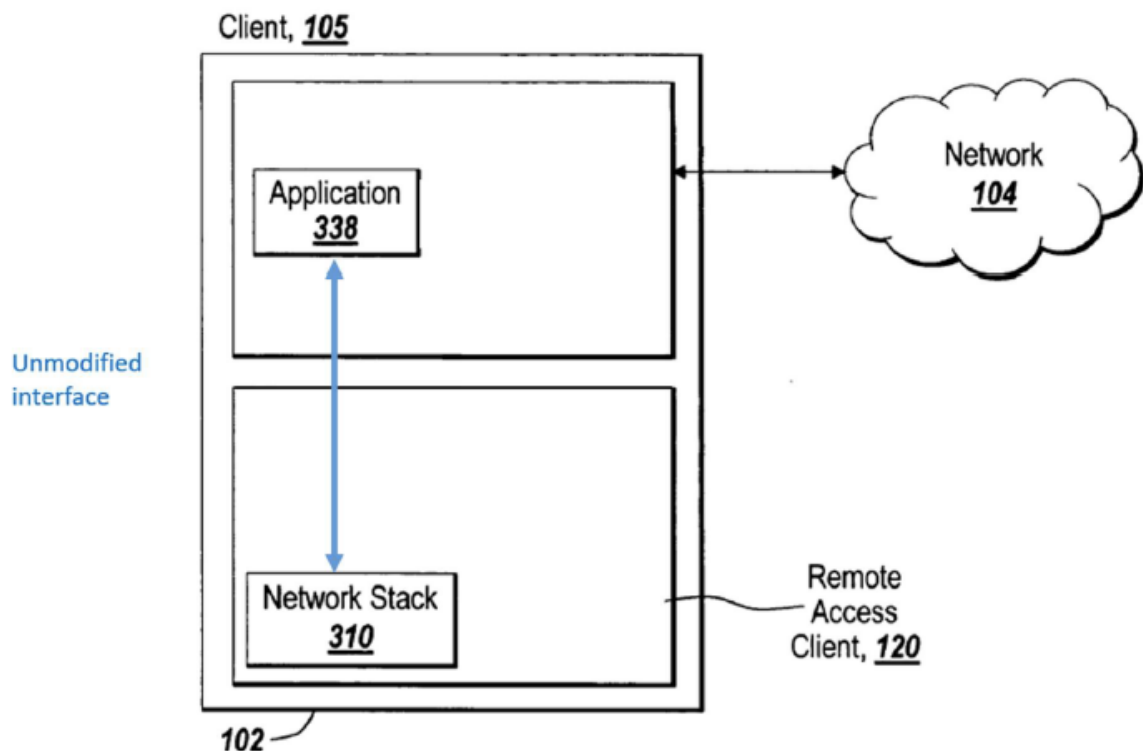
211. RAD renders [20] obvious. *See* EX1005, ¶¶80, 99, FIGS. 1C, 3A.

212. For example, Rao teaches that “[t]he remote access client transparently ***intercepts*** network communications associated with applications executing on the client, detects that the network communication is associated with an application, and ***determines priorities for the network communications*** based on a priority for the application.” EX1005, ¶80. A POSITA would have recognized

⁶ I understand that Petitioner is not advocating for one construction over any other—the claim is rendered obvious regardless of the construction applied.

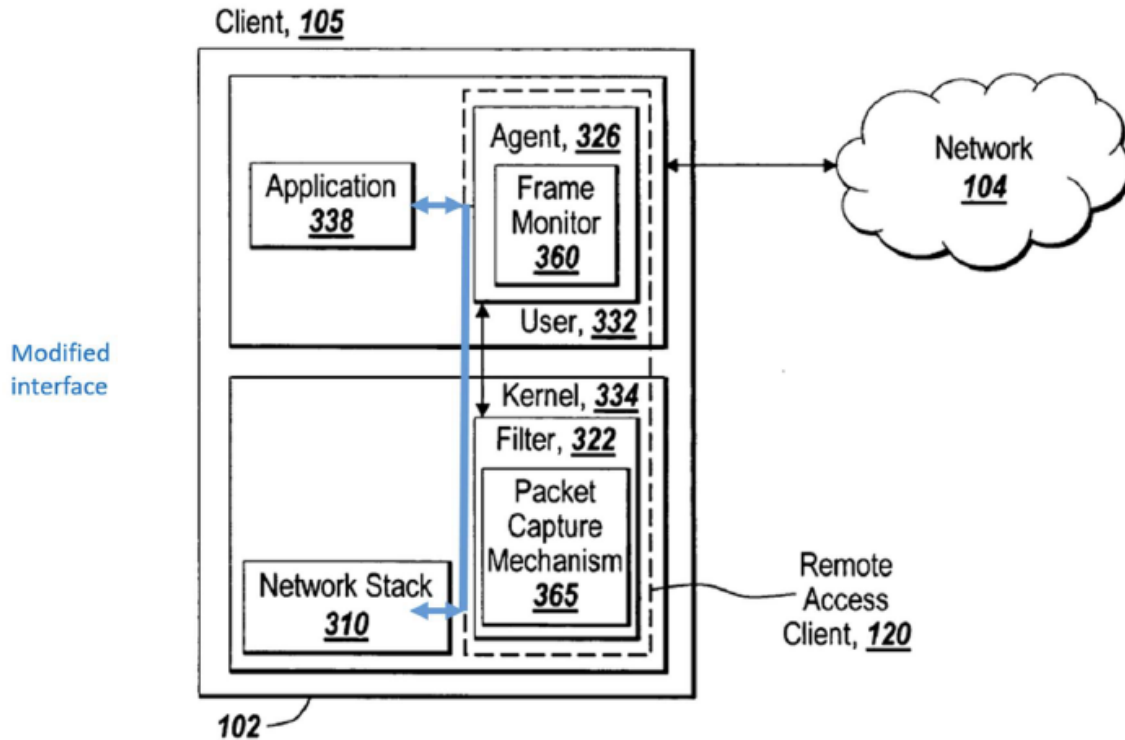
“determining priorities of the network communication” as “implementing traffic control” of the particular network service usage activity (e.g., as described in [12] and [18]).

213. Rao’s remote access client modifies the network stack interface of the wireless end-user device to intercept the network communications because Rao teaches inserting the remote access client between the network stack 310 and the application 338. A POSITA would have recognized that an unmodified network stack interface would exist between applications and the network stack, as illustrated below.



EX1005, FIG. 1C (excerpted, colored text and arrows added)

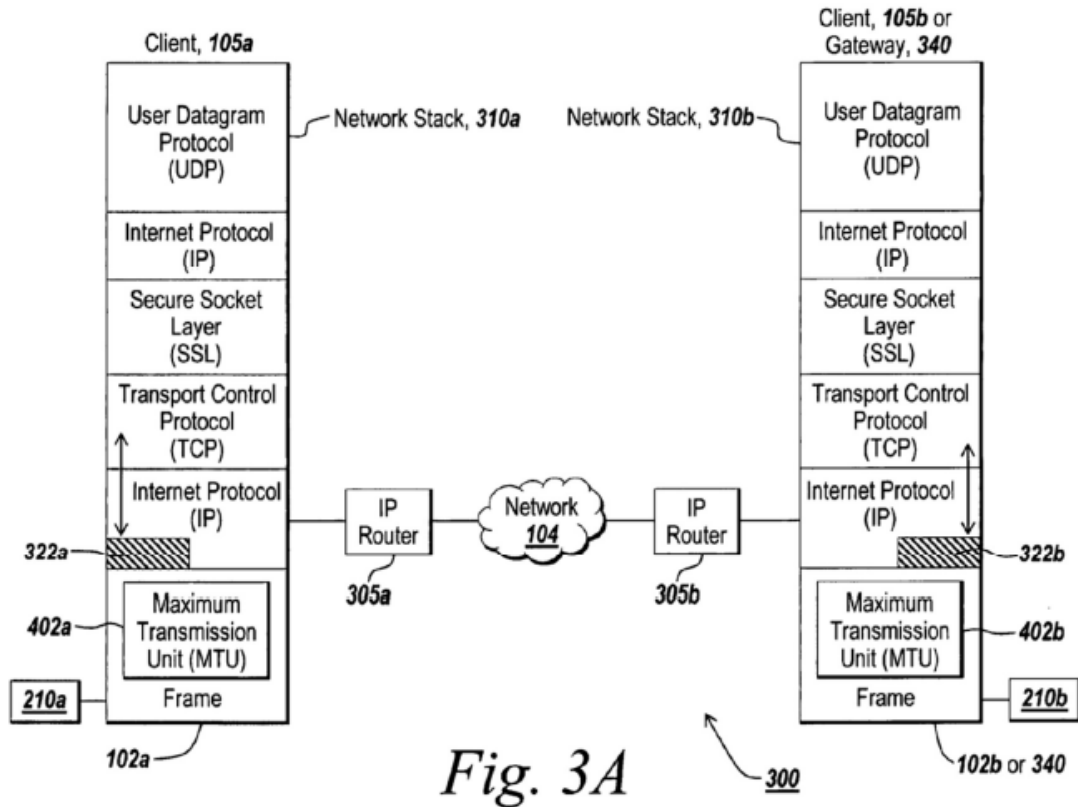
214. Rao’s modified network stack interface is illustrated below.



EX1005, FIG. 1C (annotated)

215. In the unmodified interface, packets pass directly from an application to the network stack, whereas in the modified interface, packets pass from the application to the remote access client to the network stack. *See, also*, §X.B.[5] (discussion of emulation).

216. Rao further illustrates the modified stack interface in FIG. 3A, reproduced below.



EX1005, FIG. 3A

217. Rao's 322a and 322b are the filter modifications to the network stack interface. EX1005, ¶99, Fig. 3A. Accordingly, RAD renders [21] obvious.

[22] The wireless end-user device of claim 1, wherein the power control state is a power save state of the device.

218. Rao-Araujo renders [22] obvious. See EX1006, ¶4.

219. As described in reference to [7], Araujo teaches that a "machine may comprise various devices" and each of these devices may have various power states" including "on," "off", and "lower-power-consumption mode, such as when a computer turns down the monitor brightness and processor speed when its

remaining battery power drops below a certain threshold.”. EX1006, ¶4, 14; § X.B ([7]). As explained in § X.B ([7]), a POSITA would have understood that the power control state of the device (e.g., the “machine” in Araujo) is the aggregate state of the devices comprising the machine. § X.B ([7]). Therefore, Araujo teaches that the power control state can be the power save state of the device (e.g., the machine), including based on Araujo’s lower-power-consumption mode.

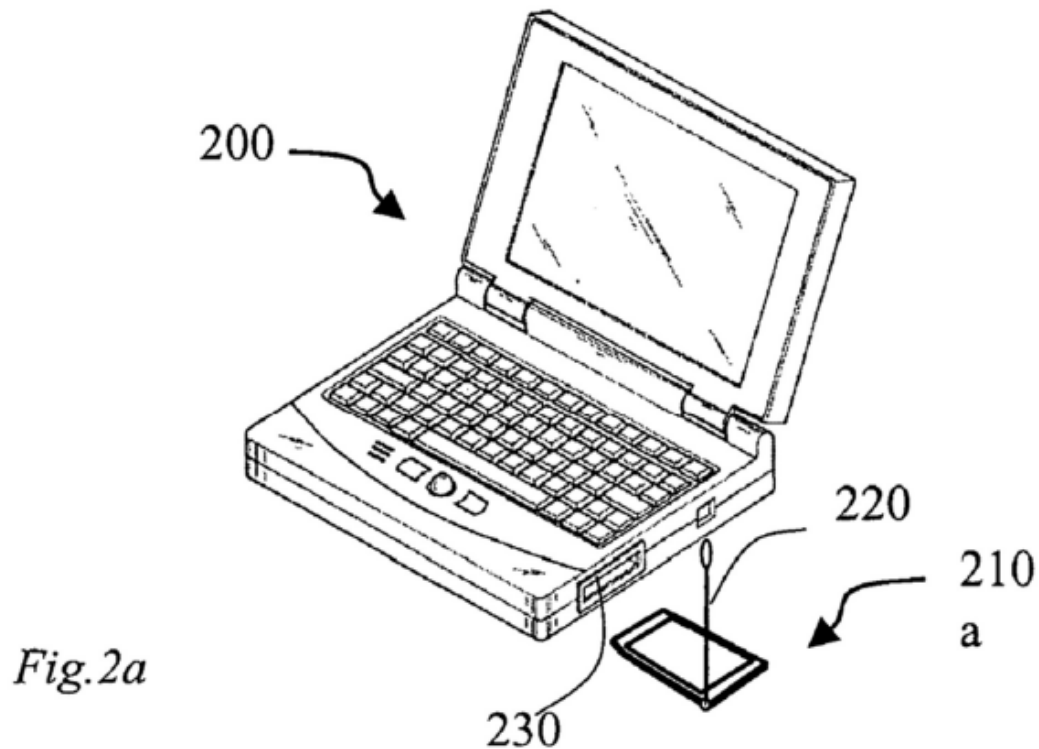
[23] The wireless end-user device of claim 1, wherein the power control state is a power state of the wireless modem.

220. Rao-Araujo renders obvious [23], including rendering obvious dynamically determining whether to apply the network service usage control policy to the particular network service usage activity based on a power state of the wireless modem. *E.g.*, EX1005, ¶95; EX1006, ¶¶19, 39.

221. As described above, the Rao-Araujo Device includes a wireless modem. *See* §X.A; EX1005, ¶95 (“The client ... can connect to one or more networks 104 through a variety of connections including ... wireless connections ...”). A POSITA would have known the wireless modem used to connect the Rao-Araujo Device to a “wireless connection” is an example of a device as taught by Araujo. *Id.*

222. As of the Critical Date, modems could take various forms. For example, in larger devices, it was common to include a card (such as a PCMCIA

card), while in smaller devices such as mobile phones, modems can be in the form of a chip. For example, Adams illustrates a PCMCIA wireless modem card 210:



EX1020, FIG 2a

223. Similarly, Altbaum teaches “a wireless modem card 22 according to an exemplary embodiment of the invention coupled to a handset 20, which may be a cellular phone as illustrated or other host devices” and “that the wireless modem device may be a card which is removably installed in a card slot or the like provided in the handset 20, or may be originally integrated with the handset 20 on manufacture.” EX1021, 3:50-57.

224. All such form factors would be devices as described by Araujo.

225. Araujo teaches that “devices may be able to assume an intermediate power usage between fully-on and fully-off,” and that “[o]n and off are examples of power states, as are any kind of discrete or continuous intermediate states.” EX1006, ¶19.

226. Araujo further teaches that power states of a device, including its network card (e.g., wireless modem), can be used in policies, giving an example in which “a program requests to use a device that is turned off (e.g., a disk, *a network card*, etc.), and the power management policy does not allow the device to be turned on at the time of the request, the request may be queued so that it can be serviced at some later.” EX1006, ¶39.

227. Therefore, a POSITA would have understood that, in RAD, the power control state can be the power state of RAD’s wireless modem. Accordingly, RAD renders [23] obvious.

XI. GROUND 1B: Rao in view of Araujo and Freund renders obvious claims 2, 17 and 19-21

A. Rao-Araujo-Freund Combination

228. Rao, Araujo and Freund describe using policies/rules to control network traffic. For example, as described above, Rao “may apply a policy to determine a condition of the client 105, or endpoint, at the time of transmission of the packet.” EX1005, ¶109. In other embodiments, the frame monitor “may identify an application 338 that generated the packet.” *Id.* Further, the frame

monitor “may make a policy-based determination to transmit the packet to the gateway 340 responsive to the identified application 338.” *Id.* Rao explains such “*policies 520 may be specified by any suitable means and/or mechanisms,*” including “the name of the application, and “whether an application is running in the foreground or the background of the client 105.” *Id.*, ¶182. Rao notes that “[o]ne ordinarily skilled in the art will recognize and appreciate the multitude of ways to define client-side application priorities.” *Id.* Araujo gives a similar example in which “the power management policy does not allow the device to be turned on at the time of the request,” and “the request may be queued so that it can be serviced at some later,” e.g., “if at some later time the power management policy allows the device to be turned on, then the program’s request may be dequeued and processed.” EX1006, ¶39.

229. A POSITA would have recognized that the network traffic control policies of Freund are simply additional examples of client-side policies, such as those Rao and Araujo contemplate. For example, Freund include “access rules [that] can include criteria such as total time a user can be connected to the Internet (e.g., per day, week, month, or the like), time a user can interactively use the Internet (e.g., per day, week, month, or the like), a list of applications or application versions that a user can or cannot use in order to access the Internet, a list of URLs (or WAN addresses) that a user application can (or cannot) access, a

list of protocols or protocol components (such as Java Script™) that a user application can or cannot use, and rules to determine what events should be logged (including how long are logs to be kept).” EX1007, 4:8-19. A POSITA would have recognized that Freund’s policy examples are among the “multitude of ways to define client-side application priorities” as contemplated by Rao. EX1005, ¶182.

230. Rao teaches that “[t]he policies 520 may be configurable by a user by any suitable means and/or mechanism ... such as a user interface, graphical or otherwise, design and constructed for configuring or specifying the policies 520.” EX1005, ¶183. For details on the user interface (UI), a POSITA would have looked to references such as Freund, which shows “bitmap screenshots illustrating a preferred user interface or ‘wizard’ dialog for configuring rules” including “a preferred interface 700 [that] provides a ‘view’ of rules governing operation of the Internet access monitor, displaying all of the rules which are available for a current configuration.” EX1007, 6:47-49, 24:17-20, FIGS. 7A-K. While policies can be specified as text, administrators often find it more convenient and easier to learn to specify policies using a graphical user interface (GUI), and the results can be less error prone. As described above, such a UI “allows the user to create a new rule,” “edit an existing rule,” and “delete a rule.” EX1007, 24:22-24.

231. Rao explains that “[t]he policies 520 may be accessible by the agent 326, configured into the agent 326, or loaded by the agent 326,” e.g., “the policies

520 may be provided by or downloaded via the gateway 340.” EX1005, ¶183. For implementation details on how to obtain the policies, a POSITA would have looked to references such as Freund. As described above, Freund teaches an example of policies being loaded by an agent: “the Supervisor filters rules appropriate for the client (i.e., application, Host, and other rules), and transmits them to the Client Monitor,” and “the Client Monitor confirms successful reception of rules.” EX1007, 28:14-18.

232. Because both Rao and Freund teach using policies/rules to control network traffic, including defining and loading policies/rules, it would have been obvious to a POSITA to combine the teachings of Rao and Araujo with the teachings of Freund to achieve the benefits of Freund’s user interface for configuring rules and for more detailed enumeration of network traffic control policies not explicitly described in Rao. As described above, the introduction of Freund simplifies policy specification through a GUI.

233. In operation, the resulting Rao-Araujo-Freund Device (RAFD) would use the combined policies of Rao, Araujo and Freund to determine whether a network request was permitted, and when a request was permitted, use the traffic queuing policies of Rao and Araujo to determine when, and in what order, network packets were delivered. EX1005, ¶¶182-83; EX1007, 4:9-19; EX1006, Abstract, ¶¶3, 39-40. In one example, a POSITA would have recognized or found obvious a

RAFD policy in which network traffic is permitted only if a user had not exceeded a configured Internet access limit (e.g., 30 minutes, 60 minutes, etc.) and the application is permitted to access the Internet (per Freund), an application is in the foreground (per Rao) giving it “VIP” status (per Araujo) and the power state of the device is plugged-in or the battery is above a threshold charging level. EX1005, ¶182; EX1006, ¶22; EX1007, Abstract.

234. In addition, the policies governing the operation of RAFD can be configured with the UI techniques of Freund and/or loaded from a network element using the techniques of Rao and Freund. EX1006, ¶22; EX1005, ¶¶182-83; EX1007, 24:22-24.

235. A POSITA would have expected success in creating a combination, which would have required only routine programming knowledge well within the skill of a POSITA. EX1006, ¶22; EX1005, ¶¶182-83; EX1007, 24:22-24. Indeed, the combination would have amounted to nothing more than the use of a known technique to improve similar mobile devices in a similar way, including combining similar types of policies, and combining prior art elements according to known methods to yield the predictable results described above. *Id.* User interfaces for specifying policies were common as of the Critical Date. (*See, e.g.*, EX1028, EX1029, EX1030 among many examples.) RAFD’s processor would be configured to perform the operations discussed in this Ground. *See also* §X.A.

B. Analysis of the Claims

[2] The wireless end-user device of claim 1, wherein the processor executing the instructions determines that the first device application is in the foreground of user interaction when the user of the device is directly interacting with that application or perceiving any benefit from that application.

236. RAJD renders [2] obvious. *See* EX1007, 10:16-24, 10:40-44.

237. As described in §IX.C, Freund teaches “monitoring of time spent by an employee for ‘actively’ interacting with the Internet,” and notes that “[a]ctive use occurs when a user directly interacts with an Internet application (e.g., Web browser) while that application accesses the Internet.” EX1007, 10:16-24.

238. A POSITA would have known that directly interacting with a Web browser occurs when the Web browser is in the UI foreground. For example, Paquette teaches that foreground application “may refer *to an application that is currently configured to receive certain input*, such as input from a keyboard. Such an application may be referred to as having the ‘keyboard focus’ (or ‘focus’ of other input devices) of the computing system 100, meaning any keyboard input that is received is likely to be routed to that application.” EX1019, 6:31-37 (emphasis added).

239. Freund further explains that “[a] given application itself can be examined for determining whether it is ‘active’ by determining whether the

application receives ‘focus’ and/or receives user input (e.g., mouse clicks or keystrokes).” EX1007, 10:40-44.

240. A POSITA would have known that mouse clicks and keystrokes are instances of direct interaction with an application. Freund differentiates mouse or keyboard use from “background use which occurs when an application or process executing in the background (i.e., does not have ‘focus’) accesses the Internet, such as a mail client which intermittently polls an Internet-based mail server.” EX1007, 10:20-24.

241. Thus, Freund teaches determining that the first device application is in the foreground of user interaction when the user of the device is directly interacting with that application. EX1007, 10:40-44.

[17] The wireless end-user device recited in claim 1, wherein the network service usage control policy includes traffic control policy filters using a network busy state and/or a time of day as an index into a traffic control setting.

242. RAJD renders [17] obvious. See EX1005, ¶195; EX1007, 10:13-17, 30:51-57. As discussed for [15], Rao-Araujo renders obvious traffic control policy filters. See discussion of [15].

243. Rao-Araujo also renders obvious traffic control policy filters using an “***index into a traffic control setting.***” E.g., EX1005, ¶182. For example, Rao’s client manages network communication prioritization per application “in

accordance with policies for the client and *in further view of any network statistics and other factors occurring on the network.*” EX1005, ¶195 (“the client 105 controls and manages the prioritization of network communications of the client 105 on an application 338*a*-338*n* basis and in accordance with any policies 520 for the client 105 and in further view of any network statistics and other factors occurring on the network”). Rao further teaches that the remote access client “may receive an indication of network congestion, such as receiving a window size of zero for a TCP connection related to an application.” *Id.*

244. A POSITA would have recognized that Rao’s network statistics, including “network congestion,” are an example of a “network busy state” that is used as an index by Rao’s policies. As described in reference to [12], network congestion and other network statistics can be used to optimize network use.

