

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

SECURE COMMUNICATION TECHNOLOGIES, LLC,
Patent Owner.

Case IPR2026-00099

Patent No. 8,116,749

**DECLARATION OF MARK R. LANNING IN SUPPORT
OF PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 8,116,749**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	QUALIFICATIONS.....	5
III.	LEGAL UNDERSTANDINGS.....	8
A.	My Understanding of Claim Construction.....	8
B.	My Understanding of Anticipation	10
C.	My Understanding of Obviousness.....	11
IV.	THE '749 PATENT.....	15
A.	Overview of the '749 patent	15
B.	The Prosecution History	18
C.	IPR2020-00978	21
D.	Priority Date of the Claims	22
V.	LEVEL OF ORDINARY SKILL IN THE ART	22
VI.	CLAIM CONSTRUCTION	24
VII.	GROUND OF UNPATENTABILITY	24
VIII.	DETAILED ANALYSIS OF GROUNDS FOR CHALLENGE.....	25
A.	GROUND 1: BUCUK ANTICIPATES CLAIMS 1-3, 13, AND 17-20.....	25
a.	Overview of Bucuk (EX1051).....	26
b.	Anticipation and Obviousness	28
c.	The '749 Patent Claims.....	30
i)	Claim 1	30
ii)	Claim 2	40
iii)	Claim 3	41
iv)	Claim 13.....	42
v)	Claim 17	43
vi)	Claim 18.....	44
vii)	Claim 19.....	44
viii)	Claim 20.....	45

B. GROUND 2: BUCUK IN VIEW OF NORDMAN RENDERS OBVIOUS CLAIMS 1-3, 7-9, 13, 15, AND 17-26.....	46
a. Overview of Bucuk (EX1051).....	46
b. Overview of Nordman (EX1011)	46
c. Overview of Bucuk’s and Nordman’s combined teachings	48
d. The ’749 Patent Claims.....	51
i) Claim 1	51
ii) Claim 2	57
iii) Claim 3	58
iv) Claim 7	60
v) Claim 8	64
vi) Claim 9	64
vii) Claim 13	65
viii) Claim 15	65
ix) Claim 17	65
x) Claim 18	66
xi) Claim 19	67
xii) Claim 20	71
xiii) Claim 21	73
xiv) Claim 22	74
xv) Claim 23	74
xvi) Claim 24	74
xvii) Claim 25	75
xviii) Claim 26	75
C. GROUND 3: BUCUK IN VIEW OF NORDMAN AND KALLIO RENDERS OBVIOUS CLAIMS 4-6 AND 10-12	75
a. The ’749 Patent Claims.....	78
i) Claim 4	78
i) Claim 5	80

i)	Claim 6	81
i)	Claim 10	83
i)	Claim 11	85
i)	Claim 12	85
D.	GROUND 4: BUCUK IN VIEW OF NORDMAN AND PERTILA RENDERS OBVIOUS CLAIMS 14 AND 16	85
a.	The '749 Patent Claims	89
i)	Claim 14	89
ii)	Claim 16	91
IX.	SECONDARY CONSIDERATIONS	92
X.	CONCLUSION	93

I. INTRODUCTION

1. My name is Mark R. 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. 8,116,749 (“the ’749 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 1-26 of the ’749 patent (“Challenged Claims”) are anticipated and/or obvious over the prior art references identified below.

2. The ’749 patent is titled “PROTOCOL FOR ANONYMOUS WIRELESS COMMUNICATION,” names as inventors James Arthur Proctor, Jr. and James Arthur Proctor, III, and is currently owned by Secure Communication Technologies, LLC. I have considered the ’749 patent. I understand that the ’749 patent has been provided as EX1001.

3. The file history of the ’749 patent has been provided as EX1002. I have considered this file history, and I will refer to it as the “’749 File History” or by its exhibit number.

4. I understand that the ’749 patent 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 '749 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 '749 patent; my own knowledge and experiences gained from my work experience in the field of the '749 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. 2010/0274859 to Bucuk, titled “METHOD AND SYSTEM FOR THE CREATION, MANAGEMENT AND AUTHENTICATION OF LINKS BETWEEN ENTITIES,” was filed on July 14, 2010 and published on October 28, 2010. I understand that a copy of this reference has been designated as EX1051. Throughout my declaration, references to “Bucuk” are to EX1051.

9. U.S. Patent Application Publication No. 2002/0174364 to Nordman, titled “METHOD FOR PROTECTING PRIVACY WHEN USING A BLUETOOTH DEVICE” was filed on May 21, 2001 and published on November 21, 2002. I understand that a copy of this reference has been designated as EX1011. Throughout my declaration, references to “Nordman” are to EX1011.

10. U.S. Patent Application Publication No. 2003/0224756 to Kallio, titled “SYSTEM AND METHOD FOR SERVICES ACCESS” was filed on May 30, 2002 and published on December 4, 2003. I understand that a copy of this reference has been designated as EX1047. Throughout my declaration, references to “Kallio” are to EX1047.

11. U.S. Patent Application Publication No. 2004/0243519 to Perttila, titled “PROMPTED ELECTRONIC MOBILE-SERVICE INFORMATION COMMUNICATIONS WITH VALIDATION” was 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. 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.

