UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

SECURE COMMUNICATION TECHNOLOGIES, LLC,
Patent Owner.

Case IPR2025-01181

Patent No. 11,334,918

DECLARATION OF MARK LANNING IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 11,334,918

TABLE OF CONTENTS

I. INTRODUCTION

1. My name is Mark Lanning and I am currently the President of Telecom Architects, Inc., and Reticle Consulting, LLC. I have been retained on behalf of Google LLC ("Google" or "Petitioner"), to provide my opinions on certain issues related to U.S. Patent No. 11,334,918 ("the '918 patent") in connection with the above-captioned inter partes review (IPR) proceeding. In particular, I have been asked to provide my insights, analysis, and opinions regarding whether claims 1-4, 8-20, 22-25, 27-29, and 31 of the '918 patent ("Challenged Claims") are obvious over the prior art references identified below.

2. The '918 patent is titled "EXCHANGING IDENTIFIERS BETWEEN WIRELESS COMMUNICATION TO DETERMINE FURTHER INFORMATION TO BE EXCHANGED OR FURTHER SERVICES TO BE PROVIDED," names as inventors James A. Proctor, Jr. and James Arthur Proctor, III, and is currently owned by Secure Communication Technologies, LLC. I have considered the '918 patent. I understand that the '918 patent has been provided as EX1001.

3. The file history of the '918 patent has been provided as EX1002. I have considered this file history, and I will refer to it as the "'918 File History" or by its exhibit number.

4. I understand that the '918 patent claims to be a continuation of many

patent applications (as shown on the first two pages of EX1001) and also claims priority to provisional application Nos. 61/095,359 (filed September 9, 2008) and 61/095,001 (filed September 8, 2008) ("'the Provisional Applications"). I have been asked to assume the Challenged Claims are entitled to the September 8, 2008 filing date for the purposes of rendering my opinions in this declaration.

5. My analysis and conclusions set forth in this declaration are based on my educational background and experiences in the field (*see* Section II). I am qualified to opine concerning what a person of ordinary skill in the art would have known and understood during that time. Before September 8, 2008, my level of skill in the art was at least that of a person of ordinary skill. I am qualified to opine concerning what a person of ordinary skill in the art would have known and understood at the time of the '918 patent's purported invention. My analysis and conclusions herein are from the perspective of a person of ordinary skill in the art as of September 8, 2008.

6. As part of my independent analysis for this declaration, I have considered the following: the background knowledge/technologies that were commonly known to persons of ordinary skill in this art during the time before the earliest claimed priority date for the '918 patent; my own knowledge and experiences gained from my work experience in the field of the '918 patent and related disciplines; and my experience in working with others involved in this field

and related disciplines.

7. I have considered the following non-exhaustive list of references in preparing my declaration. I have been instructed to assume that each of these references qualifies as prior art.

8. U.S. Patent Application Publication No. 2005/0250552 to Eagle et al., titled "COMBINED SHORT RANGE RADIO NETWORK AND CELLULAR TELEPHONE NETWORK FOR INTERPERSONAL COMMUNICATIONS" filed on May 5, 2005 and published on November 10, 2005. I understand that a copy of this reference has been designated as Exhibit EX1005. Throughout my declaration, references to "Eagle" are to Exhibit EX1005.

9. U.S. Patent Application Publication No. 2010/0138481 to Behrens, titled "DEVICE AND METHOD FOR ESTABLISHING SOCIAL NETWORKS THROUGH THE USE OF WIRELESS TECHNOLOGY" filed on April 30, 2008 and published on June 3, 2010. I understand that a copy of this reference has been designated as EX1006. Throughout my declaration, references to "Behrens" are to EX1006.

10. U.S. Patent No. 7,590,086 to Olkkonen et al., titled "AD HOC NETWORK DISCOVERY MENU," filed on November 3, 2004 and issued on September 15, 2009. I understand that a copy of this reference has been designated as Exhibit EX1007. Throughout my declaration, references to "Olkkonen" are to

EX1007.

11. U.S. Patent Application Publication No. 2004/0243519 to Perttila et al., titled "PROMPTED ELECTRONIC MOBILE-SERVICE INFORMATION COMMUNICATIONS WITH VALIDATION" filed on June 2, 2003 and published on December 2, 2004. I understand that a copy of this reference has been designated as EX1037. Throughout my declaration, references to "Perttila" are to EX1037.

12. U.S. Patent Application Publication No. 2007/0264991 to Jones et al., titled "SERVICES NEAR ME: DISCOVERING AND CONNECTING TO AVAILABLE WIRELESS SERVICES UTILIZING PROXIMITY DISCOVERY" filed on May 15, 2006 and published on November 15, 2007. I understand that a copy of this reference has been designated as EX1038. Throughout my declaration, references to "Jones" are to EX1038.

13. I am being compensated by Google at my standard hourly consulting rate of $550 for my time on this matter. My compensation is not dependent on the outcome of this proceeding or any other proceeding between the parties.

14. In forming my opinions, I relied on the documents cited in this declaration and the documents identified in the table below. These documents comprise patents, file histories, printed publications, and other related documents. As I discuss below, each document is a type that experts in my field would have

reasonably relied upon when forming their opinions. Further, a person of ordinary skill in the art ("POSITA") would have had access to each document either through the applicable patent offices and/or well-known libraries, conferences, or publications in the field. My opinions are also based upon my personal and professional experience.

Exhibit	Description
1001	U.S. Patent No. 11,334,918
1002	Prosecution History of U.S. Patent No. 11,334,918
1005	U.S. Patent Application No. 2005/0250552 ("Eagle")
1006	U.S. Patent Application Publication No. 2010/0138481 ("Behrens")
1007	U.S. Patent No. 7,590,086 ("Olkkonen")
1008	Bluetooth Special Interest Group, Bluetooth Core Specification Version 2.1 + EDR (July 26, 2007)
1009	Bluetooth Special Interest Group, Assigned Numbers (December 14, 2002) (https://web.archive.org/web/20021214114356/http://www.bluetooth.org/assigned-numbers/baseband.htm)
1010	U.S. Patent Application Publication No. 2002/0131445
1011	U.S. Patent Application Publication No. 2002/0174364
1012	U.S. Patent Application Publication No. 2005/0164717
1013	U.S. Patent Application Publication No. 2006/0165100
1035	Apple Inc., iPhone 3G Technical Specifications (https://web.archive.org/web/20080725084414/http://www.apple.com/iphone/specs.html)
1036	Apple Inc., iPhone User Guide for iPhone OS 3.1 Software (https://cdsassets.apple.com/live/6GJYWVAV/user/ma616_iphone_ios3_1_user_guide.pdf)
1037	U.S. Patent Application Publication No. 2004/0243519 ("Perttila")
1038	U.S. Patent Application Publication No. 2007/0264991 ("Jones")
1039	U.S. Patent No. 8,321,497 ("Steiner")
1040	U.S. Patent Application Publication No. 2007/0219875 ("Toulotte")

II. QUALIFICATIONS

15. I am qualified by education and experience to testify as an expert in the field of telecommunications including circuit-switched networks, multiple generations of cellular networks, and packet-switched networks. The following overview of my background pertains to my qualifications for providing expert testimony in this matter.

16. I am currently the president of two consulting companies: Telecom Architects, Inc. and Reticle Consulting, LLC. Telecom Architects provides consulting services to fixed and wireless telecom service providers and their equipment suppliers. I have been President of Telecom Architects since 1999.

17. I have over 40 years of experience working in the telecommunications industry that began in the U.S. Army Signal Corp. My experience relevant to this case includes my work as an architect of various telecommunications systems and my work developing equipment used in telecommunications systems. This experience includes extensive design, implementation and testing work on the wireless interface functionality (between the base station and mobile phones) for multiple generations of cellular standards.

18. I received a B.S. in Computer Science from Southern Methodist University (SMU) in 1983.

19. DSC, now a part of Alcatel, hired me in 1983 where I was a software

development manager on the team responsible for updating DSC's PSTN telephone switch into a Mobile Switching Center (MSC) for Motorola to sell as a part of their cellular product offering in the U.S. and many other countries.

20. In 1991, I began working as a consultant to Motorola for its "SuperCell" base station product and as a consultant to British Telecom to upgrade its current analog cellular network, and I was one of the network architects responsible for the design and rollout of its Global System for Mobile Communications (GSM) network known as Cellnet. Beginning in the early 1990s, I was responsible for implementation of the SMS service, including working with suppliers of the SMS Center (SMSC), Mobile Switching Centers (MSCs) and cellular phones to define and roll out the functionality that was to be provided.

21. I was personally involved with Nokia, Ericsson, Motorola and other equipment suppliers in this effort.

22. Since 1995, I have also provided second generation (2G) and third generation (3G) Code Division Multiple Access ("CDMA") network architecture and equipment design and implementation consulting services to companies such as Sprint, Nextel, Nokia, and Ericsson. While consulting to Nextel, which has since become part of Sprint, as one of the network architects for its iDEN network, one of my responsibilities was to define the network and mobile phone functionality required to support MMS and advanced data communications

capability.

23. In addition to the above, since at least 2007, I have experience analyzing Bluetooth functionality, designs and implementations related to smart phones, pads, watches, computers and other devices that use Bluetooth functionality to connect with these devices, for example, earpieces, headsets and music players. Specifically, I have performed detailed Bluetooth analysis on Apple iPhones, iPads, watches, Mac computers and at least Samsung's Android smart phones.

24. In addition to my cellular experience listed above, for at least the past ten years, I have kept up to date my knowledge of the present-day 3G, 4G, and 5G cellular network and wireless standards and their associated equipment and protocols. I have done this through my study of each new release of these standards, technical books and trade publications as well as my expert work in legal cases, which has involved evaluating the functionality of many different types of network equipment, mobile devices, and baseband chipsets. I have also evaluated thousands of cellular technology patents, and most of these were for cellular phone and/or base station functionality.

25. I am a member of the Institute of Electrical and Electronics Engineers (IEEE), including the IEEE Standards Association. I am also a member of the Association for Computing Machinery (ACM). While employed at DSC, I was a

member of the ANSI T1 and T1X1 standard groups responsible for the definition and standardization of the Advanced Intelligent Network (AIN) and Signaling System 7 (SS7) protocol.

26. A detailed record of my professional qualifications, including a list of publications, awards, and professional activities, is set forth in my curriculum vitae submitted with this report as EX1004.

III. LEGAL UNDERSTANDINGS

A. My Understanding of Claim Construction

27. I am not an attorney and offer no legal opinions, but in the course of my work, I have had experience studying and analyzing patents and patent claims from the perspective of a person skilled in the art.

28. I have been informed that patent claims are construed from the viewpoint of a person of ordinary skill in the art of the patent at the time of the invention (a "POSITA"). I have been informed that patent claims generally should be interpreted consistent with their plain and ordinary meaning as understood by a person of ordinary skill in the art in the relevant time period (i.e., at the time of the purported invention, or the so called "effective filing date" of the patent application), after reviewing the patent claim language, the specification, and the prosecution history (i.e., the intrinsic record).

29. I have further been informed that a person of ordinary skill in the art

must read the claim terms in the context of the claim itself, as well as in the context of the entire patent specification. I understand that in the specification and prosecution history, the patentee may specifically define a claim term in a way that differs from the plain and ordinary meaning. I understand that the prosecution history of the patent is a record of the proceedings before the U.S. Patent and Trademark Office and may contain explicit representations or definitions made during prosecution that affect the scope of the patent claims. I understand that an applicant may, during the course of prosecuting the patent application, limit the scope of the claims to overcome prior art or to overcome an examiner's rejection, by clearly and unambiguously arguing to overcome or distinguish a prior art reference, or clearly and unambiguously disavowing claim coverage.

30. In interpreting the meaning of the claim language, I understand that a person of ordinary skill in the art may also consider "extrinsic" evidence, including expert testimony, inventor testimony, dictionaries, technical treatises, other patents, and scholarly publications. I understand this evidence is considered to ensure that a claim is construed in a way that is consistent with the understanding of those of ordinary skill in the art at the time of the claimed invention. For example, this can be useful for a technical term whose meaning may differ from its ordinary English meaning. I understand that extrinsic evidence may not be relied on if it contradicts or varies the meaning of claim language provided by the intrinsic evidence,

particularly if the applicant has explicitly defined a term in the intrinsic record.

B. My Understanding of Anticipation

31. I understand that a patent claim is invalid as "anticipated" if all the limitations of the claim are present, either expressly or inherently, in a single prior art publication or patent.

32. I also understand that a prior art reference can disclose a claimed feature because the feature is expressly described or because the feature is inherent in the disclosure. I understand that something is inherent in a prior art reference if the missing descriptive matter must necessarily be present, not merely probably or possibly present, and it would be so recognized by a person of ordinary skill in the art as of the priority date of the patent. I understand that it is acceptable to examine evidence outside of the prior art reference (i.e., extrinsic evidence) in determining whether a feature, while not expressly discussed in the reference, is necessarily present in it.

33. I have further been informed that where a reference discloses multiple embodiments, the reference should not be limited to a preferred embodiment. Instead, each disclosed embodiment may anticipate.

34. Moreover, I have been informed that as part of an anticipation analysis, it is proper to take into account not only specific teachings of the reference, but also the inferences that one skilled in the art would reasonably be

expected to draw therefrom. A reference can anticipate a claim even if it does not expressly spell out all the limitations arranged or combined as in the claim, if a person of skill in the art, reading the reference, would at once envisage the claimed arrangement or combination.

C. My Understanding of Obviousness

35. I understand that a claim may be invalid if the subject matter described by the claim as a whole would have been obvious to a hypothetical person of ordinary skill in the art in view of a prior art reference or in view of a combination of references at the time the claimed invention was made. Therefore, I understand that obviousness is determined from the perspective of a hypothetical person of ordinary skill in the art and that the asserted claims of the patent should be read from the point of view of such a person at the time the claimed invention was made. I further understand that a hypothetical person of ordinary skill in the art is assumed to know and to have all relevant prior art in the field of endeavor covered by the patent in suit.

36. I have been informed that there are two criteria for determining whether prior art is analogous and thus can be considered prior art: (1) whether the art is from the same field of endeavor, regardless of the problem addressed, and (2) if the reference is not within the field of the patentee's endeavor, whether the reference still is reasonably pertinent to the particular problem with which the

patentee is involved. I have also been informed that the field of endeavor of a patent is not limited to the specific point of novelty, the narrowest possible conception of the field, or the particular focus within a given field. I have also been informed that a reference is reasonably pertinent if, even though it may be in a different field from that of the patentee's endeavor, it is one which, because of the matter with which it deals, logically would have commended itself to a patentee's attention in considering their problem.

37. I have also been advised that an analysis of whether a claimed invention would have been obvious should be considered in light of the scope and content of the prior art, the differences (if any) between the prior art and the claimed invention, and the level of ordinary skill in the pertinent art involved. I understand as well that a prior art reference should be viewed as a whole.

38. I have also been advised that in considering whether a claimed invention would have been obvious over a combination of prior art references, I may assess whether there are apparent reasons to combine known elements in the prior art in the manner claimed in view of interrelated teachings of multiple prior art references, the effects of demands known to the design community or present in the marketplace, and/or the background knowledge possessed by a person of ordinary skill in the art. I understand that other principles may be relied on in evaluating whether a claimed invention would have been obvious, and that these

principles include the following:

- A combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results;
- When a device or technology is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or in a different one, so that if a person of ordinary skill can implement a predictable variation, the variation is likely obvious;
- If a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond their skill;
- An explicit or implicit teaching, suggestion, or motivation to combine two prior art references to form the claimed combination may demonstrate obviousness, but proof of obviousness does not depend on or require showing a teaching, suggestion, or motivation to combine;
- Market demand, rather than scientific literature, can drive design trends and may show obviousness;
- In determining whether the subject matter of a patent claim would have been obvious, neither the particular motivation nor the avowed purpose of the named inventor controls whether the claim is obvious;
- One of the ways in which a patent's subject can be proved obvious is by noting that there existed at the time of invention a known problem for which there was an obvious solution encompassed by the patent's claims;
- Any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed;
- "Common sense" teaches that familiar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle;

- A person of ordinary skill in the art is also a person of ordinary creativity, and is not an automaton;
- A patent claim can be proved obvious by showing that the claimed combination of elements was "obvious to try," particularly when there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions such that a person of ordinary skill in the art would have had good reason to pursue the known options within his or her technical grasp; and
- One should be cautious of using hindsight in evaluating whether a claimed invention would have been obvious.

39. I further understand that, in deciding as to whether the claimed invention would have been obvious to a person of ordinary skill, the Board may consider certain objective factors if they are present, such as: commercial success of products practicing the claimed invention; long-felt but unsolved need; teaching away; unexpected results; copying; and praise by others in the field. These factors are generally referred to as "secondary considerations" or "objective indicia" of nonobviousness. I understand, however, that for such objective evidence to be relevant to the obviousness of a claim, there must be a causal relationship (called a "nexus") between the claim and the evidence, and that this nexus must be based on a novel element of the claim rather than something in the prior art. I also understand that even when they are present, secondary considerations may be unable to overcome primary evidence of obviousness (such as motivation to combine with predictable results) that is sufficiently strong.

IV. TECHNOLOGY BACKGROUND AND STATE OF THE ART

A. The ’918 Patent’s Short Range or Bluetooth Wireless Protocol

40. The claims of the ’918 patent require a “short range transmissions” that include, for example, a “Bluetooth BD_ADDR.” Therefore, a POSITA would have recognized that the “short range transmissions” can be related to the Bluetooth protocol.

41. The Bluetooth protocol is not novel to the disclosures or claims of the ’918 patent. Multiple versions of the Bluetooth specifications were defined and were publicly available before the ’918 patent.

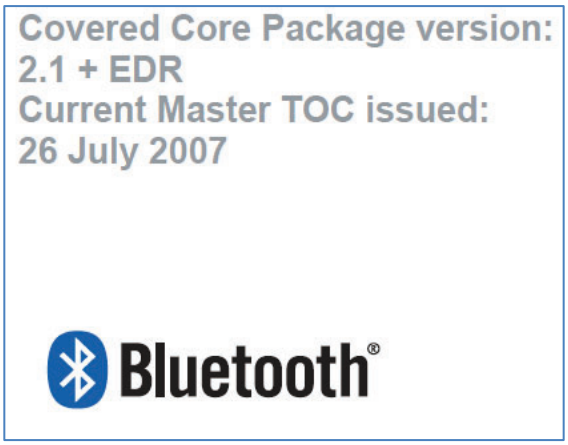
B. The Bluetooth Standard

42. Specifically, the table and text below shows the Bluetooth specifications that were defined and that were publicly available before the September 8, 2008, Priority Date of the ’918 patent. Specifically, the first version of the Bluetooth “Baseband and Link Manager Protocol” (version number 0.7) was defined on October 19, 1998 and the “first version of the Bluetooth Specification published on the public web site” (version 1.0a) was on July 26, 1999.

1.0a	July 26 1999	The first version of the Bluetooth Specification published on the public web site. Added part: Bluetooth Compliance Requirements.
1.0 draft	July 5th 1999	The following parts were added: Service Discovery Protocol (SDP), Telephony Control Specification (TCS), Bluetooth Assigned Numbers (appendix) and Message Sequence Charts (appendix)
0.9	April l30 1999	The following parts were added: IrDA Interoperability, HCI RS232 Transport Layer, HCI UART Transport Layer and Test Mode
0.8	Jan 21 1999	The following parts were added: Radio Specification, L2CAP, RFCOMM, HCI & HCI USB Transport Layer
0.7	Oct 19 1998	This first version only included Baseband and Link Manager Protocol

EX1008, p. 47 (highlighting in original).

43. Multiple updated and enhanced versions were also made publicly available after version 1.0a including the "Bluetooth Core V2.1 + EDR" specification, July 26, 2007 ("Bluetooth Specification") that I am using to describe the Bluetooth functionality in this declaration. EX1008.



EX1008, p. 1.

a. Many Technology Companies and Engineers Are Involved with Defining the Bluetooth Specification

44. Many of the leading technology companies and their representatives were involved with the definition of the Bluetooth standards and compliance requirements as listed on 24 pages of this specification. EX1008, pp. 49-72. Based on at least the number of specifications that were published, the number of technical companies involved in defining and developing the functionality and the number of subject matter experts, and based on my own personal experience, the development and functionality of the Bluetooth functionality were of high interest to the communications industry and would have been well known by a person of ordinary skill in the art.

b. Bluetooth General Description

45. The Bluetooth Specification provides the following general description. I note that it is characterized as a "short-range communication system" that uses a "protocol stack," which is related to how devices communicate in the '918 patent and in the prior art.

BLUETOOTH SPECIFICATION Version 2.1 + EDR [vol 1] page 13 of 96

Architecture

Bluetooth

1 GENERAL DESCRIPTION

Bluetooth wireless technology is a short-range communications system intended to replace the cable(s) connecting portable and/or fixed electronic devices. The key features of Bluetooth wireless technology are robustness, low power, and low cost. Many features of the core specification are optional, allowing product differentiation.