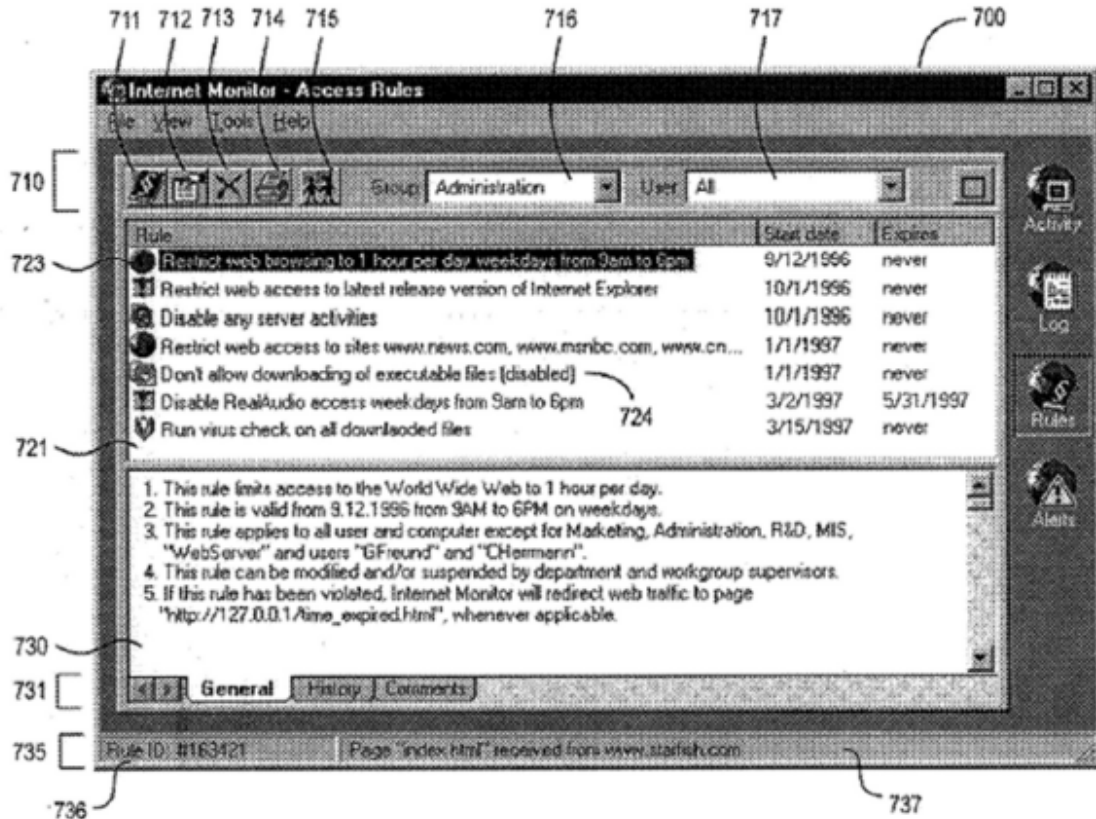
245. In addition, Freund teaches that “access rules can be qualified by optionally specifying: ... *time of day* when the rule should be applied (for example from 9am to 5pm).” EX1007, 13:13-17. Like Rao, Freund teaches network busy state, stating that “if the Supervisor determines that congestion exists for Internet access (either by interpreting the log messages from the Client Monitors, its own monitoring of access speed, or third party monitoring tools), it notifies the Client Monitors of temporary access restrictions.” *Id.*, 30:51-57. In response, Freund teaches that “depending on the specific rules in force, the individual Client

Monitors can either: (a) Delay Internet access for non-critical Applications or Protocols...” *Id.*, 30:57-60. The Rao-Araujo-Freund Device uses each as an index by Rao’s policies. A POSITA would have found it obvious for the Rao-Araujo-Freund Device to include filters to account for a variety of traffic control policies that can be applied to optimize device operation and to use either or both (network congestion/busy state and time of day) as “indexes into a traffic control setting.”

[19] The wireless end-user device recited in claim 1, wherein the processor executes the instructions further to: differentially control the particular network service usage activity based on the network service usage control policy based on a user input and/or a current wireless network.

246. RAFD renders [19] obvious. *See* EX1007, FIGS. 7A-7K, 24:16-20, 25:1-13.

247. For example, Freund figures 7A-7K illustrate an example of user input (into a user interface) used for differentially controlling network service usage activity based on a policy. Freund, FIGS. 7A-7K. For example, Freund FIG. 7A shows:



EX1007, FIG. 7A

248. Freund further states, "FIGS. 7A-K illustrate a preferred user interface or "wizard" dialogs for configuring rules" and "in FIG. 7A, a preferred interface 700 provides a 'view' of rules governing operation of the Internet access monitor, displaying all of the rules which are available for a current configuration."

EX1007, 24:16-20. Freund further teaches that the policies (rules) can be associated with applications using the wizard dialog which "asks the user what kind or type of new rule should be created" and that "any given rule is a combination of access rights granted on the basis of available applications, permitted time limits, permitted user activities, permitted protocols, and the like"

and “the user can select type 742 for limiting what applications (including individual applications) can do on the Internet.” *Id.*, 25:1-13.

249. A POSITA would have recognized that the network service usage control policies specified in Freund’s wizard dialog are based on a user input with the wizard dialog. User interface dialogs commonly accept user input, such as keystrokes and mouse clicks. As discussed regarding [18], for example in the analysis of [18], the network service usage control policy disclosed by Rao and Freund serves as a differential control policy because it distinguishes the first application’s network service usage activity—and, user input, as a POSITA would have understood—from those of other applications. Accordingly, RAJD renders [17] obvious.

[20] The wireless end-user device recited in claim 1, wherein the processor executes the instructions further to: modify or replace a network stack interface of the wireless end-user device to provide for intercept or discontinuance of network access messaging for implementing traffic control of the particular network service usage activity.

250. RAJD renders [20] obvious. *See* EX1007, 15:22-24, 15:28-33.

251. In addition to the teachings of Rao, Freund’s client “includes a client-side monitor—data acquisition[sic] module 440—which ‘hooks into’ the communication driver 430.” §IX.C; EX1007, 15:22-24.

252. Freund notes that for the “Windows Winsock communication driver, for example, a process can hook into the driver using Winsock VxD extensions.” EX1007, 15:24-26. In RAFD, the network interface can “intercept the communications for determining whether the request is permitted under the rules,” and “when a request for access is received from an application, the monitor first verifies that, according to the rules in place, such an application is permitted to access the Internet.” *Id.*, 15:28-33.

253. A POSITA would have recognized that Freund’s client-side monitor modifies a network stack interface (hooks into the driver) to provide for network access messaging for implementing traffic control of network service usage activity. In addition, as described in [5], to implement traffic control, both Rao and Araujo modify the stack interface by interposing components between applications and network stacks. *See, e.g.*, EX1005, FIG. 1C, FIG. 3A; EX1006, FIG. 6; §X.B.[5].

[21] The wireless end-user device recited in claim 1, wherein the processor executes the instructions further to: store a network capacity controlled service list, wherein the network capacity controlled service list is periodically updated based on monitored network service usage activities.

254. RAFD renders [21] obvious. *See* EX1005, ¶¶116, 182-83; EX1007, 4:8-14, 4:62-63, 30:12-16, 10:45-50.

255. First, RAFD stores a network capacity controlled service list. For example, Rao teaches that its policies are used to specify “client-side prioritization of network communications related to applications,” and the policies “may be specified by the name of the application, “the type of application,” “the type of one or more protocols used by the applications” and/or “the size of the payload of the network packet.” EX1005, ¶182.

256. A POSITA would have known that an application can run as a service,⁷ and because policies are used to prioritize network communication of applications by assigning a priority level to a network packet (e.g., the client may have policies for specifying “client-side prioritization of network communications related to applications”), the applications are network capacity controlled applications (services). EX1005, ¶182; *see* § X.B ([12]). In more detail, packets

⁷ Rao itself illustrated the functional equivalence, explaining “the agent 326, frame monitor 360, the filter 322, and packet capture mechanism 365 may comprise an application, module, service, computer program, software component, web service, web component, library, function, process, task, thread, or any other type and/or form of executable instruction which is designed to and capable of executing the functionality of the present invention as described herein.” EX1005, ¶116. A POSITA would have known that applications can run as services.

from applications are placed in queues according to the priority of the applications.

By queuing the packets according to priority, RAFD is implementing network capacity control. (Priority queuing was a well-known technique for controlling use of network capacity.)

257. To associate priorities with the applications (services), RAFD maintains a list of applications and the associated priorities. Rao explains that the “[t]he policies 520 may comprise any type and format of syntax and/or language for specifying a policy, and may be provided via any type and/or form of medium, such as electronically by one or more network packets or via a file, such as an XML file.” *Id.*, ¶183. A POSITA would have understood that a “file” such as XML is a stored list of application-related policies (e.g., a network capacity controlled service list) that may be accessed by Rao’s agent 326. RAFD therefore renders obvious storing a network capacity controlled service list. *Id.* Rao alternatively discloses that filter 322 may use a filter table to filter network packets according to the policy, where “filter 322 receives configuration settings from the agent 326 and stores the configuration settings in [the] filtering table.” *Id.*, ¶¶102-103. The configuration settings “may include information regarding which networks, protocols, or types of packets to filter.” *Id.* ¶104. The filter then “intercepts a packet generated by an application 338” and “[i]f the packet satisfies a condition listed in the filtering table, the filter 322 may transmit the packet to the agent 326.”

Id. ¶105. Rao's filtering table additionally discloses storing a network capacity controlled service list because it provides Rao's policies which network packets (e.g., associated with a service) to filter via conditions "listed in the filtering table." *Id.*.

258. Like Rao, Freund also discloses access rules that can include "a list of applications or application versions that a user can or cannot use in order to access the Internet," among others. EX1007, 4:8-14. A POSITA would have recognized that the RAFD, which includes the access rules of Freund, would thus include Freund's list of network capacity controlled services (applications), a list that includes the network capacity controlled services to which the access rules apply.

259. RAFD further updates the list based on monitored network service usage activities. For example, Freund teaches that a "Client Monitor maintains a list of active Applications (processes) with various fields to track activities and a global activity record." EX1007, 30:12-16. A POSITA would have recognized that one such field includes the amount of time an application has accessed the Internet, as such data are used to enforce access limits. For example, Freund teaches "monitoring the total time particular applications access the Internet" which is done "on a per application basis--that is, access broken down by the application or applications used for the access" and such data are used to evaluate and enforce time limitations. EX1007, 10:45-50, 4:62-63. A POSITA would have recognized

that to enforce Freund's time limitations, the aggregate access time would be stored, and particularly would be stored in the "various fields to track activities and a global activity record." EX1007, 30:12-16. Because these fields are updated based on monitored activities (e.g., Internet access), Freund's list is updated based on those monitored activities. For example, if a user had accessed the Internet using a particular application for 15 minutes, then uses that application for another 10 minutes, the list is updated to 25 minutes of cumulative usage. Such monitoring would occur periodically, e.g., when the monitoring component of RAFD was executed, resulting in the list being updated periodically. In addition to the reasons explained in § XI.A, it would have been obvious in RAFD to implement a network capacity controlled service list—as Rao's "file" or "filtering table," or alternatively as Freund's "list of applications"—as a stored list that is periodically updated based on monitored activity in Freund (e.g., based on Freund's disclosure of tracking activity). EX1007, 30:12-16. Implementing RAFD in this way would have achieved Freund's goals of limiting the amount of time an application has accessed the Internet.

XII. GROUND 1C: Rao in view of Araujo and Singh renders obvious claim 3

A. Rao-Araujo-Singh Combination

260. Rao describes an example in which an "application is running in the foreground and currently in active use by the user, a network packet generated or

received for an application running in the background may be processed ahead of a network packet generated or received for the application running in the foreground. EX1005, ¶3. Such a situation is undesirable because “network packets for [background] applications may be processed ahead of the real-time network packets of [a foreground] VoIP telephone call thereby increasing the latency and reducing the quality of the voice communication.” *Id.* To prevent background traffic from interfering with foreground traffic, Rao teaches “policies 520 [that] define prioritization based on whether an application is running in the foreground or the background of the client” and “the network packets are communicated according to the determined priority.” EX1005, ¶¶182, 184.

261. A POSITA would have recognized that, in cases where multiple windows are displayed simultaneously (e.g., with the highest-priority window having “focus” and covering portions of lower-priority windows) in RAD it may be challenging for Rao’s device to determine which application running in the foreground to prioritize. Such an issue would be more acute in devices with larger displays, such as tablets. In such cases, multiple windows are in the foreground but partially displayed and one window has the focus (and thus should have the highest priority). Consider an example in which a user is playing, in the window with focus, an interactive on-line game that requires real-time communication. Another foreground window displays the user’s email, but the user interacts with email only

infrequently, such as between rounds of the interactive game. In such cases, while both windows are in the foreground, network traffic related to the game should receive priority when the game has focus.

262. Therefore, a POSITA would have recognized and appreciated “the multitude of ways to define client-side application priorities” and further recognized that the window priority of Singh represents such an example. EX1005, ¶182. As one example, a POSITA would have recognized or found obvious a RAD policy in which network traffic is permitted only if an application is displaying the highest priority window (per Rao as clarified by Singh) giving it “VIP” status (per Araujo) and the power state of the device is plugged-in or the battery is above a threshold charging level. EX1006, ¶22; EX1008, Abstract, 4:52-55. Among other examples, such an application might correspond to an interactive game that requires low-latency network communication. Assigning VIP status to such applications provides the best network responsiveness.

263. In operation, the processor of the resulting Rao-Araujo-Singh Device (RASD) would use the policy-based network traffic management techniques of Rao and Araujo as clarified by Singh to use networking resources efficiently. EX1007, Abstract; EX1005, ¶¶182-83; EX1008, 4:52-55, Abstract.

264. A POSITA would have expected success in creating a combination, which would have required only routine programming knowledge well within the

skill of a POSITA. Indeed, the combination would have amounted to nothing more than the use of a known technique to improve similar mobile devices in a similar way and combining prior art elements according to known methods to yield the predictable results described above. *Id.* RASD's processor would be configured to perform the operations discussed in this Ground.

B. Analysis of the claims

[3] The wireless end-user device of claim 1, wherein the processor executing the instructions determines that the first device application is in the foreground of user interaction based on a state of user interface priority for the application.

265. RASD renders [3] obvious. *See* EX1008, 9:33-35.

266. For example, Singh teaches that “when a user interacts with a window, the window becomes the highest priority window.” EX1008, 9:33-35. A POSITA would have known that when users interact with foreground windows, in Singh, users interact with the highest priority window (as any interaction causes the window to be assigned the highest priority). For example, Paquette includes the similar teaching that foreground application “may refer to an application that is currently configured to receive certain input, such as input from a keyboard. Such an application may be referred to as having the ‘keyboard focus’ (or ‘focus’ of other input devices) of the computing system 100, meaning any keyboard input that is received is likely to be routed to that application.” EX1019, 6:31-37. In this

example, the foreground application is the highest priority application as taught by Singh.

267. Therefore, a POSITA would have known to classify that the end-user application is interacting with the user in the UI foreground based on a state of user interface priority, i.e., the highest priority, as is the case where the foreground window is accepting user input (per Singh). EX1008, 9:33-35; EX1019, 6:31-37.

XIII. GROUND 1D: Rao in view of Araujo and Montemurro renders obvious claim 11.

A. Rao-Araujo-Montemurro Combination

268. As described above, in RAD, the device would use the techniques of Rao and Araujo to manage access to networks, considering various criteria, such as application priority and power factors. See §§ X.A, X.B ([1.5]). A POSITA would have recognized that, in some circumstances, further efficiency would have been gained over the Rao-Araujo Device (*see* §§ X.B. ([1.2]-[1.5])) by assigning different networks to different applications, such as the examples disclosed in Montemurro, where “the MP3 download application 204D runs on the lowest cost network ... available” and “the CRM application ... only synchronizes the sales contact database (e.g. 120B) over a WLAN network 106.” EX1009, ¶29.

269. Assigning applications to networks using such techniques can reduce cost to the user and lower the likelihood of causing network congestion. For example, assigning applications that require substantial bandwidth to high-

bandwidth networks (e.g., WLANs instead of WWANs) both improves the performance of the application (by moving data through faster) and limits network impact (by not flooding a lower-bandwidth network).

270. Thus, to improve the operation of RAD and further improve efficiency, a POSITA would have looked to teachings of other references, such as Montemurro.

271. The resulting Rao-Araujo-Montemurro Device (RAMD) would have used Montemurro's techniques to select a network appropriate for an application and then used the techniques of Rao and Araujo to manage device resources, such as network access and power. *See* §X.A. As applications such as VoIP and email execute on RAMD, Montemurro's "rules engine [would] evaluate[] its policies" to select a network appropriate for the particular application. *Id.*; EX1009, ¶11. On the selected networks, RAMD would use the techniques of Rao and Araujo to prioritize network traffic. *See* X.A. In one example, if VoIP and MP3 downloads were both assigned to the WLAN, the techniques of Rao would prioritize the real-time traffic of the VoIP data stream over the MP3 download. EX1005, ¶¶3, 179-84.

272. RAMD's processor would be configured to perform these operations in [12], [20] for at least the reasons described above.

273. Combining Rao, Araujo and Montemurro would have involved (1) combining prior art elements according to known methods to yield predictable

results; and (2) use of known techniques to improve similar devices (methods, or products) in the same way. Such a combination would have involved nothing more than the use of a known technique to improve similar smart phone devices equipped with network interfaces in a similar way and combining prior art elements according to known methods to yield the predictable results described above.

B. Analysis of the claims

[11] The wireless end-user device recited in claim 1, wherein dynamically determining whether to apply the network service usage control policy to the particular network service usage activity is further based on a current wireless network and/or the network service usage control policy is based on a current wireless network.

274. RAMD renders [11] obvious. *See* EX1009, ¶¶11, 13, 29; EX1005, ¶¶95, 119.

275. RAMD includes a network interface that enables connectivity to different types of networks and thereby provides different connectivity scenarios, including roaming and non-roaming cellular networks. EX1005, ¶¶95, 125; EX1009, ¶¶11, 13, 29.

276. For example, Montemurro includes a rules engine that “configures the communication operations with a set of rules/policies that could include various factors such as radio access technology (e.g. for high/low bandwidth properties),

cost, presence, time of day, location (e.g. geo-based policies, *network roaming*), destination IP address, application type, and Quality of Service (QoS) requirements, among others.” EX1009, ¶29 (emphasis added).

277. A POSITA would have recognized that when RAMD is roaming (i.e., connected to a cellular network of a provider other than the carrier providing contracted service to the device), RAMD can be connected to any network that supplies roaming cellular service.

278. For example, if there are three cellular providers, one provider is typically the carrier contracted to provide service, and using the other two networks would entail roaming. Since roaming can occur on either of those two networks, the mere fact that the device is roaming does not identify the network being used. Therefore, absent any additional information about the network, RAMD cannot identify a particular current wireless network. However, when RAMD is not roaming, the device is connected to the particular cellular network contracted to provide service to RAMD.

279. As discussed in §IX.E, to account for the connectivity scenarios discussed above, Montemurro leverages a rules engine that “configures the communication operations with a set of rules/policies that could include various factors such as...network roaming.” EX1009, ¶29.

280. A POSITA would have understood and found obvious that if rules applied by the rules engine of RAMD include factors such as network roaming, then certain rules specify actions to be taken when RAMD is currently connected to a roaming network, and other rules specify actions to be taken when RAMD is currently connected to a contracted (i.e., non-roaming) cellular network. In one example, a policy would specify that a large file transfer can only occur on a non-roaming network. In another example, a policy would specify that tethering is permitted only on non-roaming networks. Indeed, Montemurro indicates that “the CRM application (i.e. one of 204B) only synchronizes the sales contact database (e.g. 120B) over a WLAN network.” EX1009, ¶29. From this disclosure, a POSITA would have recognized that RAMD would have used policies to regulate certain file transfers (e.g., a database) so that they can only occur over a preferred network (e.g., non-roaming network).

281. Therefore, a POSITA would have understood or found obvious that Montemurro teaches determining whether to apply the network service usage control policy to the particular network service usage activity is further based on a current wireless network and/or the network service usage control policy is based on a current wireless network (e.g., applying only to the contracted carrier (non-roaming)). RAMD’s processor would be configured to perform the operations in [11] for at least the reasons described above.

XIV. GROUND 1E: Rao in view of Araujo and Wright renders obvious claims 9-10, 13 and 18.

A. Rao-Araujo-Wright Combination

282. As described above, RAD would use the policy-based management techniques of Rao and Araujo to manage access to networks, considering various criteria, such as quality of service, application priority and power factors. *See* §§ X.A–X.B. In RAD, such policy decisions are made locally by RAD through the frame monitor and power policy manager (e.g., PPM), which serve as the device’s LPDP, and enforced by the Packet Capture Mechanism (including a request deflector), which serves as RAD’s PEP. *Id.*

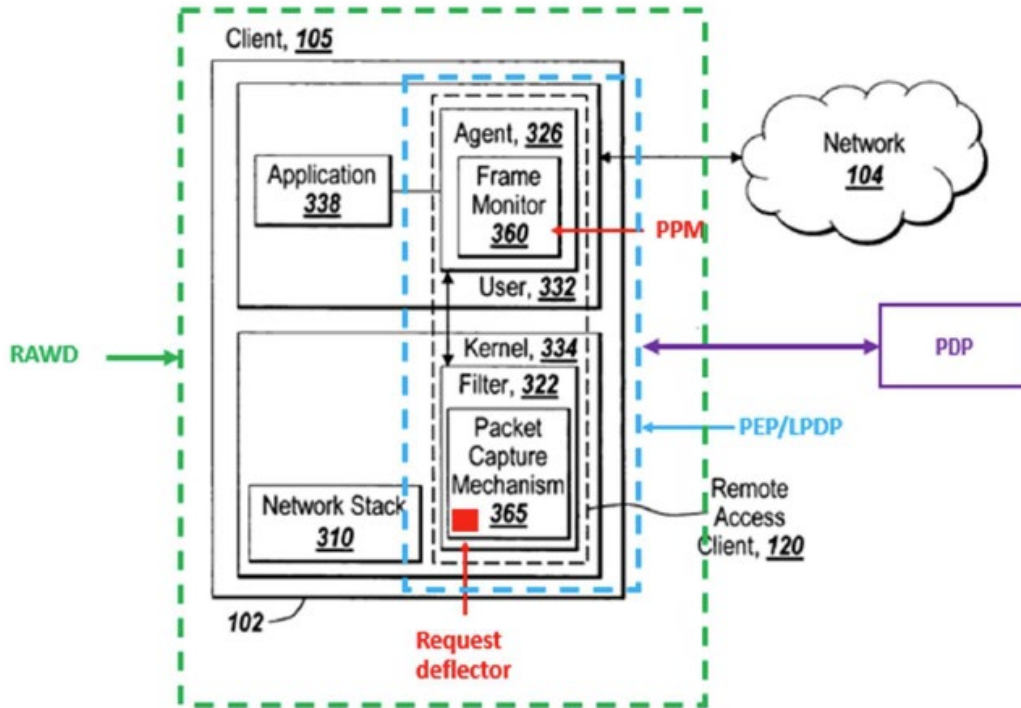
283. A POSITA would have recognized that constraining policy decisions to factors known locally at the device, however, limits the effectiveness of global network management techniques such as policy-based traffic engineering. To address this limitation, a POSITA would have looked to Wright’s approach, which “can include policy systems related to one or more of policy-based load balancing in traffic-engineered MPLS networks and traffic engineering of load distribution,” and also includes “feedback from a PEP ... to a PDP.” EX1010, ¶¶23, 65. Providing data from multiple PEPs to a PDP enables the PDP to make policy determinations based on network-wide factors, which can achieve network-wide efficiencies.

284. One example is traffic shaping, which is a form of traffic engineering that can be used to manage the allocation of bandwidth, and requires a more global

view of network use. In such systems, statistics from throughout a network are collected and used to achieve the traffic engineering goals, which benefit all network users, including mobile devices with RAD. Thus, to improve the operation of the Rao-Araujo Device by further improving network efficiency, a POSITA would have looked to teachings of other references, such as Wright.

285. In operation, the resulting Rao-Araujo-Wright System (RAWS) would use the techniques of Rao and Araujo to manage the resources of the Rao-Araujo-Wright Device (RAWD), such as network access and power. To enable more efficient use of global network resources, RAWD would provide network statistics to a PDP, enabling policy decisions to be outsourced to the PDP. EX1010, ¶21 (“[i]n policy outsourcing, events can occur at the PEPs 130 and require a policy-based decision, and the PEP 130 can request the decision from the PDP 120.”), ¶23 (the “feedback can include-information such as changes in dynamic state of network resources, link failures and congestion, statistics related to installed policy, etc.”)

286. In RAWS, illustrated below, the Remote Access Client 120 of RAWD acts as the PEP/LPDP and is enhanced by the techniques of Wright to provide data to a PDP, a separate component of RAWS that makes policy decisions based on a broader view of network state. RAWS’s PDP would serve multiple devices, although only one is shown below. EX1010, FIG. 6; see also §IX.F.



EX1005, FIG. 1C (annotated)

287. Combining Rao, Araujo, and Wright would have involved (1) combining prior art elements according to known methods to yield predictable results; and (2) use of known techniques (introducing a PDP) to improve similar devices (methods, or products) in the same way. Such a combination would have involved nothing more than the use of a known technique (introducing a PDP) and combining prior art elements according to known methods to yield the predictable results described above. RAWs's processor would be configured to perform the operations described in this Ground for at least the reasons described above. *See* §X.A.