13. 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. 8,116,749
1002	Prosecution History of U.S. Patent No. 8,116,749
1010	U.S. Patent Application Publication No. 2002/0131445
1011	U.S. Patent Application Publication No. 2002/0174364 (“Nordman”)
1012	U.S. Patent Application Publication No. 2005/0164717
1013	U.S. Patent Application Publication No. 2006/0165100
1028	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00978, Paper 2 (Petition for <i>Inter Partes</i> Review) (P.T.A.B. June 1, 2020)

Exhibit	Description
1029	<i>Target Corporation v. Proxicom Wireless, LLC</i> , IPR2020-00978, Paper 10 (Decision Denying Institution) (P.T.A.B. Dec. 4, 2020)
1037	U.S. Patent Application Publication No. 2004/0243519 (“Perttila”)
1047	U.S. Patent Application Publication No. 2003/0224756 (“Kallio”)
1051	U.S. Patent Application Publication No. 2010/0274859 (“Bucuk”)
1052	U.S. Patent Application Publication No. 2009/0028082
1053	U.S. Patent No. 9,305,119
1054	U.S. Patent Application Publication No. 2005/0204309

II. QUALIFICATIONS

14. 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.

15. 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.

16. 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.

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

18. 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.

19. 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.

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

21. 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.

22. 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.

23. 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.

24. 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.

25. 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

26. 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.

27. 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).

28. 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.

29. 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

30. 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.

31. 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.

32. 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.

33. 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

34. 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.

35. 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.

36. 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.

37. 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.

38. 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

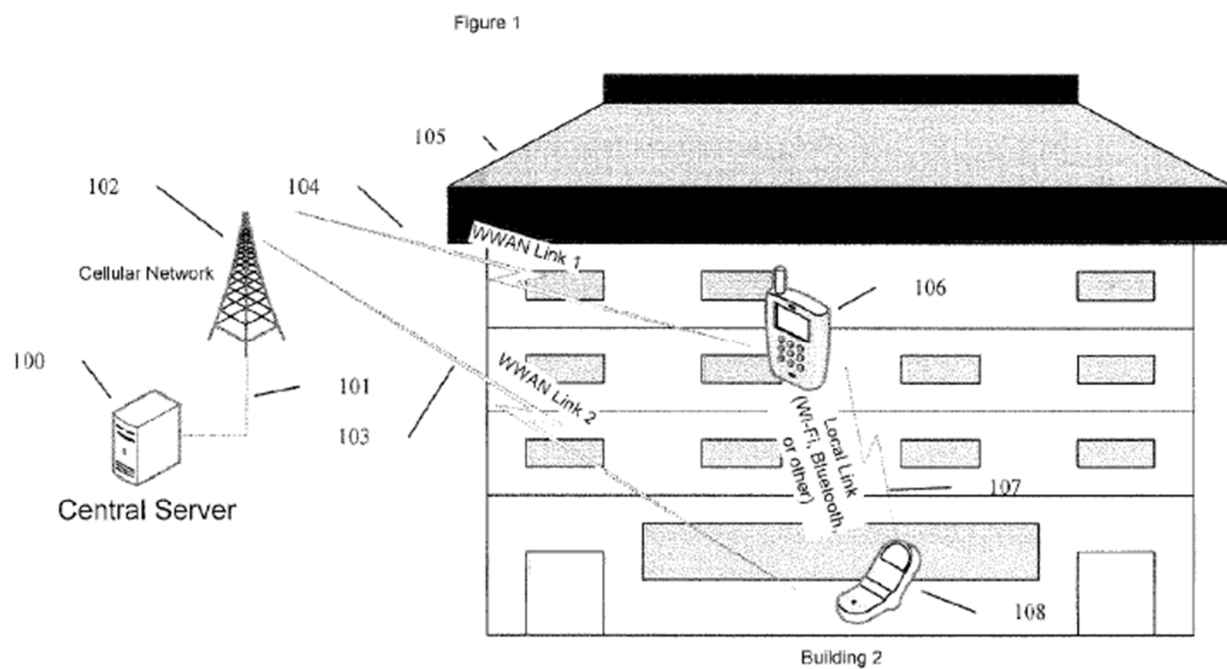
a novel element of the claim rather than something in the prior art. I also understand that even when they are present, secondary considerations may be unable to overcome primary evidence of obviousness (such as motivation to combine with predictable results) that is sufficiently strong.