The Bluetooth core system consists of an RF transceiver, baseband, and protocol stack. The system offers services that enable the connection of devices and the exchange of a variety of classes of data between these devices.

EX1008, p. 87.

c. Overview of Operation

46. The Bluetooth Specification provides many Radio Frequency (RF) and protocol requirements that are beyond the scope of this declaration. I have highlighted some of the details in the passages below that are relevant.

> The Bluetooth RF (physical layer) operates in the unlicensed ISM band at 2.4 GHz. The system employs a frequency hop transceiver to combat interference and fading and provides many FHSS carriers. RF operation uses a shaped, binary frequency modulation to minimize transceiver complexity. The symbol rate is 1 Megasymbol per second (Ms/s) supporting the bit rate of 1 Megabit per second (Mb/s) or, with Enhanced Data Rate, a gross air bit rate of 2 or 3Mb/s. These modes are known as Basic Rate and Enhanced Data Rate respectively.
>
> **During typical operation a physical radio channel is shared by a group of devices that are synchronized to a common clock and**

frequency hopping pattern. One device provides the synchronization reference and is known as the master. All other devices are known as slaves. A group of devices synchronized in this fashion form a piconet. This is the fundamental form of communication in the Bluetooth wireless technology.

Devices in a piconet use a specific frequency hopping pattern, which is algorithmically determined by certain fields in the Bluetooth address and clock of the master. The basic hopping pattern is a pseudo-random ordering of the 79 frequencies in the ISM band. The hopping pattern may be adapted to exclude a portion of the frequencies that are used by interfering devices. The adaptive hopping technique improves Bluetooth co-existence with static (non-hopping) ISM systems when these are co-located.

The physical channel is sub-divided into time units known as slots. Data is transmitted between Bluetooth devices in packets, that are positioned in these slots. When circumstances permit, a number of consecutive slots may be allocated to a single packet. Frequency hopping takes place between the transmission or reception of packets. Bluetooth technology provides the effect of full duplex transmission through the use of a Time-Division Duplex (TDD) scheme.

Above the physical channel there is a layering of links and channels and associated control protocols. The hierarchy of channels and links from the physical channel upwards is physical channel, physical link, logical transport, logical link and L2CAP channel. These are discussed in more detail in Section 3.3 on page 33 to Section 3.6 on page 49 but are introduced here to aid the understanding of the

remainder of this section.

Within a physical channel, a physical link is formed between any two devices that transmit packets in either direction between them. In a piconet physical channel there are restrictions on which devices may form a physical link. There is a physical link between each slave and the master. Physical links are not formed directly between the slaves in a piconet.

The physical link is used as a transport for one or more logical links that support unicast synchronous, asynchronous and isochronous traffic, and broadcast traffic. Traffic on logical links is multiplexed onto the physical link by occupying slots assigned by a scheduling function in the resource manager.

A control protocol for the baseband and physical layers is carried over logical links in addition to user data. This is the link manager protocol (LMP). **Devices that are active in a piconet have a default asynchronous connection-oriented logical transport that is used to transport the LMP protocol signaling.** For historical reasons this is known as the ACL logical transport. **The default ACL logical transport is the one that is created whenever a device joins a piconet**. Additional logical transports may be created to transport synchronous data streams when this is required.

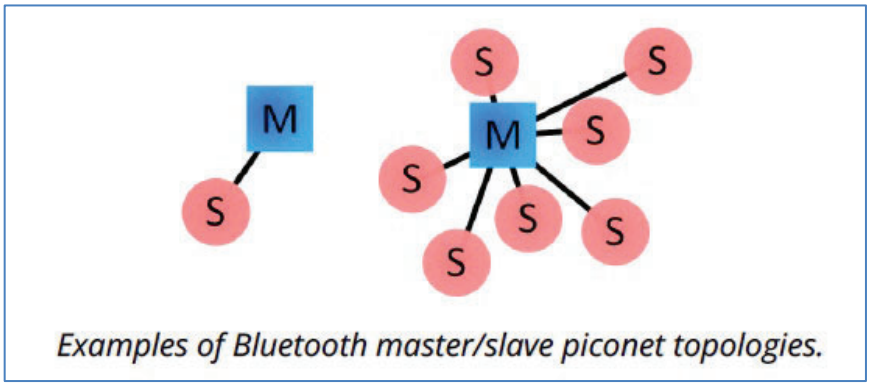
The Link Manager function uses LMP to control the operation of devices in the piconet and provide services to manage the lower architectural layers (radio layer and baseband layer). The LMP protocol is only carried on the default ACL logical transport and the default broadcast logical transport.

> Above the baseband layer the L2CAP layer provides a channel-based abstraction to applications and services. It carries out segmentation and reassembly of application data and multiplexing and de-multiplexing of multiple channels over a shared logical link. L2CAP has a protocol control channel that is carried over the default ACL logical transport. Application data submitted to the L2CAP protocol may be carried on any logical link that supports the L2CAP protocol.

EX1008, pp. 87-88.

d. Topology and Communications

47. As described in the section directly above, a Bluetooth network is referred to as a piconet. A piconet uses a star topology and has a master device and one to a maximum of seven slave devices as shown by the basic diagram below.



Examples of Bluetooth master/slave piconet topologies.

(image from https://learn.sparkfun.com/tutorials/bluetooth-basics)

48. The Bluetooth Specification defines the same two topologies as the basic diagram above as "a" and "b" below. It also defines a larger and more complex network topology where one or more piconets can be interconnected to

form a scatternet as shown by "c" below.

Piconets that have common devices are called a *scatternet,* see (c) in Figure 1.1 on page 59. Each piconet only has a single master, however, slaves can participate in different piconets on a time-division multiplex basis. In addition, a master in one piconet can be a slave in other piconets. Piconets shall not be frequency synchronized and each piconet has its own hopping sequence.

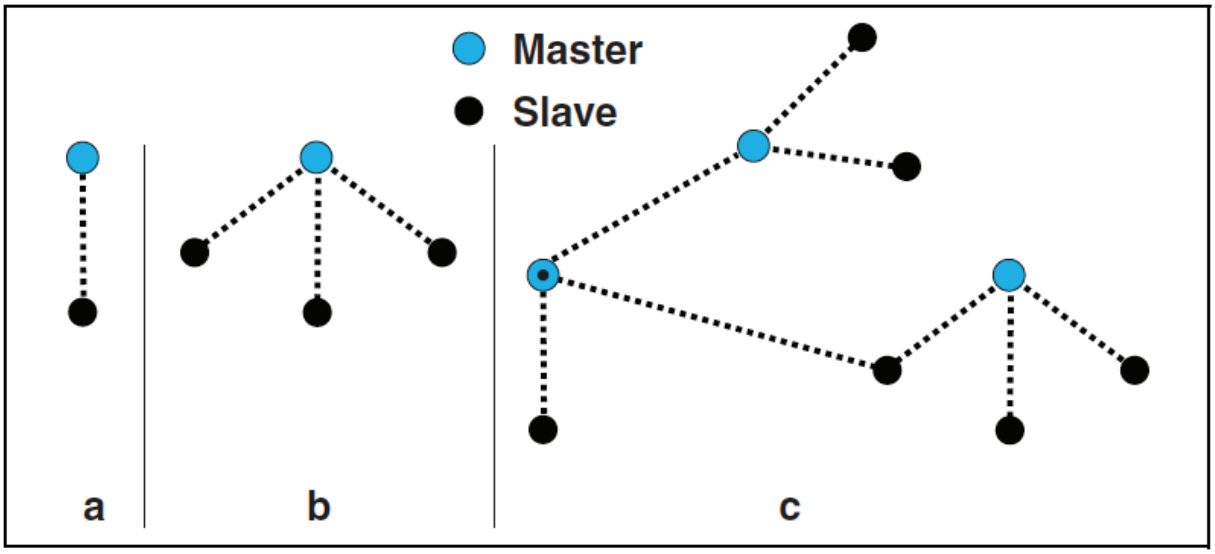


Figure 1.1: Piconets with a single slave operation (a), a multi-slave operation (b) and a scatternet operation (c).

EX1008, p. 229.
See also EX1008, pp. 124-125.

e. Bluetooth Operational Procedures and Modes

49. Bluetooth Devices can operate in multiple modes and there are many operational procedures that are used. However, the two relevant modes for this declaration are the (1) Inquiry and (2) Paging and Connection Mode, which are described below.

i) *Inquiry (Discovering) Procedure*

50. Basically, the Inquiry procedure is used for Bluetooth devices to

discover other devices that are operating in their area.[1] The Bluetooth Specification describes the Inquiry procedure with at least the following passage.

> "Bluetooth devices use the inquiry procedure to discover nearby devices, or to be discovered by devices in their locality.
>
> The inquiry procedure is asymmetrical. A Bluetooth device that tries to find other nearby devices is known as an **inquiring device and actively sends inquiry requests**. Bluetooth devices that are available to be found are known as discoverable devices and listen for these inquiry requests and send responses. The inquiry procedure uses a special physical channel for the inquiry requests and responses."

EX1008, p. 126.

ii) ***The Inquiry Response Message Contains the Device Address, Class of Device and Extended Response Information***

51. As shown below, inquiry response messages contain a Bluetooth device address, Class of Device information, and extended inquiry response information.

[1] The typical indoor range for Bluetooth devices is about 10 meters (33 feet) and can extend up to 100 meters (330 feet) in optimal outdoor conditions.

6.1 GENERAL INQUIRY

6.1.1 Purpose

The purpose of the general inquiry procedure is to provide the initiator with the Bluetooth device address, clock, Class of Device, page scan mode, and extended inquiry response information of general discoverable devices (i.e. devices that are in range with regard to the initiator and are set to scan for inquiry messages with the General Inquiry Access Code). Also devices in limited discoverable mode will be discovered using general inquiry.

The general inquiry should be used by devices that need to discover devices that are made discoverable continuously or for no specific condition.

EX1008, p. 1288.

6.1.3 Description

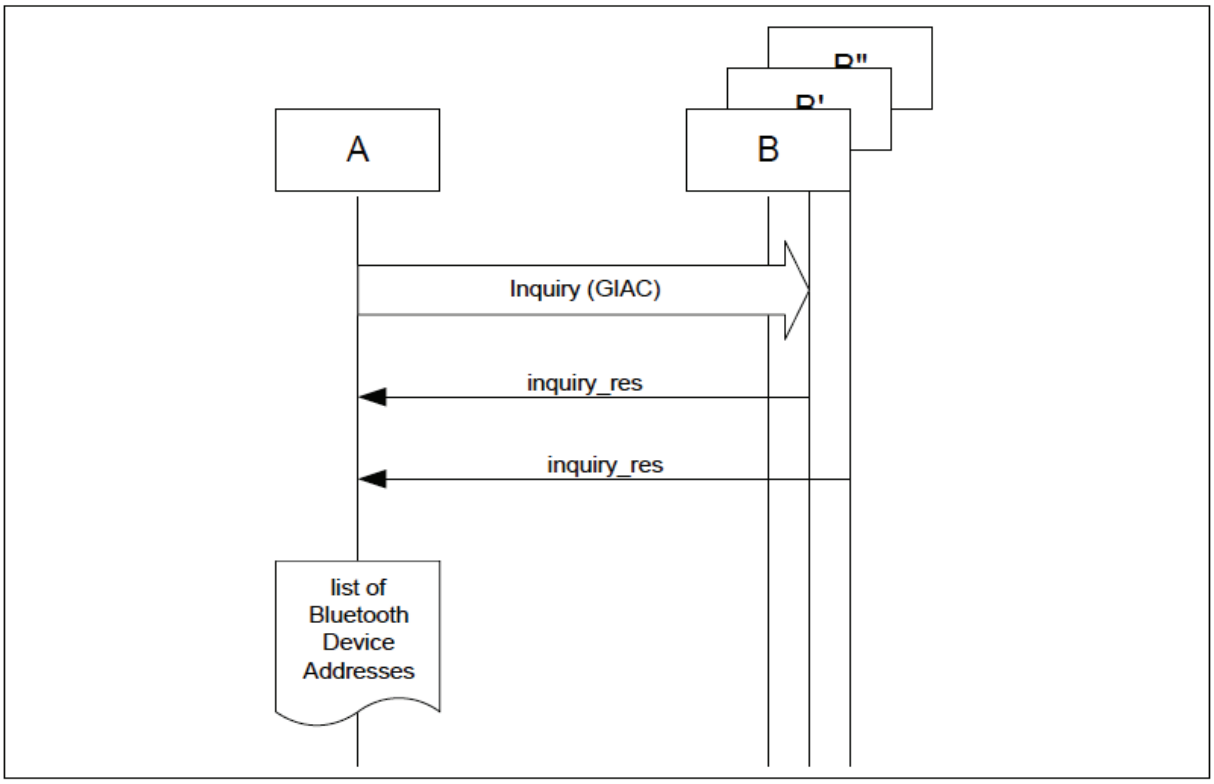


Figure 6.1: General inquiry ,where B is a device in non-discoverable mode, B´ is a device in limited discoverable mode and B" is a device in general discoverable mode. (Note that all discoverable devices are discovered using general inquiry, independent of which discoverable mode they are in.)

EX1008, p. 1288.

52. This information is included in a frequency hop synchronization (FHS) packet that is transmitted for inquiry responses and that facilitates frequency hop synchronization between devices (so the devices align their transmitting and receiving frequencies). In addition to clock information, FHS packets include fields for the device address (Bluetooth device address, BD_ADDR, separated into

lower, upper, and non-significant address parts (LAP, UAP, NAP), class of device information, and bits indicating that extended inquiry response (EIR) follows. As I discuss further below, the EIR includes additional fields for names, service classes, and more.

6.5.1.4 FHS packet

The FHS packet is a special control packet containing, among other things, the Bluetooth device address and the clock of the sender. The payload contains 144 information bits plus a 16-bit CRC code. The payload is coded with a rate 2/3 FEC with a gross payload length of 240 bits.

Figure 6.9 on page 113 illustrates the format and contents of the FHS payload. The payload consists of eleven fields. The FHS packet is used in page master response, inquiry response and in role switch.

The FHS packet contains real-time clock information. This clock information shall be updated before each retransmission. The retransmission of the FHS payload is different than retransmissions of ordinary data payloads where the same payload is used for each retransmission. The FHS packet is used for frequency hop synchronization before the piconet channel has been established, or when an existing piconet changes to a new piconet.

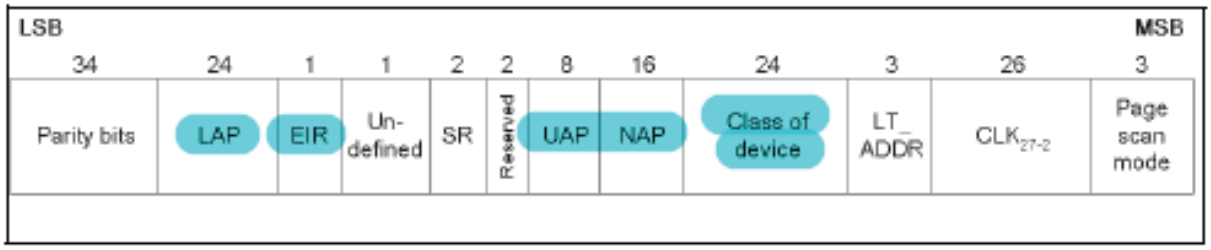


Figure 6.9: Format of the FHS payload.

Each field is described in more detail below:

Parity bits	This 34-bit field contains the parity bits that form the first part of the sync word of the access code of the device that sends the FHS packet. These bits are derived from the LAP as described in Section 1.2 on page 62.
LAP	This 24-bit field shall contain the lower address part of the device that sends the FHS packet.
EIR	This bit shall indicate that an extended inquiry response packet may follow. See Section 8.4.3 on page 158.
Undefined	This 1-bit field is reserved for future use and shall be set to zero.
SR	This 2-bit field is the scan repetition field and indicates the interval between two consecutive page scan windows, see also Table 6.4 and Table 8.1 on page 147
Reserved	This 2-bit field shall be set to 10.
UAP	This 8-bit field shall contain the upper address part of the device that sends the FHS packet.
NAP	This 16-bit field shall contain the non-significant address part of the device that sends the FHS packet (see also Section 1.2 on page 62 for LAP, UAP, and NAP).
Class of device	This 24-bit field shall contain the class of device of the device that sends the FHS packet. The field is defined in Bluetooth Assigned Numbers.
LT_ADDR	This 3-bit field shall contain the logical transport address the recipient shall use if the FHS packet is used at connection setup or role switch. A slave responding to a master or a device responding to an inquiry request message shall include an all-zero LT_ADDR field if it sends the FHS packet.
CLK_{27-2}	This 26-bit field shall contain the value of the native clock of the device that sends the FHS packet, sampled at the beginning of the transmission of the access code of this FHS packet. This clock value has a resolution of 1.25ms (two-slot interval). For each new transmission, this field is updated so that it accurately reflects the real-time clock value.
Page scan mode	This 3-bit field shall indicate which scan mode is used by default by the sender of the FHS packet. The interpretation of the page scan mode is illustrated in Table 6.5.

Table 6.3: Description of the FHS payload

EX1008, pp. 283-284.

iii) *The Bluetooth Device Address Provided in an Inquiry Response Message is the Same as a MAC Address*

53. The Bluetooth device address (BD_ADDR) provided in an inquiry

response message is a unique identifier for the responding device and is similar to a unique MAC address used for a Wi-Fi device. Both are a 48-bit value.

BLUETOOTH SPECIFICATION Version 2.1 + EDR [vol 2] page 62 of 906

Baseband Specification

1.2 BLUETOOTH DEVICE ADDRESSING

Each Bluetooth device shall be allocated a unique 48-bit Bluetooth device address (BD_ADDR). This address shall be obtained from the IEEE Registration Authority. The address is divided into the following three fields:

- LAP field: lower address part consisting of 24 bits
- UAP field: upper address part consisting of 8 bits
- NAP field: non-significant address part consisting of 16 bits

The LAP and UAP form the significant part of the BD_ADDR. The bit pattern in Figure 1.5 is an example BD_ADDR.

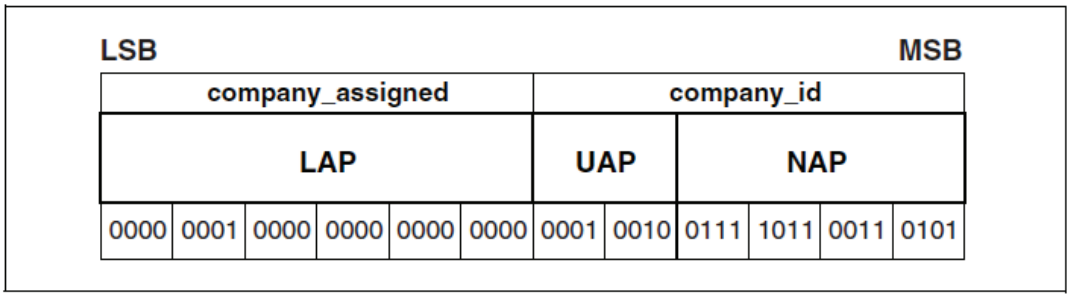


Figure 1.5: Format of BD_ADDR.

EX1008, p. 232.

iv) *The Class of Device Information Field in the Inquiry Response Defines the Type of Bluetooth Device and the Services it Offers*

54. The class of device information receiving in an inquiry response includes Bluetooth Device Class and Bluetooth Service Type information defining the type of Bluetooth device that is responding and its supported services.

Class of device	This 24-bit field shall contain the class of device of the device that sends the FHS packet. The field is defined in Bluetooth Assigned Numbers.

EX1008, p. 284 (blue text is in original).

6.25 CLASS OF DEVICE

The Class_of_Device parameter is used to indicate the capabilities of the local device to other devices.

Value	Parameter Description
0xXXXXXX	Class of Device for the device.

EX1008, p. 580.

3.2.4 Class of Device

3.2.4.1 Definition

Class of device is a parameter received during the device discovery procedure, indicating the type of device and which types of service that are supported.

3.2.4.2 Term on user interface level

The information within the Class of Device parameter should be referred to as 'Bluetooth Device Class' (i.e. the major and minor device class fields) and 'Bluetooth Service Type' (i.e. the service class field). The terms for the defined Bluetooth Device Types and Bluetooth Service Types are defined in [12].

When using a mix of information found in the Bluetooth Device Class and the Bluetooth Service Type, the term 'Bluetooth Device Type' should be used.

3.2.4.3 Representation

The Class of device is a bit field and is defined in [12]. The UI-level representation of the information in the Class of device is implementation specific.

EX1008, pp. 1259-1260.

55. Examples of Major Service Classes and Major Device Classes are shown below. A 2002 version of the Bluetooth Assigned Numbers is shown below, and while the Assigned Numbers list is a living document that changes over time, from 2002 to 2008 to 2025, its general usage and format has remained the same.