B. Analysis of the claims

***[9.1] The wireless end-user device recited in claim 1,
wherein the processor executes the instructions further to:***

288. Element [9.1] is substantively identical to [1]. *See* §X.B, ([1]).

***[9.2] execute a router for dynamically managing one or
more network capacity controlled services and/or QoS
sessions for the wireless end-user device; and***

289. Element [9.2] is substantively identical [8]. *See* § X.B, ([8]).

***[9.3] send network busy state information to a service
controller, wherein the service controller provides a policy
decision point for management for a plurality of wireless
end- user devices in communication with one or more base
stations.***

290. RAWs renders [9.3] obvious. *See* EX1010 ¶¶21, 23, FIG. 6.

291. As described in §IX.E, Wright teaches that policy decisions can be “outsourced” to a policy decision point (PDP), which is a service controller, or can be included in a service controller that performs additional functions. EX1010, ¶¶21, 23; *see, e.g.*, EX1018 at 6, 8 (explaining the terms “outsourced policy” and “Policy Decision Point,” among other related terms).

292. Generally, the service controller can be a dedicated PDP or, as in the '544 Patent, the service controller can include a policy management server, which is more conventionally called a PDP, a billing event server, access control, etc. EX1001, FIG. 3. Regarding outsourcing, Wright explains that in “policy

outsourcing, events can occur at the PEPs 130 and require a policy-based decision, and the PEP 130 can request the decision from the PDP 120.” EX1010, ¶21.

293. Further, as described above, RAWD sends data, including network busy state information to RAWS’s service controller (PDP). See §X.F. For example, Wright explains that the PEP provides feedback to the PDP such as “changes in dynamic state of network resources, link failures and congestion, statistics related to installed policy, etc.” EX1010, ¶23. A POSITA would have recognized that congestion is a network busy state. In addition, the PDP (service control) provides PDP function (policy decisions) for multiple devices, which allows systems administrators to manage policies at fewer locations instead of managing policies at every device. EX1010, FIG. 6, ¶116 (policies can be communicated to multiple devices as shown in FIG. 8); EX1005, ¶86 (disclosing multiple client devices as shown in FIG. 1A); *see* §IX.F.

294. In addition, a POSITA would have known that RAWDs, such as wireless mobile devices, are in communication with base stations as taught by Wright, and the base stations provide access to the Internet. For example, Wright teaches that RAWDs’ “data communications can be carried by one or more communications channels of the one or more networks” that “can include...wireless communication links (e.g., satellite communication links, terrestrial wireless communication links, satellite-to-terrestrial communication

links, a combination thereof, and so on). EX1010, ¶123. And a POSITA would have understood that Wright's wireless communication link involves a "mobile device" that "may communicate through cellular network 104 and a representative base station 108 coupled to the Internet[.]". EX1009, ¶13.

295. Therefore, RAWs renders obvious [9], including rendering obvious sending network busy state information (congestion indications) to a service controller (PDP) that provides a policy decision point for multiple devices that are in communication with base stations.

[10.1] The wireless end-user device recited in claim 1, wherein the processor executes the instructions further to:

296. Element [10.1] is substantively identical to [1] and [9.1]. See §X.B, ([1], [9.1]).

[10.2] execute a router for dynamically managing one or more network capacity controlled services and/or QoS sessions for the wireless end-user device;

297. Element [10.2] is substantively identical to [8] and [9.2]. See §X.B, ([8], [9.2]).

[10.3] send network busy state information to a service controller, wherein the service controller provides a policy decision point for management for a plurality of wireless end-user devices in communication with one or more base stations; and

298. Element [10.3] is substantively identical to [9.3]. See §X.B ([9.3]).

[10.4] receive router traffic control instructions from the service controller, wherein the service controller provides the router traffic control instructions to assist in dynamically managing network capacity usage for the plurality of wireless end-user devices in communication with the one or more base stations.

299. RAWs renders [10.4] obvious. *See* EX1005, ¶182; EX1010, ¶¶21, 23, FIG. 6.

300. As described above, RAWs's PDP provides router traffic control instructions to the PEP in RAWD. *See* [9.3], §X.F, §XV.A. For example, Wright explains that policy decisions can be "outsourced" to a policy decision point (PDP), which is a service controller. EX1010, ¶21, 23; *see, e.g.*, EX1018 at 6, 8 (explaining the terms "outsourced policy" and "Policy Decision Point," among other related terms).

301. A POSITA would have known that when a policy decision is outsourced to a PDP, the PDP evaluates the policies to determine applicable actions. For example, as explained in Rao, the policy decision can result in "client-side prioritization of network communications related to applications." EX1005, ¶182. A POSITA would have recognized that network prioritization is a router traffic control instruction as such prioritization instructs the router regarding how traffic should be controlled, and specifically, how packets should be prioritized.

302. As further described above, RAWs's PDP assists in managing network capacity usage for the multiple devices. EX1010, FIG. 6; *see* §IX.F (discussing the Wright reference and explaining that Wright's Policy Decision Point (PDP) PDP provides policy decisions for multiple Policy Enforcement Points (PEPs)), §XIV.A (discussing the Rao-Araujo-Wright combination and explaining that its PDP would serve multiple devices). This includes, for example, communicating policies to multiple network devices as shown in Figure 8 of Wright (*e.g.*, EX1010, ¶116) and as shown in multiple client devices depicted in Figure 1A of Rao (*e.g.*, EX1005, ¶86).

303. In addition, as described in [9.3], a POSITA would have known that RAWDs, such as wireless mobile devices, are in communication with base stations as taught by Wright, and the base stations provide access to the Internet. For example, Wright teaches that RAWDs' "data communications can be carried by one or more communications channels of the one or more networks" that "can include...wireless communication links (*e.g.*, satellite communication links, terrestrial wireless communication links, satellite-to-terrestrial communication links, a combination thereof, and so on). EX1010, ¶123. A POSITA also would have understood that Wright's wireless communication link involves a "mobile device" that "may communicate through cellular network 104 and a representative base station 108 coupled to the Internet[.]". EX1009, ¶13.

***[13] The wireless end-user device recited in claim 1,
wherein associating includes querying a network element
for determining an association of the first device
application with the network service usage control policy.***

304. RAWD renders [13] obvious. *See* EX1005, ¶182; EX1010, ¶21.

305. Wright teaches that policy decisions can be made by a PDP in response to a query from a PEP. EX1010, ¶21 (“[i]n policy outsourcing, events can occur at the PEPs 130 and require a policy-based decision, and the PEP 130 can request the decision from the PDP 120”). A POSITA would have recognized that a PDP is a network element since communication between the PEP and PDP occurs over a network.⁸

306. Further, as explained in Rao, policies “may be specified by the name of the application” and/or “the type of application,” thus associating an application with a particular policy. EX1005, ¶182.

307. A POSITA would have known that since policy evaluation can be outsourced to a network element serving as a PDP (per Wright), and policies can be specified based on the application (per Rao), in RAWs, outsourcing the policy decision includes querying a network element (PDP) for determining an association of an application and a policy, enabling the PDP to make the policy

⁸ In some cases, the PDP and PEP can reside on the same physical server, but this configuration is atypical.

decision. *Id.*; EX1010, ¶21. In Wright, such a query is described as the PEP

“request[ing] the decision from the PDP 120.” EX1010, ¶21.

[18] The wireless end-user device recited in claim 1, wherein the processor executes the instructions further to: differentially control the particular network service usage activity based on the network service usage control policy based on a network busy state.

308. RAWs renders [18] obvious. *See* EX1005, ¶¶182, 184; EX1010, ¶23.

309. Rao describes policies that are used to differentially control network usage, e.g., through priority queuing. EX1005, ¶182 (“the remote access client 120 may have one or more policies 520 for specifying client-side prioritization of network communications related to applications”); EX1005, ¶184 (“a priority for the intercepted and queued network packet is determined based on the type and/or priority of the application”); *see also* X.B (discussion of [18]).

310. Wright further describes policies that are dependent on various factors. EX1010, ¶23. For example, Wright explains that the policy management system can include feedback from a PEP to a PDP, which can include “changes in dynamic state of network resources, link failures and congestion.” *Id.*

311. A POSITA would have recognized “congestion” as a “busy state.” Wright further explains that the PDP can use this information to “make changes to current policy decisions.” *Id.* Thus, a POSITA would have recognized that Wright teaches policies based on busy state (congestion). The network service usage

control policy disclosed by Rao and Wright serves as a differential control policy, including because it distinguishes the first application's network service usage activity from those of different applications. Accordingly, RAWs renders obvious [18], including because RAWs differentially controls the particular network service usage activity (through Rao's priority queuing) based on the network service usage control policy based on a network busy state (as taught by Wright).

XV. GROUND 1F: Rao in view of Araujo and Vignaud renders obvious claim 5.

A. Rao-Araujo-Vignaud Combination

312. As described above, the Rao-Araujo Device would have used Rao's and Araujo's techniques to manage access to networks, considering various criteria, such as network prioritization and power factors. *See* §X.A (discussing the Rao-Araujo combination and explaining that a POSITA would have incorporated Araujo's power policy manager and request deflector components in Rao's remote access client, including to manage access to networks while considering network prioritization and power factors).

313. A POSITA would have recognized that, in some circumstances, further efficiency would have been gained by applying Vignaud's "method for the optimization of network traffic, and associated implementation devices." EX1011, ¶2. Especially in the context of Rao-Araujo's queueing and not transmitting network packets (*see* §§X.A, X.B ([4])), a POSITA would have looked to

incorporate Vignaud based on its “aim of...reduc[ing] the stream of information received and sent out by the mobile client to access different services to which the user subscribes.” EX1011, ¶3.

314. As one example, a POSITA would have known the Rao-Araujo device would have benefited from incorporating Vignaud because Vignaud’s “decoy” reduces the amount of network traffic by reducing the number of interrogations to network servers that the client has to perform. *E.g.*, EX1011¶¶10-12, 73-75 (explaining that interrogations by the client application over the network are reduced because they are relayed only after Vignaud’s local proxy intermediary is opened), 85; EX1027, ¶¶124-26 (similarly explaining that interrogations of the server for connectivity states, which a POSITA would have understood to include whether an available wireless network is unavailable, are reduced by use of a local intermediary to ensure updates are not being attempted when (i) “connectivity does not exist” and updates would result in failure or (ii) only “limited connectivity” exists that would cause the update to have “negative effects”).

315. Like the Rao-Araujo Device’s “application-aware, client-specific prioritization of packet traffic,” as taught by Rao (*e.g.*, EX1005, ¶ 3), a POSITA would have understood that Vignaud’s proxy intermediary’s network optimization is application-aware and client-specific, as it “assumes the role of the client application by engaging in dialog with the service server.” See EX1011, ¶16. The

resulting Rao-Araujo-Vignaud Device (“RAVD”) would have used Vignaud’s network optimization techniques in combination with RAD’s.

316. A POSITA would have been motivated to apply Vignaud’s teachings to RAVD to further RAVD’s power management goals. As explained in Araujo, RAVD aims “to use [its] energy in a way that strikes a balance between providing functionality and maintaining longevity of the charge[,]” as explained by Araujo. EX1006, ¶1. A POSITA would have furthered this goal by incorporating Vignaud, which “aim[s]...to reduce the power consumption of a mobile client” while optimizing network traffic. *See* EX1011, ¶¶2, 5. Like the reduction in network traffic, a POSITA would have known the Rao-Araujo device would have further benefitted from incorporating Vignaud because Vignaud “avoids unnecessarily wasting the power of the” client device by reducing the number of server interrogations by the client device. EX1011, ¶85, *see also* ¶¶10-12, 73-75; EX1027, ¶¶124-26 (similarly explaining that interrogations of the server for connectivity states, which a POSITA would have understood to include whether an available wireless network is unavailable, are reduced by use of a local intermediary including to further power management goals and “not significantly effect battery life or battery charge time”).

317. A POSITA also would have specifically been motivated to modify RAVD’s network access API to incorporate Vignaud’s network messaging

emulation functionality. As described above, RAVD's request deflector component serves as a network access API that emulates access to the network. See §X.B ([5]); EX1017; EX1006, ¶¶ 5, 50. A POSITA would have looked to incorporate Vignaud's local proxy with RAVD's request deflector component to make the client application "believe that communication has truly been set up with" a server via network access. EX1011, Abstract, ¶¶ 51, 56; EX1006, ¶¶ 5, 50.

318. A POSITA would have understood that this would have spoofed the requesting application to "think that it has set up communication with the [server via network access]." EX1011, ¶56. (explaining Vignaud's emulation functionality "aim[s] at being a decoy for the application 108. Indeed, the application 108 must think it has set up communication with the [server via network access].").

Incorporating this functionality would have furthered Rao's goal of transparently intercepting network messages (*see* EX1005, ¶80) because a POSITA would have understood that Rao's use of the term "transparent" refers to the client application in the combined system remaining unaware that its communication is being provided to an intermediary instead of being provided directly to a network server. EX1011 ¶¶6, 51, 56; *see* EX1025, 1:50-53, 2:58-65.

319. Combining Rao, Araujo, and Vignaud would have involved (1) combining prior art elements according to known methods to yield predictable results; and (2) use of known techniques to improve similar devices (methods, or

products) in the same way. The combination would have involved nothing more than the use of a known technique to improve similar smart phone devices equipped with network interfaces in a similar way and combining prior art elements according to known methods to yield the predictable results described above.

B. Analysis of the claims

[5] The wireless end-user device of claim 1, wherein when the network service usage control policy is applied it disallows the particular network service usage activity, and wherein the processor executes the instruction further to, when it is determined that the particular network access request is disallowed, queue that particular network service usage activity until a power state change occurs.

320. The Rao-Araujo-Vignaud device renders [5] obvious. *See* EX1006, FIG. 6, ¶¶ 5, 48, 50; EX1011, ¶¶ 51, 56.

321. Vignaud discloses that its client application sends a request at step 201 and the intermediary provides a response at step 203. EX1011, ¶¶ 51, 56. The intermediary's response is a "standard response defined by the protocol used" and indicates that the connection to the server is busy. *Id.*, ¶ 56. Notably, this response is "aimed at being a decoy for the application 108" to make the application "think that it has set up communication with the service server 115." *Id.*

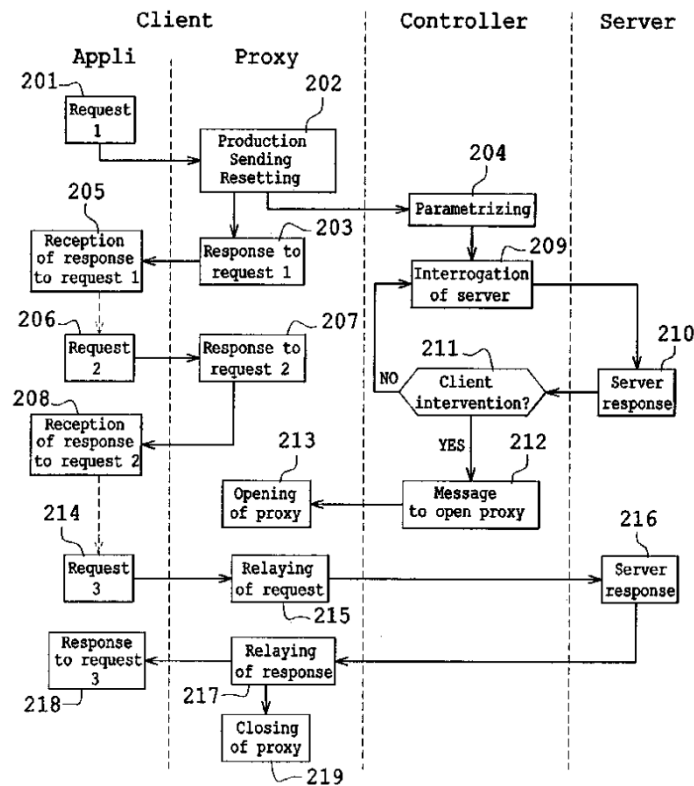


Fig. 2

EX1011, FIG. 2

322. A POSITA would have understood Vignaud's methods to disclose emulation because Vignaud's intermediary proxy makes the client application "believe that communication has truly been set up with" a server via network access. *Id.*, Abstract.

323. A POSITA also would have understood that Vignaud's request to the intermediary, and the intermediary's response indicating whether the connection is busy, discloses an emulated network access API's indication to a first device application that an available wireless network is unavailable. EX1011, ¶¶51, 56.

324. As discussed above, RAVD renders obvious a dynamic determination applying the network service usage control policy to the particular network service usage activity based on Araujo's disclosures. See § X.B ([5]). Accordingly, a POSITA would have understood that RAVD's emulation functionality further renders obvious [5].

XVI. CONCLUSION

325. For the reasons set forth above, it is my opinion that claims 1-23 of the '544 Patent are unpatentable in view of the prior art. In signing this declaration, I understand that the declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I acknowledge that I may be subject to cross-examination in this case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

326. I declare that all statements made herein of my knowledge are true, and that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Date: January 14, 2026

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'K Butler', written over a horizontal line.

Dr. Kevin Butler

APPENDIX A

KEVIN RAYMOND BOYCE BUTLER

Professor	Address :	1889 Museum Rd.
Department of Computer & Information Science and Engineering		PO Box 116120
University of Florida		Gainesville FL 32611
email: butler@ufl.edu	Phone:	+1 (352) 294-2090
URL: http://www.kevinbutler.org	Fax:	+1 (352) 392-1220

Current Academic Appointment

Professor, Department of Computer and Information Science and Engineering, University of Florida, Aug. 2021 - *present*

Director, Florida Institute for Cybersecurity Research, University of Florida, Aug. 2022 - *present*

Educational Background

Ph.D. in Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, August 2010 (Dissertation Title: *Leveraging Emerging Storage Functionality for New Security Services*; Advisor: Dr. Patrick McDaniel)

M.S. in Electrical Engineering, Columbia University, New York, NY, USA, May 2003 (Advisor: Dr. Henning Schulzrinne)

B.Sc. in Electrical Engineering, Queen's University, Kingston, ON, Canada, May 1999

Honors & Awards

Social Impact Award, New York University CSAW Applied Research Competition, 2025.

Internet Defense Prize Runner Up Award, USENIX Security Symposium, 2025.

Distinguished Paper Honorable Mention, USENIX Security Symposium, 2025.

Best Paper Award, ACM Conference on Reproducibility and Replicability (REP), 2025.

University of Florida Research Foundation Professor, University of Florida, 2025-2028.

Fellow, European Alliance for Innovation (EAI), 2024.

Distinguished Paper Award, ACM Conference on Computer and Communications Security (CCS), 2024.

Best Paper Award, ACM Conference on Data and Application security and Privacy (CODASPY), 2024.

Best Paper Award, ACM HotStorage, 2023.

Privacy-Enhancing Technology Award, Meta Research Labs, 2022.

Best Paper Finalist, IEEE European Symposium on Security and Privacy, 2022.

University Term Professor, University of Florida, 2021-2024.

Best Paper Nominee, IEEE Conference on Virtual Reality, 2021.

Doctoral Dissertation Advisor/Mentoring Award, Herbert Wertheim College of Engineering, University of Florida, 2019.

Distinguished Poster Award, ACM CODASPY, 2019.

Arnold and Lisa Goldberg Rising Star Endowed Professorship, University of Florida, 2018-2024 (*relinquished in 2021 upon promotion to Professor*).

University Term Professor, University of Florida, 2018-2021.
Recognition of Service Award, Association for Computing Machinery (ACM), 2018.
Research Promotion Initiative Award, University of Florida, 2018.
Senior Member, Association for Computing Machinery, 2018.
International Educator of the Year, Herbert Wertheim College of Engineering, University of Florida, 2017.
Senior Member, Institute for Electrical and Electronics Engineers (IEEE), 2017.
Outstanding Community Service Award, IEEE Technical Committee on Security and Privacy, 2017.
Rising to National Preeminence Hire, University of Florida, 2014.
Best Teacher Award, Dept. of Computer and Information Science, University of Oregon, 2013.
CAREER Award, National Science Foundation, 2013.
Alumni Association Dissertation Award, Pennsylvania State University, 2010.
Symantec Intern Project Showcase Winner, Symantec Corp, 2009.
Graduate Research Assistant Award, Computer Science and Engineering Department, Pennsylvania State University, 2009.
Symantec Graduate Fellowship, Symantec Research Labs, 2009-2010.
Special Award of Meritorious Service, Third International Conference on Information Systems Security, December 2007.
University Graduate Fellowship, Pennsylvania State University, 2006.
C. Norwood Wherry Memorial Graduate Fellowship, Pennsylvania State University, 2004.

Expert Witness Experience

During the course of my expert witness consulting engagements, I have written numerous expert reports, given eight depositions, and have testified four times across two jury trials, with regards to both patent infringement and invalidity.

Testifying Expert, *Headwater Research LLC v. Apple Inc. and Google LLC*, retained by Finnegan, Henderson, Farabow, Garrett & Dunner LLP, regarding mobile devices, representing defendant, October 2025 - present.

Testifying Expert, *Headwater Research LLC v. Samsung America Inc.*, No. 2:22-cv-00422, 2:22-cv-00467, 2:23-cv-00103 (E.D. Texas), retained by Fish and Richardson, regarding mobile devices, representing defendant, April 2023 - present. Testified in deposition.

Testifying Expert, *Webroot, Inc. et al. v. Trend Micro Inc.*, No. 6:22-cv-00239-ADA-DTG (W.D. Texas), retained by Paul Hastings LLP and White & Case LLP, regarding intrusion detection devices, representing defendant. July 2022-January 2024.

Consulting Expert, *Department of Justice, Antitrust Division, defendant confidential*, retained by USDOJ, regarding mobile devices. June 2022-June 2023.

Testifying Expert, *Research in Motion Limited ats Glen Snowball (File No. 13-57203CP), Blackberry Limited ats Michael Blackette (File No. 500-06-000583-118)*, retained by Torys LLP, regarding the Blackberry network, representing defendant. March 2021-present.

Testifying Expert, *IOENGINE LLC vs Roku Inc.* regarding portable devices, engaged by plaintiff in patent infringement case, October 2021-March 2023. Testified in deposition.

Testifying Expert, *Finjian, Inc. v. Juniper Networks, Inc.* (3:17-cv-0569-WHA, District Court, N.D. California), retained by Irell and Manella LLP, regarding intrusion detection systems, representing

defendant. June 2019-August 2019.

Testifying Expert, *Ingenico Inc v. IOENGINE LLC (1:18-cv-00826, District Court, D. Delaware)*, retained by Dechert LLP, regarding secure portable devices, representing defendant. October 2018-December 2022. Testified in deposition.

Testifying Expert, *IOENGINE LLC v. Imation Corp. (1:14-cv-01572, District Court, D. Delaware)*, retained by Simpson Thacher & Bartlett LLP, regarding secure portable storage devices, representing plaintiff. March 2015-February 2017. Testified in multiple depositions and at jury trial.

Testifying Expert, *IOENGINE LLC v. Interactive Media Corp. (1:14-cv-01571, District Court, D. Delaware)*, retained by Simpson Thacher & Bartlett LLP, regarding secure portable storage devices, representing plaintiff. March 2015-January 2017. Testified in multiple depositions and at jury trial.

Consulting Expert, *Vir2us, Inc.*, retained by Bunsow, De Mory, Smith, and Allison LLP, regarding virtualization and antivirus software. December 2014 - April 2015

Consulting Expert, *Envosys v. AT&T*, retained by Baker Botts, regarding location services in mobile devices, representing defendant. October 2013-December 2013.

Research Support (\$44.1M total, \$14.0M as PI, \$12.3M investigator share)

Major Peer-Reviewed Grants (\$41.3M total, \$12.2M as PI, \$10.7M investigator share)

- **PI**, “Collective Modeling for Cybersecurity”, DARPA/Avometric, \$1,181,584 (\$1,181,584 investigator share), 03/01/2025-02/28/2028.
- **co-PI**, NSF CNS-2446321, “SaTC: CORE: Small: Measuring and Improving Reproducibility”, National Science Foundation, \$600,000 (\$262,323 investigator share), 04/01/2025-03/31/2028.
- **PI**, ONR N68335-19-C-0633, “ARTUS Protocol, Phase 2”, Office of Naval Research / P & J Robinson Corporation, \$300,000 (\$254,033 investigator share), 8/1/2023-7/31/2025.
- **co-I**, NIH 1R01MH136195, “AVAIL: Anonymization of Videos using AI for Large scale data sharing”, National Institutes of Health, \$3,916,308 (\$277,546 investigator share), 5/13/2024-5/12/2029.
- **PI**, NSF CNS-2206950, “Collaborative Research: SaTC: Frontiers: Securing the Future of Computing for Marginalized and Vulnerable Populations”, National Science Foundation, \$7,500,000 (\$2,630,872 investigator share), 10/1/2022-9/30/2027.
- **Site PI**, NSF CNS-2055014, “Collaborative Research: SaTC: CORE: Medium: Enabling Practically Secure Cellular Infrastructure”, National Science Foundation, \$1,199,985 (\$598,019 investigator share), 1/1/2022-12/31/2026.
- **co-PI**, NSF CNS-2055123, “SaTC: CORE: Medium: Countering Surveillanceware Using Deception-Based Generative Models and Systems Mechanisms”, National Science Foundation, \$1,199,997 (\$618,531 investigator share), 1/1/2021-12/31/2026.
- **co-PI**, ONR N00014-20-1-2205, “Reconstructing Human Physiological Features from Audio Samples”, Office of Naval Research, \$700,000 (\$333,232 investigator share), 6/11/2021-6/10/2024.