IV. The '749 patent

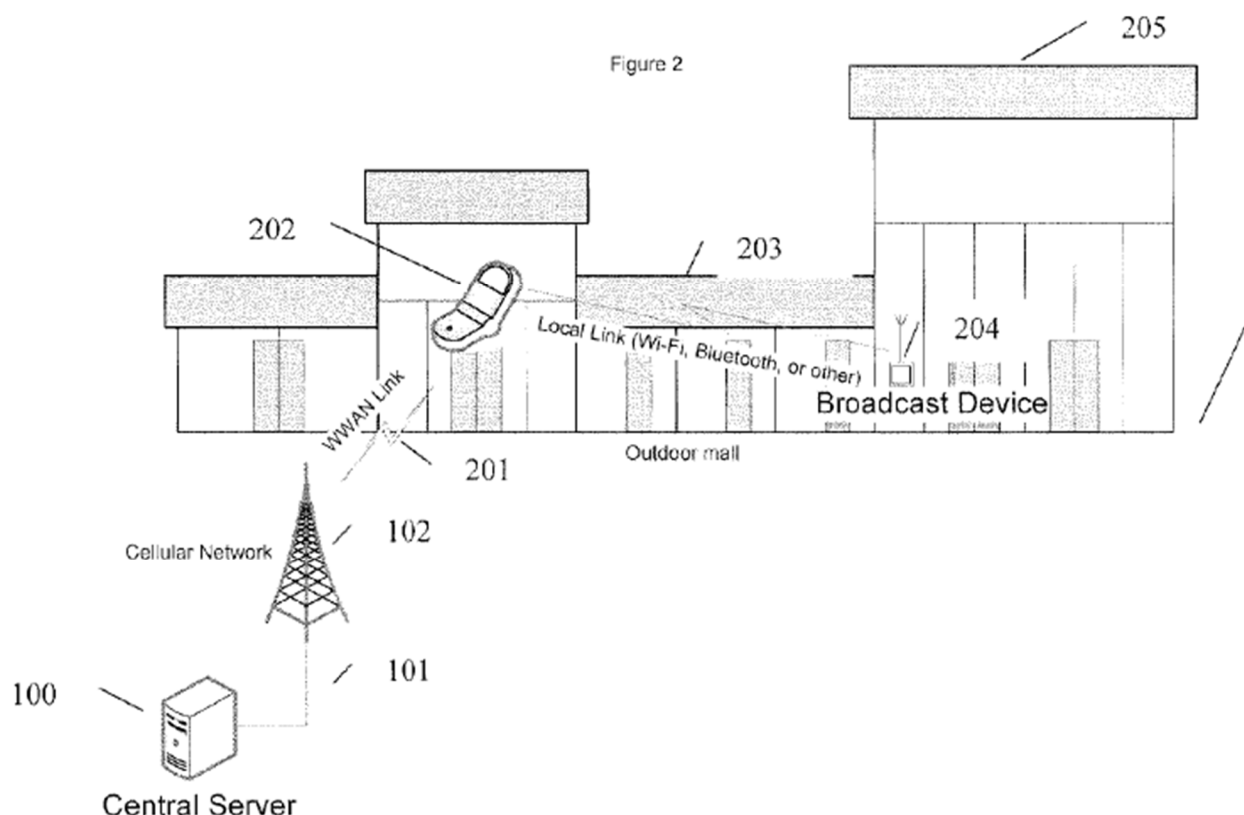
A. Overview of the '749 patent

39. The '749 patent issued from U.S. Patent Application No. 12/364,938 ("’749 Application"), filed February 3, 2009.

40. The purported "invention" of the '749 patent relates to the use of a server to manage communications between two devices. EX1001, Abstract, 2:34-54, 2:66-3:8. In particular, the '749 patent concerns the facilitation of information between wireless devices having both short-range communications and long-range communications. EX1001, 2:8-4:57. 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, 5:40-49, 6:29-49.



41. 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, 7:16-25.



42. 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, 7:20-37. 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, 4:28-45, 8:50-58, 15:33-43. 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, 7:41-47.

43. The ’749 patent explains that devices in short-range proximity (i.e., devices 202 and 204 in the example above) identify themselves with various identifiers such as MAC addresses, basic service set identifiers (BSSIDs), network names, and service set identities (SSIDs). EX1001, 7:5-15, 9:23-26, 10:9-14. The system may also include a server with an application that has access to a pool of identifiers that it assigns to devices. EX1001, 16:58-64. For example, it may update a device’s identifier, regularly or randomly, using a list or range of identifiers, or identifiers that are algorithmically generated. EX1001, 16:62-17:3.

B. The Prosecution History

44. During prosecution of the ’749 patent, the Examiner rejected pending claims as being obvious in view of several prior art references: U.S. Patent No. 7,213,742 to Birch; U.S. Patent No. 6,629,149 to Fraser; and U.S. Patent Publication 2008/0214166 to Ramer. EX1002, 91-98, 145-157.

45. Facing rejection based on these prior art references, the Applicant added a large number of limitations to the claims. For example, independent claim 1 (a method) and independent claim 7 (a server) were amended as follows:

1. (Currently Amended) A method for exchange of information between one or more applications executing on ~~at least two wireless devices~~ at least a first wireless device and a second wireless device, the method comprising the steps of:

at the first wireless device, providing initial identification information [[,]] to a central server, said initial identification information having been collected by [[a]] the first wireless device from [[a]] the second wireless device via a first, direct, short range separate local wireless link between the second and first wireless devices, wherein the initial identification information is associated at the central server with an identity of a user or entity associated with the second wireless device, and wherein the initial identification information is provided to the central server, by the first wireless device, over a second wireless link; [[and]]

at the second wireless device, upon [[the]] an occurrence of a predetermined event coordinated with said central server, within a specific application on the second wireless device, providing modified identification information over the first, direct, short range local wireless link in place of the initial identification information, such that the modified identification information is associated at the central server with said identity of a user or entity associated with the second device; and

at the first wireless device, collecting said modified identification information.