1.2 THE CLASS OF DEVICE/SERVICE FIELD

The Class of Device/Service (CoD) field has a variable format. The format is indicated using the 'Format Type field' within the CoD. The length of the Format Type field is variable and ends with two bits different from '11'. The version field starts at the least significant bit of the CoD and may extend upwards.

In the 'format #1' of the CoD (Format Type field = 00), 11 bits are assigned as a bit-mask (multiple bits can be set) each bit corresponding to a high level generic category of service class. Currently 7 categories are defined. These are primarily of a 'public service' nature. The remaining 11 bits are used to indicate device type category and other device-specific characteristics.

Any reserved but otherwise unassigned bits, such as in the Major Service Class field, should be set to 0.

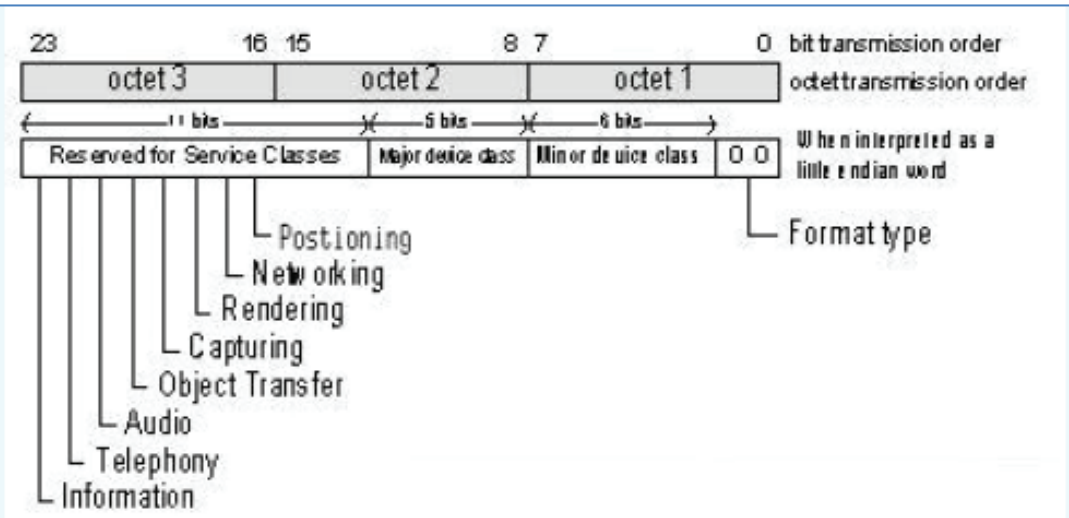


Figure 1.2: The Class of Device/Service field (first format type). Please note the order in which the octets are sent on the air and stored in memory. Bit number 0 is sent first on the air.

1.2.1 MAJOR SERVICE CLASSES

Bit no	Major Service Class
13	Limited Discoverable Mode [Ref #1]
14	(reserved)
15	(reserved)
16	Positioning (Location identification)
17	Networking (LAN, Ad hoc, ...)
18	Rendering (Printing, Speaker, ...)
19	Capturing (Scanner, Microphone, ...)
20	Object Transfer (v-Inbox, v-Folder, ...)
21	Audio (Speaker, Microphone, Headset service, ...)
22	Telephony (Cordless telephony, Modem, Headset service, ...)
23	Information (WEB-server, WAP-server, ...)

TABLE 1.2: MAJOR SERVICE CLASSES

[Ref #1 As defined in See Generic Access Profile, Bluetooth SIG]

1.2.2 MAJOR DEVICE CLASSES

The Major Class segment is the highest level of granularity for defining a Bluetooth Device. The main function of a device is used to determine the major class grouping. There are 32 different possible major classes. The assignment of this Major Class field is defined in Table 1.3.

12	11	10	9	8	Major Device Class
0	0	0	0	0	Miscellaneous [Ref #2]
0	0	0	0	1	Computer (desktop,notebook, PDA, organizers, ...)
0	0	0	1	0	Phone (cellular, cordless, payphone, modem, ...)
0	0	0	1	1	LAN /Network Access point
0	0	1	0	0	Audio/Video (headset,speaker,stereo, video display, vcr.....
0	0	1	0	1	Peripheral (mouse, joystick, keyboards, ...)
0	0	1	1	0	Imaging (printing, scanner, camera, display, ...)
1	1	1	1	1	Uncategorized, specific device code not specified
X	X	X	X	X	All other values reserved

EX1009, 1-2.

56. When a General Inquiry Access Code (GIAC) is used in the Inquiry Message, all the listening devices may respond. However, a Dedicated Inquiry Access Code (DIAC) may be specified in the Inquiry message so that only the devices that support this code respond as described by the passage below.

> The inquiry message broadcast by the source does not contain any information about the source. **However, it may indicate which class of devices should respond.** There is one general inquiry access code (GIAC) to inquire for any device, and a **number of dedicated inquiry access codes (DIAC) that only inquire for a certain type of device.**

> The inquiry access codes are derived from reserved Bluetooth device addresses and are further described in Section 6.3.1.

EX1008, p. 325.

57. The Class of Device (CoD) code is a " 24-bit field shall contain the class of device of the device that sends the FHS packet. The field is defined in Bluetooth Assigned Numbers." EX1008, p. 284. The Class_of_Device parameter is used to indicate the capabilities of the local device to other devices. EX1008, p. 580.

58. The Bluetooth Specification also defines the capability of the receiving device to filter Inquiry Responses based on at least the received "Class of Device" and/or the "BD_ADDR" as described by the following passage.

> The Inquiry Result filter allows the Controller to filter out Inquiry Result events. The Inquiry Result filter allows the Host to specify that the Controller only sends Inquiry Results to the Host if the Inquiry Result event meets one of the specified conditions set by the Host. For the Inquiry Result filter, the Host can specify one or more of the following Filter Condition Types:
>
> 1. Return responses from all devices during the Inquiry process
> 2. A device with a specific Class of Device responded to the Inquiry process
> 3. A device with a specific BD_ADDR responded to the Inquiry process
>
> The Inquiry Result filter is used in conjunction with the Inquiry and Periodic Inquiry command.

EX1008, p. 673.

v) *The Extended Inquiry Response Fields Define the Responding Device's Local Name and its Supported Services.*

59. The Extended Inquiry Fields in the Response message include at least the device's local name and the services it supports as described by at least the passage below.

> "Data types are defined for such things **as local name**[2] and **supported services, information that otherwise would have to be obtained during a connection.** A device that receives **a local name and a list of supported services in an extended inquiry response** does not have to connect to do a remote name request and an SDP service search, thereby shortening the time to useful information."

EX1008, p. 126.

60. The following passage also describes that the device receiving the Inquiry Response message can determine if it desires to make a connection with it.

> During the inquiry substate, the discovering device collects the Bluetooth device addresses and clocks of all devices that respond to the inquiry message. In addition, the discovering **device also collects extended information (e.g. local name and supported services)** from devices that respond with an extended inquiry response packet. **It can then, if desired, make a connection to any one of the discovered devices** by means of the previously described page procedure.

EX1008, p. 325.

[2] All emphasis and highlighting has been added by me unless otherwise noted.

61. The following describes and shows the Extended Inquiry Response Data Format. Specifically, the number of data fields contained is variable so each type of data begins with a one-byte length indicator followed by its "EIR Data Type" and then the actual data. The receiving device uses these fields to decode the message and also to determine the number of data fields contained.

8 EXTENDED INQUIRY RESPONSE DATA FORMAT

The extended inquiry response data format is shown in Figure 8.1. The data is 240 octets and consists of a significant part and a non-significant part. The significant part contains a sequence of data structures. Each data structure shall have a length field of one octet, which contains the Length value, and a data field of Length octets. The first n octets of the data field contain the extended inquiry response (EIR) data type. The content of the remaining Length - n octets in the data field depends on the value of the EIR data type and is called the EIR data. The non-significant part extends the extended inquiry response to 240 octets and shall contain all-zero octets.

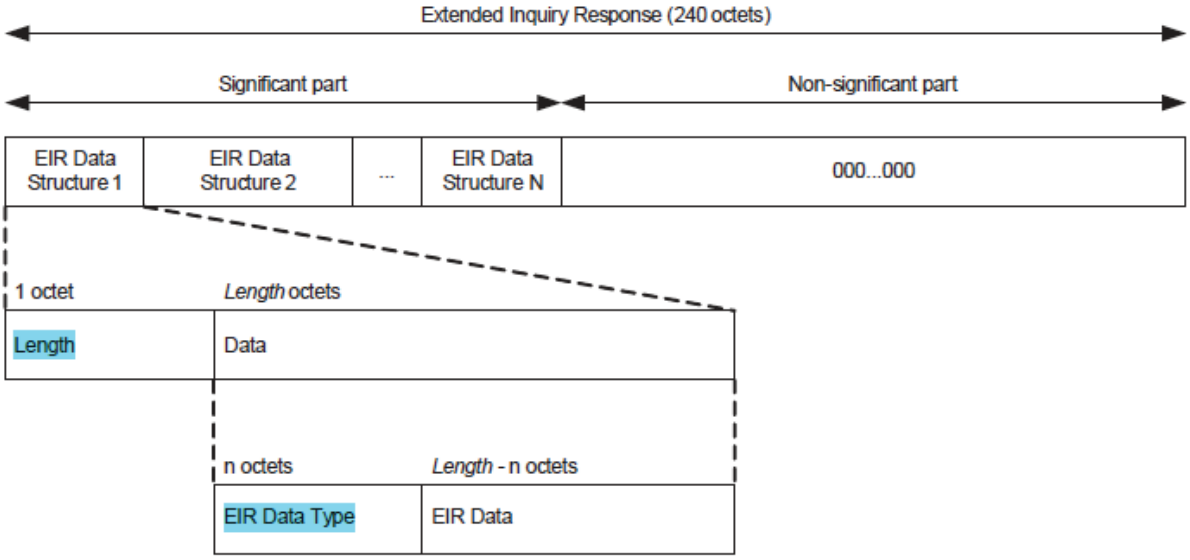


Figure 8.1: Extended Inquiry Response data format

[1] The extended inquiry response data types are specified in the Assigned Numbers document.

EX1008, p. 1305.

vi) *Service Class UUIDs Can Be Included in the Inquiry Response Message*

62. The EIR data further includes service class universally unique identifiers (UUIDs).

The EIR data shall always be sent during inquiry response state. EIR data can contain device name, Tx power level, service class UUIDs, as well as manufacturers data, as defined in Section 8.1. In selecting the packet type to be used, FEC (DM1 or DM3) should be considered to maximize the range.

EX1008, p. 1305.

2.5.1 UUID

A UUID is a universally unique identifier that is guaranteed to be unique across all space and all time. UUIDs can be independently created in a distributed fashion. No central registry of assigned UUIDs is required. A UUID is a 128-bit value.

To reduce the burden of storing and transferring 128-bit UUID values, a range of UUID values has been pre-allocated for assignment to often-used, registered purposes. The first UUID in this pre-allocated range is known as the Bluetooth Base UUID and has the value 00000000-0000-1000-8000-00805F9B34FB, from the Bluetooth Assigned Numbers document. UUID values in the pre-allocated range have aliases that are represented as 16-bit or 32-bit values. These aliases are often called 16-bit and 32-bit UUIDs, but it is important to note that each actually represents a 128-bit UUID value.

EX1008, p. 1197.

The full 128-bit value of a 16-bit or 32-bit UUID may be computed by a simple arithmetic operation.

$128\_bit\_value = 16\_bit\_value * 2^{96} + Bluetooth\_Base\_UUID$

$128\_bit\_value = 32\_bit\_value * 2^{96} + Bluetooth\_Base\_UUID$

Id.

vii) *The Paging (Connecting) Procedure*

63. The procedure for forming a connection between two Bluetooth devices requires one device to send out a Page message and the other device, that is scanning for the Page message, responds. Only one Bluetooth device should respond to a Page message as described below.

4.2.2 Paging (Connecting) Procedure

The procedure for forming connections is asymmetrical and requires that one Bluetooth device carries out the page (connection) procedure while the other Bluetooth device is connectable (page scanning.) The procedure is targeted, so that the page procedure is only responded to by one specified Bluetooth device.

The connectable device uses a special physical channel to listen for connection request packets from the paging (connecting) device. This physical channel has attributes that are specific to the connectable device, hence only a paging device with knowledge of the connectable device is able to communicate on this channel.

Both paging and connectable devices may already be connected to other Bluetooth devices in a piconet. Any time spent paging or occupying the page scan physical channel needs to be balanced with the demands of the QoS commitments on existing logical transports.

EX1008, p. 127.

64. After a successful Paging Procedure, the two devices are connected in a piconet and this is referred to as the "Connected Mode."

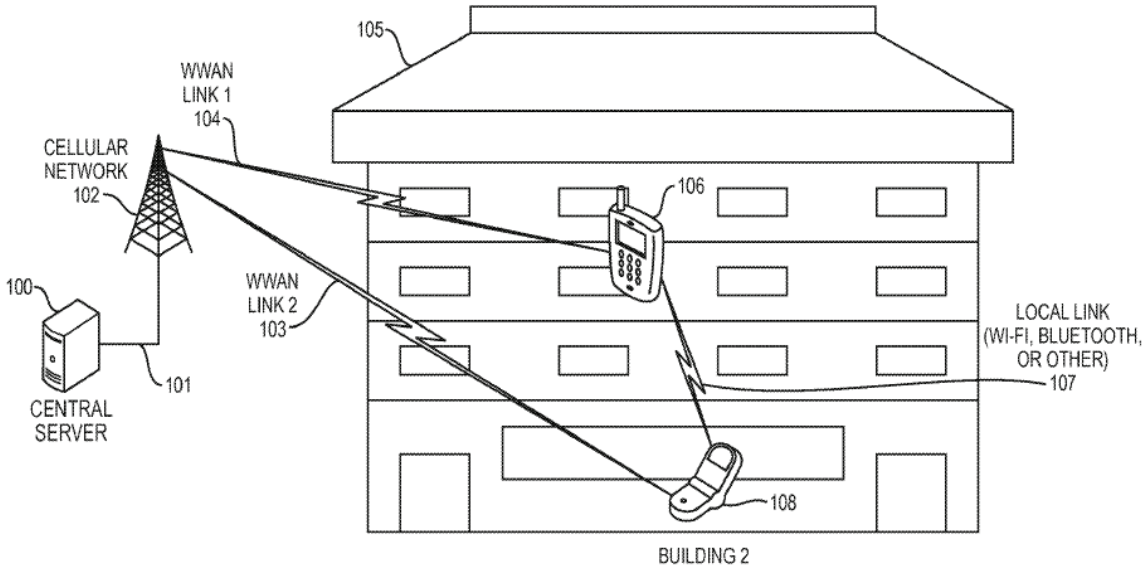
V. The '918 patent

A. Overview of the '918 patent

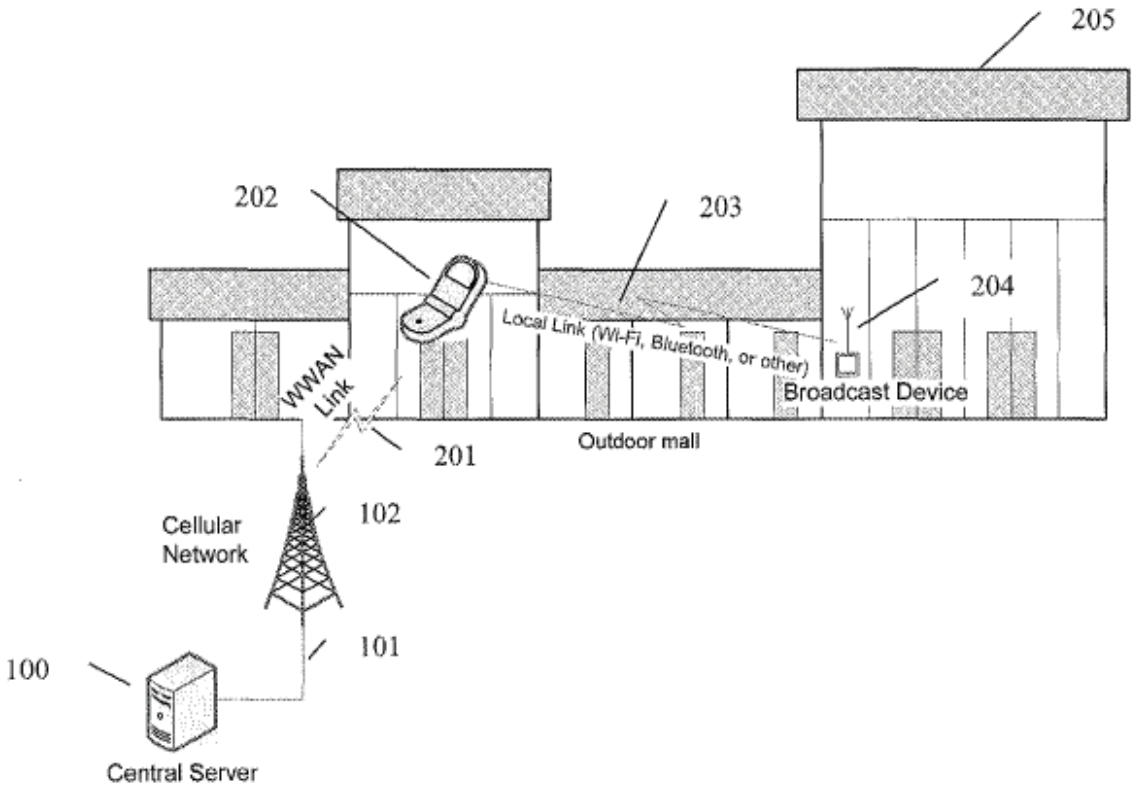
65. The '918 patent issued from U.S. Patent Application No. 15/271,410 ("'918 Application"), filed September 21,2016.

66. The purported "invention" of the '918 patent relates to the use of a server to manage communications between two devices. EX1001, Abstract, 2:66-5:12. In particular, the '918 patent concerns the facilitation of information between wireless devices having both short-range communications and long-range

communications. EX1001, 2:66-5:12. For example, in Fig. 1 (below), two devices 106 and 108 are in close proximity to each other and detect each other's presence over short-range wireless link 107 (for example, Bluetooth), and each of the devices is separately in communication with central server 100 over wide area wireless network (WWAN) connection 103 or 104 (for example, a cellular network). EX1001, 5:64-6:6, 6:55-7:9.



67. Fig. 2 (below) shows one implementation with devices 202 and 204 in short-range communication, and device 202 and server 100 in long-range communication. EX1001, 7:44-53.



68. Device 204 is, for example, a device associated with a museum exhibit that "transmits identifying information [to device 202] using short range wireless link 203," which device 202 "passes… to the central server 100," and the server 100 recognizes the identifying information as being associated with device 204. EX1001, 7:49-65. The server uses stored account settings or policy information to determine "what information and under which situations information may be disclosed to another device or user" to facilitate further short-range communications. EX1001, 4:49-67, 9:12-21, 16:5-16. The information returned and disclosed to the device may include "text, pictures, web pages, application software such as games, informative display applications, or other

content such as audio or video." EX1001, 8:3-8.

69. The '918 patent explains that devices in short-range proximity (i.e., devices 202 and 204 in the example above) identify themselves with beacon transmissions including a MAC address, unique identifier, and beacon service identifier. EX1001, claim 1. For example, a "MAC address is always broadcast in any operation of a Bluetooth or Wi-Fi link," but a MAC address may also be used as a device identifier. EX1001, 9:54-57, 10:54-65. Examples of service identifiers in an ad hoc Wi-Fi network include basic service set identifiers (BSSIDs, such as a 48-bit address) and service set identities (SSIDs, which are network names). EX1001, 10:31-11:6. BSSIDs and SSIDs were well-known identifiers used in IEEE 802.11 (Wi-Fi) systems, and different but similar values used for identifying and connecting devices were also well-known for Bluetooth systems (such as class of device and addressing information). *See* Olkkonen, 32:20-25 ("[BSSID] is a unique identifier for a particular [IEEE 802.11] ad hoc network"), 33:44-60 (SSIDs have no format or content restrictions), 33:54-58 (SSID "can perform the same informational function as… the class of device (CoD) in the Bluetooth standard, such as designating a device's node as a printer or fax machine"), 27:52-56 (Bluetooth piconets use "access codes" based on the piconet master device's BD_ADDR for access), 12:24-30 and 18:60-19:39 (device names and application programs as searchable service attributes).

B. The Prosecution History

70. The ’918 Application was prosecuted over approximately five years and involved several rejections by the Examiner, several amendments by the Application, and an appeal decision by the USPTO. The claim language changed significantly during this time. *See* EX1002, 384-409, 471-490, 692-712, 1311-1331, 1425-1430, 1495-1504, 1675-1681, 1683-1693 (Examiner actions), 428-465, 509-560, 749-778, 1407-1424, 1571-1581, 1697-1711, 2163-2174 (Applicant amendments), 1443-1492, 1582-1674, 1683-1693, 1697-1711 (Examiner and Applicant appeal briefs), 1722-1736 (USPTO PTAB affirming-in-part the Examiner’s rejections).