- **co-PI**, DHS 70RSAT20CB0000017, “Deploying Defenses for Cellular Networks Using the AWARE Testbed”, DHS, \$3,122,033 (\$657,536 investigator share), 9/30/2020-9/29/2024.
- **PI**, ONR BAA-N00014-19-S-B001 Grant 12941701, “Mobile Interface Security Analysis”, Office of Naval Research, \$700,000 (\$376,242 investigator share), 1/1/2020-12/31/2022.
- **PI**, AFOSR AACOE, “Interpretable Security Reference Monitor for Deep Networks”, Air Force Office of Scientific Research, \$185,000 (\$185,000 investigator share), 12/1/2019-8/31/2021.
- **co-PI**, ONR DOD-19-STTR, “ArtusProtocol”, Office of Naval Research, \$800,000 (\$400,000 investigator share), 8/1/2019-7/31/2021.
- **co-PI**, AFOSR FA8650-19-1-1741, “University Center of Excellence: CYAN: Enabling Cyber Defense in Analog and Mixed Signal Domain”, Air Force Office of Scientific Research, \$5,000,000 (\$300,000 investigator share), 10/1/2019-9/30/2024. Selected for funding by AFOSR on 5/24/2019.
- **co-PI**, AFRL-FA9550-19-1-0169, “AFOSR University Center of Excellence in Assured Autonomy in Contested Environments (AACOE)”, Air Force Office of Scientific Research and Air Force Research Labs, \$5,999,515 (\$389,999 investigator share), 3/1/2019-2/28/2024.
- **co-PI**, DARPA HR00118S0052, “RACE: Resilient Communications for Everyone”, Defense Advanced Research Projects Agency, \$1,133,856 (\$382,698 investigator share), 3/1/2019-2/28/2023. Selected for funding by DARPA on 11/20/2018.
- **PI**, NSF/SRC CNS-1815883, “SaTC: STARSS: Small: Domain Informed Techniques for Detecting and Defending Against Malicious Firmware”, National Science Foundation, \$499,990 (\$250,000 investigator share), 11/01/2018-10/31/2021.
- **co-PI**, NSF CNS-1662976, “Collaborative Research: SURPASS: NSF SFS Unique Scholarship Program in Hardware and Systems Security”, National Science Foundation, \$2,508,541 (\$35,408 investigator share), 01/01/2017-12/31/2021.
- **co-PI**, NSF CNS-1562485, “TWC: Medium: Digital Healthcare-Associated Infection: Measurement, Defense and Prevention in a Modern Digital Healthcare Ecosystem”, National Science Foundation, \$1,200,000 (\$387,931 investigator share), 06/01/2016-05/31/2020.
- **PI**, “Developing Research Capability in Cyber-Physical Systems at the University of Florida”, Defense University Research Instrumentation Program (DURIP), Army Research Office, \$199,919 (\$100,000 investigator share), 09/01/2015-08/31/2016.
- **PI**, NSF CNS-1445983/1540216, “EAGER: Collaborative: Secure and Efficient Data Provenance”, National Science Foundation, \$205,000 (\$110,000 investigator share), 10/01/2014-03/31/2016.
- **PI**, NSF CNS 1254198/1540217, “CAREER: Securing Critical Infrastructure with Autonomously Secure Storage”, National Science Foundation, \$400,000, 04/01/2013-03/31/2018.
- **PI**, NSF CNS 1118046/154028, “TC:Small:Protection Mechanisms for Portable Storage”, National Science Foundation, \$515,530, 09/01/2011-08/31/2016.
- **co-PI**, “GAANN Program on Computer Systems Security”, US Department of Education, \$1,476,931 (\$184,616 investigator share), 08/16/2015-08/15/2018.

- **co-PI**, DARPA BAA 10-81, “Characterizing and Implementing Efficient Primitives for Privacy-Preserving Computation”, Defense Advanced Research Projects Agency and Air Force Research Labs, \$550,000 (\$262,375 investigator share), 05/01/2011-01/31/2015.

Industry and Other Support

- **PI**, “Proposal for a Florida Department of Management Services Cybersecurity Operations Center”. Florida Department of Management Services, \$1,551,303 (\$1,012,812 investigator share), 08/01/2025-07/31/2028.
- **PI**, “RADIOBEAR. Nightwing, \$199,291 (\$103,140 investigator share), 08/07/2025-2/6/2026.
- **co-PI**, “Mitigating Threat of Re-Identification from Eye-Tracking Data”, Meta Privacy-Enhancing Technology Award, \$100,000 (\$49,000 investigator share), 09/01/2022-08/31/2023.
- **co-PI**, “Center for Aerospace Resilience”, Florida Department of Education, \$875,000 (\$126,214 investigator share), 07/01/2020-06/31/2021.
- **PI**, “Secure Enclave Computing”, Royal Bank of Canada, \$87,347 (\$87,437 investigator share), 11/01/2019-01/01/2021.
- **PI**, NSF 1823067, “Travel Grant Support for ACM WiSec”, *National Science Foundation*, \$9,000, 05/27/2018-05/26/2019.
- **Co-PI**, “Formal Analysis of SGX Platform Software”, *Intel Corporation*, \$50,000 (\$25,000 investigator share), 01/01/2018-12/31/2018.
- **PI**, “Smartphones and Mobile Money: Analysis and Recommendations for Security”, *GSMA Mobile For Development Foundation*, \$28,500 (\$13,500 investigator share), 12/01/2017-03/31/2018.
- **PI**, “Provenance-Based Enforcement Mechanisms”, *MIT Lincoln Laboratory*, \$137,000, 11/01/2013-10/31/2016.
- **PI**, “Securing Storage for Insider Threat Mitigation”, *Florida Cyber Consortium Seed Grant*, \$40,000 (\$20,000 investigator share), 2015.
- **co-PI**, “Resilience in BGPsec”, *Battelle*, \$180,000 (\$80,000 investigator share), 02/01/2012-08/31/2013.
- **co-PI**, “A Cyber-Security Center of Excellence for Oregon”, *Oregon Engineering, Technology, and Industry Council*, \$180,000 (\$60,000 investigator share), 06/01/2014-05/31/2015.
- **co-PI**, “I3: An Interdisciplinary Approach to Internet Privacy”, *University of Oregon Research, Innovation and Graduate Education*, \$50,000, 04/10/2014-03/31/2015.
- **PI**, NSF CNS 1329307, “Oregon Security Day”, *National Science Foundation*, \$8,000, 03/01/2013-04/30/2014.
- **Recipient**, “USB Fingerprinting”, *Ellisys*, *equipment donation*, \$8,000, 2011.
- **Recipient**, “Project HAWAII”, *Microsoft Research*, *equipment donation*, \$1,000, 2011.

Publications (7013 citations [Google Scholar, January 2026], h-index=44, i10-index=100)

Book Chapters

1. Adam Bates, Devin Pohly, and Kevin R. B. Butler. “Secure and Trustworthy Provenance Collection for Digital Forensics.” In C. Wang, R. M. Gerdes, Y. Guan, and S. K. Kasera, eds., *Digital Fingerprinting* (pp. 141–176). New York: Springer-Verlag, 2016.
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.

Journal Publications

3. Efe Bozkir, Süleyman Özdel, Mengdi Wang, Brendan David-John, Hong Gao, Kevin Butler, Eakta Jain, and Enkelejda Kasneci. “Eye-tracked Virtual Reality: A Comprehensive Survey on Methods and Privacy Challenges.” *Proceedings of the IEEE*, accepted for publication January 2026.
4. Weidong Zhou, Grant Hernandez, Washington Garcia, Dave (Jing) Tian, Sara Rampazzi, and Kevin Butler. “SrFTL: Leveraging Storage Semantics for effective Ransomware Defense in Flash-based SSDs”. *ACM Transactions on Storage*, 21(4), Article 29, pg. 1-42, November 2025.
5. Seth Layton, Daniel Olszewski, Kevin Warren, Kevin Butler, and Patrick Traynor. “Every Breath You Don’t Take: Deepfake Speech Detection Using Breath”. *ACM Digital Threats: Research and Practice*, 6(3), Article 13, pg. 1-18, September 2025.
6. Chris Moore, Catherine Gill, Nadya Bliss, Kevin Butler, Stephanie Forrest, Dan Lopresti, Mary Lou Maher, Helena Mentis, Shashi Shekhar, Amanda Stent, and Matthew Turk. “Concerning the Responsible Use of AI in the US Criminal Justice System.” *Communications of the ACM*, 68(9), pg. 41-44, August 2025.
7. Cassidy Gibson, Kevin R. B. Butler, Tadayoshi Kohno, and Elissa M. Redmiles. “The Tools and Tolls of AI Nudification.” *USENIX ;login*, July 2025.
8. Cassidy Gibson, Patrick Traynor, and Kevin Butler. “Copycat Crimes: Characterizing Code Reuse in the Mobile Android Stalkerware Ecosystem.” *IEEE Security and Privacy*, 23(4), pg. 71-79, July 2025.
9. Kevin Butler, Kurt Hugenberg, Eakta Jain, Apu Kapadia, Tadayoshi Kohno, Elissa M. Redmiles, Franziska Roesner, Mattea Sim, Patrick Traynor, and Hanna Barakat. “Extending the Heilmeier Catechism to Evaluate Security & Privacy Systems: Who is Left Out?” *IEEE Security and Privacy*, 23(3), pg. 91-95, May/June 2025.
10. Ethan Wilson, Azim Ibragimov, Michael J. Proulx, Sai Deep Tetali, Kevin Butler, and Eakta Jain. “Privacy-Preserving Gaze Data Streaming in Immersive Interactive Virtual Reality: Robustness and User Experience.” *IEEE Transactions on Visualization and Computer Graphics*, 30(5), pg. 2257-2268, January 2024. *Selected for presentation at IEEE VR 2024 conference.*
11. Brendan David-John, Kevin Butler, and Eakta Jain. “Privacy-Preserving Datasets of Eye-tracking Samples with Applications in XR.” *IEEE Transactions on Visualization and Computer Graphics*, 29(5), pg. 2774-2784, January 2023. *Selected for presentation at IEEE VR 2023 conference.*
12. Weidong Zhu and Kevin Butler. “NASA: NVM-Assisted Secure Deletion for Flash Memory.” *IEEE*

Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), 41(11), pg. 3779-3790, July 2022. *Accepted for presentation at the International Conference on Embedded Software (EMSOFT) 2022.*

13. Tuba Yavuz, Farhaan Fowze, Grant Hernandez, Ken (Yihang) Bai, Kevin Butler, and Dave (Jing) Tian. "ENCIDER: Detecting Timing and Cache Side Channels in SGX Enclaves and Cryptographic APIs." *IEEE Transactions on Dependable and Secure Computing*, 20(2), pg. 1577-1595, March/April 2022.
14. Brendan David-John, Diane Hosfelt, Kevin Butler, and Eakta Jain. "A Privacy-Preserving Approach to Streaming Eye-Tracking Data." *IEEE Transactions on Visualization and Computer Graphics*, 27(5), pg. 2555-2565, March 2021. **Best paper nominee at IEEE VR 2021 conference.**
15. Farhaan Fowze, Grant Hernandez, Dave (Jing) Tian, Kevin Butler, and Tuba Yavuz. "ProXray: Protocol Model Learning and Guided Firmware Analysis." *IEEE Transactions on Software Engineering*, 47(9), pg. 1907-1928, September 2019.
16. Grant Hernandez, Dave (Jing) Tian, Farhaan Fowze, Tuba Yavuz, Patrick Traynor, and Kevin Butler. "Towards Automated Firmware Analysis in the IoT Era." *IEEE Security and Privacy*, 17(5), pg. 38-46, Sept.-Oct. 2019.
17. Joseph Choi and Kevin Butler. "Secure Multiparty Computation and Trusted Hardware: Examining Adoption Challenges and Opportunities". *Security and Communication Networks*, vol 2019, Article ID 1368905, 28 pages, April 2019.
18. Benjamin Mood and Kevin Butler. "PAL: A System for Optimizing Secure Function Evaluation in Mobile Devices". *Journal of Information Security and Applications*, 40(2018), pg. 78-91, March 2018.
19. Bradley Reaves, Luis Vargas, Nolen Scaife, Dave (Jing) Tian, Logan Blue, Patrick Traynor, and Kevin Butler. "Characterizing the Security of the SMS Ecosystem with Public Gateways". *ACM Transactions on Privacy and Security*, 22(1), Article 2, January 2018.
20. Nolen Scaife, Patrick Traynor, and Kevin Butler. "Making Sense of the Ransomware Mess (and planning a sensible path forward)". *IEEE Potentials*, 36(6), pg. 28-31, Nov/Dec. 2017.
21. Dave (Jing) Tian, Kevin R. B. Butler, Joseph Choi, Patrick D. McDaniel, and Padma Krishnaswamy. "Securing ARP/NDP From the Ground Up." *IEEE Transactions on Information Forensics and Security*, 12(9), pg. 2131-2143, September 2017.
22. Adam Bates, Dave (Jing) Tian, Grant Hernandez, Thomas Moyer, Kevin R. B. Butler, and Trent Jaeger. "Taming the Costs of Trustworthy Provenance through Policy Reduction." *ACM Transactions on Internet Technology*, 17(4), Article 34, September 2017.
23. Bradley Reaves, Jasmine Bowers, Nolen Scaife, Adam Bates, Arnav Bhartiya, Patrick Traynor, and Kevin Butler. "Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications". *ACM Transactions on Privacy and Security*, 20(3), Article 11, August 2017.
24. Bradley Reaves, Jasmine Bowers, Sigmund Albert Gorski III, Rahul Bobate, Raymond Cho, Hiranava Sas, 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*, 49(3), Article 55, November 2016.
25. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. "Outsourcing Secure Two-Party

Computation as a Black Box”. *Security and Communication Networks*, 9(14), pg. 2261-2275, September 2016.

26. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. “Secure Outsourced Garbled Circuit Evaluation for Mobile Devices.” *Journal of Computer Security*, 24(2), pg. 137-180, 2016.
27. Adam Bates, Kevin Butler, Micah Sherr, Clay Shields, Patrick Traynor, and Dan Wallach. “Accountable Wiretapping -or- I Know That You Can Hear Me Now”. *Journal of Computer Security*, 23 (2015), pg. 167-195, 2015.
28. Adam Bates, Benjamin Mood, Joe Pletcher, Hannah Pruse, Masoud Valafar, and Kevin Butler. “On Detecting Co-Resident Cloud Instances Using Network Flow Watermarking Techniques”. *International Journal of Information Security*, 13(2), pg. 171-189, April 2014.
29. Thomas Moyer, Kevin Butler, Joshua Schiffman, Patrick McDaniel, and Trent Jaeger. “Scalable Web Content Attestation”. *IEEE Transactions on Computers*, 61((5), pg. 686-699, May 2012.
30. Kevin Butler, Stephen McLaughlin, Thomas Moyer, and Patrick McDaniel. “New Security Architectures Based on Emerging Disk Functionality”. *IEEE Security and Privacy*, 8(5), pg. 34-31, Sept./Oct. 2010.
31. Kevin Butler, Toni Farley, Patrick McDaniel, and Jennifer Rexford. “A Survey of BGP Security Issues and Solutions”. *Proceedings of the IEEE*, 98(1), pg. 100-122, January 2010.
32. 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)*. 2009.
33. 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*, 20(12), pg. 1803-1815, December 2009.
34. Patrick McDaniel, William Aiello, Kevin Butler, and John Ioannidis, Origin Authentication in Interdomain Routing. *Computer Networks*, 50(16), pg. 2953-2980, 14 November 2006.

Conference Publications

Top-4 Security Conferences

35. Nathaniel Bennett, Tyler Tucker, Carson Stillman, William Enck, Patrick Traynor, and Kevin Butler. “Fizz: A Framework for Deterministic and Reproducible Network Fuzzing.” *47th IEEE Symposium on Security and Privacy (Oakland’26)*, San Francisco, CA, USA, May 2026.
36. Seth Layton, Bernardo B. P. Medeiros, Kevin Butler, and Patrick Traynor. “AI Wrote My Paper and All I Got Was This False Negative: Measuring the Efficacy of Commercial AI Text Detectors.” *47th IEEE Symposium on Security and Privacy (Oakland’26)*, San Francisco, CA, USA, May 2026.
37. Weidong Zhu, Carson Stillman, Sara Rampazzi, and Kevin Butler. “Enabling Secure and Efficient Data Loss Prevention with a Retention-aware Versioning SSD.” *32nd ACM Conference on Computer and Communication Security (CCS’25)*, Taipei, Taiwan, October 2025. (Acceptance Rate: 14.4%)
38. Daniel Olszewski, Tyler Tucker, Kevin Butler, and Patrick Traynor. “SoK: Towards a Unified Approach to Applied Replicability for Computer Security.” *34th USENIX Security Symposium (Secu-*

city'25), Seattle, WA, USA, August 2025. (Acceptance Rate: 17.1%)

39. Cassidy Gibson, Daniel Olszewski, Natalie Grace Brigham, Anna Crowder, Kevin Butler, Patrick Traynor, Elissa M. Redmiles, and Tadayoshi Kohno. "Analyzing the AI Nudification Application Ecosystem." *34th USENIX Security Symposium (Security'25)*, Seattle, WA, USA, August 2025. **Internet Defense Prize Runner Up Award. Distinguished Paper Honorable Mention.** (Acceptance Rate: 17.1%.)
40. Anna Crowder, Allison Lu, Kevin Childs, Carson Stillman, Patrick Traynor, and Kevin Butler. "Data to Infinity and Beyond: Examining Data Sharing and Usage Practices in the Computer Security Community." *46th IEEE Symposium on Security and Privacy (Oakland'25)*, San Francisco, CA, USA, May 2025. (Acceptance Rate: 14.8%)
41. Magdalena Pasternak, Kevin Warren, Daniel Olszewski, Susan Nittrover, Patrick Traynor, and Kevin Butler. "Characterizing the Impact of Audio Deepfakes in the Presence of Cochlear Implant Simulated Audio." *32nd ISOC Symposium on Network and Distributed System Security (NDSS'25)*, San Diego, CA, USA, February 2025. (Acceptance Rate: 16.1%.)
42. Tyler Tucker, Nathaniel Bennett, Martin Kotuliak, Simon Erni, Srdjan Capkun, Kevin Butler, and Patrick Traynor. "Detecting IMSI-Catchers by Characterizing Identity Exposing Messages in Cellular Traffic." *32nd ISOC Symposium on Network and Distributed System Security (NDSS'25)*, San Diego, CA, USA, February 2025. (Acceptance Rate: 16.1%.)
43. Kevin Childs, Cassidy Gibson, Anna Crowder, Kevin Warren, Carson Stillman, Elissa M. Redmiles, Eakta Jain, Patrick Traynor, and Kevin R. B. Butler. "'I Had Sort of a Sense that I was Always Being Watched...Since I Was': Examining Interpersonal Discomfort From Continuous Location-Sharing Applications." *31st ACM Conference on Computer and Communications Security (CCS'24)*, Salt Lake City, UT, USA, October 2024. (Acceptance rate: 16.9%.)
44. Nathaniel Bennett, Weidong Zhu, Benjamin Simon, Ryon Kennedy, William Enck, Patrick Traynor, and Kevin R. B. Butler. "RANSacked: A Domain-Informed Approach for Fuzzing LTE and 5G RAN-Core Interfaces." *31st ACM Conference on Computer and Communications Security (CCS'24)*, Salt Lake City, UT, USA, October 2024. (Acceptance rate: 16.9%.)
45. Kevin Warren, Tyler Tucker, Anna Crowder, Daniel Olszewski, Allison Lu, Caroline Fedele, Magdalena Pasternak, Seth Layton, Kevin Butler, Carrie Gates, and Patrick Traynor. "'Better Be Computer Or I'm Dumb': A Large-Scale Evaluation of Humans as Audio Deepfake Detectors." *31st ACM Conference on Computer and Communications Security (CCS'24)* Salt Lake City, UT, USA, November 2024. **Distinguished Paper Award.** (Acceptance rate: 16.9%.)
46. Seth Layton, Tyler Tucker, Daniel Olszewski, Kevin Warren, Carrie Gates, Kevin Butler, and Patrick Traynor. "SoK: The Good, The Bad, and The Unbalanced: Measuring Structural Limitations of Current Deepfake Datasets". *33rd USENIX Security Symposium (Security'24)*, Philadelphia, PA, USA, August 2024. (Acceptance rate: 17.6%)
47. Jennifer Sheldon, Weidong Zhu, Adnan Abdullah, Sri Hrushikesh Varma Bhupathiraju, Takeshi Sugawara, Kevin Butler, Md Jahidul Islam, and Sara Rampazzi. "AquaSonic: Acoustic Manipulation of Underwater Data Center Operations and Resource Management". *45th IEEE Symposium on Security and Privacy (Oakland'24)*, San Francisco, CA, USA, May 2024. (Acceptance rate: 17.8%)
48. Daniel Olszewski, Allison Lu, Carson Stillman, Kevin Warren, Cole Kitroser, Alejandro Pascual, Divyajyoti Ukirde, Kevin Butler, and Patrick Traynor. "'Get in Researchers; We're Measuring Re-

producibility”: A Reproducibility Study of machine Learning Papers in Tier 1 Security Conferences”. *30th ACM Conference on Computer and Communications Security (CCS’23)*, Copenhagen, Denmark, November 2023. *Acceptance rate: 19.2%*.