7. (Currently Amended) A server for exchanging information between one or more applications executing on at least two wireless devices, the server comprising:
- a receiver, for receiving initial identification information having been collected by a first wireless device from a second wireless device via a ~~separate~~, first, direct, short range local wireless link between the first and second wireless devices, wherein the initial identification information is associated at the server with an identity of a user or entity associated with the second wireless device, and wherein the initial identification information is received by the server from the first wireless device over a second wireless link distinct from the first wireless link; and
 - a transmitter for, upon ~~[[the]]~~ an occurrence of a predetermined event coordinated with the second wireless device, sending a message to the second wireless device to change the identification information within a specific application on the second wireless device and for subsequently providing modified identification information over the first, direct, short range local wireless link in place of the initial identification information, and such that the modified identification information is associated at the server with said identity of a user or entity associated with the second device.

EX1002, 182-193.

46. The Examiner allowed these claims but also rejected a different set of claims, which the Applicant later cancelled. EX1002, 210-219, 239-246.

47. The Examiner allowed the pending claims and pointed to the following underlined limitations in their reasons for allowance:

A method for exchange of information between one or more applications executing on at least a first wireless device and a second wireless device, the method comprising the steps of:

at the first wireless device, **providing initial identification information to a central server, said initial identification information having been collected by the first wireless device from the second wireless device via a first, direct, short range separate local wireless link** between the second and first wireless devices, wherein the initial identification information is associated at the central server with an identity of a user or entity associated with the second wireless device, and

wherein the initial identification information is provided to the central server, by the first wireless device, over a second wireless link;

at the second wireless device upon an occurrence of a predetermined event coordinated with said central server, within a specific application on the second wireless device, **providing modified identification information over the first, direct, short range local wireless link in place of the initial identification information, such that the modified identification information is associated at the central server with said identity of a user or entity associated with the second device;** and

at the first wireless device, collecting said modified identification information.

EX1002, 267.

C. IPR2020-00978

48. I understand the '749 patent was previously asserted in a petition for *inter partes* review by another party (Target, Inc.). That petition put forth two prior art: U.S. Patent No. 7,545,784 to Mgrdechian and WIPO Patent Publication 2007/084973 to Kulakowski. EX1028, 12.

49. I also understand that the PTAB did not institute *inter partes* review on that petition, and so a full trial was not held. In the decision not to institute *inter partes* review, the PTAB stated that the petition there “[did] not address the ‘upon

an occurrence of a predetermined event’ recitation.” EX1029, 15. Additionally, the PTAB stated that the petitioner there “fail[ed] to explain adequately how Mgrdechian discloses or teaches providing modified identification information as required by claim 1.” EX1029, 16. Furthermore, the PTAB stated that the petitioner there did not “explain[] adequately why it would have been obvious to use [Kulakowski’s] covert teaching to enhance the security of Mgrdechian’s system by transmitting the covert identifier to another client device. EX1029,19-20.

50. Neither Mgrdechian nor Kulakowski are related or relevant to the prior art of Bucuk, Nordman, Kallio, and Perttila used in Grounds 1-4 discussed below.

D. Priority Date of the Claims

51. 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.

V. LEVEL OF ORDINARY SKILL IN THE ART

52. 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.

53. I have been informed that the POSITA's level of skill used in prior proceedings involving other patents in the same family as the '749 patent (claiming priority to the same provisional applications) 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 '749 patent and file history, I agree that this is an appropriate level of skill for a POSITA.

54. 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.

VI. CLAIM CONSTRUCTION

55. I have been instructed that the Challenged Claims of the '749 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.

VII. GROUNDS OF UNPATENTABILITY

56. 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
Bucuk	1051	2010/0274859	October 28, 2010
Nordman	1011	2002/0174364	November 21, 2002
Kallio	1047	2003/0224756	December 4, 2003
Perttila	1037	2004/0243519	December 2, 2004

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

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

- **Ground 1:** Claims 1-3, 13, and 17-20 of the '749 patent are anticipated by Bucuk.
- **Ground 2:** Claims 1-3, 7-9, 13, 15, and 17-26 of the '749 patent are rendered obvious by Bucuk in view of Nordman.
- **Ground 3:** Claims 4-6 and 10-12 of the '749 patent are rendered obvious by Bucuk in view of Nordman and Kallio.
- **Ground 4:** Claims 14 and 16 of the '749 patent are rendered obvious by Bucuk in view of Nordman and Perttila.

58. It is my opinion that Challenged Claims of the '749 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.

VIII. DETAILED ANALYSIS OF GROUNDS FOR CHALLENGE

59. As I explain in Section IV above, the '749 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.

60. In this section, I explain why the Challenged Claims of the '749 patent are anticipated and/or rendered obvious by the teachings of Bucuk, and also obvious over Bucuk in view of Nordman, Kallio, and/or Perttila.

A. GROUND 1: BUCUK ANTICIPATES CLAIMS 1-3, 13, AND 17-20

a. Overview of Bucuk (EX1051)

61. U.S. Patent Application Publication No. 2010/0274859 to Bucuk (“Bucuk,” EX1051), titled “METHOD AND SYSTEM FOR THE CREATION, MANAGEMENT AND AUTHENTICATION OF LINKS BETWEEN ENTITIES,” was filed on May 23, 2008 and published on October 28, 2010.