71. In the Examiner’s notice of allowance finding pending claims allowable, the Examiner stated that they allowed the claims because the prior art did not disclose “each of the proximity beacon transmissions including a MAC address and a unique identifier, determining if a particular short range transmission of the plurality of short range transmissions includes a MAC address, and utilizing the unique identifier.” EX1002, 2187-2190.

C. Priority Date of the Claims

72. I have been asked to assume the Challenged Claims are entitled to a September 8, 2008 filing date for the purposes of rendering my opinions in this declaration.

VI. LEVEL OF ORDINARY SKILL IN THE ART

73. In rendering the opinions set forth in this declaration, I was asked to consider the patent claims and the prior art through the eyes of a person of ordinary skill in the art at the time of the alleged invention. I understand that the factors considered in determining the ordinary level of skill in a field of art include the level of education and experience of persons working in the field; the types of problems encountered in the field, the teachings of the prior art, and the sophistication of the technology at the time of the alleged invention. I understand that a person of ordinary skill in the art is not a specific real individual, but rather is a hypothetical individual having the qualities reflected by the factors above. I understand that a person of ordinary skill in the art would also have knowledge from the teachings of the prior art, including the art cited below.

74. I have been informed that the POSITA's level of skill used in prior proceedings involving other patents in the same family as the '918 patent included a Bachelor's degree in electrical engineering, computer engineering, or the equivalent thereof, and approximately three years of professional experience working with wireless communications, where additional education could substitute for professional experience, or vice-versa. Upon consideration of the factors above, and based on my knowledge and experience in the field and my review of the '918 patent and file history, I agree that this is an appropriate level of

skill for a POSITA.

75. Based on my experiences, I have at least the skills of a person having ordinary skill in the art as well as a good understanding of the capabilities of a person having ordinary skill in the art. To be clear, all of my opinions in this declaration are from the perspective of one of ordinary skill in the art as I have defined it here during the relevant timeframe.

VII. CLAIM CONSTRUCTION

76. I have been instructed that the Challenged Claims of the '918 patent are to be given their ordinary and customary meaning as understood by one of ordinary skill in the art at the time of the alleged invention in light of the specification and the prosecution history pertaining to the patent. I have followed these principles in my analysis set forth in this document.

A. "determining…proximity"

77. Claims [1.G] and [9.E] of the '918 patent recite, in part: "determining [if/that] an entity or object… is [in/within] proximity to the mobile wireless device, by utilizing the identifier related information and the unique identifier."

78. During prosecution, Applicant provided examples of alleged support for these limitations (and others) to argue that they did not contain new matter. EX1002, 521-540. I understand that these statements were presented as examples of the claimed limitations (and not explicit definitions), and so the limitations may

be interpreted to encompass those particular features in addition to their plain and ordinary meaning.

79. For example, *determining proximity* may be satisfied by disclosing a device's presence to another device. *See* EX1002, 524 ("Device 1… notifies the user that the entity… is in proximity"), 539 ("process… allows for disclosure of a user's presence (that is, their 'proximity')"). That is, if one device's presence is not disclosed (or not permitted to be disclosed) to another device, those devices are determined not to be in "proximity."

80. Furthermore, *utilizing identifier related information* may be satisfied by using identifier information as a filter to determine which identifiers to pass to a server to determine whether there is permission to disclose a device's presence to another. *See* EX1002, 524 ("if identifiers are found… employ an action… as a filter that determines which… identifiers should be passed to the server," "permission… may require being on a friends list").

VIII. GROUNDS OF UNPATENTABILITY

81. As I explain above in Section IV above, methods of short-range communication were already well-known in the art via Bluetooth communications, including the various identifying information (for example, Bluetooth addresses,) with which one Bluetooth device identifies itself to another.

82. In this section, I will explain why the teachings or combinations of

teachings from the following references render obvious each of the Challenged Claims:

Name	Ex.	Publication/ Patent No.	Published/ Issued
Eagle	1005	2005/0250552	November 10, 2005
Behrens	1006	2010/0138481	June 3, 2010
Olkkonen	1007	7,590,086	September 15, 2009
Perttila	1037	2004/0243519	December 2, 2004
Jones	1038	2007/0264991	November 15, 2007

I have been instructed to assume that each of these references qualifies as prior art.

83. As I explain below, the Challenged Claims are invalid based upon the following prior art grounds:

- **Ground 1**: claims 1-4, 8-20, 22-25, 27-28, and 31 of the '918 patent are rendered obvious by Eagle in view of Behrens and Olkkonen.
- **Ground 2**: claim 17 of the '918 patent is rendered obvious by Eagle in view of Behrens, Olkkonen, and Perttila.
- **Ground 3**: claim 29 of the '918 patent is rendered obvious by Eagle in view of Behrens, Olkkonen, and Jones.

84. It is my opinion that Challenged Claims of the '918 patent are unpatentable as explained below. I note that in this discussion, I may focus on the particular language in the specific claims, but it should be understood that my analysis applies to the corresponding elements of all Challenged Claims containing

identical or substantially identical language.

IX. DETAILED ANALYSIS OF GROUNDS FOR CHALLENGE

85. As I explain in Section V above, the ’918 patent purports to have invented a method for managing communications between two devices using a remote server. However, such methods were well-known in the art. As described below, the cited prior art provides these teachings.

86. In this section, I explain why the Challenged Claims of the ’918 patent are rendered obvious by the teachings of Eagle, Behrens, Olkkonen, Perttila, and Jones. I note that, in this discussion, I may focus on the particular language in specific claims, but it should be understood that my analysis applies to the corresponding limitations of all claims containing identical or substantially identical language.

A. GROUND 1: EAGLE IN VIEW OF BEHRENS, AND FURTHER IN VIEW OF OLKKONEN, RENDERS OBVIOUS CLAIMS 1-4, 8-20, 22-25, 27-28, and 31

a. Overview of Eagle (EX1005)

87. U.S. Patent Application Publication No. 2005/0250552 to Eagle et al. (“Eagle,” EX1005), titled “COMBINED SHORT RANGE RADIO NETWORK AND CELLULAR TELEPHONE NETWORK FOR INTERPERSONAL COMMUNICATIONS,” was filed on May 5, 2005 and published on November 10, 2005.

88. Eagle is directed to a mobile communication architecture or "social software introduction system" for "facilitating direct communications between consenting persons having similar interests." Eagle, [0002], [0065].

89. The system includes cellular phones enabled with Bluetooth that "are able to… identify other such devices that are nearby" by a unique identification value such as a Bluetooth address value. Eagle, [0003], [0018]. When one device (hereinafter referred to as a "Requester Device") detects a new device (hereinafter referred to as an "Identified Device") using the Identified Device's unique identification value, the Requester Device notifies a remote server of the unique identification value via a long-range cellular network. Eagle, [0003], [0020]. An example of two such devices 203 and 205, and a server 220, are shown in Fig. 2 (below).

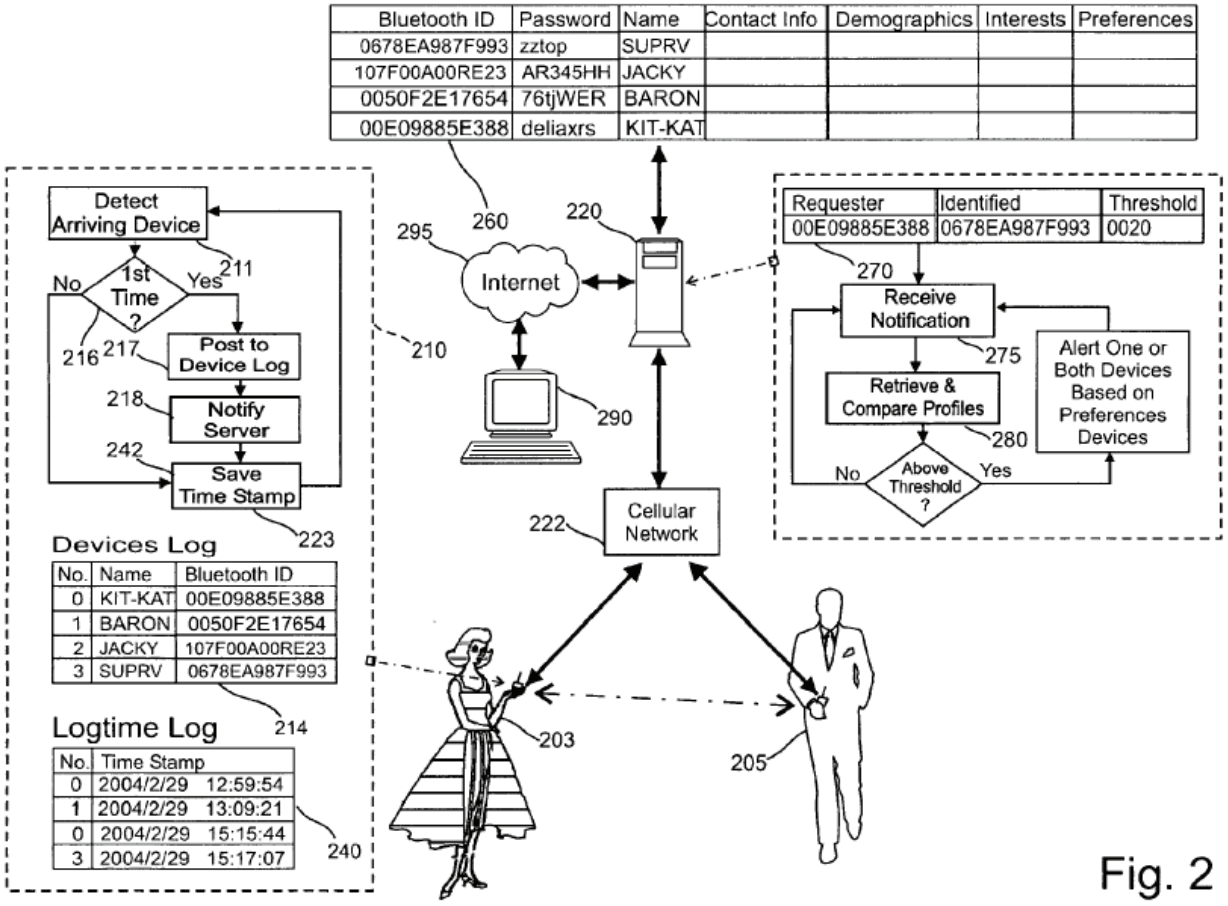


Fig. 2

90. The server stores profile data describing devices and their owners, and when it receives unique identification values in a notification, "fetches the profile data associated with each of the two identified devices and performs a comparison." Eagle, [0005], [0020]. If the profiles of a Requester Device and an Identified device match (because, for example, their profiles indicate they attended the same college), then an alert message is sent to each device. Eagle, [0005]-[0007], [0045], [0047], [0063]. An alert may contain contact information, descriptions of the device's owner's personal interests, "or any other information which is of use in a specific application [that] may be of use to identify, or promote

communications between, nearby devices and their owners." Eagle, [0007], [0021].

b. Overview of Behrens (EX1006)

91. U.S. Patent Application Publication No. 2010/0138481 to Behrens ("Behrens," EX1006), titled "DEVICE AND METHOD FOR ESTABLISHING SOCIAL NETWORKS THROUGH THE USE OF WIRELESS TECHNOLOGY," was filed on April 30, 2008 and published on June 3, 2010.

92. Behrens is directed to a system for automatically establishing contact between users who are in close proximity to each other. Behrens, Abstract, [0001].

93. In one example, a wireless device detects the presence of another wireless device by receiving unique identifiers (UIDs) via Bluetooth transmissions. Behrens, [0094], [0097]-[0098]. Behrens explains that UIDs used for this purpose "consist of any unique or quasi-unique code, number, address, symbol, or a combination thereof, which uniquely identifies a device, and, by association, the owner of the device," and may include MAC addresses and Bluetooth Device Addresses. Behrens, [0097].

94. As discussed above, UIDs may be used in combination. Furthermore, a "user may… exercise control over which or how many UIDs are transmitted by his device." Behrens, [0061], [0103], [0115], [0122]. Accordingly, a user has "multiple or changing UIDs." Behrens, [0061], [0115]. Users supply their UIDs to servers, keeping device UIDs in sync with the servers. Behrens, [0065], [0076].

c. Overview of Olkkonen (EX1007)

95. U.S. Patent No. 7,590,086 to Olkkonen et al. ("Olkkonen," EX1007), titled "AD HOC NETWORK DISCOVERY MENU," was filed on November 3, 2004 and issued on September 15, 2009.

96. Olkkonen is directed to short-range wireless systems and connecting users for common purposes via ad hoc networking (for example within "piconets" in Bluetooth). Olkkonen, 1:13-16, 1:46-2:3. Piconets serve a variety of purposes, for example, "collaborative work projects, collaborative games, multi-user gateways to the Internet, and the like" that interested users may join. Olkkonen, 2:60-65. Olkkonen's system thereby alerts users of nearby piconets (or other ad hoc networks) that are of interest. Olkkonen, 4:65-5:4.

97. Olkkonen teaches that a wireless device may search for nearby piconets through inquiry and discovery processes. Olkkonen, 12:39-60, 13:33-50, 18:49-63; *see also* piconet examples illustrated throughout, 13:29-31:25. For example, "when a new short-range wireless device arrives within the communication range of any member of [an] ad-hoc network, its inquiry signals are answered by a member detecting the inquiry," who "responds with information… characterizing the ad hoc network." Olkkonen, 5:27-33. Responses are compiled into a discovery menu listing those characteristics "in accordance with the type of characteristics of interest to the user." Olkkonen, 6:29-38. An

exemplary menu 205 is shown in Fig. 1 (below).

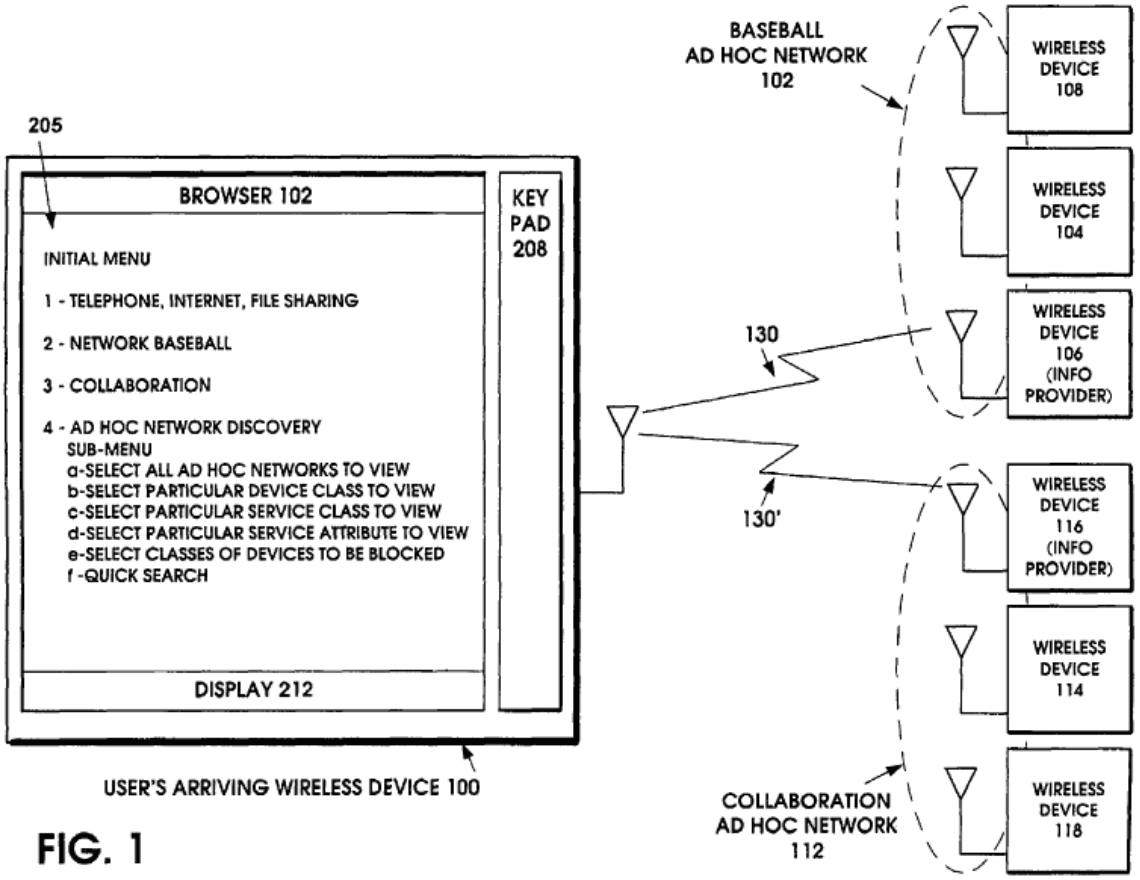


FIG. 1

98. Users have the ability to filter and view certain devices in the menu, for example by blocking and/or displaying devices associated with certain devices classes, service classes, or service attributes. Olkkonen, 11:33-60, 22:8-21.

d. Overview of Eagle's, Behrens', and Olkkonen's combined teachings

i) ***Eagle, Behrens, and Olkkonen are analogous art and their combined teachings renders obvious claims of the '918 patent***

99. The '918 patent is in the field of wireless communications and concerns, for example, secure communications using wireless service identifiers,

safety and privacy with locally stored policies, and facilitating the exchange of information between two entities associated with two wireless devices. *See* EX1001, 2:48-57, 2:66-3:3.

100. Eagle, Behrens, and Olkkonen are each analogous to the '918 patent, as they are in the same field of wireless communications and/or reasonably pertinent to the problems identified above. Eagle, Abstract ("Bluetooth enabled cellular phones[] communicate with and identify like devices that are nearby, and send notification messages to a remote server… [that] facilitates communications between the devices when appropriate"), [0008] (using Bluetooth communications "avoids some privacy problems"); Behrens, [0001] ("relates to… establishing contact… through the use of wireless technology," "between users who come into proximity of one another"), [0136] (making contact between "individuals who are otherwise unknown"), [0141] (applications in social networking, Internet forums, blogs); Olkkonen, 1:13-16 (relating to short-range wireless systems), 4:65-5:4 (addressing need to provide a discovery menu listing collaborative activities in nearby networks that would interest users).

101. To the extent Eagle is argued by Patent Owner as failing to expressly disclose details of particular information communicated from a wireless device via a short-range protocol as claimed in the '918 patent (for example, receiving different first and second different MAC addresses and unique identifiers, and

receiving a same beacon service identifier, as in claims 1, 3, 9-10, and 12 of the ’918 patent), determinations that transmissions include a beacon service identifier (for example, as in claims 1 and 9 of the ’918 patent), the user of received information to determine the proximity of an entity or object for example, as in claim 1 and 9 of the ’918 patent), or specific types of received information (for example, information relating to a multiuser game or application, as in claims 22-23 of the ’918 patent), such obvious variations would have been well within the skill of a POSITA in view of Behrens’ teachings of changing the unique identifier transmitted from a same device for maintaining privacy, Behrens’ teachings of ignoring devices on blacklists, and in view of Olkkonen’s teachings of service identifiers in ad hoc networking to facilitate collaborative activities via Bluetooth®.

102. For example, a POSITA seeking to address privacy risks in Eagle would have found it obvious to provide for changing unique identifiers from time to time, per Behrens. To make Eagle’s system more efficient, a POSITA would have found it obvious to have participating devices broadcast a specific service identifier, per Olkkonen, to identify Eagle’s social introduction application. A user’s device would thus first filter unique identifiers for the correct service and then send the unique identifiers to Eagle’s remote server, which maps unique identifiers to user profile information to facilitate connections between wireless

devices, and then take and potential further action, such as displaying contact information or joining a collaborative game as taught by Olkkonen. And, as an overall security measure, the user's device would have been configured to ignore blacklisted unique identifiers, as taught by Behrens.

ii) *Behrens teaches combined and changing UIDs*

103. The claims of the '918 patent require receiving, at a wireless device from a single transmitter device, different beacon transmissions at two different times, including a first transmission with a MAC address and unique identifier, and a second transmission with a different MAC address and different unique identifier. *See*, for example, EX1001, claims 1, 3, 8-10, and 31. In other words, a device transmitting *short range transmissions (Bluetooth)* to the claimed *wireless device* changes its identifying data as a function of time to enhance security. EX1001, 4:42-48, 10:18-30, 17:33-59.

104. Eagle describes that Identified Devices identify themselves to Requester Devices with a "unique identification value, such as a Bluetooth device address value." Eagle, [0003]. To the extent it is argued that Eagle does not explicitly describe the *wireless device* receiving different first and second MAC addresses and different unique identifiers from the same device, it would have been obvious to a POSITA for the following reasons.

105. Behrens teaches that devices in short-range proximity "uniquely

identif[y]" themselves and their owners with "at least one unique identifier (UID)," which may "consist of" or be included in a "combination" of unique identifiers (UIDs) including WLAN MAC addresses, Bluetooth Device addresses, unique numbers, and/or unique symbols. Behrens, [0061], [0097], [0111], [0115], [0122]. Moreover, a user can have "multiple or changing UIDs" and has "control over which or how many UIDs are transmitted by his device." Behrens, [0103], [0115].