49. Kyungtae Kim, Sungwoo Kim, Kevin Butler, Antonio Bianchi, and Dave (Jing) Tian. “Fuzz The Power: Dual-role State Guided Black-box Fuzzing for USB Power Delivery”. *32nd USENIX Security Symposium (Security’23)*, Anaheim, CA, USA, August 2023. *Acceptance rate: 29%*.
50. Yazhou Tu, Liqun Shen, Md Imran Hossen, Sara Rampazzi, Kevin Butler, and Xiali Hei. “Auditory Eyesight: Demystifying μ s-Precision Keystroke Tracking Attacks on Unconstrained Keyboard Inputs”. *32nd USENIX Security Symposium (Security’23)*, Anaheim, CA, USA, August 2023. *Acceptance rate: 29%*.
51. Yan Long, Pirouz Naghavi, Blas Kojusner, Kevin Butler, Sara Rampazzi, and Kevin Fu. “Side eye: Characterizing the Limits of POV Acoustic Eavesdropping from Smartphone Cameras with Rolling Shutters and Movable Lenses”. *44th IEEE Symposium on Security and Privacy (Oakland’23)*, San Francisco, CA, USA, May 2023. *Acceptance rate: 17.1%*.
52. Tyler Tucker, Hunter Searle, Kevin Butler, and Patrick Traynor. “Blue’s Clues: Practical Discovery of Non-Discoverable Bluetooth Devices”. *44th IEEE Symposium on Security and Privacy (Oakland’23)*, San Francisco, CA, USA, May 2023. *Acceptance rate: 17.1%*.
53. 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)?” *31st USENIX Security Symposium (Security’22)*, Boston, MA, USA, Aug 2022. *Acceptance rate: 18.1%*.
54. Kyungtae Kim, Taegyu Kim, Ertza Warriach, Byoungyoung Lee, Kevin Butler, Antonio Bianchi, and Dave (Jing) Tian. “FuzzUSB: Hybrid Stateful Fuzzing of USB Gadget Stacks.” *43rd IEEE Symposium on Security and Privacy (Oakland’22)*, San Francisco, CA, USA, May 2022. *Acceptance rate: 14.5%*.
55. Grant Hernandez, Marius Muench, Dominik Maier, Alyssa Milburn, Shinjo Park, Tobias Scharnowski, Tyler Tucker, Patrick Traynor, and Kevin Butler. “FirmWire: Transparent Dynamic Analysis for Cellular Baseband Firmware.” *2022 ISOC Network and Distributed System Security Symposium (NDSS’22)*, San Diego, CA, USA, April 2022. *Acceptance rate: 16.2%*.
56. Grant Hernandez, Dave (Jing) Tian, Anurag Yadav, Byron J. Williams, and Kevin Butler. “Big-MAC: Fine-Grained Policy Analysis of Android Firmware.” *29th USENIX Security Symposium (Security’20)*, Boston, MA, USA, August 2020. (*Acceptance rate: 16.1%*.)
57. Dave (Jing) Tian, Grant Hernandez, Joseph Choi, Vanessa Frost, Peter Johnson, and Kevin Butler. “LBM: A Security Framework for Peripherals within the Linux Kernel.” *40th IEEE Symposium on Security and Privacy (Oakland’19)*, San Francisco, CA, USA, May 2019. (*Acceptance rate=12.0%*.)
58. Luis Vargas, Logan Blue, Vanessa Frost, Christopher Patton, Nolen Scaife, Kevin Butler, and Patrick Traynor. “Digital Healthcare-Associated Infection Analysis of a Major Multi-Campus Hospital System.” *26th ISOC Network and Distributed System Security Symposium (NDSS’19)*, San Diego, CA, USA, February 2019. (*Acceptance rate=17.1%*)
59. Hadi Abdullah, Washington Garcia, Christian Peeters, Patrick Traynor, Kevin Butler, and Joseph Wilson. “Practical Hidden Voice Attacks against Speech and Speaker Recognition Systems.” *26th ISOC Network and Distributed System Security Symposium (NDSS’19)*, San Diego, CA, USA, February 2019. (*Acceptance rate=17.1%*)

60. Luis Vargas, Gyan Hazarika, Rachel Culpepper, Kevin Butler, Thomas Shrimpton, Doug Szjada, and Patrick Traynor. "Mitigating Risk while Complying with Data Retention Laws." *25th ACM Conference on Computer and Communications Security (CCS'18)*, Toronto, ON, Canada, October 2018. (Acceptance rate=17.0%)
61. Dave (Jing) Tian, Grant Hernandez, Joseph Choi, Vanessa Frost, Christie Ruales, Patrick Traynor, Hayawardh Vijaykumar, Lee Harrison, Amir Rahmati, Mike Grace, and Kevin Butler. "ATtention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem." *27th USENIX Security Symposium (Security'18)*, Baltimore, MD, USA, August 2018. (Acceptance rate=19.1%)
62. Dave (Jing) Tian, Nolen Scaife, Deepak Kumar, Michael Bailey, Adam Bates, and Kevin Butler. "SoK: "Plug & Pray" Today – Understanding USB Insecurity in Versions 1 through C." *2018 IEEE Symposium on Security and Privacy (Oakland'18)*, San Francisco, CA, USA, May 2018. *Nominated for Distinguished Paper Award.* (Acceptance rate=11.5%)
63. 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." *2018 IEEE Symposium on Security and Privacy (Oakland'18)*, San Francisco, CA, USA, May 2018. (Acceptance rate=11.5%)
64. Grant Hernandez, Farhaan Fowze, Dave (Jing) Tian, Tuba Yavuz, and Kevin Butler. "FirmUSB: Vetting USB Device Firmware using Domain Informed Symbolic Execution." *24th ACM Conference on Computer and Communications Security (CCS'17)*, Dallas, TX, USA October 2017. (Acceptance rate=18.1%.)
65. Dave (Jing) Tian, Adam Bates, Kevin Butler, and Raju Rangaswami. "ProvUSB: Block-level Provenance-Based Data Protection for USB Storage Devices." *23rd ACM Conference on Computer and Communications Security (CCS'16)*, Vienna, Austria, October 2016. (Acceptance rate=16.5%.)
66. Dave (Jing) Tian, Nolen Scaife, Adam Bates, Kevin Butler, and Patrick Traynor. "Making USB Great Again with USBFILTER". *25th USENIX Security Symposium (Security'16)*, Austin, TX, USA, August 2016. (Acceptance rate=15.5%.)
67. Bradley Reaves, Dave Tian, Nolen Scaife, Logan Blue, Patrick Traynor, and Kevin Butler. "Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways". *2016 IEEE Symposium on Security and Privacy (Oakland'16)*, San Jose, CA, USA, May 2016. (Acceptance rate=13.3%.)
68. Adam Bates, Dave Tian, Kevin Butler, and Thomas Moyer. "Trustworthy Whole-System Provenance for the Linux Kernel". *24th USENIX Security Symposium (Security'15)*, Washington, DC, USA, August 2015. (Acceptance rate=15.7%)
69. 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". *24th USENIX Security Symposium (Security'15)*, Washington, DC, USA, August 2015. (Acceptance rate=15.7%)
70. Benjamin Mood, Debayan Gupta, Kevin Butler, and Joan Feigenbaum. "Reuse It Or Lose It: More Efficient Secure Computation Through Reuse of Encrypted Values". *21st ACM Conference on Computer and Communications Security (CCS'14)*, Scottsdale, AZ, USA, November 2014. (Acceptance rate=19%)

71. Adam Bates, Joe Pletcher, Tyler Nichols, Braden Hollemback, Dave Tian, Abdulrahman Alkhelaifi, and Kevin Butler. "Securing SSL Certificate Verification through Dynamic Linking". *21st ACM Conference on Computer and Communications Security (CCS'14)*, Scottsdale, AZ, USA, November 2014. (Acceptance rate=19%)
72. Adam Bates, Ryan Leonard, Hannah Pruse, Daniel Lowd, and Kevin Butler. "Leveraging USB to Establish Host Identity Using Commodity Devices." *21st ISOC Network and Distributed System Security Symposium (NDSS'14)*, San Diego, CA, USA, February 2014. (Acceptance rate=18.6%)
73. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. "Secure Outsourced Garbled Circuit Evaluation for Mobile Devices". *22nd USENIX Security Symposium (Security'13)*, Washington, DC, USA, August 2013. (Acceptance rate=16.2%)
74. Benjamin Kreuter, ahbi shelat, Benjamin Mood, and Kevin Butler. "PCF: A Portable Circuit Format For Scalable Two-Party Secure Computation". *22nd USENIX Security Symposium (Security'13)*, Washington, DC, USA, August 2013. (Acceptance rate=16.2%)
75. Adam Bates, Kevin Butler, Micah Sherr, Clay Shields, Patrick Traynor, and Dan Wallach. "Accountable Wiretapping -or- I Know That You Can Hear Me Now". *19th ISOC Network and Distributed System Security Symposium (NDSS'12)*, San Diego, CA, USA, February 2012. (Acceptance rate=17.6%)
76. Kevin Butler, Stephen McLaughlin, and Patrick McDaniel. Rootkit Resistant Disks. *15th ACM Conference on Computer and Communications Security (CCS'08)*, Alexandria, VA, USA, October 2008. (Acceptance rate=18.1%)
77. Patrick Traynor, Kevin Butler, William Enck, and Patrick McDaniel. Realizing Massive-Scale Conditional Access Systems Through Attribute-Based Cryptosystems. *15th Annual Network and Distributed System Security Symposium (NDSS'08)*, San Diego, CA, USA, February 2008. (Acceptance rate=17.8%)
78. Kevin Butler, William Aiello, and Patrick McDaniel. Optimizing BGP Security by Exploiting Path Stability. *13th ACM Conference on Computer and Communications Security (CCS'06)*, Alexandria, VA, USA, November 2006. (Acceptance rate=14.8%)

Other Refereed Conference Publications

79. Caroline Brandon, Carson Stillman, Joel Hirschmann, Marina Blanton, Christopher Petersen, Sara Rampazzi, and Kevin Butler. "The Final Security Frontier: Using Privacy-Preserving Computation to Secure Satellite Rendezvous and Proximity Operations." *Proceedings of the 19th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'26)*, Saarbrücken, Germany, June 2026. (Acceptance rate TBD)
80. Weidong Zhu, Wenxuan Bao, Vincent Bindschaedler, Sara Rampazzi, and Kevin Butler. "Enabling Plausible Deniability in Flash-based Storage through Data Permutation." *Proceedings of the 2025 Annual Computer Security Applications Conference (ACSAC 2025)*, Honolulu, HI, USA, December 2025. (Acceptance rate=20.7%)
81. Carson Stillman, Jennifer Sheldon, Ian Garrett, Patrick Traynor, Ryan Gerdes, Sara Rampazzi, and Kevin Butler. "EM-Flow: Advanced Electromagnetic Control Flow Verification for Embedded Systems." *Proceedings of the 2025 Annual Computer Security Applications Conference (ACSAC 2025)*,

Honolulu, HI, USA, December 2025. (Acceptance rate=20.7%)

82. Kevin Childs, Mollie Brewer, Spencer Thomas, Celeste Wilkins, Jennifer A. Nichols, Kristy Elizabeth Boyer and Kevin R. B. Butler. "Mapping the Flow of Information from Continuous Wearables: Insights from Elite Collegiate Athletes in the United States." *Proceedings of the 2025 ACM Conference on Human-Computer Interaction and Sports (SportsHCI 2025)*, Twente, The Netherlands, November 2025.
83. Daniel Olszewski, Allison Lu, Anna Crowder, Nathaniel Bennett, Seth Layton, Sri Hrushikesh Varma Bhupathiraju, Tyler Tucker, Siddhant Kalgutkar, Hunter Ver Helst, Carson Stillman, Kevin Butler, Sara Rampazzi, and Patrick Traynor. "Reproducibility in Applied Security Conferences: An 11-Year Review on Artifacts and Evaluation Committees." *Proceedings of the 2025 ACM Conference on Reproducibility and Replicability (REP 2025)*, Vancouver, BC, Canada, July 2025. **Best Paper Award.**
84. Mollie Brewer, Kevin Childs, Spencer Thomas, Celeste Wilkins, Kristy Elizabeth Boyer, Jennifer A. Nichols, Kevin R. B. Butler, Garrett F. Beatty, and Daniel P. Ferris. "Coach, Data Analyst, and Protector: Exploring Data Practices of Collegiate Coaching Staff." *Proceedings of the 2025 ACM CHI Conference on Human Factors in Computing Systems (CHI'25)*, Yokohama, Japan, April 2025. (Acceptance rate=24.9%)
85. Anna Crowder, Daniel Olszewski, Patrick Traynor, and Kevin R. B. Butler. "I Can Show You the World (of Censorship): Extracting Insights from Censorship Measurement Data Using Statistical Techniques." *Proceedings of the 40th Annual Computer Security Applications Conference (ACSAC 2024)*, Honolulu, HI, December 2024. (Acceptance rate = 21.8%.)
86. Weidong Zhu, Grant Hernandez, Washington Garcia, Dave (Jing) Tian, Sara Rampazzi, and Kevin Butler. "Minding the Semantic Gap for Effective Storage-Based Ransomware Defense." *Proceedings of the 38th International Conference on Massive Storage Systems and Technology (MSST)*, Santa Clara, CA, USA, June 2024.
87. Seaver Thorn, K. Virgil English, Kevin Butler, and William Enck. "5GAC-Analyzer: Identifying Over-Privilege Between 5G Core Network Functions." *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, Seoul, Korea, May 2024. (Acceptance rate: 29%)
88. K. Virgil English, Nathaniel Bennett, Seaver Thorn, Kevin Butler, William Enck, and Patrick Traynor. "Examining Cryptography and Randomness Failures in Open-Source Cellular Cores." *Proceedings of the ACM Conference on Data and Application Security and Privacy (CODASPY)*, Porto, Portugal, June 2024. **Best paper award.** (Acceptance rate: 19%)
89. Caroline Fedele, Christopher Petersen, Tyler Lovelly, and Kevin Butler. "Protecting Satellite Proximity Operations via Secure Multi-Party Computation." *American Institute of Aeronautics and Astronautics (AIAA) SciTech Forum*, Orlando, FL, USA, January 2024.
90. Christian Peeters, Tyler Tucker, Anushri Jain, Kevin Butler, and Patrick Traynor. "LeopardSeal: Detecting Call Interception via Audio Rogue Base Stations". *21st ACM International Conference on Mobile Systems, Applications, and Services (MobiSys'23)*, Helsinki, Finland, June 2023. Acceptance rate: 20.7%
91. Washington Garcia, Pin-Yu Chen, Hamilton Scott Clouse, Somesh Jha, and Kevin Butler. "Less is More: Dimension Reduction Finds On-Manifold Adversarial Examples in Hard-Label Attacks".

IEEE Conference on Secure and Trustworthy Machine Learning (SatML 2023), Raleigh, NC, USA, February 2023. *Acceptance rate: 25.3%*

92. Daniel Olszewski, Weidong Zhu, Sandeep Sathyanarayana, Kevin Butler, and Patrick Traynor. "HallMonitor: A Framework for Identifying Network Policy Violations in Software". *2022 IEEE Conference on Communications and Network Security (CNS 2022)*, Austin, TX, USA, October 2022. (*Acceptance rate =35%.*)
93. 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." *22nd Privacy Enhancing Technologies Symposium (PETS 2022)*, Sydney, Australia, July 2022. (*Acceptance rate: 24%*)
94. Washington Garcia, Scott Clouse, and Kevin Butler. "Disentangling Categorization in Multi-agent Emergent Communication." *2022 Conference of the North American Chapter of the Association for Computational Linguistics (NAACL 2022)*, Seattle, WA, USA, July 2022. *Acceptance rate: 21%*
95. Shantanu Ghosh, Zheng Feng, Kevin Butler, and Mattia Prosperi. "DR-VIDAL: Doubly Robust Variational Information-theoretic Deep Adversarial Learning for Counterfactual Prediction and Treatment Effect Estimation." *2022 American Medical Informatics Association Annual Symposium (AMIA 2022)*, Washington, DC, USA, November 2022.
96. Brendan David-John, Kevin Butler, and Eakta Jain. "For Your Eyes Only: Privacy-Preserving Eye-Tracking Datasets." *14th ACM Symposium on Eye Tracking Research and Applications (ETRA 2022)* Seattle, WA, USA, June 2022. (*Acceptance rate: 42%*)
97. Mounir Elbharabawy, Blas Kojusner, Mohammad Mannan, Kevin Butler, Byron Williams, and Amr Youssef. "SAUSAGE: Security Analysis of Unix domain Socket Usage in Android." *7th IEEE European Symposium on Security and Privacy (Euro S&P'22)*, Genoa, Italy, June 2022. (*Acceptance rate TBD.*) **Best paper award finalist.**
98. Arslan Khan, Joseph Choi, Dave (Jing) Tian, Tyler Ward, Kevin Butler, Patrick Traynor, John M. Shea and Tan Wong. "Privacy-Preserving Localization Using Enclaves." *12th IEEE Ubiquitous Computing, Electronics and Mobile Communication Conference (IEEE UEMCON 2021)*, Virtual Conference, December 2021.
99. Washington Garcia, Animesh Chhotaray, Joseph Choi, Suman Adari, Kevin Butler, and Somesh Jha. "Brittle Features of Device Authentication." *11th ACM Conference on Data and Application Security and Privacy (CODASPY'21)*, virtual event, April 2021. (*Acceptance rate: 24.5%.*)
100. Joseph Choi, Dave (Jing) Tian, Grant Hernandez, Christopher Patton, Benjamin Mood, Thomas Shrimpton, Patrick Traynor, and Kevin Butler. "A Hybrid Approach to Secure Function Evaluation using SGX." *14th ACM ASIA Conference on Computer and Communications Security (ASIACCS'19)*, Auckland, New Zealand, July 2019. (*Acceptance rate [full papers]: 17%.*)
101. Vanessa Frost, Dave (Jing) Tian, Christie Ruales, Patrick Traynor, and Kevin Butler. "Examining DES-based Cipher Suite Support within the TLS Ecosystem." *14th ACM ASIA Conference on Computer and Communications Security (ASIACCS'19)*, Auckland, New Zealand, July 2019. (*Acceptance rate: 22%.*)
102. Jasmine Bowers, Imani Sherman, Kevin Butler, and Patrick Traynor. "Characterizing Security and Privacy Practices in Emerging Digital Credit Applications." *12th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'19)*, Miami, FL, USA, May 2019. (*Acceptance*

rate=25.5%)

103. Dave (Jing) Tian, Joseph Choi, Grant Hernandez, Patrick Traynor, and Kevin Butler. "A Practical Intel SGX Setting for Linux Containers in the Cloud." *9th ACM Conference on Data and Application Security and Privacy (CODASPY'19)*, Dallas, TX, USA, March 2019. (Acceptance rate=23.5%)
104. Lianying Zhao, Joseph Choi, Didem Demirag, Kevin Butler, Mohammad Mannan, Erman Ayday, and Jeremy Clark. One-Time Programs Made Practical. *23rd International Conference on Financial Cryptography and Data Security (FC'19)*, St. Kitts, February 2019. (Acceptance rate=18.5%)
105. Robert Karam, Tamzidul Hoque, Kevin Butler, and Swarup Bhunia. Mixed-Granular Architectural Diversity for Device Security in the Internet of Things. *Asian Hardware Oriented Security and Trust Symposium (AsianHOST 2017)*, Beijing, China, October 2017.
106. Tyler Ward, Joseph Choi, Kevin Butler, John M. Shea, Patrick Traynor, and Tan Wong. Privacy Preserving Localization Using a Distributed Particle Filtering Protocol. *IEEE MILCOM*, Baltimore, MD, October 2017.
107. Jasmine Bowers, Bradley Reaves, Imani N. Sherman, Patrick Traynor, and Kevin Butler. Regulators, Mount Up! Analysis of Privacy Policies for Mobile Money Services. *13th Symposium on Usable Privacy and Security (SOUPS 2017)*, Santa Clara, CA, July 2017. (Acceptance rate=26.5%)
108. Adam Bates, Wajih Ul Hassan, Kevin Butler, Alin Dobra, Brad Reaves, Patrick Cable, Thomas Moyer, and Nabil Schear. Transparent Web Service Auditing via Network Provenance Functions. *26th World Wide Web Conference (WWW 2017)*, Perth, Australia, April 2017. (Acceptance rate=17.0%)
109. Benjamin Mood, Debayan Gupta, Henry Carter, Kevin Butler, and Patrick Traynor. "Frigate: A Validated, Extensible, and Efficient Compiler and Interpreter for Secure Computation". *1st IEEE European Symposium on Security and Privacy (Euro S&P 2016)*, Saarbrücken, Germany, March 2016. (Acceptance rate=17.3%.)
110. Sriharsha Etigowni, Dave (Jing) Tian, Grant Hernandez, Saman Zonouz, and Kevin Butler. CPAC: Securing Critical Infrastructure with Cyber-Physical Access Control. *32nd Annual Computer Security Applications Conference*, Los Angeles, CA, USA, December 2016. (Acceptance rate=22.8%)
111. Thomas Moyer, Patrick Cable, Karishma Chadha, Robert Cunningham, Nabil Schear, Warren Smith, Adam Bates, Kevin Butler, Frank Capobianco, and Trent Jaeger. "Leveraging Data Provenance to Enhance Cyber Resilience". *1st IEEE Cybersecurity Development Conference (SecDev 2016)*, Boston, MA, November 2016. (Acceptance rate=52.2%.)
112. Bradley Reaves, Dave Tian, Nolen Scaife, Logan Blue, Patrick Traynor, and Kevin Butler. "Detecting SMS Spam in the Age of Legitimate Bulk Messaging". *9th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'16)*, Darmstadt, Germany, July 2016. (Acceptance rate=35%.)
113. Nolen Scaife, Henry Carter, Patrick Traynor, and Kevin Butler. "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data". *36th IEEE International Conference on Distributed Computing Systems (ICDCS 2016)*, Nara, Japan, June 2016. (Acceptance rate=17.6%)
114. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. "Outsourcing Secure Two-Party Computation as a Black Box". *14th International Conference on Cryptology and Network Security (CANS 2015)*, Marrakesh, Morocco, December 2015. (Acceptance rate=52.9%.)

115. Dave Tian, Adam Bates, and Kevin Butler. "Defending Against Malicious USB Firmware with GoodUSB". *31st Annual Computer Security Applications Conference (ACSAC 2015)*, Los Angeles, CA, USA, December 2015. (Acceptance rate=24.4%.)
116. Ethan Shernan, Henry Carter, Jing (Dave) Tian, Patrick Traynor, and Kevin Butler. "More Guidelines Than Rules: CSRF Vulnerabilities from Noncompliant OAuth 2.0 Implementations". *12th Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA 2015)*, Milano, Italy, July 2015. (Acceptance rate=22.7%)
117. Jing (Dave) Tian, Kevin Butler, Patrick McDaniel, and Padma Krishnaswamy. "Securing ARP From the Ground Up". *5th ACM Conference on Data and Application Security and Privacy (CODASPY 2015)*, San Antonio, TX, USA, March 2015. (Acceptance rate=33.3%)
118. Adam Bates, Joe Pletcher, Tyler Nichols, Braden Hollembaek, and Kevin Butler. "Forced Perspectives: Evaluating an SSL Trust Enhancement at Scale". *2014 ACM Internet Measurement Conference (IMC'14)*, Vancouver, BC, Canada, November 2014. (Acceptance rate=22.9%)
119. Adam Bates, Benjamin Mood, Masoud Valafar, and Kevin Butler. "Towards Secure Provenance-Based Access Control in Cloud Environments". *3rd ACM Conference on Data and Application Security and Privacy (CODASPY 2013)*, San Antonio, TX, USA, February 2013. (Acceptance rate=31.8%)
120. Vasant Tendulkar, Joe Pletcher, Ashwin Shashidharan, Ryan Snyder, Kevin Butler, and William Enck. "Abusing Cloud-based Browsers for Fun and Profit". *28th Annual Computer Security Applications Conference (ACSAC 2012)*, Orlando, FL, USA, December 2012. (Acceptance rate=19.0%)
121. Devin J. Pohly, Stephen McLaughlin, Patrick McDaniel, and Kevin Butler. "Hi-Fi: Collecting High-Fidelity Whole-System Provenance". *28th Annual Computer Security Applications Conference (ACSAC 2012)*, Orlando, FL, USA, December 2012. (Acceptance rate=19.0%)
122. Benjamin Mood, Lara Letaw, and Kevin Butler. "Memory-Efficient Garbled Circuit Generation for Mobile Devices". *16th IFCA International Conference on Financial Cryptography and Data Security (FC'12)*, Bonaire, February 2012. (Acceptance rate=26.1%)
123. Kevin Butler, Stephen McLaughlin, and Patrick McDaniel. "Kells: A Protection Framework for Portable Data". *26th Annual Computer Security Applications Conference (ACSAC 2010)*, Austin, TX, USA, December 2010. (Acceptance rate=16.3%)
124. Machigar Ongtang, Kevin Butler, and Patrick McDaniel. "Porscha: Policy Oriented Secure Content Handling in Android." *26th Annual Computer Security Applications Conference (ACSAC 2010)*, Austin, TX, USA, December 2010. (Acceptance rate=16.3%)
125. Kevin Butler, Stephen McLaughlin, and Patrick McDaniel. "Disk-Enabled Authenticated Encryption" (short paper). *26th IEEE Symposium on Massive Storage Systems and Technologies (MSST 2010)*, Incline Village, NV, USA, May 2010. (Acceptance rate=45.5%.)
126. Thomas Moyer, Kevin Butler, Joshua Schiffman, Patrick McDaniel, and Trent Jaeger. Scalable Web Content Attestation. *25th Annual Computer Security Applications Conference (ACSAC 2009)*, Honolulu, HI, USA. December 2009. (Acceptance rate=19.0%.)
127. William Enck, Kevin Butler, Thomas Richardson, Patrick McDaniel, and Adam Smith. Defending Against Attacks on Main Memory Persistence. *24th Annual Computer Security Applications Conference (ACSAC 2008)*, Anaheim, CA, USA. December 2008. (Acceptance rate=24.3%)
128. Dhananjay Bapat, Kevin Butler, and Patrick McDaniel. Towards Automatic Privilege Separation.

3rd International Conference on Information Systems Security (ICISS 2007), Delhi, India. December 2007. (Acceptance rate=25.0%)

129. Lisa Johansen, Kevin Butler, Michael Rowell, and Patrick McDaniel. Email Communities of Interest. *Fourth Conference on Email and Anti-Spam (CEAS 2007)*, Mountain View, CA, USA. August 2007. (Acceptance rate=19.0%.)
130. Anusha Sriraman, Kevin Butler, Patrick McDaniel, and Padma Raghavan. Analysis of the IPv4 Address Space Delegation Structure. *IEEE Symposium on Computers and Communications (ISCC'07)*, Aveiro, Portugal, July 2007. (Acceptance rate=40%.)
131. Sunam Ryu, Kevin Butler, Patrick Traynor, and Patrick McDaniel. Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems. *3rd IEEE International Symposium on Security in Networks and Distributed Systems (SSNDS'07)*, Niagara Falls, ON, Canada, May 2007. (Acceptance rate=40%)
132. Kevin Butler, Patrick Traynor, William Enck, Jennifer Plasterr, and Patrick McDaniel. Privacy Preserving Web-Based Email. *2nd International Conference on Information Systems Security (ICISS 2006)*, Kolkata, India, December 2006. (Acceptance rate=30.4%)
133. Trent Jaeger, Kevin Butler, David King, Serge Hallyn, Joy Latten, and Xiolan Zhang. Leveraging IPsec for Mandatory Per-Packet Access Control. *2nd IEEE Communications Society/CreateNet International Conference on Security and Privacy in Communication Networks (SecureComm'06)*, August 2006. Baltimore, MD, USA. (Acceptance rate=25.4%.)
134. Kevin Butler and Patrick McDaniel, Understanding Mutable Internet Pathogens, or How I Learned to Stop Worrying and Love Parasitic Behavior. *1st International Conference on Information Systems Security (ICISS 2005)*, December 2005. Kolkata, India. (Invited paper.)