62. Bucuk is directed to a system for establishing links between users and devices, through transmission identifiers sent using short-range communications between devices and long-range communications to a server, to facilitate access to data, devices, services, and the like. Bucuk, Abstract, [0001], [0007]-[0011].

63. An exemplary system including a user device 172 (for example, a mobile phone), a device 170 to be accessed (for example, a car), and an authentication server 174 is shown in Fig. 1c (below). Bucuk, [0153]-[0177].

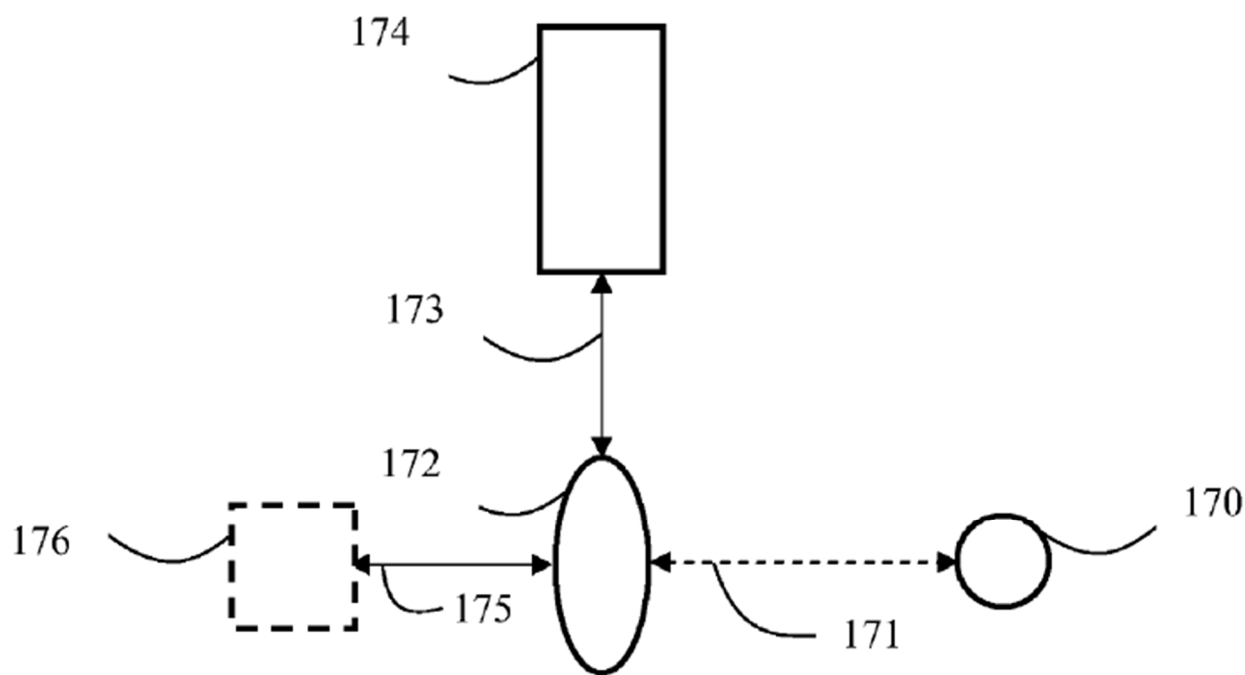


Figure 1c

64. In this example, phone 172 and car 170 each search for nearby devices and read each other's Bluetooth name. Car 170 reads phone 172's name as "John@1c1c.5c5c" and remains locked (as the phone does not presently have valid unlocking information). Bucuk, [0166]. Phone 172 reads car 170's name as "Car15#2c2c.8c8c" and provides, to authentication server 174, car 170's information (for example, extracted IP address "2c2c" and device ID "8c8c") as well as information about itself (for example, IP address "1c1c" and device ID "5c5c"). Bucuk, [0166]-[0167].

65. The server recognizes that there is an authorized link between the user of device 172 and the entity in control of device 170 and subsequently issues an

unlocking key (“1f1f”) to phone 172 that will unlock car 170. Bucuk, [0164], [0168]-[0169]. Phone 172 changes its own Bluetooth name to incorporate the received number (for example, from “John@1c1c.5c5c” to “John@1c1c.1f1f”), which, when read by car 170, results in car 170 unlocking. Bucuk, [0169].

66. After being unlocked, car 170 changes its identifying information according to a pre-arranged scheme, such that a sequence of IDs are used, “effectively guaranteeing only one device ID (unlocking key) at the time can unlock device (170).” Bucuk, [0170]-[0171].

b. Anticipation and Obviousness

67. Bucuk anticipates claims of the ’749 patent. The mappings below primarily rely on the embodiment shown in Fig. 1c of Bucuk with additional details explained in other sections of Bucuk, for example, from Bucuk’s description of Fig. 1a and other disclosures. A POSITA would have recognized that these additional details and features are necessarily present in the embodiment of Fig. 1c, and thus anticipatory, and are not merely obvious modifications.