106. Thus, Behrens explicitly discloses above that the device can use at least two different MAC addresses as its UID. Specifically, the "WLAN MAC address" and the "Bluetooth Device address" are different 48-bit values that uniquely define a device; the WLAN MAC address is the unique 48-bit value for the device's Wi-Fi Network Interface Card (NIC) and the Bluetooth Device Address (BD_ADDR) is the unique 48-bit value for the devices Bluetooth NIC. Having both Wi-Fi and Bluetooth capabilities—and respective addresses—in wireless devices was a configuration well-known to POSITAs. For example, Apple Inc.'s iPhone 3G in 2008 included Wi-Fi and Bluetooth capabilities (*see* EX1035), and its documentation shows each having an address (*see* EX1036, 142). *See also* Behrens, [0077] (BD_ADDR and WLAN MAC addresses retrieved separately). The '918 patent similarly acknowledges that the BD_ADDR can be considered the claimed *MAC address*. EX1001, claim 11. The Bluetooth BD_ADDR is explained in detail in Section IV above.

107. Behrens also teaches that the use of changing UIDs comprised of combinations of different information advantageously allows a user to have a single managed account with different online identities (for example for different social events or parties). Behrens, [0115]. Eagle teaches adding an additional method for users to create distinct or particular profile data to "contact experts in a particular field" or for seeking "a person of the opposite sex of a particular age having common interests." Eagle, [0063]. Thus "the same user may supply profile data for use in professional encounters, and other profile dat[a] for use in social encounters." Eagle, [0063]. Thus, both Behrens and Eagle teach that a user may have a single account for an application that is capable of supporting multiple online identities (UIDs) for that user depending on specific interests and situations.

108. In addition to the benefits of providing multiple online identities for a user, a POSITA would have understood that there were other benefits that would be realized by changing the UID of the device. These benefits would provide anonymity, security, and anti-tracking.

109. A device would have anonymity because changing the UID would make it more difficult for the device to be tracked or identified by malicious devices even when it is transmitting a consistent signal. A changing UID would also provide additional security by making it harder for a malicious device to impersonate it and gain unauthorized access to data or security systems by

capturing and replaying the device's signal.

110. Thus, one implementation to meet these claim limitations, would be for a transmitting Bluetooth device to use its BD_ADDR (*MAC address)* in the *first time period* to uniquely identify itself to the *wireless device* over the *short range wireless protocol/Bluetooth protocol* and then use its WLAN MAC address in the *second time period* to uniquely identify itself to the *wireless device* over the *short range wireless protocol/Bluetooth protocol*.

111. A POSITA would have further recognized that (1) privacy and security concerns in short-range wireless devices that transmit beacons using fixed identifying information were well-known, and (2) changing identification information, as taught by Behrens, addresses those concerns. EX1010, [0002]-[0004] (temporary and/or randomly generated identification numbers mitigates threats to security and privacy); EX1011, Abstract, [0006] (randomizing Bluetooth addresses prevents the correlation of identities, routes, and activities with a device); EX1012, [0002]-[0008] (preventing tracking through a randomly generated Bluetooth address); EX1013, [0008]-[0011] (same). *See also* Behrens, [0003] (apprehension in sharing of personal information freely). Thus, where Bluetooth addresses and UIDs are potentially transmitted "continuously or repeatedly" (Behrens, [0097]; Eagle, [0003]), the changing of identifiers advantageously prevents the tracking and correlating of users, activities, and

devices over time.

112. The described modification would have been further obvious to a POSITA as it is no more than the application of a known technique (for example, Behren's teaching of changing combination UIDs) to a known device ready for improvement (for example, Eagle's system that identifies devices by unique identification values and identifies profile data by mode indicator values) to yield predictable results (for example, allowing for different online identities; enhancing privacy with changing UIDs).

113. A POSITA would have also had a reasonable expectation of success in modifying Eagle with the teachings of Behrens. Use of UIDs (which are data values used as identifiers) in place of Eagle's unique identification values would have required no more than ordinary software coding skills to change such values, and track, select, store, communicate, and analyze those values as known in the art. Moreover, where Behrens teaches that UIDs borrow from existing values such as a wireless device's addresses, Behrens provides techniques for obtaining those values manually, and for updating the server with those UIDs by supplying the UIDs to the server. Behrens, [0065], [0076]-[0077]. Modification would have been well within the skill of a POSITA.

iii) *Eagle and Olkkonen teach filtering beacon service identifiers*

114. The claims of the ’918 patent require determining that beacon transmissions include a proximity beacon service identifier (which is calls a PBSI) that indicates that the short range transmission it is received in is associated with a proximity beacon service, which is related to one or more servers in communication with the wireless device. *See*, for example, EX1001, claims 1 and 9. The same claims further require that the above determination is made before further processing of the received transmissions, thereby filtering the beacon transmissions which include a particular beacon service identifier.

115. To the extent Patent Owner argues that Eagle does not explicitly describe *beacon service identifiers* (or *PBSIs*) as claimed, it would have been obvious to a POSITA to filter UIDs based on beacon service identifiers (for example, service class information that identifies Eagle’s social introduction “BlueAware” application) received in inquiry responses, consistent with the teachings of Olkkonen, for the following reasons.

116. Eagle teaches that it is unnecessary for a Requester Device to notify the server of every UID that it receives from nearby Identified Devices. For example, when an Identified Device is detected, the Requester Device “determine[s] whether the detection of a given device warrants the transmission of

a notification message to the server" by filtering out recently detected devices. Eagle, [0023]-[0025]. Thus, Eagle teaches selectively notifying the server of nearby devices such that the user is not alerted of every device that is nearby, and communications with the server and mobile device communication processing are minimized.

117. Olkkonen additionally teaches filtering techniques that would have been known to a POSITA in the context of Bluetooth ad hoc networks. For example, service class information (which may include service "attributes") describes and identifies programs running in ad hoc networks (for example, a network baseball game). Olkkonen, Fig. 5 (showing a service class with a program identity service attribute), 30:22-28. This service identification information is received in Bluetooth inquiry responses. *See* Olkkonen, 5:27-33, 12:40-48, 13:33-43, and 17:49-63 (Identified Devices' inquiry responses include service registry information "characterizing the ad hoc network"); 5:13-17 and 17:17-22 (service classes "characterize the ad hoc network" and include, for example, the type of distributed program running).

118. It would have been obvious to use Olkkonen's disclosed service class information to identify Eagle's social introduction application (which is a service and a program running on wireless devices) such that Identified Devices identifying Eagle's service are included in notifications to the server rather than

non-participating devices.

119. For example, Olkkonen teaches that lists of discovered Identified Devices presented to the user in a discovery menu should be customized to user preferences, for example, by ignoring or blocking undesirable Identified Devices and by listing Identified Devices of interest. Olkkonen, 11:30-60. One such filter blocks all devices identifying themselves as providing an advertisement broadcast service. Olkkonen, 11:33-42, 22:34-43. While Olkkonen describes "advertisements" and "advertisement broadcaster" as classes of devices, a POSITA would have recognized that "ADVERTISEMENTS" was a non-standard type of Bluetooth device class. EX1009 (Bluetooth assigned numbers). To the extent "advertisement" is a non-standard class, a POSITA would have recognized that advertisement would have been a type of intended use or service provided by the device, and it would have been obvious to alternatively identify advertisement functions as custom service information. In another example, a user may only want to see devices in particular service classes or having particular service attributes (such as those identifying a particular program, such as a "GAME PROGRAM"). Olkkonen, 11:43-60.

120. As Eagle requires users to actively participate in its social introduction system by running a particular program ("BlueAware") on their devices (Eagle, [0019], [0029], [0038], [0065]) and by registering information with a server

(Eagle, [0029], [0045]-[0046]), a POSITA would have recognized that it would have been wasteful and inefficient to notify the remote server of *every* Bluetooth device that the Requester Device encounters without screening/filtering them first as participating in the service. In this regard, Eagle emphasizes that its system links users with "selection criteria that [are] useful to service users." Eagle, [0011]. A notification identifying a device that is not even participating in Eagle's social introduction system would have been useless to the remote server and would have increased communications and server load for no benefit. Therefore, it would have been obvious to modify Eagle's Identified Devices to specifically identify Eagle's social introduction system within inquiry response service class information (when the particular Identified Device participates in Eagle's services) and to modify Eagle's Requester Device to filter inquiry responses so that only UIDs identifying themselves as being relevant to Eagle's social introduction program would be notified to the server. As a result, only UIDs from Identified Devices that "warrant the transmission of a notification message to the server" (Eagle, [0024]) are actually notified to the server.

121. Additionally, Eagle teaches that wireless device resources are limited. Eagle, [0024] (conserving memory by deleting old logs of Identified Devices), [0026] (continuous scanning and logging expends phone battery life). This would also apply to only contacting the server with useful UIDs so its resources are

further conserved. In other words, irrelevant Identified Devices do not need to be logged or tracked and do not need to be passed to the server using long-range wireless communications.

122. The described modifications would have been further obvious to a POSITA as no more than the application of a known technique (for example, Olkkonen's teachings of including service information in inquiry responses and filtering responses based on that information) to a known device ready for improvement (for example, Eagle's system that determines whether detection of an Identified Device warrants notification to the server) to yield predictable results (for example, selectively notifying the server of Identified Devices).

123. A POSITA would have also had a reasonable expectation of success in modifying Eagle to implement Olkkonen's teachings to receive and analyze service information in inquiry responses. For example, a POSITA would have recognized that Bluetooth communications include several methods for conveying service and class information including, but not limited to, through various message fields within class-of-device information or extended inquiry responses (EIRs) that include fields for service class universally unique identifiers (UUIDs) and manufacturer specific data. Eagle, [0032]; EX1008, 1305-1310. Service information may be included in these fields or as appended to any inquiry response so that the necessary descriptive information is conveyed, as discussed above.

Furthermore, the Bluetooth Specification defined using class of device or service class information as identifier values and the capability of a receiving device to filter based on the values in these fields before the ’918 patent, as described in Section IV.B.e.iv above, so a POSITA would have been aware of this functionality in at least one form. Filtering based on the values taught by Eagle and Olkkonen would have therefore required no more than ordinary message parsing and processing skills that would have been well within the skill of a POSITA.

iv) *Eagle and Olkkonen teach different networking applications*

124. Claims of the ’918 patent require receiving information about another user that is a “user of an application” (claim 22) such as a “multiuser game” (claim 23).

125. Eagle broadly describes that its social introduction system “enables a diverse suite of applications,” for example, connecting people working on similar projects, connecting users with like interests, as greeting beacons at trade shows, notifications of nearby resources, and more. Eagle, [0061]-[0068]. Alerts returned to the Requester Device therefore include “any… information which is of use in a specific application” and useful to “promote communication between[] nearby devices and their owners,” including contact information. Eagle, [0007], [0041], [0050].

126. Olkkonen, like Eagle, teaches that users of wireless devices may connect for a variety of applications. For example, Olkkonen describes that wireless Bluetooth devices form ad hoc networks or piconets for telephone, internet, and for participating in network games. Olkkonen, 2:59-65, 6:19-21, 11:61-12:2, 18:60-63, 19:13-16, 20:41-43, 25:48-52, 25:63-26:33.

127. Accordingly, to the extent Eagle does not expressly describe that a user of a nearby Identified Device is using an application such as a multiuser game, it would have been obvious to a POSITA that users in collaborative settings would have been participating in any of a number of activities, including multiuser games, as taught by Olkkonen. That the user of the Identified device is a user of a multiuser game would have been no more than a simple substitution of known elements (for example, Olkkonen's teaching that networks facilitate multiuser games for participants) for another (for example, Eagle's discussions that users collaborate for a variety of social activities) to obtain predictable results (for example, facilitating the introduction to, and connection with, a user playing a multiuser game).

128. Furthermore, modification of Eagle to encompass users playing multiuser games, as claimed in the '918 patent, require more than ordinary skill. As I discuss above, both Eagle and Olkkonen explain that many uses for social introductions and collaboration existed. The user of another device may have

participated in any number of those activities, including playing a multiuser game or application on a Bluetooth network. Including those users and others in Eagle's social introduction system would have required no more than ordinary skill for a POSITA.

v) *Eagle and Behrens teach lists for filtering*

129. Claims of the '918 patent require receiving information and using that information to determine whether another device (or an entity or object) is in proximity to a user device (for example, as in claims 1 and 9). Eagle and Behrens teach the use of information in this manner via blacklists, which are lists of unique identifiers (UIDs) to be ignored), and friend lists, which are lists of UIDs to be trusted.

130. As discussed above, Eagle teaches that the Requester Device "determine[s] whether the detection of a given device warrants the transmission of a notification message to the server" by filtering out recently detected devices. Eagle, [0023]-[0025]. And, as discussed above, by selectively notifying the server of nearby devices by their UIDs, communications with the server and mobile device communication processing are minimized.

131. Behrens teaches an additional mechanism for filtering UIDs via blacklists, with which a server may instruct a Requester Device to ignore devices having certain UIDs. In particular, the Requester Device "may store [unique

identifiers (UIDs)] to be ignored in a blacklist," received as instructions from the server, to eliminate spam and other unwanted behavior. Behrens, [0101]-[0102], [0124].

132. Similarly, Eagle also teaches the use of lists—friend lists—that create a trust network of devices that, conversely, should be identified to the Requester Device. For example, the server stores profile information "specifying a set of device IDs for devices owned by 'friends'" that form a "trust network" of devices. Eagle, [0056], [0066]-[0067]. Based on the friend list, the Requester Device is "only" alerted to the presence of nearby Identified Devices that are in the Requester Device's friend list and determined to have "common interests" in their profiles. Eagle, [0056]. Eagle's server therefore uses friend list information as an exemplary filtering tool.

133. It would have been obvious to a POSITA to alternatively store Eagle's friend list on the Requester Device to act as a filter for UIDs sent to the server. As discussed above, selectively notifying the server of nearby devices through filtering minimizes communications with the server and minimizes the mobile device's communications processing. Therefore, by performing a basic check of received UIDs against a friends list prior to notification to the server, irrelevant UIDs may be ignored outright, conserving those server and device resources. Thus, for a user that only wants to have connections with others in their trust network,

(Eagle, [0056]), a UID that is not on the friend list would not have produced a positive result (sending an alert back to the Requester Device), and so it would be wasteful to send those UIDs to the server in the first place.

134. Behrens further teaches that known configurations for storing and using lists for filtering, such as Behrens' blacklist and Eagle's friend list, included storage on the wireless device, on the server, or both. Behrens, [0101]-[0102]. Indeed, there would have been a limited number of ways to store lists for filtering UIDs in relation to the Requester Device—in a location local to the device, or in a location remote of the device. Both produce similar results (filtering) and only differ by which device is storing and processing the information. As Eagle already discloses one form of UID filter via its devices log (Eagle, [0023]-[0024]), an additional filter based on a blacklist or friend list would have required no more than ordinary skill for a POSITA.

135. Moreover, where UIDs change over time (in view of Behrens, as discussed above), Behrens provides for updating those UIDs with the server. Behrens, [0065], [0076] (user supplies UIDs to the server to link to user accounts). Accordingly, because it is the server that supplies the blacklisted and/or friend listed UIDs to the wireless device, a POSITA would have recognized that those UIDs would have been synced as needed.

136. Furthermore, modification of Eagle to implement known blacklist and

friend list techniques at the Requester Device would have yielded predictable results (of selectively notifying the server of Identified Devices) and required no more than ordinary skill. As discussed above, Eagle already teaches filtering UIDs based on comparisons to its devices log, which also includes a list of identifiers to check, like blacklists and friend lists. Indeed, lists for blocking and allowing connections are well known in computing systems, one common form being lists of IP addresses for which networking components should block or allow traffic. The use of additional lists would have required no more than basic data processing skills to implement.

vi) *Eagle and Behrens teach presenting previous alerts*

137. Claims of the ’918 patent require receiving information and using that information to determine whether another device (or an entity or object) is in proximity to a user device (for example, as in claims 1 and 9). Eagle and Behrens teach the use of previously presented alerts in this manner to determine another device’s proximity.

138. Eagle teaches that the same Identified Device may be encountered more than once. Eagle, [0023]-[0024]. While a Requester Device would not notify the server again of an Identified Device that it recently encountered (for example, when an Identified Device has not yet been removed from the Devices Log; Eagle, [0023]-[0024]), Eagle leaves to a POSITA whether the profile information of an

Identified Device found on the recently encountered log would be presented again.

139. Behrens teaches that it would have been obvious to present the alert information on the Requester Device again for an Identified Device previously encountered. For example, Behrens teaches that if an Identified Device, "of which [a Requester Device] has previously stored the identifier and possibly received other data from, … has reentered [the Requester Device's] range," then it is preferable to notify the user of that device again to make a connection. Behrens, [0035]. A POSITA would have recognized that there are numerous situations where it would have been advantageous to repeat alerts on a Requester Device. For example, if a user of a Requester Device did not or could not connect to the Identified Device the first time it was alerted to the Identified Device, an additional alert would have presented them a second opportunity to connect. Or, if the Identified Device (and its owner) are of particular interest to the Requester Device, the Requester Device may have found it beneficial to be alerted to the Identified Device's presence frequently. And if a user of the Requester Device often misses alerts, repeated alerts would have advantageously provided them multiple opportunities to see those alerts.

140. Eagle's notifications to the user of the Requester Device are in the form of alerts including received profile information, and it would have been obvious to present that alert information again, facilitating a connection between

the devices. Eagle, [0007] (alerts include information useful to promote communication); Behrens, [0035] (sharing contact information). Furthermore, to conserve resources (a common concern, as discussed above), the Requester Device would not, again, notify the server and receive alert information, and it would have been obvious to present the same alert it previously received from the server. Eagle leaves to a POSITA what the Requester Device does with received alerts, but it would have been obvious to a POSITA to store alerted information for future use instead of requesting information from the server every time. Indeed, alerts are only provided to the Requester Device when a match between their users is found, and the alerts are thus more relevant to the user than, for example, the bulk UID information that the Requester Device logs for every device it sees (which are discarded periodically). Eagle, [0020]-[0023]. Therefore, it would have been obvious to store alert information and, furthermore, to store the alert information so that it is retrievable by their associated UIDs. UIDs (unique identifiers) are the identifying information used in Eagle's system—by the server that retrieves profile information (Eagle, [0019]-[0021], [0041], [0045], [0051] (identification values used to fetch profile data)) and by the wireless devices that identify themselves. Eagle, [0003], [0022], [0031]. Accordingly, it would have been obvious to use the same UIDs as relevant identifiers to catalog the information for storage and retrieval using this known method.

141. Therefore, it would have been obvious to modify Eagle's Requester Device to store received alert information for presentation to the user when a nearby Identified Device is detected more than once. The described modification would have been further obvious to a POSITA as no more than the application of a known technique (for example, Behrens' teaching to provide an alert for a previously-alerted device) to a known device ready for improvement (for example, Eagle's system that presents alerts but leaves to a POSITA whether alerts should be presented in certain situations) to yield predictable results (for example, re-alerting the user).

142. A POSITA would have also had a reasonable expectation of success in modifying Eagle to implement Behrens' teachings as discussed above. Eagle already teaches receiving and presenting alerts on the Requester Device. Longer-term storage of an alert and later retrieval of an alert would have only required basic data management skills well within the skill of a POSITA.

e. Claims

i) *Claim 1*

(1) [1.PRE] "A mobile wireless device comprising:"

143. Eagle teaches *a mobile wireless device* (for example, a Bluetooth phone). Eagle describes that a first Bluetooth phone carried by individual 203 (a Requester Device) is a wireless device that includes "short range radio transceivers

that use the Bluetooth protocol" for communications. Eagle, Abstract, [0018]. For example, Fig. 2 (below) illustrates communications between a first Bluetooth phone carried by individual 203, a second Bluetooth phone carried by individual 205, and remote server 220. Eagle, Fig. 2, [0018], [0022].