Peer-Reviewed Workshop Publications

135. Jennifer Sheldon, Weidong Zhu, Adnan Abdulla, Kevin Butler, Md Jahidul Islam, and Sara Ram-pazzi. "Position: Deep Note: Can Acoustic Interference Damage the Availability of Hard Disk Storage in Underwater Data Centers?" *15th ACM Workshop on Hot Topics in Storage and File Systems (Hot-Storage 2023)*, Boston, MA, USA, July 2023. **Best Paper Award.**
136. Brendan David-John, Diane Hosfelt, Kevin Butler, and Eakta Jain. "Let's SOUP Up XR: Collected thoughts from an IEEE VR workshop on privacy in mixed reality." *1st International Workshop on Security for XR and XR for Security (VR4Sec)*, in conjunction with SOUPS 2021, virtual event, August 2021.
137. Sushrut Shringarputale, Patrick McDaniel, Kevin Butler, and Thomas La Porta. "Co-residency Attacks on Containers are Real." *2020 ACM Cloud Computing Security Workshop (CCSW'20)*, Orlando, FL, USA, November 2020.
138. Suman Adari, Washington Garcia, and Kevin Butler. "Adversarial Video Captioning". *2019 Dependable and Secure Machine Learning Workshop (DSML'19)*, Portland, OR, USA, June 2019.
139. Siddhant Deshmukh, Henry Carter, Grant Hernandez, Patrick Traynor, and Kevin Butler. "Efficient and Secure Template Blinding for Biometric Authentication". *2nd IEEE Workshop on Security and Privacy in the Cloud (SPC 2016)*, Philadelphia, PA, USA, October 2016.
140. Debayan Gupta, Benjamin Mood, Joan Feigenbaum, Kevin Butler and Patrick Traynor. "Using Intel

Software Guard Extensions for Efficient Two-Party Secure Function Evaluation.” *2016 Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC’16)*, Barbados, February 2016.

141. Adam Bates, Kevin Butler, and Thomas Moyer. “Take Only What You Need: Leveraging Mandatory Access Control Policy to Reduce Provenance Storage Costs.” *7th Annual Workshop on Theory and Practice of Provenance (TaPP’15)*, Edinburgh, Scotland, July 2015.
142. Adam Bates, Kevin Butler, Andreas Haeberlen, Micah Sherr, and Wenchao Zhou. “Let SDN Be Your Eyes: Secure Forensics in Data Center Networks.” *NDSS Workshop on Security of Emerging Network Technologies (SENT)*, San Diego, CA, USA, February 2014.
143. Matt Bishop, Emily Rine Butler, Kevin Butler, Carrie Gates, and Steven Greenspan. “Forgive and Forget: Return to Obscurity”. *New Security Paradigms Workshop (NSPW 2013)*, Banff, AB, Canada, September 2013.
144. Peter McKay, Bryan Clement, Sean Haverty, Elijah Newton, and Kevin Butler. “Read My Lips: Towards Use of the Microsoft Kinect as a Visual-Only Automatic Speech Recognizer.” *2013 Workshop on Home Usable Privacy and Security (HUPS)*, Newcastle, UK, July 2013.
145. Adam Bates, Benjamin Mood, Joe Pletcher, Hannah Pruse, Masoud Valafar, and Kevin Butler. “Detecting Co-Residency with Active Traffic Analysis Techniques”. *4th ACM Cloud Computing Security Workshop (CCSW 2012)*, Raleigh, NC, USA, October 2012. (*Acceptance rate=12.0% for full papers.*)
146. Lara Letaw, Joe Pletcher, and Kevin Butler. “Host Identification via USB Fingerprinting”. *6th IEEE International Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE 2011)*, Oakland, CA, USA, May 2011. (*Acceptance rate=34.8%.*)
147. Kevin Butler, William Enck, Harri Hursti, Stephen McLaughlin, Patrick Traynor, and Patrick McDaniel. Systemic Issues in the Hart InterCivic and Premier Voting Systems: Reflections Following Project EVEREST. *2008 USENIX/ACCURATE Electronic Voting Workshop (EVT’08)*, July 2008. San Jose, CA, USA. (*Acceptance rate=44.1%*)
148. Shiva Chaitanya, Kevin Butler, Anand Sivasubramaniam, Patrick McDaniel and Murali Vilayanur. Design, implementation and evaluation of security in iSCSI-based network storage systems. *2nd International Workshop on Storage Security and Survivability (StorageSS 2006)*, October 2006. Alexandria, VA, USA. (*Acceptance rate=68%*)
149. Patrick McDaniel, Kevin Butler, Stephen McLaughlin, Radu Sion, Erez Zadok, and Marianne Winslett. “Towards a Secure and Efficient System for End-to-End Provenance”. *USENIX Workshop on Theory and Practice of Provenance (TaPP)*, February 2010. (*Acceptance rate=68.8%*)
150. Kevin Butler and Petros Efstathopoulos. U Can’t Touch This: Block-Level Protection for Portable Storage. *International Workshop on Software Support for Portable Storage (IWSSPS 2009)*, October 2009. Grenoble, France.
151. Kevin Butler, Stephen McLaughlin, and Patrick McDaniel. Non-Volatile Memory and Disks: Avenues for Policy Architectures. *1st Computer Security Architectures Workshop (CSAW 2007)*, November 2007. Fairfax, VA, USA. (*Acceptance rate=30%*)
152. Kevin Butler and Patrick McDaniel, Testing Large Scale BGP Security in Replayable Network Environments. *DETER Community Workshop on Cyber Security Experimentation and Test*, June 2006. Arlington, VA, USA.

153. Sophie Qiu, Kevin Butler, and Patrick McDaniel, BGPRV: Retrieving and Processing BGP Data with Efficiency and Convenience. *DETER Community Workshop on Cyber Security Experimentation and Test*, June 2006. Arlington, VA, USA.

Technical Reports

154. Kevin Butler, Sunny Consolvo, Katie Siek, Tammy Toscos, Pamela Wisniewski, Haley Griffin, Nazanin Andalibi, Rasa I. Arriaga, Beenish Moalla Chaudhry, Munmum De Choudhury, Jeremy Epstein, Oliver L. Haimson, Sharon Heung, Zaidat Ibrahim, Patrick Gage Kelley, Vera Khovanskaya, Aqueasha Martin-Hammond, Jessica McClearn, Vivian Genaro Motti, Chinasa T. Okolo, Jessica Pater, Wanda Pratt, Sydney Saubestre, Vincent M.B. Silenzio, Dhanaraj Thakur, Alexandra To, Emily Tseng, and Rebecca Umbach. Supporting At-Risk Users Through Responsible Computing. Washington, D.C.: Computing Research Association (CRA), October 2025. <http://cra.org/ccc/wp-content/uploads/2025/10/supporting-at-risk-users-through-responsible-computing.pdf>
155. Azim Ibragimov, Ethan Wilson, Kevin Butler, and Eakta Jain. “Toward Practical Privacy in XR: Empirical Analysis of Multimodal Anonymization Mechanisms.” *arXiv:2506.13882*, June 2025.
156. Michela Taufer, Rada Mihalcea, Matthew Turk, Dan Lopresti, Adam Wierman, Kevin Butler, Sven Koenig, David Danks, William Gropp, Manish Parashar, Yolanda Gil, Bill Regli, Rjmohan Rajaraman, David Jensen, Madya Bliss, and Mary Lou Maher. “Now More Than Ever, Foundational AI Research and Infrastructure Depends on the Federal Government.” Computing Community Consortium, Quadrennial White Paper, 2024.
157. Pamela Wisniewski, Kevin Butler, Katie Siek, Gabrielle Allen, Weisong Shi, Manish Parashar, Ufuk Topcu, and Haley Griffin. “Prioritizing Computing Research to Empower and Protect Vulnerable Populations.” Computing Community Consortium, Quadrennial White Paper, 2024.
158. Nadya Bliss, Kevin Butler, David Danks, Ufuk Topcu, and Matthew Turk. “Addressing the Unforeseen Harms of Technology.” Computing Community Consortium. http://cra.org/ccc/addressing_unforeseen_harms_of_technology_ccc_whitepaper, 2024.
159. Washington Garcia, Pin-Yu Chen, Somesh Jha, Scott Clouse, and Kevin Butler. “Hard-label Manifolds: Unexpected Advantages of Query Efficiency for Finding On-manifold Adversarial Examples.” *arXiv:2013.03325*, March 2021.
160. Kevin Butler. “Digital Financial Services security audit guideline.” Security, Infrastructure and Trust Working Group, Financial Inclusion Global Initiative, published by International Telecommunications Union (ITU), March 2021.
161. Kevin Butler and Vijay Mauree. “Digital Financial Services security assurance framework.” Security, Infrastructure and Trust Working Group, Financial Inclusion Global Initiative, published by International Telecommunications Union (ITU), January 2021. **Published as ITU Technical Recommendation ITU-T X.1150, March 2024.**
162. Washington Garcia, Joseph Choi, Suman Adari, Somesh Jha, and Kevin Butler. “Explainable Black-Box Attacks Against Model-based Authentication.” *arXiv:1810.00024*, September 2018.
163. Kevin Butler, Patrick Traynor, and Tiago Novais. “MM App Security Best Practices.” Official Document MM.01, GSM Association, London, United Kingdom, June 2018.

164. Kevin Butler, Leon Perlman, Paul Makin, Henry Gerwitz, Patrick Traynor, Yury Grin, Evgeniy Bondarenko, and Richard Miller. "ITU-T Focus Group Digital Financial Services: Security Aspects of Digital Financial Services (DFS)." Focus Group Technical Report, International Telecommunications Union, Geneva, Switzerland, January 2017.
165. Adam Bates, Joe Pletcher, Tyler Nichols, Braden Hollembaek, and Kevin Butler. "Towards Usable System-Wide Trust Agility." Technical Report CIS-TR-2013-13, Department of Computer and Information Science, University of Oregon, Eugene, OR, October 2013.
166. Benjamin Mood and Kevin Butler. "Optimizing Secure Function Evaluation for Mobile Devices". Technical Report CIS-TR-2013-10, Department of Computer and Information Science, University of Oregon, Eugene, OR, September 2013.
167. Henry Carter, Benjamin Mood, Patrick Traynor, and Kevin Butler. "Secure Outsourced Garbled Circuit Evaluation for Mobile Devices". Technical Report GT-CS-12-09, College of Computing, Georgia Institute of Technology, Atlanta, GA, December 2012.
168. Kevin Butler and Petros Efstathopoulos. U Can't Touch This: Block-Level Protection for Portable Storage. Technical Report Symantec-SRL/MV2009-11, Symantec Research Labs, Mountain View, CA, June 2009.
169. Kevin Butler, Stephen McLaughlin, Thomas Moyer, Joshua Schiffman, Patrick McDaniel, and Trent Jaeger. Firma: Disk-Based Foundations for Trusted Operating Systems. Technical Report NAS-TR-0114-2009, Networking and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, May 2009.
170. Kevin Butler, Stephen McLaughlin, Thomas Moyer, Patrick McDaniel, and Trent Jaeger. Switch-Blade: Policy-Driven Disk Segmentation. Technical Report NAS-TR-0098-2008, Networking and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, November 2008.
171. P. McDaniel, K. Butler, W. Enck, H. Hursti, S. McLaughlin, P. Traynor, M. Blaze, A. Aviv, P. Cerny, S. Clark, E. Cronin, G. Shah, M. Sherr, G. Vigna, R. Kemmerer, D. Balzarotti, G. Banks, M. Cova, V. Felmetsger, W. Robertson, F. Valeur, J. Hall, and L. Quilter, EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing. Public Report, Ohio Secretary of State, December 2007.
172. Kevin Butler, Stephen McLaughlin, Patrick McDaniel, and Youngjae Kim. Autonomously Secure Disks. Technical Report NAS-TR-0072-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, May 2007. (*Updated September 2007.*)
173. 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-0060-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, January 2007.
174. Luke St. Clair, Lisa Johansen, Kevin Butler, William Enck, Matthew Pirretti, Patrick Traynor, Patrick McDainel, and Trent Jaeger. Password Exhaustion: Predicting the End of Password Usefulness. Technical Report NAS-TR-0030-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, May 2006. (*Updated January 2007.*)

Articles for Media

175. Patrick Traynor and Kevin Butler. "Mobile money in developing countries: study reveals security flaws in apps". *The Guardian*. 24 September 2015. http://www.theguardian.com/global-development-professionals-network/2015/sep/24/mobile-money-apps-security-flaws-study-reveals?CMP=twt_gu

Patents and Applications

Patents

U.S. Patent 8,856,918, Host validation mechanism for preserving integrity of portable storage data. Petros Efstathopoulos, Bruce Montague, Dharmesh Shah, Kevin Butler. October 7, 2014.

U.S. Patent 10,685,114, Malware Detection Via Data Transformation Monitoring. Walter N. Scaife, Kevin Butler, Henry Carter, Patrick G. Traynor. June 16, 2020.

U.S. Patent 11,265,717, Detecting SS7 Redirection Attacks with Audio-Based Distance Bounding. Patrick G. Traynor, Christian Peeters, Bradley G. Reeves, Hadi Abdullah, Kevin Butler, Jasmine Bowers, Walter N. Scaife. March 1, 2022.

U.S. Patent 11,568,044, Method and Apparatus For Vetting Universal Serial Bus Device Firmware. Kevin Butler, Tuba Yavuz, Jing Tian, Grant Hernandez, Farhaan Fowze. January 31, 2023.

U.S. Patent 11,640,464, Protocol Model Learning and Guided Firmware Analysis. Tuba Yavuz, Farhaan Fowze, Kevin Raymond Boyce Butler, Jing Tian, Grant Haydock Hernandez. May 2, 2023.

U.S. Patent 11,663,388, Automated Security Analysis of Baseband Firmware. Grant Haycock Hernandez, Kevin R. Butler, Patrick G. Traynor. May 31, 2023.

U.S. Patent 12,445,727, Acoustic Eavesdropping Using a Smartphone Camera. Yan Long, Kevin Fu, Kevin Butler, Sara Rampazzi, Pirouz Naghavi. October 14, 2025.

Patent Applications

Non-provisional Application 18/748,590, Detecting Deepfake Audio Using Turbulence. Patrick G. Traynor, Kevin Butler, Daniel Olszewski, Logan E. Blue, Magdalena Pasternak. Filed June 20, 2024.

Provisional Application 63/567,568, Identifying Deepfake Audio Using Breath Detection And Measurement. Patrick G. Traynor, Kevin S. Warren, Kevin Butler, Seth Layton, Daniel Olszewski, Thiago de Andrade, Carrie Gates. Filed March 20, 2024.

Non-Provisional Application 18/334,765, System, Method, and Apparatus for Detecting Call Interception. Patrick G. Traynor, Kevin Butler, Christian Peeters, Tyler Tucker. Filed June 14, 2023.

Provisional Application US 2023/0343342 A1, Detecting Audio Deepfakes Through Acoustic Prosodic Modeling. Patrick G. Traynor, Kevin S. Warren, Kevin Butler, Seth Layton, Daniel Olszewski, Carrie Gates. Filed October 26, 2023.

Teaching

University of Florida

- *CIS 6930/4930: Special Topics: Security and Privacy for Marginalized and Vulnerable / At-Risk Populations*, graduate/undergraduate, Fall 2025, Spring 2024.
- *CIS 5370: Computer and Information Security (Systems Security)*, graduate, Spring 2023, Spring 2019, Spring 2018, Spring 2017.

- *CIS 6930: Special Topics: Mobile and Embedded System Security*, graduate, Spring 2020.
- *CIS 4360: Computer and Information Security*, undergraduate, Fall 2020, Fall 2019, Fall 2018, Fall 2017.
- *CNT 5410: Computer and Network Security*, graduate, Fall 2015.

University of Oregon

- *CIS 415: Operating Systems (substantially revised)*, Spring 2014, Spring 2013, Spring 2012, Spring 2011.
- *CIS 607: Seminar on Generating Trustworthy Data (new)*, Winter 2014.
- *CIS 607: Seminar on Embedded Systems and Security (new)*, Spring 2013.
- *CIS 433/533: Computer and Network Security*, Winter 2013, Winter 2011.
- *CIS 607: Seminar on Computer Security in the Physical World (new)*, Spring 2012.
- *CIS 330: C/C++ and UNIX (substantially revised)*, Winter 2012.
- *CIS 610: Advanced Topics in Systems Security (new)*, Fall 2011.
- *CIS 607: Seminar on Security in Systems, Storage, and Clouds (new)*, Fall 2010.

The Pennsylvania State University

- *EE/CSE 458: Computer Networks*, Summer 2006.

Professional Service

Editorial Positions, Panels, and Boards

Editorial Boards:

Associate Editor, ACM Transactions on Security and Privacy (TOPS), 2021-present.

Associate Editor, Journal of Computer Security, 2020-present.

Associate Editor, IEEE Transactions on Dependable and Secure Computing (*Impact Factor: 4.41*), 2019-2025.

Associate Editor, ACM Digital Threats: Research and Practice, 2017-present.

Editorial Board, International Journal of Cybersecurity Science and Technology, 2017-2022.

Review Board, IEEE Systems Journal, Special Issues on Security and Privacy in Complex Systems, 2012.

Scientific Grant and Award Panels:

Referee, European Research Council, 2025.

Co-Chair, ACM SIGSAC Doctoral Dissertation Committee, 2024.

Site Visit Reviewer, National Science Foundation, 2025, 2024, 2021.

Review Panelist, National Science Foundation, 2025 (3), 2024, 2022, 2021, 2020, 2018, 2017, 2016, 2014 (2), 2013, 2012.

Grant Reviewer, Natural Science and Engineering Research Council of Canada, 2024, 2023, 2022, 2019, 2018, 2017.

Review Panelist, American Association for the Advancement of Science (AAAS), 2019.

Grant Reviewer, Austrian Science Fund, 2018.

Grant Reviewer, Israel Science Foundation, 2016.

Conference Steering Committees:

Steering Committee Member, USENIX Security Symposium, 2023-*present*.

Steering Committee Member, ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2019 -*present*.

Steering Committee Member, Annual Computer Security Applications Conference, 2014 -*present*.

Service to National and International Organizations:

Co-Organizer, National Science Foundation Secure and Trustworthy Cyberspace Principal Investigator Meeting, 2025-2026.

Executive Committee Member, Computing Research Association Computing Community Consortium (CRA CCC), 2025-*present*.

Co-Chair, Computing Research Association Workshop on Visioning the Future of Drone Computing, 2025-*present*.

Member, Review Working Group, President's Council of Advisors on Science and Technology (PCAST), White House Office of Science and Technology Policy, 2024.

Organizing Committee Member, Computing Research Association Visioning Workshop on Supporting At-Risk Users through Responsible Computing, 2024-2025.

Council Member, Computing Research Association Computing Community Consortium (CRA CCC), 2023-*present*.

Co-Chair, Security, Infrastructure, and Trust Working Group, Financial Inclusion Global Initiative, International Telecommunications Union, 2017-2022.

Co-Chair and Leader of Security Workstream, Technology, Innovation, and Competition Working Group, Focus Group on Digital Financial Services, International Telecommunications Union, 2015-2016.

Conference & Workshop Chairships

Program and Conference Committee Chairs

1. **Technical Program Co-Chair**, 32nd USENIX Security Symposium (USENIX Security'22), Boston, MA, USA, August 2022.
2. **Conference General Chair**, 36th and 37th Annual Computer Security Applications Conference (ACSAC'20, ACSAC'21), Austin, TX, USA, 2020,2021.
3. **Technical Program Co-Chair**, 16th EAI International Conference on Security and Privacy in Communication Networks (Securecomm 2020), Washington, DC, USA, October 2020.
4. **Technical Program Co-Chair**, 2020 USENIX Summit on Hot Topics in Security (HotSec'20), Boston, MA, USA, August 2020 (*suspended due to COVID-19 pandemic*)
5. **Technical Program Co-Chair**, 11th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'18), Stockholm, Sweden, July 2018.
6. **Conference General Chair**, 38th IEEE Symposium on Security and Privacy, San Jose, CA, May 2017.
7. **Technical Program Chair**, 30th Annual Computer Security Applications Conference (ACSAC 2014), New Orleans, LA, December 2014.
8. **Technical Program Co-Chair**, 29th Annual Computer Security Applications Conference (ACSAC 2013), New Orleans, LA, December 2013.

Other Committee Chairs

9. **Chair, Test of Time Award Committee**, ACM Conference on Computer and Communications Security, 2026.
10. **Associate Program Committee Chair**, 2026 Network and Distributed Systems Security Symposium (NDSS'26), San Diego, CA, USA, February 2026.
11. **Vice Chair and Registration Chair**, 37th IEEE Symposium on Security and Privacy, San Jose, CA, May 2016.
12. **Chair, Test of Time Award Committee**, Annual Computer Security Applications Conference (ACSAC), 2019.
13. **Short Talks Co-Chair**, USENIX Security Symposium, 2017.
14. **Panels Chair**, Annual Computer Security Applications Conference (ACSAC), 2012, 2011.
15. **Publicity Chair**, Annual Computer Security Applications Conference (ACSAC), 2010.

Other Conference and Workshop Organization Activities

16. **Research Ethics Committee Member**, USENIX Security Symposium, 2026.
17. **Test of Time Award Committee Member**, IEEE Symposium on Security and Privacy, 2026.
18. **Test of Time Award Committee Member**, ACM Conference on Computer and Communications Security, 2025.
19. **Research Ethics Committee Member**, USENIX Security Symposium, 2025.
20. **Test of Time Committee Member**, IEEE Symposium on Security and Privacy, 2025.
21. **Doctoral Symposium Committee Member**, ACM Conference on Computer and Communications Security, 2024.
22. **Research Ethics Committee Member**, USENIX Security Symposium, 2024.

Technical Program Committee Memberships (125 Tech. Program Committees)

Top-4 Security Conferences

23. **USENIX Security Symposium**: *TPC Member*, 2026, 2025, 2021, 2020, 2019, 2018, 2017, 2015, 2014.
24. **IEEE Symposium on Security and Privacy (Oakland)**: *TPC Member*, 2025, 2024, 2023, 2021, 2020, 2018, 2017, 2016, 2012; *Publications Chair*, 2014, 2013, 2012, 2011, *Submissions Chair*, 2008.
25. **ISOC Network and Distributed Security Symposium (NDSS)**: *TPC Member*, 2021, 2020, 2019, 2018, 2017, 2016.
26. **ACM Conference on Computer and Communications Security (CCS)**: *TPC Member*, 2020, 2016, 2015, 2014, 2013; *TPC Member (Industry Track)*, 2007, 2004.

Other Conferences and Workshops

27. **IEEE Workshop on Meta-Science and Critical Reflections in Security and Privacy Research (MetaCRiSP)**, *TPC Member*, 2026.
28. **USENIX Conference on Offensive Technologies (WOOT)**, *TPC Member*, 2026.
29. **Workshop on SOC Operations and Construction (WOSOC)**, *TPC Member*, 2026.
30. **ACM Conference on Reproducibility and Replicability (REP)**, *TPC Member*, 2025.
31. **Privacy Enhancing Technologies Symposium (PETS)/Journal of Privacy Enhancing Technologies**, *Senior PC Member*, 2023, *TPC Member/Editorial Board*, 2014-2016.
32. **IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)**: *TPC Member*, 2023.
33. **USENIX Symposium on Usable Security and Privacy (SOUPS)**: *TPC Member*, 2024.
34. **ACM Conference on Security in Wireless and Mobile Networks (WiSec)**: *TPC Member*, 2024, 2023, 2022, 2021, 2020, 2019, 2017, 2016, 2015, 2014.
35. **IEEE Secure Development Conference (SecDev)**: *TPC Member*, 2023, 2022.