68. To the extent Patent Owner argues that Bucuk does not expressly disclose a single “embodiment” anticipating claims of the ’749 patent because, for example, Bucuk’s Figs. 1a-1d are each described as “another” embodiment and allegedly distinct, this would be incorrect because Bucuk’s “embodiments” are not wholly separate systems to be considered in isolation. For example, Bucuk

references the “system mentioned in FIG. 1” or “described in FIG. 1” despite there being no figure “1,” implying that, despite the variations between Figs. 1a-1d, Figs. 1a-1d are directly related and anticipatory. Bucuk, [0181], [0183]. Indeed, Figs. 1a-1d vary in their broad configurations (for example, what types of servers are included, what devices have internet access) and not the underlying technologies that are intrinsic to the devices and connections themselves (for example, the technologies used for the short-range and long-range communications common to each figure).

69. For example, where the description of Fig. 1c explains that “software” is used to change a device’s Bluetooth name (Bucuk, [0169]), but does not explicitly state that “software” is also used to exchange information between devices in short-range proximity (as may be required for [1.PRE]’s recitation of an “exchange of information between one or more applications”), a POSITA would have recognized that the devices of Fig. 1c are configured similarly to the devices of Fig. 1a—as computing devices—wherein installed software is executed for exchanging identifying information (Bucuk, [0118], [0147]). Such disclosures in Bucuk are therefore anticipatory.

70. Nevertheless, these same features in Bucuk, if not anticipating the claims, render the claims obvious. It would have been obvious to a POSITA to combine these well-known features from, for example, Figures 1a-d, because

Bucuk teaches that “[a]spects of any of the examples... may be combined with aspects of any of the other examples described to form further examples” (Bucuk, [0073], [0310]) and, at the very least, features of Bucuk’s embodiments are all directed to closely related variations of wireless devices in short-range proximity and remote servers. Indeed, a POSITA in the ordinary course of routine optimization and experimentation in implementing a system according to Bucuk’s disclosures would have considered the various embodiments to be so close that features in one embodiment would have readily been considered for implementation in any other embodiment in this same Bucuk disclosure, apart from clearly conflicting configurations.

71. Therefore, Ground 1 is based on anticipation (and obviousness in the alternative) by Bucuk, and Grounds 2-4 further below are based on obvious combinations with Bucuk and additional prior art references.

c. The ’749 Patent Claims

i) Claim 1

(1) [1.PRE] “A method for exchange of information between one or more applications executing on at least a first wireless device and a second wireless device, the method comprising the steps of:”

72. Bucuk discloses *a method for exchange of information* (for example, exchanging identification information) *between one or more applications executing* (for example, between software executing on devices communicating via

Bluetooth) *on at least a first wireless device* (for example, phone 172) *and a second wireless device* (for example, car 170).

73. Bucuk discloses devices 170 and 172, shown in Fig. 1c (below), exchange identification information, such as Bluetooth names and unique IDs (or “UIDs”), via short-range wireless communications. Bucuk, [0157], [0162]-[0163], [0166], [0169]; *see also* [0100]-[0108] (examples of UIDs exchanged in short-range communications include device names, device addresses, phone numbers, numbers, strings, and algorithmically changing IDs). Device 172 (*a first wireless device*) and device 170 (*a second wireless device*) are, for example, a mobile phone 172 and a car 170, respectively. Bucuk, [0153].