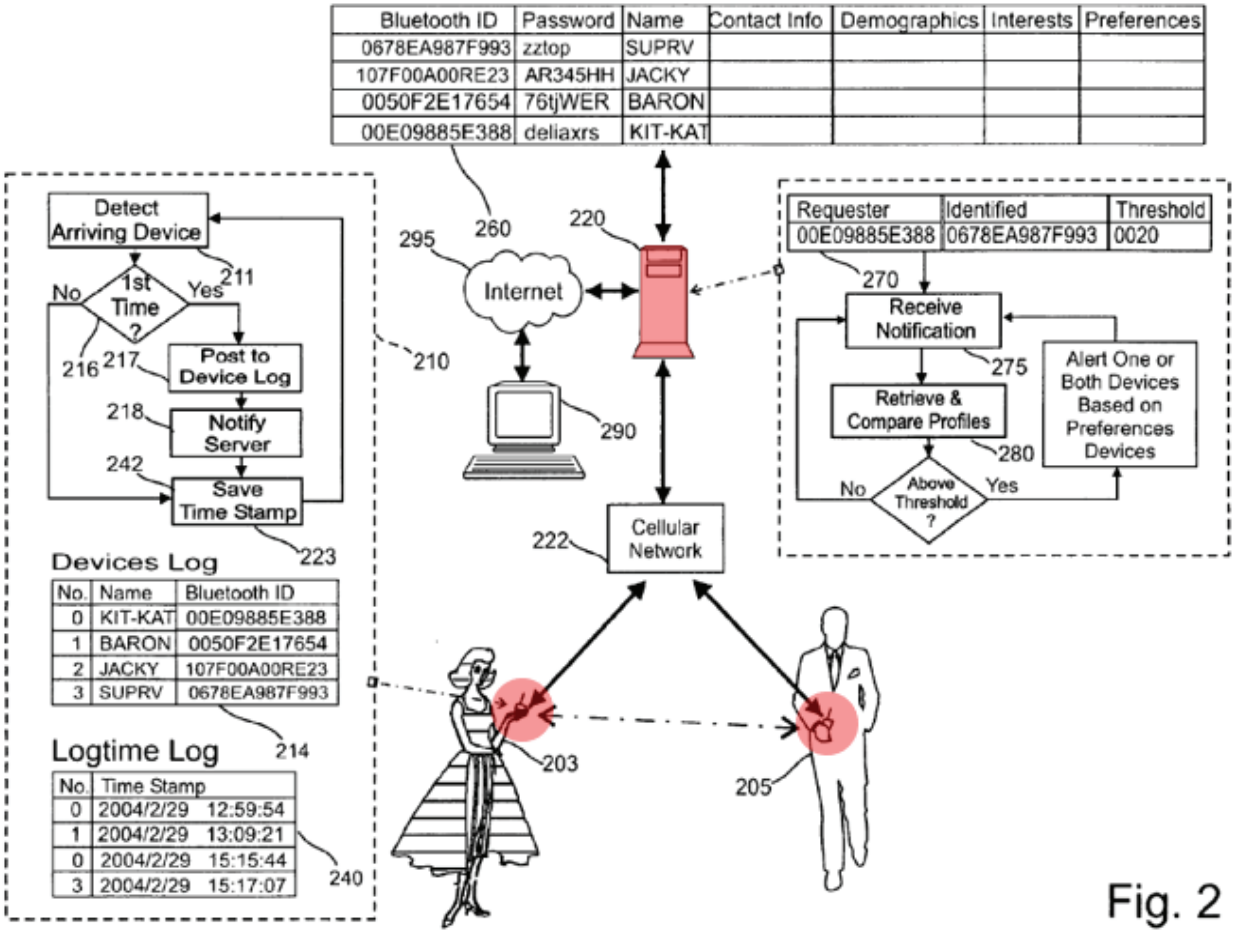


Fig. 2

(2) [1.A] "a first radio; a second radio;"

144. Eagle teaches *first* and *second radios*.

145. Eagle teaches that the Requester Device is a cellular telephone that includes a "long range communications interface coupled to [a] long range

communications network" (*i.e.*, a first radio) and "short range radio transceivers that use the Bluetooth protocol" (*i.e.*, a second radio). Eagle, [0018], claim 2; *see also* [0019]-[0020], [0022], [0028], [0038]-[0040].

(3) [1.B] "one or more processors; one or more memory devices coupled to the one or more processors, the one or more memory devices storing a set of instructions that when executed by the one or more processors cause the one or more processors to perform operations including:"

146. Eagle teaches the Requester device including *one or more processors*. Eagle, [0019] ("Each… Bluetooth enabled cellular phone[] includes a processor that is specially programmed"); *see also* [0020], [0028], claim 2.

147. Eagle teaches the Requester Device including *one or more memory devices coupled to the one or more processors, the one or more memory devices storing a set of instructions that when executed by the one or more processors cause the one or more processors to perform operations* (for example, the processor executes programming installed on the Requester Device).

148. Eagle teaches that its method for facilitating networking communications is performed, in part, by executing an application program that is "downloaded" and "installed" on the Requester Device. Eagle, [0028]-[0029]. A POSITA would have recognized that downloading, installing, and executing an application program as described obviously, if not necessarily, requires a *memory*

on the device coupled to the processor. Processors executing instructions stored on memory is a well-known configuration for digital computing systems. *See* Olkkonen, 15:31-34, 35:39-41, 49:56-59 (describing programs stored in memory and executed by processors). *See also* Eagle, [0023]-[0024] (describing a memory for storing log data).

(4) [1.D] "receiving, using the first radio, identifier related information associated with a proximity beacon service, from one or more servers;"

149. Eagle-Behrens teaches *receiving, using the first radio* (for example, receiving using the long-range communications interface)*, identifier related information associated with a proximity beacon service* (for example, information associated with Eagle's social introduction system, such as blacklists, friend lists, and alerts)*, from one or more servers* (for example, from a server).

150. Eagle teaches the Requester Device communicating with a server using the long-range communications interface. Eagle, [0004], [0007], [0011], [0020]-[0021]. The server performs functions for Eagle's social introduction system ("BlueAware"), which is a *proximity beacon service* that facilitates communications between Bluetooth devices such as the Requester Device and other Bluetooth devices "used as beacons to identify [themselves] to other nearby devices." Eagle, [0008], [0043]-[0061] (describing server operations).

151. The Requester Device receives *identifier related information from the*

server as discussed below.

(a) Receiving blacklists and friend lists

152. As discussed above, it would have been obvious for the Requester Device to receive blacklist information and/or friend list information from the server.

153. Regarding blacklists, Behrens teaches that the Requester Device "may store [unique identifiers (UIDs)] to be ignored in a blacklist," received as instructions from the server, to eliminate spam and other unwanted behavior. Behrens, [0101]-[0102], [0124]. The blacklist received and used by the Requester Device to ignore UIDs (identifiers) and is therefore *identifier related information*.

154. Regarding friend lists, Eagle teaches that the server stores profile information "specifying a set of device IDs for devices owned by 'friends'" that form a "trust network" of devices. Eagle, [0056], [0066]-[0067]. Based on the friend list, the Requester Device is only alerted to the presence of nearby Identified Devices that are in the Requester Device's friend list—*i.e.*, part of its trust network. Eagle, [0056].

155. As discussed above, it would have been obvious for the Requester Device to receive the friend list from the server and use it to filter received UIDs locally. Accordingly, the friend list received and used by the Requester Device to identify trusted UIDs (identifiers) is *identifier related information*.

(b) Receiving alerts

156. Eagle teaches notifying the server with the unique identifiers of the nearby devices (nearby Identified Devices). Eagle, [0048]; "UIDs" are unique identifiers as taught by Behrens, as discussed above. The server uses the received UIDs to fetch profile information from a profile database. Eagle, [0005], [0020], [0041], [0045], [0050]-[0051].

157. The server compares the Requester Device's profile information with the Identified Device's profile information to determine whether they satisfy matching criteria. Eagle, [0005], [0020], [0024], [0040], [0042], [0048], [0051]. If so, an alert message is transmitted to the Requester Device. Eagle, [0006], [0020], [0052].

158. The alert message includes stored profile information associated with the matching Identified Device, for example, contact information and "any other information which is of use in a specific application" and useful to "promote communication between[] nearby devices and their owners." Eagle, [0007], [0020]-[0021], [0053], [0058].

159. The server generates alerts from profile information fetched from a database using the UIDs (identifiers) of Identified Devices, and so the profile information is *identifier related information*.

(5) [1.E.I] "receiving, using the second radio, a plurality of short range transmissions, including a plurality of proximity beacon transmissions when the device is located within a detection range of one or more beacon transmitter devices associated with the proximity beacon service, each of the proximity beacon transmissions including"

160. Eagle-Behrens-Olkkonen teaches receiving, using the second radio (for example, receiving the short range transceivers via Bluetooth protocol), a plurality of short range transmissions including a plurality of proximity beacon transmissions (for example, inquiry responses containing identifying information from Identified Devices), when the device is located within a detection range of one or more beacon transmitter devices (for example, the Requester Device receives inquiry responses from discoverable Identified Devices in Bluetooth range) associated with the proximity beacon service each of the proximity transmissions including (for example, Identified Devices participating in Eagle's social introduction system transmit certain information, *see* [1.E.II]-[1.E.IV] discussed below).

161. Eagle explains that Bluetooth devices transmit beacon transmissions when "used as beacons to identify a device to other nearby devices" by transmitting "device identification codes." Eagle, [0008]. The device log (Fig. 2, below) shows exemplary separate fields "name," "Bluetooth ID," etc.

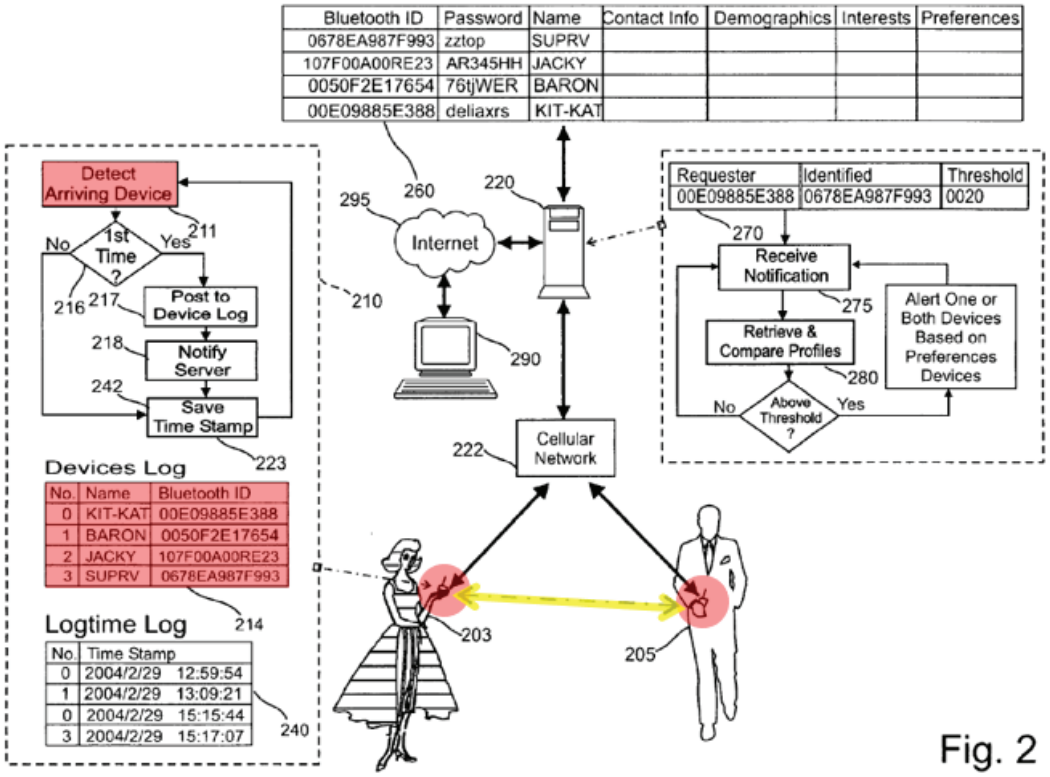


Fig. 2

162. By way of example, the Requester Device may detect the presence (step 211) of a second Bluetooth phone carried by individual 205 (an Identified Device) via reception of the Identified Device's beacon transmissions, including for example a "Bluetooth ID" (an assigned address value). Eagle, Fig. 2, [0022]. This information is received when a Requester Device "perform[s] an inquiry function to determine the identity and Device Class of other 'discoverable' Bluetooth devices," and the Identified Device responds to the inquiry. Eagle, [0033]-[0038]. Discoverable Bluetooth devices must be "within Bluetooth range" of the Requester Device to receive and respond to inquiry messages—approximately 10-100 meters—and so transmissions from an Identified Device are

only received when the devices are located within a detection range of one another. Eagle, [0003]-[0005], [0020], [0030], [0033]-[0037].

163. Additionally, a Devices Log 214 stored in the Requester Device "indexes every device encountered by the phone" and, as shown in Fig. 2 above, the Requester Device has encountered several devices. Eagle, [0022]-[0025]. Accordingly, based on communications with Identified Devices, Eagle teaches that the Requester Device receives a plurality of beacon transmissions from a plurality of Identified Devices.

164. Discussed with respect to limitations [1.E.II]-[1.E.IV] below, Eagle-Behrens-Olkkonen teaches that Identified Devices participating in Eagle's social introduction system (i.e., associated with the proximity beacon service) transmit certain information in each of the proximity beacon transmissions, as claimed.

(6) [1.E.II] "a respective MAC address,"

165. Eagle-Behrens discloses respective beacon transmissions including *a respective MAC address* in two separate ways discussed below.

(a) UIDs include a MAC address

166. Eagle-Behrens teaches *a respective MAC address* (for example, a BD_ADDR is included in the UIDs).

167. As discussed above, Behrens teaches that the Identified Device identifies itself to the Requester Device with a transmission including a

combination of UIDs including, for example, its respective 48-bit "Bluetooth Device Address" or BD_ADDR. Behrens, [0061], [0097], [0122]. The '918 patent similarly acknowledges that a "MAC address" is, for example, a "Bluetooth BD_ADDR." EX1001, 9:41, 26:4-7.

168. Eagle-Behrens's 48-bit BD_ADDR included as a UID identifying the Identified Device is therefore *a respective MAC address*.

(b) Bluetooth communications include a MAC address

169. Eagle teaches that the Requester Device and Identified Device use Bluetooth protocols. Eagle, [0018], [0028]. Accordingly, the Identified Device identifying itself to the Requester device would have included *a respective MAC address* in its inquiry response. Eagle, [0033]-[0037] (describing a Bluetooth discovery process between devices, such as a Requester Device (sending inquiries) and Identified Device (responding to inquiries)); Olkkonen, 2:23-31 ("inquiry response is a message packet containing the responding device's Bluetooth Device Address"), 27:12-20 (FHS packet structure for an inquiry response contains a BD_ADDR and clock); EX1008, 283 (FHS packet sent in response to an inquiry contains the Bluetooth device address of the sender).

170. The '918 patent similarly acknowledges that the MAC address of the transmitting device is "always broadcast in any operation of a Bluetooth or [Wi-Fi]

link." EX1001, 10:61-63.

(7) [1.E.III] "a respective unique identifier, and"

171. Eagle-Behrens teaches each beacon transmission comprising *a respective unique identifier* (for example, UIDs including a unique number uniquely identifying a device and its owner).

172. As discussed above, the Identified Device identifies itself to the Requester Device with a transmission including a combination of UIDs. Behrens teaches that UIDs are "any unique or quasi-unique code, number, address, symbol, or a combination thereof, which uniquely identifies a device, and, by association, the owner of the device." Behrens, [0061], [0097]. Eagle-Behrens therefore teaches the beacon transmission including *a unique identifier*, such as a unique number or symbol that identifies the Identified Device and its owner. UIDs like a unique number or symbol are included in beacon transmissions in addition to the MAC address identified for [1.E.II] above because UIDs may be a combination of different unique identifiers. Behrens, [0097], [0122].

173. Accordingly, Eagle-Behrens's UID includes *a respective unique identifier*.

(8) [1.E.IV] "a Proximity Beacon Service Identifier (PBSI);"

174. Eagle-Olkkonen teaches each beacon transmission comprising *a*

Proximity Beacon Service Identifier (PBSI) (for example, service class information that identifies Eagle's social introduction system).

175. As discussed above, it would have been obvious for an Identified Device to respond to inquiries from a Requester Device with *beacon service identifiers* such as service class information for the purpose of filtering UIDs.

176. Service class information includes information that Identified Devices access from their service registries "characterizing the ad hoc network" of which it is a member. Olkkonen, 5:27-33, 12:40-48, 13:33-43, and 17:49-63. This information includes service class information identifying running application programs (Olkkonen, 5:13-17, 17:17-22, 30:22-28, Fig. 5) and, in view of Eagle, would have included an identification of Eagle's social introduction system—a *PBSI* identifying the *proximity beacon service* provided by Eagle's application program and server.

177. I note that while Proximity Beacon Service Identifier is capitalized in this claim and given the initialism of PBSI, "PBSI" is not a term of art conveying any particular or specialized meaning to a POSITA. Eagle's social introduction system, which facilitates communications between devices in proximity to one another through the use of short-range (Bluetooth) beacons is therefore a *proximity beacon service*, and identifiers used in Eagle's system (as modified by Olkkonen) are *PBSIs*.

(9) [1.F.I] "determining if a particular short range transmission of the plurality of short range transmissions a) includes a MAC address, and"

178. Eagle teaches the Requester Device *determining if a particular short range transmission of the plurality of short range transmissions a) includes a MAC address*.

179. Eagle teaches that the Requester Device maintains a Devices Log of detected Identified Devices by their unique identifiers, such as its Bluetooth device address (BD_ADDR) (*a MAC address*). Eagle, [0022]-[0023]. Logging the MAC address requires the Requester Device to parse inquiry responses to find the location of the MAC address and, if it finds a value in that location (*i.e.*, *determines* that the inquiry response *includes a MAC address*), then record the value. Moreover, according to Bluetooth protocols, an inquiry response (as used in Eagle's system) includes a MAC address (BD_ADDR) of the responding device. See my discussion of Bluetooth inquiry responses in at least Section IV.B.e.ii above. A Requester Device receiving an inquiry response will parse the response and look for the BD_ADDR in the appropriate field to understand who it is receiving the information from and to who future communications should be directed to.

(10) [1.F.II] "b) includes the proximity beacon service identifier (PBSI) and if c) the PBSI indicates the particular short range transmission is a proximity

beacon transmission associated with the proximity beacon service;"

180. Eagle-Olkkonen teaches the Requester Device determining if a particular short range transmission *includes the proximity beacon service identifier (PBSI) and if c) the PBSI indicates the particular short range transmission is a proximity beacon transmission associated with the proximity beacon service* (for example, determining if received transmissions include service class information identifying Eagle's social introduction system).

181. Eagle-Olkkonen teaches the Requester Device receiving, from Identified Devices, inquiry responses including *PBSIs* such as service class information identifying Eagle's social introduction system. *See* [1.E.IV].

182. As discussed above, Eagle teaches the Requester Device determining "whether the detection of [each Identified Device] warrants the transmission of a notification message to the server" (Eagle, [0020], [0024]), and Olkkonen teaches that it would have been obvious to filter and select only the UIDs of Identified Devices that identify Eagle's social introduction system based on the received service class (identifying service relevant to Eagle's social introduction system; Olkkonen, 11:33-60, 22:34-43). Selection and filtering techniques would have been well-known to a POSITA, including, for example, by analyzing received information and determining if they match a desired value. Olkkonen, 22:8-12,

22:34-43.

183. To determine whether inquiry responses include service class information indicating that the UIDs in those inquiry responses should be selected for notification to the server (*i.e.*, *determines if the PBSI indicates the particular short range transmission is a proximity beacon transmission associated with the proximity beacon service*), the Requester Device must therefore parse the inquiry responses to find the service class information, and, if it finds values in those service class locations (*i.e.*, *determines that the inquiry response includes the PBSI*), then determines if the service class information identifies Eagle's social introduction system. As similarly discussed with respect to the MAC address above, according to Bluetooth protocols, an inquiry response (as used in Eagle's system) and extended inquiry response includes fields for service class information from the responding device. See my discussion of Bluetooth inquiry responses in at least Section IV.B.e.ii above. A Requester Device receiving an inquiry response will parse the response and look for service class information in the appropriate fields to understand the capabilities of the device it is receiving information from.

(11) [1.G] "then: determining if an entity or object associated with the proximity beacon service is in proximity to the mobile wireless device, by utilizing the identifier related information and the unique identifier."

(a) Eagle

184. As an initial matter, the claim language here, of *determining if an entity or object… is in proximity to the mobile wireless device* is automatically true for received Bluetooth transmissions because the "proximity" of a Bluetooth device is necessarily confirmed by the mere transmission and reception of signals using Bluetooth protocols due to Bluetooth's limited range. As discussed for [1.E.I], Bluetooth beacon transmissions are received from devices in detection range, which is approximately 10-100 meters. Therefore, a beacon transmission received from a Bluetooth device, which has an entity/person associated with it, is already in "proximity" to the Requester Device.

185. Additionally, Eagle's system *then determines if an entity or object associated with the proximity beacon service* (*e.g.*, with respect to an Identified Device that had been determined to be relevant to Eagle's social introduction system, showing an alert) *is in proximity to the mobile wireless device* (*e.g.*, the alert indicates the device is nearby)*, by utilizing the identifier related information* (*e.g.*, by displaying received profile information) *and the unique identifier* (*e.g.*, alerts received and displayed as showing proximity are associated with the UIDs utilized for identifying the particular Identified Device). For example, a "nearby…restroom" (Eagle, [0061]) is determined to be in proximity to a tradeshow beacon by alerting the user of its presence or location with the information received from the server (Eagle, [0020]-[0021], [0048]). The restroom

in proximity is directly associated with a tradeshow beacon's UIDs because the associated UIDs' server data identifies that particular restroom via the server's visual notification/alert functions processed by the device (Eagle, [0020]-[0021], [0048]), and is therefore *utilized* in the determination of proximity.