36. **USENIX Annual Technical Conference (ATC):** *TPC Member*, 2021, 2020.
37. **IEEE European Symposium on Security and Privacy (Euro S&P):** *TPC Member*, 2020.
38. **USENIX Workshop on Cyber Security Experimentation and Test (CSET):** *TPC Member*, 2019, 2015, 2014, 2013.
39. **International Workshop on the Theory and Practice of Provenance (TaPP):** *TPC Member*, 2019.
40. **USENIX Enigma Conference:** *TPC Member*, 2019, 2018.
41. **ACM Cloud Computing Security Workshop (CCSW):** *TPC Member*, 2019, 2014.
42. **International Provenance and Annotation Workshop (IPAW):** *TPC Member*, 2018.
43. **ACM Symposium on Information, Computer and Communications Security (ASIACCS):** *TPC Member*, 2018, 2017, 2015, 2014.
44. **Annual Computer Security Applications Conference (ACSAC):** *TPC Member*, 2018, 2017, 2012.
45. **World Conference on Information Security Applications (WISA):** *TPC Member*, 2017.
46. **International Conference on Cryptology and Network Security (CANS):** *TPC Member*, 2017.
47. **New Security Paradigms Workshop (NSPW):** *TPC Member*, 2016, 2015, 2014, 2013.
48. **IEEE Mobile Security Technologies Workshop (MOST):** *TPC Member*, 2015, 2014.
49. **Symposium and Bootcamp on the Science of Security (HotSoS):** *TPC Member*, 2015.
50. **Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC):** *TPC Member*, 2015.
51. **European Symposium on Research in Computer Security (ESORICS):** *TPC Member*, 2014, 2013, 2012.
52. **Smart Energy Grid Security Workshop (SEGS):** *TPC Member*, 2014, 2013.
53. **Conference on Privacy, Security and Trust (PST):** *TPC Member*, 2014, 2013.
54. **Global Internet Symposium (GI):** *TPC Member*, 2014.
55. **IEEE International Conference on Big Data (BigData):** *TPC Member*, 2013.
56. **IEEE LCN Network Security Workshop (WNS):** *TPC Member*, 2013.
57. **International Workshop on Security in Information Systems (WOSIS):** *TPC Member*, 2013, 2012.
58. **International Conference on Applied Cryptography and Network Security (ACNS):** *TPC Member*, 2013.
59. **International Workshop on Security (IWSEC):**, *TPC Member*, 2012, 2008, 2007.
60. **Workshop on Secure Network Protocols (NPSec):** *Publicity Chair*, 2012.
61. **LCN Workshop on Security in Communication Networks (SICK):** *TPC Member*, 2012.
62. **USENIX Workshop on Hot Topics in Security (HotSec):** *TPC Member*, 2012.
63. **International Workshop on Security (IWSEC):** *TPC Member*, 2011, 2010.

64. **International Conference on Security and Privacy in Communication Networks (SecureComm):** *TPC Member*, 2011.
65. **International Conference on Availability, Reliability and Security (ARES):** *TPC Member*, 2011, 2010, 2009, 2008, 2007.
66. **International Conference on Internet Monitoring and Protection (ICIMP):** *TPC Member*, 2011, 2010.
67. **International Conference on Financial Cryptography and Data Security (FC):** *TPC Member*, 2011.
68. **International Conference on Information Systems Security (ICISS):** *TPC Member*, 2009, 2008, 2007; *Submissions and Web Chair*, 2007.
69. **IEEE International Workshop on Software Security Process:** *TPC Member*, 2009.
70. **International Conference on International Conference on Information Security and Assurance (ISA):** *TPC Member*, 2009, 2008; *Publicity Co-Chair*, 2008.
71. **International Workshop on Security in Systems and Networks (SSN):** *TPC Member*, 2009, 2007.
72. **Conference on Future Generation Communication and Networking (FGCN):** *TPC Member*, 2008, 2007.
73. **IEEE International Workshop on Security in Software Engineering (IWSSE):** *TPC Member*, 2008, 2007.
74. **IEEE/IFIP Conference on Dependable Systems and Networks (DSN):** *TPC Member (Fast Abstracts)*, 2008.
75. **International Workshop on Secure Software Engineering (SecSE):** *TPC Member*, 2008.

Conference Session Chair: USENIX Security'18, ACSAC'17, WWW'17, IEEE SP'16, CCS'16, CCS'14, HotSec'12, IEEE SP'12, CCS'09

Journal & Book Reviewing

IEEE Transactions on Dependable and Secure Computing (TDSC), 2019, 2014, 2010; Communications of the ACM (CACM), 2019; IEEE Transactions on Computers (TC), 2019, 2012, 2009; IEEE Security and Privacy, 2018, 2013, 2010; Journal of Computer Security (JCS), 2018; IEEE Transactions on Information Forensics and Security (TIFS), 2017, 2013, 2011; Journal of Internet Services and Applications (JISA), 2017; ACM Transactions on Information and System Security (TISSEC), 2016, 2015, 2014, 2010, 2009, 2008, 2006; IEEE Transactions on Reliability (TR), 2014; ACM Transactions on Internet Technologies (TOIT), 2013, 2010, 2009; ACM Computing Surveys, 2013; ACM Transactions on Storage (TOS), 2013, 2011; Elsevier Computers and Security, 2013, 2011; International Journal of Computer Mathematics, 2011; IEEE Transactions on Parallel and Distributed Systems (TPDS), 2011, 2008; Wiley and Sons (Book proposal reviewer), 2010; EURASIP Journal on Information Security (JIS), 2011, 2010; Elsevier Journal of Computer Networks, 2010, 2005; International Journal of Software and Informatics (IJSI), 2010; International Journal of Security and Networks

(IJSN), 2009, 2007; The Computer Journal (Oxford), 2009; ACM/IEEE Transactions on Networking (TON), 2008; Wireless Personal Communications, 2008; IEEE Communications Surveys and Tutorials, 2007; IEEE Transactions on Software Engineering (TSE), 2007; Software: Practice and Experience, 2007; Handbook of Information Security, 2004.

Conference & Workshop Reviewing

USENIX OSDI, 2016; IEEE INFOCOM, 2014, 2007; IEEE Symposium on Security and Privacy (S&P), 2013, 2009, 2008, 2007; ISOC Symposium on Network and Distributed Systems Security (NDSS), 2013, 2012, 2009, 2007; ACM Conference on Data and Application Security and Privacy (CODASPY), 2013; IEEE Computer Security Foundations Symposium (CSF), 2011; ACM Symposium on Computer and Communications Security (CCS), 2010, 2009, 2008, 2006; Annual Computer Security Applications Conference (ACSAC), 2010, 2007, 2006, 2005; USENIX Workshop on Hot Topics in Security (HotSec), 2010, 2007; ACM Symposium on Access Control Models and Technologies (SACMAT), 2010, 2009, 2008, 2006; IFCA International Conference on Financial Cryptography and Data Security (FC), 2010, 2008, 2007; Information Security Conference (ISC), 2009; USENIX Security Symposium, 2009, 2008, 2007, 2006, 2004; IEEE GLOBECOM, 2008; IFIP Conference on Data and Applications Security (DBSEC), 2008, 2006; USENIX Conference on File and Storage Technologies (FAST), 2008; IEEE International Conference on Computer Engineering and Systems (ICCES), 2007; IEEE International Conference on Distributed Computing Systems (ICDCS), 2007; IEEE Sarnoff Symposium, 2007; IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2007; ACM International Workshop on Storage Security and Survivability (StorageSS), 2006; International Workshop on Security (IWSEC), 2006; International Conference on Emerging Trends in Computer Science (ETRICS), 2006; International Conference on Applied Cryptography and Network Security (ACNS), 2006; European Symposium on Research in Computer Security (ESORICS), 2005.

University Service

Faculty Search Committee, Chair, UF JAX Security and Privacy, CISE, University of Florida, 2025-2026.

Mentorship Committee, Chair, CISE, University of Florida, 2025-present.

Energy Grid Security Summit, Co-Chair, Strategic Research and Development, University of Florida, 2025.

Search Committee, Director of Strategic Communications and Marketing, Chair, College of Engineering, University of Florida, 2023-2024.

Sabbatical Committee, Member, College of Engineering, University of Florida, 2021-2022.

Steering Committee, Member, University of Florida, 2018-2022.

Graduate Admissions Committee, Member, CISE, University of Florida, 2019-present.

Consortium for Media and Trust Director Search Committee, Member, University of Florida, 2019.

Faculty Search Committee, Chair, CISE, University of Florida, 2018-2021.

Faculty Search Committee, Member, CISE, University of Florida, 2017-2018.

Awards Committee, Member, CISE, University of Florida, 2015-2025.

Graduate Affairs Committee, Member, CISE, University of Florida, 2014-2018.

Graduate Education Committee, Member, CIS, University of Oregon, 2010-2014.

Undergraduate Curriculum Committee, Member, CIS, University of Oregon, 2012-2014.

General Education Committee, Member, University of Oregon, 2013-2014.

Students

Graduate Advisees

Current Ph.D. Advisees:

1. Anna Crowder (PhD, Spring 2026)
2. Magdalena Pasternak (PhD, Spring 2027)
3. Carson Stillman (PhD, Spring 2027, co-advised with Sara Rampazzi)
4. Nathaniel Bennett (PhD, Spring 2027, co-advised with Patrick Traynor)
5. Kevin Childs (PhD, Spring 2028)
6. Bernardo Medieros (PhD, Spring 2029)
7. Kollin Labowski (PhD, Spring 2029)
8. Joel Hirschmann (PhD, Spring 2029)
9. Scott Slinn (PhD, Spring 2030)

Past Ph.D Advisees:

1. Weidong Zhu, Summer 2025, co-advised with Sara Rampazzi, now **Assistant Professor of Computing and Information Sciences**, Florida International University.
2. Cassidy Gibson, Spring 2025, co-advised with Patrick Traynor, now **Postdoctoral Fellow**, Human Computing Associates.
3. Washington Garcia, Fall 2022, now **Research Scientist**, University of Dayton Research Institute.
4. Grant Hernandez, Summer 2020, now **Security Resaercher**, L3Harris.

5. Dave (Jing) Tian, Summer 2019, now **Associate Professor of Computer Science**, Purdue University (NSF CAREER award, 2022).
6. Adam Bates, Summer 2016, now **Associate Professor of Computer Science**, University of Illinois at Urbana-Champaign (NSF CAREER award, 2018).
7. Benjamin Mood Spring 2016, now **Associate Professor of Computer Science**, Point Loma Nazarene University.

Past Master's Degree Students:

1. Yunhao Wu (MS, Spring 2024),
2. Caroline Fedele (MS, Fall 2023),
3. Benjamin Simon (MS, Spring 2023),
4. Blas Kojusner (MS, Fall 2022),
5. Hunter Searle (MS, Summer 2022),
6. Vanessa Frost (MS, Spring 2022),
7. Joseph Choi (MS, Spring 2021),
8. Joseph Pletcher (MS, Spring 2013),
9. Adam Bates (MS, Spring 2012),
10. Benjamin Mood (MS, Spring 2012),
11. Masoud Valafar (MS, Fall 2011).

Other Graduate Student Advising

PhD Committee Member:

1. Ghulam Memon (PhD, University of Oregon, Fall 2013),
2. Saeed Sadeghian (PhD, University of Calgary, Fall 2015),
3. Henry Carter (PhD, Georgia Institute of Technology, Spring 2016),
4. Mehdi Sadi (PhD, University of Florida, Spring 2017),
5. Bradley Reaves (PhD, University of Florida, Summer 2017),
6. Robert Karam (PhD, University of Florida, Summer 2017),
7. Luka Malisa (PhD, ETH Zurich, Summer 2017),
8. Fengchao Zhang (PhD, University of Florida, Spring 2018),
9. Kai Yang (PhD, University of Florida, Summer 2018),
10. Nolen Scaife (PhD, University of Florida, Spring 2019),
11. Ruimin Sun (PhD, University of Florida, Spring 2019),
12. Francesco Pittaluga (PhD, University of Florida, Spring 2019),
13. Jonathan Smith (PhD, University of Florida, Spring 2020),

14. Beong Heyn Kim (PhD, University of Toronto, Spring 2020),
15. Christopher Patton (PhD, University of Florida, Summer 2020),
16. Xiaoyong Yuan (PhD, University of Florida, Summer 2020),
17. Farhaan Fowze (PhD, University of Florida, Summer 2020),
18. Tamzidul Hoque (PhD, University of Florida, Summer 2020),
19. Jasmine Bowers (PhD, University of Florida, Summer 2020),
20. Abdulrahman Alaqi (PhD, University of Florida, Fall 2020),
21. Atul Prasad Deb Nath (PhD, University of Florida, Spring 2021),
22. Olufemi Odegbile (PhD, University of Florida, Spring 2021),
23. Aritra Dhar (PhD, ETH Zurich, Summer 2021),
24. Olufemi Odegbile (PhD, University of Florida, Summer 2021),
25. Luis Vargas (PhD, University of Florida, Summer 2021),
26. Joel Mandebi Mbongue (PhD, University of Florida, Fall 2021)
27. Yazhou Tu (PhD, University of Louisiana at Lafayette, Fall 2021),
28. Shubhra Deb Paul (PhD, University of Florida, Spring 2022),
29. Hadi Abdullah (PhD, University of Florida, Summer 2022),
30. Christian Peeters (PhD, University of Florida, Summer 2022),
31. Brendan David-John (University of Florida, Summer 2022),
32. Sarah Amir (PhD, University of Florida, Summer 2022),
33. Jonathan Cruz (PhD, University of Florida, Fall 2022),
34. Logan Blue (PhD, University of Florida, Spring 2023),
35. Animesh Chhotaray (PhD, University of Florida, Spring 2023),
36. Chaoyi Ma (PhD, University of Florida, Spring 2023),
37. Martin Georgiev (PhD, University of Oxford, Spring 2023),
38. Sujan Kumar Saha (PhD, University of Florida, Summer 2023),
39. Minh Vu (PhD, University of Florida, Fall 2023),
40. Md Rakid Muttaki (PhD, University of Florida, Fall 2023),
41. Manish Merugu (PhD, University of Florida, Spring 2024),
42. Yichen Jiang (PhD, University of Florida, Spring 2024),
43. Christopher Brant (PhD, University of Florida, Summer 2024),
44. Mohammad Monir Hossain (PhD, University of Florida, Summer 2024),
45. Mohammad Sami Ul Islam Sami (PhD, University of Florida, Fall 2024),
46. Ethan Wilson (PhD, University of Florida, Spring 2025),
47. Aritra Dasgupta (PhD, University of Florida, Spring 2025),

48. Seth Layton (PhD, University of Florida, Summer 2025),
49. Tyler Tucker (PhD, University of Florida, Summer 2025),
50. Kevin Warren (PhD, University of Florida, Summer 2025),
51. Ruochen Dai (PhD, University of Florida, Summer 2025),
52. Yihang (Ken) Bai (PhD, University of Florida, Summer 2025),
53. Muhammed Kawser Ahmed (PhD, University of Florida, Summer 2025),
54. Wenxuan Bao (PhD, University of Florida, Fall 2025),
55. Rasheed Kibria (PhD, University of Florida, Fall 2025),
56. Xingli Zhang (PhD, University of Louisiana at Lafayette, Spring 2026),
57. Ron Thompson (PhD, Tufts University, Spring 2026),
58. Mrida Rahman (PhD, University of Florida, Spring 2026)),
59. Channing Ludden (PhD, University of Florida, Spring 2028),
60. Mansi Pai (PhD, University of Florida, Spring 2029),
61. Izabela Savic (PhD, University of Guelph, Spring 2029).

Other Committee Membership: Ming Liu (University of Florida, thesis proposal committee, Spring 2016), Reza Motamedi (University of Oregon, thesis proposal committee, Spring 2014), Jason Gustafson (University of Oregon, MS Committee, Winter 2012), Amir Amir Farzad (University of Oregon, MS committee, Spring 2013).

Undergraduate Students

1. Hannah Pruse (Honors BS, Oregon, Spring 2013 - **NSF Graduate Fellow**),
2. Ryan Leonard (Honors BS, Oregon, Spring 2013),
3. Peter McKay (Honors BS, Oregon, Spring 2013),
4. Braden Hollembaek (Honors BS, Oregon, Spring 2014),
5. Abdul Alkhelaifi (Honors BS, Oregon Spring 2014),
6. Devan Patel (BS, Florida, Spring 2015),
7. Cynthia Omauzo (CS, Prarie View A&M, CRA DREU, hosted Summer 2015),
8. Jared Trinkler (BS, University Scholar, Florida, Spring 2017),
9. Joshua Uduehi (CRA DREU, BS, Indiana University, hosted Summer 2017),
10. Suman Adari (BS, Florida, Spring 2021),
11. Christie Ruales (BS, CRA/ACSA SWSIS Scholar, University Scholar, University of Florida, Spring 2021),
12. César Arguello (BS, Florida, Spring 2022),
13. Katie Platt (BS, Florida, Fall 2022),
14. Gabriella Neris (BS, Florida, Spring 2023),

15. Aryaan Verma (BS, Florida, Spring 2025),
16. Carolina Boitel (Honors BS, Florida, Spring 2025),
17. Santiago Barrios (BS, Florida, Spring 2025),
18. Ishan Kumthekar (BS, Florida, Spring 2026),
19. Sema Akkaya (BS, Florida, Spring 2028).

Presentations & Invited Talks

1. Analyzing the AI Nudification Ecosystem. *AI Ethics-to-Industry Symposium*, San Francisco, CA, USA, November 2025.
2. Securing Satellite Rendezvous and Proximity Operations with MPC. *Dagstuhl Seminar on Privacy-Preserving Technologies of Societal Impact*, Wadern, Germany, July 2025.
3. **Keynote Address:** Exploring Unanticipated Functionality in Cellular Devices and Networks. *18th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, Arlington, VA, USA, June 2025.
4. DFS Application Best Practices for Mobile Application Developers. *ITU DFS Webinar - Securing Mobile Payment Applications*, virtual, March 2025.
5. Securing the Future of Computing for Marginalized and Vulnerable Populations. *Tufts University*, Boston, MA, USA, December 2024.
6. **Keynote Address:** Unsafe at any G? Implications of unintended functionality in telecommunications networks and devices for CPS environments. *EAI International Conference on Security and Privacy in Cyber-Physical Systems and Smart Vehicles (SmartSP)*, New Orleans, LA, November 2024.
7. *Distinguished Lecture:* From Blue Boxes to Black Boxes: Exposing Security Vulnerabilities in Mobile Devices and Networks. *Queen's Centre for Security and Privacy*, Queen's University, Kingston, ON, Canada, October 2024.
8. Ransom Crisis: Mitigating the Ransomware Threat. *Eastern Indonesia Financial Inclusion Lab (EIFIL)*, Denpasar, Bali, Indonesia, August 2024.
9. Systems and DFS Security: Concepts and Adversarial Thinking. *Eastern Indonesia Financial Inclusion Lab (EIFIL)*, Denpasar, Bali, Indonesia, August 2024.
10. Best Practices for DFS Application Security. *Financial Inclusion and Tech Talk (FITT)*, Jakarta, Indonesia (virtual), June 2024.
11. Securing the Future of Computing for Marginalized and Vulnerable Populations. *NITRD Privacy R&D Inter-agency Working Group*, Washington, DC (virtual), May 2024.
12. Assessing the Mobile Device Platform to Assure DFS Security. *ITU Regional Digital Financial Services Security Clinic for Asia-Pacific Region*, Seoul, Republic of Korea, April 2024.
13. Understanding the Current and Emerging Cybersecurity Threat Landscape. *Gator 100 Professional and Leadership Development Workshop*, Gainesville, FL, April 2024.
14. From Blue Boxes to Black Boxes: Telecommunications Security Research at the Florida Institute for Cybersecurity Research. *UF Eye-Opener Discovery Breakfast*, Gainesville, FL, March 2024.

15. Following the Money: Characterizing the Monetization Ecosystem of Stalkerware Through Application Analysis. *USENIX GREPSEC Workshop*, Anaheim, CA, August 2023.
16. **Keynote Address:** From Blue Boxes to Black Boxes: Adventures in Uncovering Device Functionality. *IEEE Workshop on Offensive Technology (WOOT)*, San Francisco, CA, May 2023.
17. From Blue Boxes to Black Boxes: Telecommunications Security Research at the Florida Institute for Cybersecurity Research. *Florida Cybersecurity Advisory Council*, Gainesville, FL, May 2023.
18. Privacy-Preserving Computation for Resource-Constrained Devices. *NATO Science and Technology Office ET Meeting*, Washington, DC, November 2022.
19. Security Assurance for the DFS Ecosystem. *ITU Study Group 17 Meeting*, virtual, August 2021.
20. Improving Resilience in the DFS Ecosystem with a Security Assurance Framework. *ITU/FIGI Insights on Digital Financial Services during COVID-19 Webinar Series*, virtual, July 2020.
21. Investigating External Surfaces in Android Devices. *Microsoft Research*, Cambridge, United Kingdom, February 2020.
22. Firmware-Informed Approaches to Securing Systems and Devices. *ARM Research*, Cambridge, United Kingdom, February 2020.
23. Cybersecurity and Election Security: Innovations in Research and Technology (with Juan Gilbert). *Orange and Blue Plate Luncheon*, Tallahassee, FL, February 2020.
24. Making MPC More Accessible Through Informed Compiler Design. *Workshop on Teaching Secure Computation*, Washington, DC, January 2020.
25. Analyzing Applications to Assess Security. *FIGI Security Clinic*, Geneva, Switzerland, December 2019.
26. Application Security Framework for DFS. *FIGI Security Clinic*, Geneva, Switzerland, December 2019.
27. Security Research at the Florida Institute for Cybersecurity Research (with Patrick Traynor). *UF Eye Opener Breakfast*, Gainesville, FL, USA, October 2019.
28. “Plug and Pray” Today: Reflecting on a Decade of Peripheral Security Research. *UCLA*, Los Angeles, CA, USA, April 2019.
29. Cybersecurity Challenges in a Diverging Internet. *Jean Monnet Centre of Excellence Annual Workshop on the European Union*, Gainesville, FL, USA, April 2019.
30. Designing a Security Management Framework for Digital Financial Services. *ITU Security, Infrastructure, Trust Working Group Meeting*, Washington, DC, USA, April 2019.
31. Developing a Consortium on Trust in Media and Technology. *Invited Panelist. University of Florida Foundation National Board Meeting*, Atlanta, GA, USA, March 2019.
32. Designing a Security Management Framework for Digital Financial Services. *Financial Inclusion Global Symposium*, Cairo, Egypt, January 2019.
33. Staying Safe in Cyberspace: Understanding the Threats and Defenses. *The Village at Gainesville*, Gainesville, FL, USA, October 2018.
34. Domain Informed Techniques for IoT Security (with Tuba Yavuz). *ARM Research*, San Jose, CA, USA, October 2018.
35. A Discussion on Security Education in Academia. *Invited Panelist. ACM Conference on Communi-*

- cations and Communication Security (CCS)*, Toronto, ON, Canada, October 2018.
36. New Attack Surfaces Against Mobile Platforms. *Columbia University Cybersecurity and Payments Roundtable*, New York, NY, August 2018.
 37. **Keynote Address:** Secure and Efficient Whole-System Data Provenance: A Retrospective. *2nd Workshop on Provenance-based Security*, London, UK, July 2018.
 38. “Plug and Pray” Today: Reflecting on a Decade of USB Security Research. *University of Oxford*, Oxford, UK, July 2018.
 39. “Plug and Pray” Today: Reflecting on a Decade of USB Security Research. *Chinese Academy of Sciences*, Beijing, China, June 2018.
 40. Characterizing Tooling and Interfaces for Mobile Applications and Devices. *Samsung Research America*, Mountain View, CA, USA, May 2018.
 41. “Plug and Pray” Today: Reflecting on 10 Years of USB Security Research. *Symantec Research Labs*, Culver City, CA, USA, May 2018.
 42. A Security Framework for for DFS Featurephone Applications. *ITU FIGI Security, Information, and Trust Working Group Meeting*, Washington, DC, USA, April 2018.
 43. Application Security for DFS Featurephone Applications. *Financial Inclusion Global Initiative Symposium*, Bangalore, India, November 2017.
 44. Towards More Robust Interactions with Telephones and Peripherals (with Patrick Traynor). *Florida International University*, Miami, FL, October 2017.
 45. **Keynote Address:** Making USB Safer for Hosts and Peripherals. *Third International Conference on Future Network Systems and Security (FNSS 2017)*, Gainesville, FL, August 2017.
 46. Making USB Safer for Hosts and Peripherals. *ETH Zurich*, Zurich, Switzerland, July 2017.
 47. Security Challenges in Mobile Devices. *FinTech, DFS and Payments Summit*, *Columbia Business School*, New York, NY, June 2017.
 48. Webinar: Trends and Challenges in Mobile Money and Mobile Banking Application Security. *Digital Financial Services Observatory*, *Columbia University*, June 2017.
 49. Towards Firmware Vetting on Legacy Embedded Platforms. *10th Workshop on Fault-Tolerant Spaceborne Computing Employing New Technologies*, Albuquerque, NM, May 2017.
 50. Technical Deep Dive: Foundations of Hardware-Assisted Secure Multiparty Computation with SGX. *10th Workshop on Fault-Tolerant Spaceborne Computing Employing New Technologies*, Albuquerque, NM, May 2017.
 51. Security and Privacy Challenges for Mobile Money Applications. *ITU Digital Financial Services Workshop: Exploring Innovation in Transactions and Financing in the Caribbean*, Port of Spain, Trinidad and Tobago, April 2017.
 52. Everybody Jammin’ Up on Those Tings: Challenges for the Internet of Insecure Things. *Forum on Internet of Things: Smarter Living in the Caribbean*, Port of Spain, Trinidad and Tobago, April 2017.
 53. Application Security for DFS Applications. *ITU Workshop on DFS and Financial Inclusion*, Washington, DC, April 2017.
 54. **Keynote Address:** Making USB Safer for Hosts and Peripherals. *Computer Science Research Day*, *University of Georgia*, Athens, GA, April 2017.