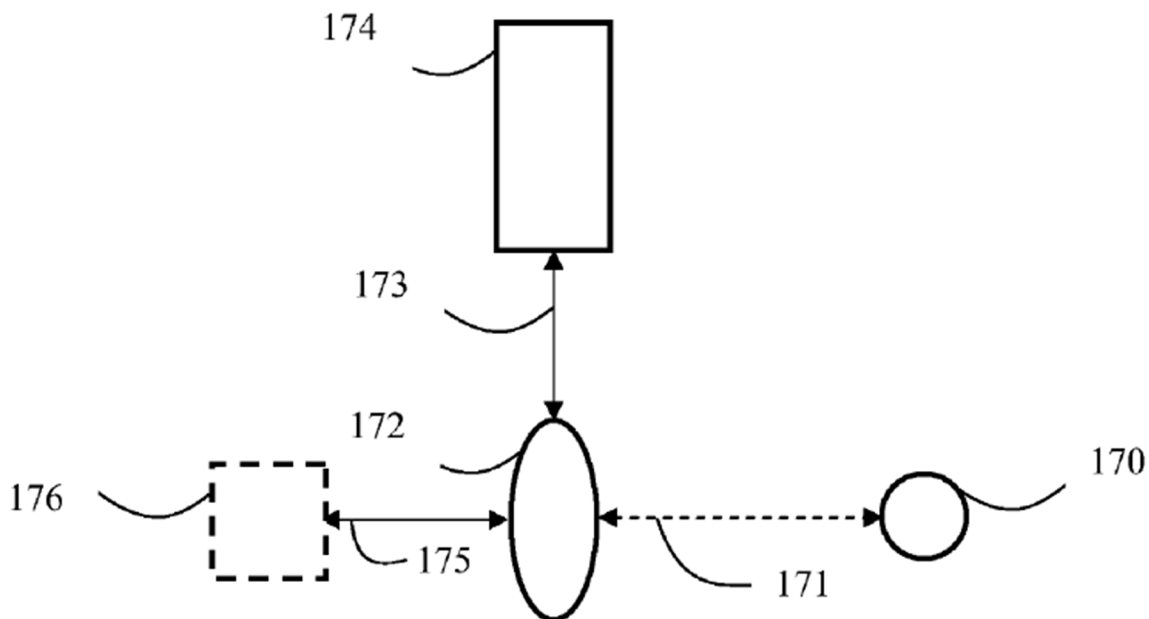


Figure 1c

74. Bucuk further discloses that phone 172 and car 170 (the respective

first and second devices) perform disclosed methods by executing installed software *applications*. Bucuk, [0071]-[0072] and [0305]-[0307] (stored software executed by a processor), [0333] (mobile devices and other computing devices with short-range communication capabilities install “software drivers and applications... necessary for functioning”). *See also* Bucuk, [0089], [0118], [0147], [0169] (describing examples of executing installed software to perform functions).

(2) [1.A.I] “at the first wireless device, providing initial identification information to a central server, said initial identification information having been collected by the first wireless device from the second wireless device via a first, direct, short range local wireless link between the second and first wireless devices,”

75. Bucuk discloses *at the first wireless device, providing initial identification information to a central server* (for example, phone 172 provides car 170’s IP address and Device ID to server 174), *said initial identification information having been collected by the first wireless device from the second wireless device via a first, direct, short range local wireless link between the second and first wireless devices* (for example, phone 172 received car 170’s IP address and Device ID via short-range communications).

76. Bucuk discloses that phone 172 searches for and reads the Bluetooth names of nearby devices, discovering car 170’s Bluetooth name

“Car15#2c2c.8c8c.” Bucuk, [0166]. Phone 172 receives car 170’s Bluetooth name via Bluetooth, which provides a *short range local wireless link between the second and first devices*, as shown in Fig. 1c (below). Bucuk, [0157], [0163]. As similarly described in the ’749 patent, a short range local wireless “link” exists between devices when used for the detection and/or advertisement of devices. EX1001, 6:37-42.

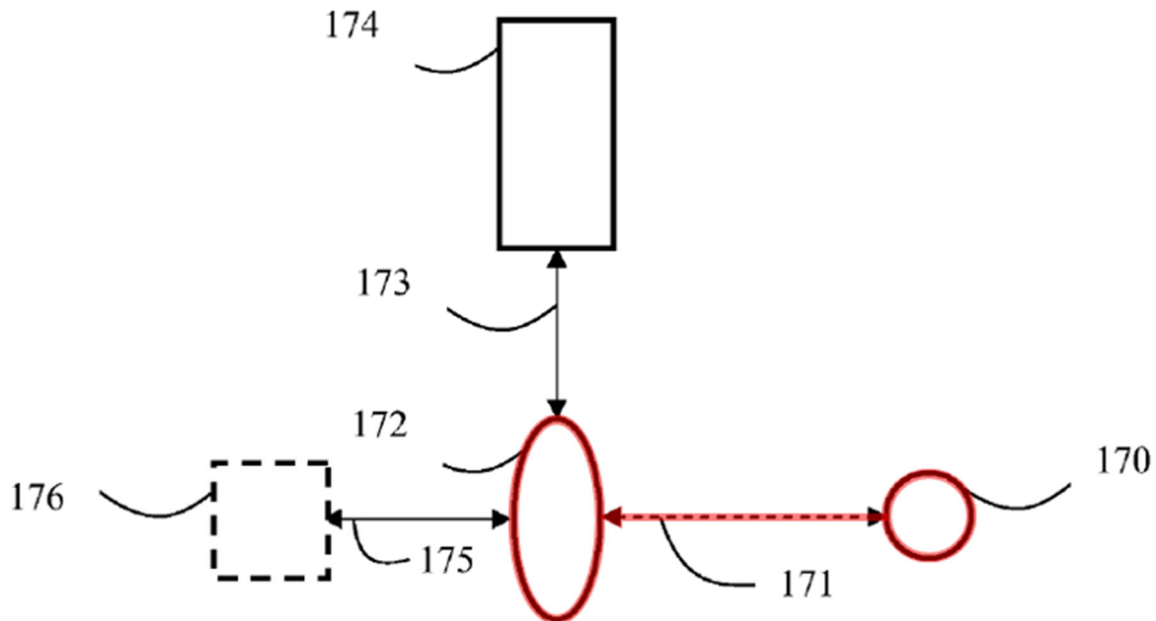


Figure 1c

77. From car 170’s Bluetooth name, phone 172 extracts car 170’s *initial identification information*—car 170’s IP address and Device ID information—and provides that *initial identification information* to server 174. Bucuk, [0167]; Fig. 1c (below). That is, phone 172 extracts “2c2c” and “8c8c” from car 170’s Bluetooth name “Car15#2c2c.8c8c” and sends it to server 174. *See also* Bucuk,

[0165] (describing the IP address and Device ID parts of the Bluetooth name).