186. To the extent proximity in [1.G] may be satisfied in other ways (for example by filtering UIDs for notification to the server and/or by determining a permission for disclosing proximity, as discussed in Section V.A above), Eagle-Behrens teaches additional proximity determinations as discussed below.

(b) Blacklists and friend lists

187. As discussed for [1.D], Eagle-Behrens teaches receiving UID blacklists and/or friend lists that identify UIDs to ignore or to select for alerts, respectively. That is, the Requester Device using a blacklist would ignore received UIDs on the blacklist and not notify the server of those UIDs. Behrens, [0101]-[0102], [0124] ("ignore" UIDs). Likewise, the Requester Device using a friend list would notify the server of UIDs when they are on the friend list. Eagle, [0056] (alert messages only for trusted persons on friend lists). The friend list only serves as an initial filter of UIDs, as the Requester must still contact the server to determine whether the UID on the trusted friend list has "common interests [and] is nearby." Eagle, [0056].

188. Accordingly, Eagle-Behrens teaches determining *if an entity or object*

associated with the proximity beacon service (for example, determining, in relation to the Identified Device that identified Eagle's social introduction system, *see* [1.F.II]) *is in proximity to the mobile wireless device* (for example, deciding to notify the server of UIDs and receive alerts in response that determine that the Identified Device is nearby) *by utilizing the identifier related information* (using the blacklist and/or friend list as a filter of UIDs) *and the unique identifier* (checking UIDs against those lists).

(c) Alerts

189. Eagle further teaches that the same Identified Device may be encountered more than once. Eagle, [0023]-[0024] (scenarios include detecting an Identified Device already in the Devices Log). While a Requester Device would not notify the server again of an Identified Device that it recently encountered (*i.e.*, Identified Device has not yet been removed from the Devices Log; Eagle, [0023]-[0024]), Eagle leaves to a POSITA whether the profile information of an Identified Device found on the recently encountered log would be presented again.

190. As discussed above, it would have been obvious to present the alert information on the Requester Device again for an Identified Device previously encountered, as taught by Behrens. For example, Behrens teaches that if an Identified Device, "of which [a Requester Device] has previously stored the identifier and possibly received other data from, … has reentered [the Requester

Device's] range," then it is preferable to notify the user of that device again to make a connection. Behrens, [0035]. As Eagle's notifications to the user of the Requester Device are in the form of alerts including received profile information, it would have been obvious to present that alert information again, facilitating a connection between the devices. Eagle, [0007] (alerts include information useful to promote communication); Behrens, [0035] (sharing contact information).

191. Accordingly, Eagle-Behrens teaches *determining if an entity or object associated with the proximity beacon service* (for example, determining, in relation to the Identified Device that identified Eagle's social introduction system, *see* [1.F.II]) *is in proximity to the mobile wireless device* (for example, deciding to alert the user of the Requester Device of identified nearby Identified Devices) *by utilizing the identifier related information* (using the previously received alert information for presentation to the user) *and the unique identifier* (for example, UIDs are the identifying information used throughout Eagle's system to, for example, log and lookup devices in the Device Log; UIDs here are used to identify the UID as previously logged and to retrieve profile information for alerts).

ii) *Claim 2: "The mobile wireless device of claim 1, wherein the MAC address is a randomly generated 48 bit number matching a format of a Bluetooth BD_ADDR."*

192. Eagle teaches that the MAC address is a 48-bit number matching a format of a Bluetooth BD_ADDR (for example, the Identified Device's

BD_ADDR).

193. To the extent Eagle does not explicitly describe that *the MAC address is a randomly generated 48 bit number matching a format of a Bluetooth BD_ADDR*, it would have been obvious to a POSITA to use a randomly generated number for the BD_ADDR for privacy and security.

194. In particular, as discussed above, a POSITA would have understood the concerns regarding privacy and tracking through identifiers—and the changing of identifiers as a solution to those concerns—was well-known in short-range wireless communications systems. Known solutions included the use of randomly generated identification numbers, such as a "randomized version of the BD_ADDR" to be "used in all the functions of the Bluetooth device that normally use the BD_ADDR." EX1011, [0006]-[0013]. As documented in the prior art, one method for randomizing the BD_ADDR included generating a pseudonym BD_ADDR with a random number generator and substituting the pseudonym BD_ADDR for the real BD_ADDR in transmissions such as inquiry responses. EX1011, [0054], [0057], [0088].

195. Therefore, a POSITA would have been motivated to modify the Identified Device (and other Bluetooth devices in the system) to randomize the BD_ADDR value transmitted in Bluetooth communications, and would have had a reasonable expectation of success in doing so.

iii) *Claim 3*

(1) [3.PRE] "The mobile wireless device of claim 1 wherein the one or more processors further execute the instructions to perform operations including:"

196. Eagle teaches the processor executing instructions. *See* [1.B].

(2) [3.A] "receiving, by the second radio, a first proximity beacon transmission including a first MAC address and a first unique identifier at a first time; and"

197. Eagle-Behrens teaches this limitation for the same reasons discussed for [1.E].

198. In particular, Eagle-Behrens teaches receiving, by the second radio, a plurality of proximity beacon transmissions including "respective" MAC addresses and unique identifiers. *See* [1.E]. The limitation merely labels a particular beacon transmission and its contents, among the plurality, as "first."

199. Furthermore, the receiving of the first beacon transmission may be defined as occurring at a *first time*.

(3) [3.B.I] "receiving, by the second radio, a second proximity beacon transmission including a second MAC address and a second unique identifier at a second time,"

200. Eagle teaches its system operating over many time periods, including at a *second time*. For example, Eagle teaches that the Requester Device periodically scans the environment for Identified Devices. Eagle, [0026], [0033]. Furthermore, the same Identified Device may be detected at different times (Eagle,

[0023]) and a Requester Device may join and leave existing networks and activities, or detect and re-detect other devices as they move in and out of range of each other (Olkkonen, 1:46-61, 2:51-65 (explaining Bluetooth operations)). Any device that is in Bluetooth range of the Requester Device and that is in a "discoverable" mode will respond to the Requester Device's inquiries and be detected as an Identified Device. Eagle, [0019], [0033]-[0037].

201. For illustrative purposes to address this claim and other related limitations, it may be assumed that a particular Identified Device is detected one or more times at a *first time*, and the same particular Identified Device is detected again one or more times at a *second time* that follows the first time period. In both time periods, the Identified Device remains a participant in the same services and networks (for example, participating in Eagle's social introduction system and running Eagle's software, participating in an ongoing baseball game or CAD design project). For example, over the course of a work week or while attending a multi-day event (for simplicity, one day would be a first time and a second day would be a second time), a user of an Identified Device has "chang[ed] UIDs" overnight to present themself with a "new online identity" on the second day while still having a "single user account" on the server. Behrens, [0061], [0115]; *see also* [0103] (user "exercise[s] control over which or how many UIDs are transmitted"). As discussed above, changing UIDs in this manner prevents tracking over time,

and Behrens explains that the user may supply their UIDs to the server for synchronization. Behrens, [0065], [0076].

202. Accordingly, for the same reasons that Eagle-Behrens teaches *receiving, by the second radio, a first proximity beacon transmission including a first MAC address and a first unique identifier at a first time* (*see* [3.A]), Eagle-Behrens teaches *receiving, by the second radio, a second proximity beacon transmission including a second MAC address and a second unique identifier at a second time*.

(4) [3.B.II] "the second MAC address being different from the first MAC address and"

(a) UIDs include a MAC address

203. As discussed above regarding the combined teachings and regarding [1.E.II] and [3.B.I], Behrens teaches that (1) UIDs may be a combination of different UID values, and (2) UIDs change. An Identified Device's UIDs may therefore be changed for the second time to use a WLAN MAC address instead of the BD_ADDR used in the first time period. Behrens, [0061], [0097], [0103], [0111], [0115], [0122].

204. A POSITA would have recognized that wireless communications device WLAN MAC addresses are different from their Bluetooth device addresses. For example, Apple Inc.'s iPhone 3G in 2008 included Wi-Fi and Bluetooth

capabilities (*see* EX1035), which had different addresses for each (*see* EX1036, 142).

(b) Bluetooth communications include a MAC address

205. To the extent Eagle does not explicitly describe that the first and second MAC addresses received from the Identified Device according to the Bluetooth protocol are *different*, a POSITA would have been motivated to modify the Identified Device (and other Bluetooth devices in the system) to periodically randomize the BD_ADDR value transmitted in Bluetooth communications for privacy and security. *See* discussion of claim 2 above.

206. Accordingly, because the BD_ADDR is periodically randomized, *the second MAC address* is *different from the first MAC address.*

(5) [3.B.III] "the second unique identifier being different from the first unique identifier; and"

207. Eagle-Behrens teaches the *second unique identifier being different from the first unique identifier* (for example, changing from the UIDs from a unique number to a unique symbol).

208. As discussed above regarding the combined teachings and regarding [1.E.III] and [3.B.I], Eagle-Behrens teaches that UIDs may be a combination of different UID values, and further that UIDs change. An Identified Device's UIDs may therefore be changed for the second time period to include, for example, a

"unique… symbol" Instead of the unique number used in the first time period. Behrens, [0061], [0097], [0103], [0115], [0122].

(6) [3.C] "associating the first and second unique identifier with a single beacon transmitter device."

209. Eagle-Behrens teaches *associating the first and second unique identifier with a single beacon transmitter device* (for example, associating with a single Identified Device).

210. As discussed above for [3.B.I], the first and second unique identifier (UIDs) received in the first and second times, respectively, are received from the same Identified Device—*i.e.*, the first and second UIDs come from the same *single beacon transmitter device*.

211. As discussed for [1.D], the Requester Device notifies the server of the UIDs so that the server fetches stored profile information from a profile database and then transmits alerts back to the Requester Device identifying the Identified Device. When the Identified Device has been removed from Eagle's log of recently detected devices between the first and second time, then the same actions of notifying the server, receiving an alert, and displaying the alert will be performed each time. Eagle, [0023]-[0024]. The first and second alerts contain, for example, the phone number or other contact information for the Identified Device and any other information useful to "promote communication between[] nearby devices and

their owners." Eagle, [0007], [0020]-[0021], [0053].

212. Accordingly, because the Requester Device receives the same contact information for the same Identified Device in response to notifying the server of the *first unique identifier* and the *second unique identifier*, the Requester Device associates both UIDs with *a single beacon transmitter device*.

iv) ***Claim 4: "The mobile wireless device of claim 1, wherein the one or more processors further execute the instructions to perform operations including: further determining that at least one beacon transmitter device associated with the proximity beacon service is in proximity to the mobile wireless device, by utilizing an action function including one or more previously downloaded unique identifiers."***

213. Eagle teaches the processor executing instructions. *See* [1.B].

214. Eagle-Behrens teaches *determining that at least one beacon transmitter device associated with the proximity beacon service is in proximity to the mobile wireless device* based on blacklists and friend lists or alerts. *See* [1.G]. I understand that the claims do not explain when or how "previously downloaded unique identifiers" were previously downloaded, but Eagle-Behrens teaches using previously downloaded unique identifiers as discussed below.

215. As discussed regarding the *determining* using blacklists and friend lists, the Requester Device checks whether UIDs received from Identified Devices are present on those blacklists and friend lists. *See* discussion of [1.G]. Accordingly, *further determining* is performed *by utilizing an action function* (for

example, comparing UIDs against the blacklist and/or friend list) *including one or more previously downloaded unique identifiers* (for example, the blacklist and friend list received from the server include UIDs of Identified Devices to be ignored or notified to the server).

216. As discussed regarding the *determining* using prior alerts of Identified Device profile information, the Requester Device presents previously received alert information to the user if a recently detected Identified Device (still on the Devices Log) is detected again by the Requester Device. *See* discussion of [1.G]. Furthermore, because Eagle and Behrens each teach that Bluetooth devices and alert information are both associated with UIDs, both the determination that an Identified Device is recently detected and the retrieval of alert information would have been performed using those UIDs. Eagle, [0031] (Bluetooth devices identified by their unique identification values), [0041] and [0051] (server fetches profile information based on unique identifiers; Behrens, [0035] (re-detected device has same "identifier"). That is, UIDs are *the* identifying information in both Eagle and Behrens, and so it would have been obvious to a POSITA continue using UIDs for information storage and retrieval whenever information relates to devices identifiable by UIDs. Accordingly, *further determining* is performed *by utilizing an action function* (for example, presenting previously received alert information) *including one or more previously downloaded unique identifiers* (for example,

Identified Devices in Eagle's Devices Log are detected by UIDs, and those UIDs were previously downloaded from Identified Devices during discovery; using UIDs to identify previously downloaded alert information).

v) *Claim 8*

(a) [8.PRE] "The mobile wireless device of claim 1 wherein the one or more processors further execute the instructions to perform operations including:"

217. Eagle teaches the processor executing instructions. *See* [1.B].

(b) [8.A] "receiving, via a second radio, the plurality of proximity beacon transmissions further includes receiving a first unique identifier at a first time that is different from a second unique identifier received at a second time; and"

218. Eagle-Behrens teaches this limitation for the same reasons discussed for [3.A] (receiving a first unique identifier at a first time via the second radio), [3.B.I] (receiving a second unique identifier at a second time via the second radio), and [3.B.III] (the first and second unique identifiers are different).

(c) [8.B] "associating the first and second unique identifier with a single beacon transmitter device."

219. *See* [3.C].

vi) *Claim 9*

(a) [9.PRE] "A method for facilitating use of proximity beacons, the method executing within a mobile device, and the method comprising:"

220. Eagle teaches *a method for facilitating use of proximity beacons* (for example, the Requester Device receives beacon transmissions from nearby Bluetooth Identified Devices), *the method executing within a mobile device* (for example, the Requester Device includes a processor to execute instructions to perform the method). *See* discussion of claim 1.

(b) [9.A] "communicating between the mobile device and one or more servers and receiving, at the mobile device, identifier related information, using a first radio;"

221. *See* [1.D].

(c) [9.B] "receiving, at the mobile device using a second radio, a plurality of short range transmissions, including a plurality of proximity beacon transmissions from one or more beacon transmitter devices associated with a proximity beacon service, each of the proximity beacon transmissions including a respective MAC address, a respective unique identifier (UID), and a Proximity Beacon Service Identifier (PBSI);"

222. *See* [1.E.I] (receiving transmissions), [1.E.II] (MAC address), [1.E.III] (UID), and [1.E.IV] (PBSI).

(d) [9.C] "a) determining that a particular short range transmission of the plurality of short range transmissions includes a MAC address,"

223. *See* [1.F.I].

(e) [9.D] "b) determining that the Proximity Beacon Service Identifier (PBSI) is present, and c) determining that the PBSI indicates the

particular short range transmission is a proximity beacon transmission associated with the proximity beacon service; and"

224. *See* [1.F.II].

(f) [9.E] "when the three determining steps a) b) and c) are each true, then d) determining that an entity or object associated with the proximity beacon service is within proximity to the mobile device, by utilizing the identifier related information and the unique identifier."

225. *See* [1.G].

vii) *Claim 10*

(a) [10.PRE] "The method of claim 9,"

226. *See* claim 9.

(b) [10.A] "wherein a first one of the plurality of proximity beacon transmissions received at a first time includes a first unique identifier, and wherein a second one of the plurality of proximity beacon transmissions received at a second time includes a second unique identifier the second unique identifier being different from the first unique identifier; and"

227. *See [3.A] (first unique identifier), [3.B.I] (second unique identifier), and [3.B.III] (first and second unique identifiers are different).*

(c) [10.B] "associating both the first unique identifier and the second unique identifier with a particular entity or object in proximity to the mobile device."

228. *See* [3.C.] (associating the first and second unique identifier with a

single Identified Device, which is an object in Bluetooth proximity to the Requester Device, and the Identified Device's user, which is an entity in Bluetooth proximity; *see* Eagle, [0007], [0020]-[0021] (alert identifies device and its owner).

viii) ***Claim 11: "The method of claim 9 wherein the MAC address is selected from a group consisting of (a) a randomly generated 48 bit number matching a format of a MAC address and (b) a Bluetooth BD_ADDR."***

229. *See* claim 2 (MAC address is a randomly generated BD_ADDR).

230. *See* [1.E.II] (MAC address is a BD_ADDR).

ix) ***Claim 12***

(a) [12.PRE] "The method of claim 9"

231. *See* claim 9.

(b) [12.A] "wherein a first one of the plurality of proximity beacon transmissions is received at a first time and includes a first unique identifier and first MAC address, and the Proximity Beacon Service Identifier (PBSI); and"

232. *See* [1.E.I]-[1.E.IV] (receiving a unique identifier, MAC address, and PBSI) and [3.A] (defining a first reception at a first time).

(c) [12.B] "wherein a second one of the plurality of proximity beacon transmissions received at a second time includes a second unique identifier different from the first unique identifier and a second MAC address different from the first MAC address, and the Proximity Beacon Service Identifier; and"

233. *See* [1.E.I]-[1.E.IV] (receiving a unique identifier, MAC address, and

PBSI) and [3.B.I]-[3.B.III] (defining a second reception at a second time with a different unique identifier and different MAC address).

234. Additionally, Eagle-Olkkonen teaches that the PBSI in the first and second transmissions is the same because, for example, the first and second transmissions are received from the same Identified Device participating in Eagle's same social introduction system, which is identified by the same PBSI. *See* [3.B.I].

(d) [12.C] "associating both the first unique identifier and the second unique identifier with the same entity or object in proximity to the mobile device."

235. *See* [10.B].

x) ***Claim 13: "The method of claim 9, further comprising preventing the sending of the unique identifier, using the first radio, to the one or more servers, based upon previous detections of the respective unique identifier associated with the proximity beacon transmission."***

236. Eagle teaches maintaining a timestamped log of devices that it has encountered. Eagle, [0022]-[0023]. Based on the timestamps, the Requester Device "determine[s] whether the detection of a given device warrants the transmission of a notification message to the server." Eagle, [0024], [0048].

237. Therefore, if it is determined that a unique identifier (UID) received in an inquiry response represents a device that had been recently detected, the Requester Device will not notify the server of the UID.

238. Accordingly, Eagle teaches *preventing the sending of the unique identifier* (for example, preventing the notification of UIDs to the server)*, using the first radio, to the one or more servers* (for example, communication with the server uses the first radio; *see* [1.A] and [1.D])*, based upon previous detections of the respective unique identifier associated with the proximity beacon transmission* (for example, based upon recent detection of the same UID received in the inquiry response).

xi) *Claim 14: "The mobile wireless device of claim 1, wherein the instructions further comprise: sending the unique identifier, using the first radio, to at least one server of the one or more servers, and receiving further information relating to an object or entity associated with being within proximity to the mobile device."*

239. Eagle-Behrens teaches *further sending the unique identifier* (for example, notifying the server with UIDs of an Identified Device not recently detected)*, using the first radio, to at least one server of the one or more servers* (for example, communication with the server uses the first radio; *see* [1.A] and [1.D])*, and receiving further information relating to an object or entity associated with being within proximity to the mobile device* (for example, receiving an alert including profile information of the nearby Identified Device and its owner).

240. Eagle teaches notifying the server with the unique identifiers of the nearby Identified Devices, for example, when an Identified Device is not on its

Devices Log of recently detected devices. Eagle, [0023]-[0024], [0048]; "UIDs" in view of Behrens. The server uses the received UIDs to fetch profile information from a profile database. Eagle, [0005], [0020], [0041], [0045], [0050]-[0051]. The server compares the Requester Device's profile information with the Identified Device's profile information to determine whether they satisfy matching criteria. Eagle, [0005], [0020], [0024], [0040], [0042], [0048], [0051]. If so, an alert message is transmitted to the Requester Device. Eagle, [0006], [0020], [0052].

241. The alert message includes stored profile information associated with the matching Identified Device, for example, contact information and "any other information which is of use in a specific application" and useful to "promote communication between[] nearby devices and their owners." Eagle, [0007], [0020]-[0021], [0053], [0058].

xii) ***Claim 15: "The mobile wireless device of claim 1, wherein the instructions further comprise: preventing the sending of the unique identifier, using the first radio, to the one or more servers, based upon previous detections of the respective unique identifier associated with the proximity beacon transmission."***

242. *See* claim 13.

xiii) ***Claim 16: "The mobile wireless device of claim 1, wherein the instructions further comprise: controlling further communications between the mobile device and at least one device or server associated with an entity or object in proximity to the mobile device."***

243. Eagle-Behrens teaches this limitation in two ways.

244. First, as discussed for claim 13, Eagle teaches preventing the Requester Device from notifying the server with UIDs of nearby Identified Devices recently encountered. Eagle therefore teaches *controlling further communications* (for example, not sending a notification to the server) *between the mobile device and at least one device or server associated with an entity or object in proximity to the mobile device* (for example, between the Requester Device and the server, which is associated with Identified Devices as providing services under Eagle's social introduction system).