55. Security in the DFS Ecosystem - Final Recommendations. *ITU Focus Group Meeting on Digital Financial Services*, Geneva, Switzerland, December 2016.
56. Making USB Great Again: New Defenses for Hosts and Devices. *MIT Lincoln Laboratory*, Lexington, MA, USA, October 2016.
57. Making USB Great Again: New Defenses for Hosts and Devices. *Dartmouth College*, Hanover, NH, USA, October 2016.
58. Recommendations for Securing Digital Finance. *ITU Focus Group Meeting on Digital Financial Services*, Dar es Salaam, Tanzania, September 2016.
59. Secure and Efficient Data Provenance. *DARPA Transparent Computing PI Meeting*, Cambridge, MA, USA, July 2016.
60. Security for Digital Alternative Data and SME Supply Chain Finance. *G20 Global Partnership for Financial Inclusion (GPFI) Forum*, Chengdu, China, July 2016.
61. Privacy-Preserving Computing Made Practical. *9th Workshop on Fault-Tolerant Spaceborne Computing Employing New Technologies*, Albuquerque, NM, USA, June 2016.
62. Host Fingerprinting for Identity and Integrity Assurance Using Machine Learning. *9th Workshop on Fault-Tolerant Spaceborne Computing Employing New Technologies*, Albuquerque, NM, USA, June 2016.
63. Security and Privacy Challenges for Mobile Money in Mobile Devices. *5th Columbia Business School Digital Financial Services and Emerging Payments Summit*, New York, NY, USA, May 2016.
64. Trustworthy Collection Architectures for Data Provenance. *Concordia University*, Montreal, QC, Canada, May 2016.
65. Analyzing the Security of Sticky SIMs. *ITU Focus Group Meeting on Digital Financial Services*, Washington, DC, USA, April 2016.
66. Secure and Trustworthy Computers, Devices, and Systems. *South Carolina Governor's School for Science and Mathematics*, Harstville, SC, USA, December 2015.
67. Security Recommendations for the DFS Ecosystem. *ITU Focus Group Meeting on Digital Financial Services*, Geneva, Switzerland, December 2015.
68. Securing Storage for Insider Threat Mitigation. *Florida Cyber Consortium Research Symposium*, Tampa, FL, USA, October 2015.
69. Tales From the Crypt(o): Spooky Stories of Ideal-World Cryptography Meeting Real-World Implementation. *University of Calgary*, Calgary, AB, Canada, November 2015.
70. Vulnerability Analysis of Branchless Banking Apps in the Developing World. *ITU Focus Group Meeting on Digital Financial Services*, Kuala Lumpur, Malaysia, October 2015.
71. New Trends in Cybersecurity: Securing Critical Cyber-Infrastructure. *US Department of State/Department of Justice Cybercrime and Cybersecurity Workshop for Lusophone Africa*, Maputo, Mozambique, September 2015.
72. Trustworthy Collection Architectures for Data Provenance. *MIT Lincoln Laboratory*, Lexington, MA, USA, August 2015.
73. Be Who You Are: Establishing Host Identity in Local and Remote Systems. *EURECOM Institute*, Sophia Antipolis, France, July 2015.

74. Be Who You Are: Establishing Host Identity in Local and Remote Systems. *Symantec Research Labs*, Mountain View, CA, USA, April 2015.
75. Be Who You Are: Challenges of Establishing Host Identity in Local and Remote Systems. *Rutgers University*, New Brunswick, NJ, USA, March 2015.
76. Certificate Validation and the Future of SSL Security. *Chi Sigma IO, University of Florida*, Gainesville, FL, USA, November 2014.
77. Forced Perspectives: Evaluating an SSL Trust Enhancement at Scale. *2014 ACM Internet Measurement Conference (IMC'14)*, Vancouver, BC, Canada, November 2014.
78. USB Host Fingerprinting. *Lockheed Martin*, Orlando, FL, October 2014.
79. Improving Security Through Collaborative Frameworks. *IEEE CollaborateCom (Invited Panelist)*, Miami, FL, October 2014.
80. Establishing Host Identity in Systems and Storage. *University of Florida*, Gainesville, FL, April 2014.
81. Establishing Host Identity Through Indirect Measurement. *Pennsylvania State University*, University Park, PA, April 2014.
82. **Keynote Address:** Trust No One? Addressing the Challenges of Bottom Up Trust in Systems and Storage. *Symantec Cutting Edge*, Springfield, OR, March 2014.
83. Leveraging Emerging Storage Functionality for New Security Services. *Oregon State University*, Corvallis, OR, June 2012.
84. Protecting Portable Storage with Host Validation. *Queen's University*, Kingston, ON, Canada, April 2012.
85. Protecting Portable Storage with Host Validation. *NSERC ISSNet Security Workshop*, Kingston, ON, Canada, April 2012.
86. Attacks and Defenses Against the Cloud Infrastructure. *Oregon Security Day*, Eugene, OR, April 2012.
87. Leveraging Emerging Storage Functionality for New Security Services. *Portland State University*, Portland, OR, November 2011.
88. Leveraging Emerging Storage Functionality for New Security Services. *Galois*, Portland, OR, August 2011.
89. Securing Homecare Rehabilitation Environments. *UW/MSR Research Retreat*, Cle Elum, WA, August 2011.
90. Challenges and Alternatives to the Host Identification Problem. *Oregon Security Day*, Eugene, OR, April 2011.
91. Porscha: Policy Oriented Secure Content Handling in Android. *ACSAC 2010*, Austin, TX, December 2010.
92. Kells: A Protection Framework for Portable Data. *ACSAC 2010*, Austin, TX, December 2010.
93. Protection Mechanisms for Portable Devices. *Symantec Research Labs*, Mountain View, CA, November 2010.
94. Challenges and Alternatives to the Host Identification Problem. *2nd ACM Northeast Forensics Exchange (NeFX2010)*, Washington, DC, September 2010.

95. Disk-Enabled Authenticated Encryption. *MSST 2010*, Incline Village, NV, May 2010.
96. Leveraging Emerging Storage Functionality for New Security Services. *Polytechnic Institute of New York University*, Brooklyn, NY, March 2010.
97. Leveraging Emerging Storage Functionality for New Security Services. *Simon Fraser University*, Surrey, BC, Canada, March 2010.
98. Leveraging Emerging Storage Functionality for New Security Services. *Stevens Institute of Technology*, Hoboken, NJ, March 2010.
99. Leveraging Emerging Storage Functionality for New Security Services. *University of Tennessee*, Knoxville, TN, March 2010.
100. Leveraging Emerging Storage Functionality for New Security Services. *University of Oregon*, Eugene, OR, March 2010.
101. Leveraging Emerging Storage Functionality for New Security Services. *Naval Postgraduate School*, Monterey, CA, February 2010.
102. Towards a Secure and Efficient System for End-to-End Provenance. *TaPP'10*, San Jose, CA, February 2010.
103. Rootkit-Resistant Disks. *Security Reading Group*, *University of Toronto*, Toronto, ON, Canada, November 2009.
104. Rootkit-Resistant Disks. *Digital Security Seminar*, *Carleton University*, Ottawa, ON, Canada, November 2009.
105. U Can't Touch This: Protections for Portable Storage. *IWSSPS 2009*, Grenoble, France, Oct. 2009.
106. FlowStor: Preserving Information Flow on Portable Storage Devices. *Symantec Corporation*, Mountain View, CA, USA, August 2009.
107. Leveraging Emerging Disk Functionality for New Security Services. *Symantec Research Labs*, Mountain View, CA, USA, June 2009.
108. Rootkit-Resistant Disks. *CCS'08*, Alexandria, VA, USA, October 2008.
109. Experimenting with BGP Security Mechanisms Using the DETER Framework. *Boeing Integrated Defense*, Philadelphia, PA, USA, October 2008.
110. Terabyte Home Security and Access Control. *Seagate Research*, Pittsburgh, PA, USA, August 2008.
111. Towards Automated Privilege Separation. *ICISS 2007*, Delhi, India, December 2007.
112. Non-Volatile Memory and Disks: Avenues for Policy Architectures. *CSAW 2007*, Fairfax, VA, USA, November 2007.
113. Autonomously Secure Disks. *Software Reading Group*, *University of Michigan*, Ann Arbor, MI, USA, September 2007.
114. Leveraging Non-Volatile Memory for Storage Security. *2007 USENIX Security Symposium, Works in Progress*, Boston, MA, USA, August 2007.
115. Analysis of the IPv4 Address Delegation Structure. *ISCC 2007*, Aveiro, Portugal, July 2007.
116. Performance Optimizations of IPsec for Storage. *2007 SNIA Summer Security Summit*, Pittsburgh, PA, June 2007.

117. Optimizing BGP Security by Exploiting Path Stability. *CCS'06*, Alexandria, VA, November 2006.
118. Threats and Attacks in Interdomain Routing. *P2INGS Quarterly Meeting*, Tempe, AZ, February 2004.
119. Network Operations in Tier-1 Internet Service Providers. *Columbia University*, New York, NY, March 2001.
120. Network Operations in Tier-1 Internet Service Providers. *Telcordia Technologies*, Morristown, NJ, August 2000.

Press Coverage

Research-Related Coverage

1. “UF research team targets nonconsensual nude photo apps to protect privacy”, Paris Carter, *The Gainesville Sun*, January 6, 2026. <https://www.gainesville.com/story/news/2026/01/06/university-of-florida-targets-nonconsensual-nude-photo-apps-to-protect-privacy/88044862007/>
2. “UF cybersecurity expert weighs in on arrest of Marion County man accused of creating AI child porn.” Ryan Wyatt Turbeville and Kayla Lewis, *WCJB News Ocala*, September 30, 2025. <https://www.wcjb.com/2025/09/30/uf-cybersecurity-expert-weighs-arrest-marion-county-man-accused-creating-ai-child-porn/>
3. “How a ‘Nudify’ site turned a group of friends into key figures in a fight against AI-generated porn.” Jonathan Vanian, *CNBC*, September 27, 2025. <https://www.cnbc.com/2025/09/27/nudify-ai-generated-deepfake-fbi.html>
4. “Critical Security Vulnerabilities in Cellular Networks Exposed by Researchers.” Gert Jan Wolf, *The Critical Communications Review*, February 5, 2025. <https://www.criticalcommunicationsreview.com/ccr/news/115288/critical-security-vulnerabilities-in-cellular-networks-exposed-by-researchers>
5. “Over 100 LTE, 5G Bugs Threaten Cellular Service Disruptions.” *ChannelE2E*, January 27, 2025. <https://www.channele2e.com/brief/over-100-lte-5g-bugs-threaten-cellular-service-disruptions>
6. “RANsacked: Over 100 Security Flaws Found in LTE and 5G Network Implementations.” Ravie Lakshmanan, *The Hacker News*, Jan 24, 2025. <https://thehackernews.com/2025/01/ransacked-over-100-security-flaws-found.html>
7. “Underwater data centres could be destroyed by loud noises.” Jeremy Hsu, *New Scientist*, January 14, 2024. <https://www.newscientist.com/article/2430616-underwater-data-centres-could-be-destroyed-by-loud-noises/>
8. “Underwater datacentres vulnerable to sonic attacks.” Dev Kundaliya, *Computing*, May 17, 2024. <https://www.computing.co.uk/news/4209265/underwater-datacentres-vulnerable-sonic-attacks>
9. “Underwater data centres risk sonic attacks.” Nick Farrell, *Fudzilla*, May 17, 2024. <https://fudzilla.com/news/59003-underwater-data-centres-risk-sonic-attacks>
10. “Underwater datacenters could sink to sound wave sabotage”. Dan Robinson, *The Register*, May 17,

2024. https://www.theregister.com/2024/05/17/underwater_datacenters_sound_waves/

11. “Acoustic attacks could be a serious threat to the future of underwater data centers.” Rob Thubron, *TechSpot*, May 20, 204. <https://www.techspot.com/news/103061-acoustic-attacks-could-serious-threat-future-underwater-data.html>
12. “Exploiting Decades-Old Telephone Tech to Break Into Android Devices.” Lily Hay Newman, *Wired*, August 29, 2018. <https://www.wired.com/story/at-commands-android-vulnerability/>
13. “Modern smartphones vulnerable to old-school attack.” Francis Navarro, *Komando.com*, August 28, 2018. <https://www.komando.com/happening-now/483269/modern-smartphones-vulnerable-to-old-school-attack>
14. “ATak na Androida: modemowe komendy standardu z lat 80 pozwalają przejąć kontrolę nad smartfonem” (Translation from Polish: “ATtack on Android: modem commands from the 80’s standard allow you to take control of your smartphone”.) Adam Golanski, *Dobreprogramy*, August 28, 2018. <https://www.dobreprogramy.pl/ATak-na-Androida-modemowe-komendy-standardu-z-lat-80-pozwalaja-przejac-kontrolę-nad-smartfonem,News,90526.html>
15. “Смартфоны ASUS, HTC, Huawei, Lenovo, LG, Samsung, Sony легко взломать технологией, созданной для древнего модема Подробнее” (Translation from Russian: “Smartphones ASUS, HTC, Huawei, Lenovo, LG, Samsung, Sony can easily crack technology created for the ancient modem.”) Roman Georgiev, *CNews Russia*, August 28, 2018. http://safe.cnews.ru/news/top/2018-08-28_smartfony_asushtchuaweilenovolgsamsungsony
16. “AT Command Hitch Leaves Android Phones Open to Attack.” Lindsey O’Donnell, *Threatpost*, August 27, 2018. <https://threatpost.com/at-command-hitch-leaves-android-phones-open-to-attack/136938/>
17. “New security risk for smartphones bring you a ‘ghost user’.” Ida Torres, *Android Community*, August 27, 2018. <https://androidcommunity.com/new-security-risk-for-smartphones-brings-you-a-ghost-user-20180827/>
18. “Android at the mercy of AT commands.” Nick Farrell, *Fudzilla*, August 27, 2018. <https://fudzilla.com/news/mobile/47037-android-at-the-mercy-of-at-commands>
19. “Android-Smartphones durch Modem-Befehle verwundbar” (Translation from German: “Android Smartphones vulnerable through modem commands”.) Sebastian Gruner, *Golem.de: IT-News Für Profis*, August 27, 2018. <https://www.golem.de/news/at-commands-android-smartphones-durch-modem-befehle-verwundbar-1808-136205.html>
20. “Telefony s Androidem lze ovládnout přes USB pomocí AT příkazů” (Translation from Czech: “Android phones can be controlled via USB using AT commands”). Petr Krcmar, *Root.cz Linux News*, August 27, 2018. <https://www.root.cz/clanky/telefony-s-androidem-lze-ovladnout-pres-usb-pomoci-at-prikazu/>
21. “У 11 производителей Android-смартфонов обнаружили уязвимость к АТ-командам” (Translation from Russian: “11 manufacturers of Android-smartphones found a vulnerability to AT-commands”.) *Tproger*, August 27, 2018. <https://tproger.ru/news/at-commands-deface-smartphones/>
22. “Smartphones From 11 OEMs Vulnerable to Attacks via Hidden AT Commands.” Catalin Cimpanu,

Bleeping Computer, August 25, 2018. <https://www.bleepingcomputer.com/news/security/smartphones-from-11-oems-vulnerable-to-attacks-via-hidden-at-commands/>

23. "Smartphone security risk compared to 'having a ghost user on your phone'." Jonathan Griffin, *University of Florida News*, August 22, 2018. <http://news.ufl.edu/articles/2018/08/smartphone-security-risk-compared-to-having-a-ghost-user-on-your-phone.php>
24. "Ransomware 'stopped' by new software." *BBC News*, July 2016. <http://www.bbc.com/news/technology-36772461>
25. "United States and Mozambique Host Cybersecurity and Cybercrime Workshop in Maputo for Lusophone Africa." *US Department of State*, September 2015. <http://www.state.gov/r/pa/prs/ps/2015/09/247088.htm>
26. "Researchers Find Security Flaws in Developing-World Money Apps." Jennifer Valentino-Devries. *Wall Street Journal*, August 2015. <http://blogs.wsj.com/digits/2015/08/11/researchers-find-security-flaws-in-developing-world-money-apps/>
27. "Hack could let browsers use cloud to carry out big attacks on the cheap." Dan Goodin, *Arstechnica*, November 2012. <http://arstechnica.com/security/2012/11/hack-could-let-browsers-use-cloud-to-carry-out-big-attacks-on-the-cheap/>

Other Coverage

28. "Largest water utility company in US targeted by cyberattack", Geoff Harris, *The National News Desk*, 8 October 2024. <https://thenationaldesk.com/news/americas-news-now/largest-water-utility-company-in-us-targeted-by-cyberattack-american-new-jersey-based-personal-information-control-system-security-billing-pause#>
29. "Cyberattacks on healthcare systems are on the rise, including here in Florida", Joe Mario Pedersen, *Central Florida Public Media*, 10 July 2024. <https://www.cfpublic.org/health/2024-07-10/cyberattacks-healthcare-systems-rise-florida>
30. "After uptick in scam calls, LCSO urges awareness of those impersonating law enforcement", Elena Barrera, *Tallahassee Democrat*, 15 June 2023. <https://www.tallahassee.com/story/news/2023/06/15/scam-calls-in-tallahassee-state-of-florida-imitate-law-enforcement/70321814007/>
31. "Voters in Two States Report Threatening 'Vote for Trump' Emails", Nick Corasanitti, Ben Decker, and Stephanie Saul, *The New York Times*, 20 October 2020. <https://www.nytimes.com/2020/10/20/us/politics/florida-alaska-trump-emails.html>
32. "What Would It Take to Shut Down the Entire Internet?" Daniel Kolitz, *Gizmodo*, 30 September 2019. <https://gizmodo.com/what-would-it-take-to-shut-down-the-entire-internet-1837984019>
33. "Devious Ransomware Frees You If You Infect Two Other People." Lily Hay Newman, *Wired*, 13 December 2016. <https://www.wired.com/2016/12/popcorn-time-ransomware/>
34. "UF experts: iPhone issue could set precedent." Christopher Curry and Dahlia Ghabour, *Gainesville Sun*, 26 February 2016. <http://www.gainesville.com/article/20160226/ARTICLES/160229743/-1/archive?Title=UF-experts-iPhone-issue-could-set-precedent>
35. "Biometric Security Comes To Your Smartphone." Mitch Kroner, *Think Out Loud, Oregon Pub-*

lic Broadcasting, 24 September 2013. <http://www.opb.org/radio/programs/thinkoutloud/segment/biometric-security-comes-to-your-smartphone/>

Previous Academic Appointments

Associate Professor, Department of Computer and Information Science and Engineering, University of Florida, Aug. 2014 - Aug. 2021

Associate Director of the Florida Institute for Cybersecurity Research. Previous co-director of the Southeastern Security for Enterprise and Infrastructure Center.

Assistant Professor, Department of Computer and Information Science, University of Oregon, Sep. 2010 - Aug. 2014

Research and teaching classes in systems security. Founder and leader of the Oregon Systems Infrastructure Research and Information Security Laboratory. Co-director of the Center for Cyber Security.

- **Leadership:** Organizer of Computer Security Day at the University of Oregon (2014, 2013, 2012, 2011, recipient of CAS program grant for three years), liaison to Oregon Engineering and Technology Council (2010-2012), faculty advisor to UO Security Club (2012-2014), faculty liaison to Women in Computer Science (2012-2013).
- **Committee Service:** University Committee on General Science Major (2014), Graduate Education Committee (2010-2012, 2014-present), Computing Resources Committee (2011-2012), Industrial Affairs Committee (2012-2014), Strategic Planning Committee (2013).

Research Assistant, Department of Computer Science, Pennsylvania State University, Jan. 2005 - Aug. 2010

- **Senior Personnel**, NSF HECURA: Collaborative Research: Secure Provenance in High-End Computing Systems, NSF (CCF), \$307,073, Aug. 2009 - present.
- Funded by NSF HECURA grant 0621429 from Aug. 2006 - Jul. 2010, investigating security of storage systems.
- Funded by NSF grant CNS-0335241 from Aug. 2005 - Aug. 2006, investigating BGP security solutions and large-scale simulation.

Lead Graduate Student, Systems and Internet Infrastructure Security (SIIS) Laboratory, Pennsylvania State University, Sep. 2007 - Dec. 2008

- Administrative and logistical lead student in the SIIS lab. Ran weekly lab meetings of 13 members, met with students individually for mentoring and development of leadership and research skills. Responsible for most daily operational activities in the lab.

Instructor, Department of Electrical Engineering, Pennsylvania State University, Jun.-Aug. 2006

- Instructor for *EE/CSE 458*, the senior undergraduate course on computer networking.

Guest Lecturer, Department of Computer Science, Pennsylvania State University, 2005-present

- *CSE 543 (Computer Security)*: presented lectures on cryptography and public key infrastructures.
- *CSE 597A (Advanced Topics in System Security)*: lectured on virtual machine security.
- *CSE 411 (Operating Systems)*: presented lectures on storage systems.
- *CSE 545 (Advanced Network Security)*: lectured on BGP security.

Teaching Assistant, Stern School of Business, New York University, Fall 2005

- Lectured, graded, and provided logistics for Computer and Network Security course offered for MBA students.

Teaching Assistant, Department of Computer Science and Engineering, Pennsylvania State University, Fall 2004

- Held lab hours and graded for Computer System Architecture course.

Graduate Research Assistant, Department of Computer Science, Columbia University, Oct. 2001 - May 2002

- Worked on SIP security, implementing authentication into the Panasonic PINTL JAIN SIP stack.

Teaching Assistant, Department of Computer Science, Queen's University, Fall 1998

- Held office hours and graded for Introduction to Computer Science course.

Industrial Experience

Co-Founder and Chief Operating Officer, CryptoDrop LLC, 2017-2019.

- Anti-ransomware startup based in Gainesville, Florida.

Research Intern, Symantec Research Labs, Mountain View, CA, Jun - Aug. 2009

- Examined host-based validation for portable storage devices, and implemented a prototype using embedded Linux.

Research Intern, Seagate Research, Pittsburgh, PA, May - Aug. 2008

- Developed security infrastructures for distributed storage in a home user environment, focussing on distributed access control mechanisms.

Research Intern, AT&T Labs - Research, Florham Park, NJ, Dec. 2003 - Aug. 2004

- Investigated security threats in BGP and created an overview of threats and currently deployed solutions. Developed cryptographic constructions allowing efficient security solutions and performed simulations based on trace data.

Technical Intern, Flarion Technologies, Bedminster, NJ, Summer 2002

- Implemented packet diversion and IP header modification program in BSD for mobile IP packet testing.

Research Scientist, Telcordia Technologies, Morristown, NJ, Sep. 2000 - Nov. 2001

- Built and maintained an HFC lab to emulate a cable plant; researched routing and service assurance methodologies for multiple service providers accessing common transport.

Technical Specialist, UUNET, Toronto, ON, May 1999 - Aug. 2000

- Monitored and troubleshoot intermediate and backbone connections across the UUNET Canadian network, as well as dealing with network security and web server issues.

Summer Intern, Royal Bank of Canada, Toronto, ON, Summer 1997, 1998

- Investigated financing opportunities for life science and high tech companies through financial and technical analysis; ported applications from mainframe to client-server environments.