245. Second, as discussed for claim 1, Eagle-Behrens teaches receiving, from a server, a blacklist of UIDs that the Requester Device should ignore. Behrens, [0101]-[0102], [0124]. A POSITA would have recognized obvious ways for implementing a blacklist of UIDs after the Requester Device receives a blacklist from a server and stores it in its memory. A first method would have included not notifying the server when one of these UIDs responded to an inquiry and, as a result, no connection is established. *See* Eagle, [0023]-[0025] ("determining whether… detection of a given device warrants the transmission of a

notification message to the server")). A second method would have included downloading the blacklist to other user devices that were members of a service so they would not respond to inquiries made by devices that were on the blacklist (for example, a Requester Device would not respond to inquiries from other Requester Devices on a blacklist. Other methods would have included blocking all further contact with blacklisted UIDs. *See* Behrens, [0026], [0101] (blacklists "stop the other user[s] from further contacting [the user to be ignored])).

246. Eagle-Behrens therefore teaches *controlling further communications between the mobile device and at least one device or server associated with an entity or object in proximity to the mobile device* (for example, not permitting communication between the Requester Device and the server for notification of blacklisted UIDs, the server being associated with Identified Devices as providing services under Eagle's social introduction system; preventing communication between the Requester Device and other Identified Devices on the blacklist).

i) *Claim 17: "The method of claim 9, further comprising: receiving, using the first radio, access code information by the mobile device from at least one of the servers; and utilizing the access code information to gain access to the entity or object determined to be in proximity to the mobile device."*

247. Eagle teaches *receiving, using the first radio, access code information by the mobile device from at least one of the servers* (for example, receiving contact information); *and utilizing the access code information to gain access to*

the entity or object determined to be in proximity to the mobile device (for example, using the contact information to connect with the nearby device or resource).

248. Eagle teaches that the Requester Devices receives alerts from the server (using the first radio, *see* [1.A] and [1.D]) including contact information, such as phone numbers, email addresses, and website URLs. Eagle, [0007], [0050]. Upon receiving an alert, the Requester Device *utilizes* the contact information to connect with (or *gain access to*) the nearby Identified Device and its owner/user. For example, Eagle describes providing a phone number to make a direct call to the Identified Device. Eagle, [0058]; *see also* [0063] (system "put[s] the attendee in contact" with others). Additionally, with respect to other uses, like website URLs, the use of beacons to provide access codes was old and well-known in informational systems. EX1039, 23:1-10 (beacon providing a link to a webpage with a special sale); EX1040, [0073] (client-server network providing a link with an embedded promotional code or special URL). Because Eagle only provides contact information to matched profiles and contact information is not freely distributed, the received contact information acts as credentials that grant access to the other devices, people, and resources, and are therefore *access codes* as claimed.

ii) ***Claim 18: "The method of claim 9, wherein receiving the identifier related information, using the first radio, is performed in response to sending at least the unique identifier to at least one of the one or more servers using the first radio."***

249. Eagle teaches *receiving the identifier related information, using the first radio*, for example, receiving alert information including profile information, as discussed for [1.D] and [9.A] above.

250. As discussed for [1.D] and claim 14, alerts are received from the server *in response to sending at least the unique identifier to at least one of the one or more servers using the first radio* (for example, notifying the server with Identified Device UIDs and receiving alerts in response; communications with the server use the first radio, *see* [1.A] and [1.D]).

iii) ***Claim 19: "The method of claim 9, additionally comprising: sending the unique identifier, using the first radio, to at least one server of the one or more servers, and receiving further information relating to an object or entity associated with being within proximity to the mobile device."***

251. *See* claim 14.

iv) ***Claim 20: "The method of claim 19, wherein the further information relates to one or more of the following: a loyalty program; a payment service; or a coupon relating to an entity in proximity to the mobile device; or advertising content."***

252. As discussed for claims 14 and 19, Eagle teaches receiving *further information* including profile information about an Identified Device and its owner.

This information is *advertising content* because it advertises the Identified Device (and its owner) as having interests relevant to the Requester Device (and its owner). Eagle, [0007], [0021], [0058].

253. Eagle further describes receiving other types of information, including "special instructions or announcements" at a trade show, "nearby resources or facilities, such as an approaching free taxi, or a nearby public restroom," and "products and expertise" from salesmen. Eagle, [0061]-[0063]. These are also *advertising content*, as they make the user of the Requester Device aware of nearby information, goods, and services.

v) *Claim 22: "The method of claim 19, wherein the further information relates to a nearby user of an application on another device, in common with an application on the mobile device."*

(1) Eagle's BlueAware application

254. Eagle teaches that *the further information* (for example, received alerts of nearby Identified Devices) *relates to a nearby user of an application on another device, in common with an application on the mobile device* (for example, users of devices include participants in Eagle's social networking system, which requires installing an application).

255. Eagle teaches that its method for facilitating networking communications is performed, in part, by executing an application program

("BlueAware") that is "downloaded" and "installed" on the Requester Device and participating Identified Devices. Eagle, [0028]-[0029]. Accordingly, where the Requester Device receives information in the form of alerts (*i.e.*, profile information of participating Identified Devices), that information is about a user that participates in Eagle's social introduction system and has installed the necessary BlueAware application and therefore *relates to a nearby user of an application on another device, in common with an application on the mobile device*.

(2) Baseball application

256. Claim 22 references "an application," and dependent claim 23 adds that "the application is a multiuser game."

257. Eagle-Olkkonen additionally teaches that *the further information* (for example, the received alert information) *relates to a nearby user of an application on another device* (for example, relates to the user of the Identified Device, who is participating in a network baseball game)*, in common with an application on the mobile device* (for example, the Requester Device also has the network baseball game).

258. As discussed for claims 14 and 19, Eagle teaches receiving an alert of profile information about an Identified Device and its owner. This information *relates to a nearby user* because the Identified Device and its owner are near the

Requester Device (for example, in Bluetooth proximity).

259. Eagle-Olkkonen further teaches that the user of the Identified Device is a *user of an application on another device,* such as a *multiuser game* (for example, a participant in a collaborative baseball game program).

260. As discussed above, uses for networking and collaboration were numerous and included, for example, collaborative games.

261. Eagle explains that its social introduction system facilitates collaboration, which may be for specific purposes, for example, for social functions, work projects, etc., and information presented on the Requester Device therefore includes contact information useful for connecting with Identified Devices, including contact information, Bluetooth addresses, and Bluetooth device names. Eagle, [0028], [0038], [0041], [0050], [0063]-[0065].

262. Olkkonen describes other similar collaborative uses of Bluetooth networks, including a collaborative baseball application that an Identified Device may already have installed and be participating in. Olkkonen, 11:29-30 ("joining… game that is… being played"), 15:10-13, 15:31-42, 19:51-20:25 and 24:48-61 (describing program modules and information exchanged for a "network baseball application program… in [the Bluetooth device]" to "play ball" and update scoreboards). Additionally, since the Requester Device may have previously been a participant in a network baseball game (*see* Olkkonen, 1:46-61, 2:51-65,

explaining Bluetooth operations and describing a Requester Device joining and leaving existing networks and activities), it would have been obvious to a POSITA that the Requester Device also stores the same network baseball application program, and so the Identified Device's application is *in common with an application on the mobile device*.

263. Accordingly, as Eagle teaches collaborative applications of its system for social functions, and as Olkkonen teaches examples of social functions including network baseball, it would have been obvious to a POSITA that Eagle may alert the Requester Device of an Identified Device such that the user of the Identified Device may be a *nearby user of an application on another device* (for example, a user of the network baseball application program on the Identified Device), *in common with an application on the mobile device* (for example, in common with the same application program on the Requester Device).

vi) *Claim 23: "The method of claim 22, wherein the application is a multiuser game."*

264. *See* claim 22.

vii) *Claim 24: "The method of claim 9, additionally comprising: controlling further communications between the mobile device and at least one device or server associated with an entity or object in proximity to the mobile device."*

265. *See* claim 16.

viii) ***Claim 25: "The method of claim 9, wherein the step of determining that an entity or object is within proximity further comprises: comparing the identifier related information with the unique identifier or information derived from the unique identifier."***

266. As discussed for claim 4, Eagle-Behrens teaches *determining* that an Identified Device *is in proximity* based on blacklists and friend lists. *See also* [1.G]. Eagle-Behrens further teaches *determining* by *comparing the identifier related information* (for example, comparing blacklists and friend list UIDs) *with the unique identifier or information derived from the unique identifier* (for example, with Identified Device UIDs).

267. For example, regarding the *determining* using blacklists and friend lists, the Requester Device checks whether UIDs received from Identified Devices are present on those blacklists and friend lists. *See* discussion of [1.G]. Accordingly, the *determining* is performed by *comparing the identifier related information with the unique identifier or information derived from the unique identifier* (for example, comparing UIDs against UIDs on the blacklist and/or friend list). *See also* discussion of claim 4.

ix) ***Claim 27: "The mobile wireless device of claim 1, wherein the one or more processors further execute the instructions to perform the operations for determining that an entity or object is within proximity by further: comparing the identifier related information with the unique identifier or information derived from the unique identifier."***

268. *See* claim 25.

x) ***Claim 28: "The mobile wireless device of claim 1, wherein the receiving of the identifier related information, using the first radio, is performed in response to the one or more processors executing instructions for: sending at least the unique identifier to at least one of the one or more servers using the first radio."***

269. Eagle teaches the processor executing instructions (*see* [1.B]), and communications with the server use the first radio (*see* [1.A] and [1.D]).

270. As discussed for [1.D], Eagle teaches *receiving identifier related information, using the first radio* (for example, receiving alerts of profile information from the server).

271. As further discussed for [1.D], Eagle teaches that the receiving *is performed in response to the one or more processors executing instructions for: sending at least the unique identifier to at least one of the one or more servers using the first radio* (for example, the Requester Device receives alerts in response to notifying the server with UIDs of nearby Identified Devices).

xi) *Claim 31*

(1) [31.PRE] "The mobile wireless device of claim 3 wherein the one or more processors further execute the instructions to perform operations including:"

272. *See* claim 3.

273. Eagle teaches the processor executing instructions. *See* [1.B].

(2) [31.A] "receiving, via a second radio, the plurality of proximity beacon transmissions further includes receiving a first unique identifier at a first time that is different from a second unique identifier received at a second time; and"

274. *See* [8.A].

(3) [31.B] "associating the first and second unique identifier with a single beacon transmitter device."

275. *See* [8.B].

B. GROUND 2: EAGLE IN VIEW OF BEHRENS, OLKKONEN, AND PERTTILA RENDERS OBVIOUS CLAIMS 17

276. Eagle, Behrens, and Olkkonen were introduced in Ground 1 above.

277. U.S. Patent Application Publication No. 2004/0243519 to Perttila et al., titled "PROMPTED ELECTRONIC MOBILE-SERVICE INFORMATION COMMUNICATIONS WITH VALIDATION," was filed on June 2, 2003 and published on December 2, 2004.

278. Eagle provides a framework for social introductions and suggests various commercial uses (e.g., taxi/transportation services, publicizing products at

a trade show, Eagle, [0061]-[0063]) but leaves to the POSITA any further transactional details regarding, e.g., how merchants would have actually provided products to users and how users would have accessed those products.

279. Perttila is in the same field of endeavor as the ’918 patent, of wireless communications (Perttila, Abstract, [0001], [0007]-[0008]), and reasonably pertinent to the ’918 patent’s objectives of facilitating the exchange of information between entities and devices (Perttila, [0006]-[0007]) and validating individuals in commercial transactions (EX1001, 2: 8-24; Perttila, [0016], [0026], [0042]-[0043]). As shown in Fig. 1a (below), a system 20 according to Perttila includes, for example, a mobile wireless device 28 communicating with a merchant promotional article 36 via short-range protocols (Bluetooth) and communicating with a server 24 over long-range protocols (cellular). Perttila, [0026], [0037].

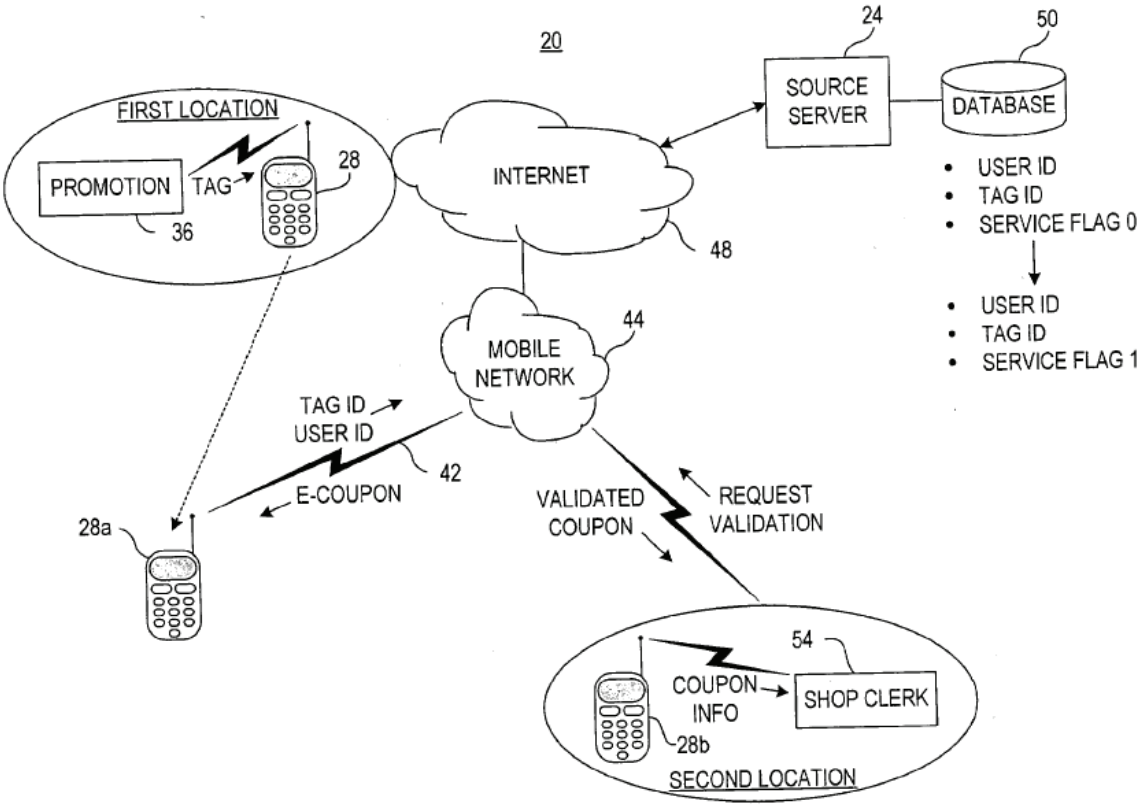


FIG. 1a

280. Perttila teaches a method for wirelessly providing users access to services and products in a secure way through electronic coupon redemptions. Perttila, Abstract, [0008]. For example, a user's Bluetooth device may detect a Bluetooth beacon inside a store, notify a server that it detected that beacon, and in return receive an electronic coupon for redemption inside that store. Perttila, [0011], [0028], [0037]-[0039]. The coupon may be a ticket to purchase or receive a "merchant offering," redeemed electronically by transferring and validating coupon information with the server. Perttila, [0005], [0041], claims 17, 26. Through validation, used/expired coupons may be rejected, providing merchant

control over its offerings. Perttila, [0043]; see [0006] (describing coupons with time/location limitations).

281. A POSITA applying Eagle's proximity-aware system for commercial purposes would have been motivated to look towards known e-commerce solutions for implementation, and it would have been obvious to a POSITA to modify Eagle's server to alert the Requester Device of nearby resources and products with an *access code* (coupon data including an "e-coupon ID" or "electronic data set") that is *utilized to gain access* to products and offerings *in proximity to the mobile device*, as taught by Perttila, to advantageously "ensure that the user has rights" to resources being offered—permitting merchants to control their offerings. Perttila, [0005]-[0015], [0043]. Specifically, while Eagle teaches that its social introduction system may be used for any of a variety of services and products, it leaves to the POSITA how to provide those services and products, and Perttila teaches one method that gives the merchant/offeror some level of control over its offerings.

282. The above modification would have been no more than the application of a known technique (Perttila's e-coupon access codes) to a known device ready for improvement (Eagle's system that identifies nearby resources facilitates interactions) to yield predictable results (controlling access to those resources) with a reasonable expectation of success (techniques for transferring and analyzing data were within the skill of a POSITA). As I discussed for claim 17 above (Ground 1),

the use of beacons to provide access codes was old and well-known in informational systems. EX1039, 23:1-10 (beacon providing a link to a webpage with a special sale); EX1040, [0073] (client-server network providing a link with an embedded promotional code or special URL).

C. GROUND 3: EAGLE IN VIEW OF BEHRENS, OLKKONEN, AND JONES RENDERS OBVIOUS CLAIM 29

283. Eagle, Behrens, and Olkkonen were introduced in Ground 1 above.

284. U.S. Patent Application Publication No. 2007/0264991 to Jones et al., titled "SERVICES NEAR ME: DISCOVERING AND CONNECTING TO AVAILABLE WIRELESS SERVICES UTILIZING PROXIMITY DISCOVERY," was filed on May 15, 2006 and published on November 15, 2007.

285. Jones, in the same field of endeavor of wireless communications (Jones, [0001]) and reasonably pertinent to the objective of facilitating the exchange of information between entities and devices (Jones, [0023]-[0026] (describing difficulties in discovering and connecting with nearby wireless services)), teaches different techniques for discovering short-range wireless services in proximity to a device. For example, one method includes a wireless device that "passively discover[s] services by listening to advertised service messages provided by other local devices" via Bluetooth. Jones, [0027]. Accordingly, devices providing services (*e.g.*, printing service, game) broadcast

advertising messages with service information "without prompting by a request message" from a user device. Jones, [0023]-[0025], [0034].

286. Claim 29 of the '918 patent requires that "the proximity beacon transmissions are received, at the mobile device, without requiring the mobile device to first perform a step of transmitting to the one or more beacon transmitter devices from which the plurality of proximity beacon transmissions are received."

287. Eagle teaches an active discovery method, where the Requester Device transmits inquiry messages and receives proximity beacon transmissions in response. *See* [1.E] above.

288. To the extent PO argues that Eagle does not teach receiving beacon transmissions *without requiring the mobile device to first perform a step of transmitting*, Jones renders obvious this alternative method for discovery.

289. A POSITA would have recognized power consumption/conservation as a universal design consideration that was especially important for battery-powered mobile devices. Eagle recognized the trade-off between scanning to "provide a rich depiction" of the user's environment and its detrimental effect on battery-life. Eagle, [0026]. A POSITA would have been motivated to find more power-efficient alternatives to Eagle's active discovery method, and Jones provides an explicit, well-known alternative to Eagle's exact problem by teaching a "passive" discovery method. By simply listening for broadcasted service

advertisements (broadcast repeatedly or periodically; see Jones [0034]), Eagle's Requester Device would not have to transmit any discovery requests and would have saved time and energy as a result. That is, with beacons transmitting repeatedly or periodically, Eagle's Requester Device may periodically process passively received transmissions without having to broadcast an inquiry message and wait for responses. Jones' passive configuration is one of a finite number of identified, predictable solutions (active, passive, or mixed; Jones [0027], [0043]-[0045]) yielding predictable results (conserving power through passive listening), and a POSITA would have had a reasonable expectation of success listening for service messages. Eagle's (and Bluetooth v2.1's) inquiry process already included a step of listening for beacon transmissions with service information. The above modification eliminates the need for Eagle's Requester Device to request that information first.

X. SECONDARY CONSIDERATIONS

290. The Challenged Claims of the '918 patent are rendered obvious by the grounds presented herein. In my opinion, the strength of the grounds that I discuss above cannot be overcome by any alleged objective indicia.

291. I am not currently aware of any alleged objective indicia that Patent Owner has asserted specifically for the '918 patent claims. To the extent Patent Owner asserts the existence of any additional secondary considerations in its

responses, or presents additional evidence or arguments, I reserve my right to address any such evidence.

XI. CONCLUSION

292. In summary, I have concluded that the Challenged Claims are rendered obvious over the prior art references as discussed above. Specifically, in my opinion, for at least the reasons above, the Challenged Claims of the '918 patent obvious.

293. To the extent it is argued that any further disclosure is required for an element in the Challenged Claims that I have identified as being disclosed, a person of ordinary skill in the art would certainly have found that element obvious to include based on the sample explicit disclosure or inherent disclosures and analysis I have identified above.

294. I reserve the right to supplement my opinions in the future to respond to any arguments that Patent Owner or its expert(s) may raise and to take into account new information as it becomes available to me.

295. In signing this declaration, I recognize 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 also recognize that I may be subject to cross-examination in the 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.

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

297. Executed this 2nd day of July, 2025, in Greenville, Texas.

Mr. Mark R. Lanning