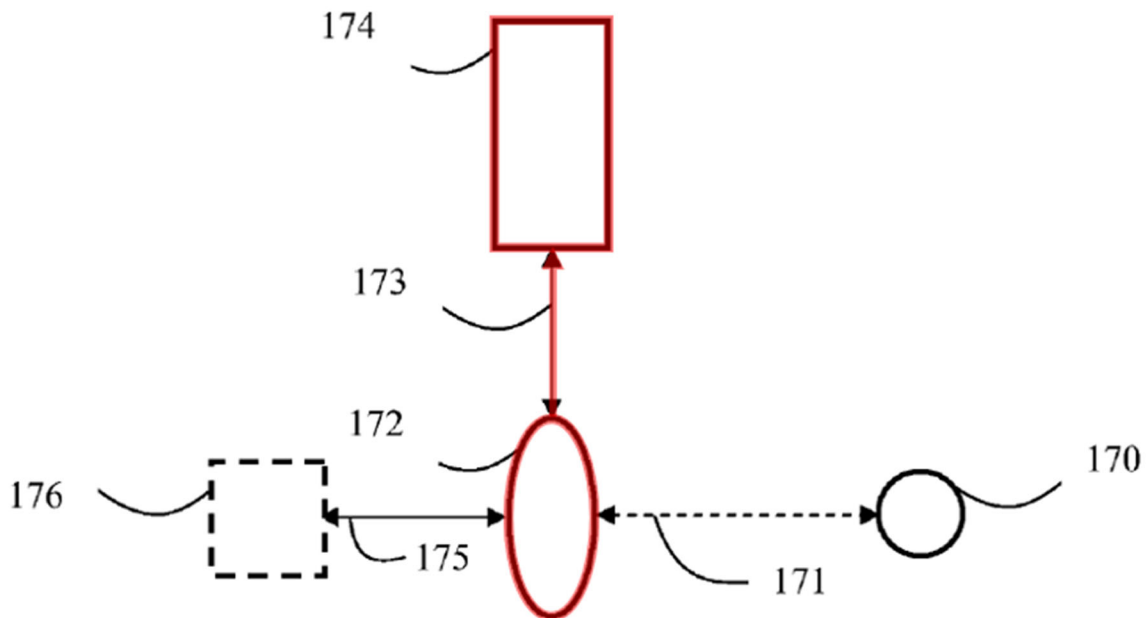


Figure 1c

(3)[1.A.II] “wherein the initial identification information is associated at the central server with an identity of a user or entity associated with the second wireless device, and”

78. Bucuk discloses that *the initial identification information* (for example, car 170’s IP address and Device ID, which are UID information) is *associated at the central server with an identity of a user or entity associated with the second wireless device* (for example, at server 174, car 170’s UID information resolves to a user and Entity ID of the car 170).

79. Car 170 initializes itself with a unique Entity ID (*identity of a user or entity associated with the second wireless device*) at server 174. Bucuk, [0155]. Therefore, because car 170’s IP address and Device ID information (*the initial*

identification information) are UID information that, “for a particular server or database,” “directly or indirectly identify an Entity (which could be a User..., an object...),” Bucuk discloses that *the initial identification information is associated at the central server with an identity of a user or entity associated with the second wireless device*. Bucuk, [0324] (also disclosing that a “[UID]... such as Device ID... will resolve [to the] Unique Entity ID and/or identify an Entity, for example through prior registration or login information”).

(4) [1.A.III] “wherein the initial identification information is provided to the central server, by the first wireless device, over a second wireless link;”

80. Bucuk discloses that *the initial identification information is provided to the central server, by the first wireless device, over a second wireless link* (for example, phone 172 provides car 170’s IP address and Device ID to server 174 over the Internet).

81. Bucuk discloses that phone 172 provides the initial identification information to server 174. *See* [1.A.I]. Communications between phone 172 and server 174 are over the Internet. Bucuk, [0165], [0167] (car 170 “has no internet connection available..., so [phone 172] will use its own connection to contact the authentication server (174)”). Bucuk explains that Internet connections between mobile devices and servers (for example, between phone 172 and server 174) include wireless links, for example, GSM, GPRS, and UMTS (2G and 3G cellular

networks), and are separate from the mobile device's short-range radio connections. Bucuk, [0089], [0333].

(5)[1.B.I] “at the second wireless device, upon an occurrence of a predetermined event coordinated with said central server,”

82. Bucuk discloses that, *at the second wireless device, upon an occurrence of a predetermined event coordinated with said central server* (for example, each time server 174 issues an unlocking key, car 170's identification information is changed according to a scheme coordinated with server 174), car 170 performs additional actions (for example, collecting modified identification information, *see* [1.B.III]-[1.C]).

83. Bucuk discloses that after server 174 authorizes phone 172 to access car 170 by providing phone 172 with the unique number or unlocking key programmed into car 170 (for example, server 174 provides “1f1f” to phone 172 to unlock car 170 once) (Bucuk, [0167]-[0169]), car 170 will “change Bluetooth® name according to a ***pre-arranged scheme*** (established at initialisation)..., effectively guaranteeing only one device ID (unlocking key) at the time can unlock [car 170].” Bucuk, [0170] (emphasis added). Thus, car 170 will change its Device ID from “8c8c” to the next device ID (unlocking key) that will be recognized by server 174 as valid (for unlocking car 170) the next time phone 172 and car 170 perform the same steps for unlocking the car (*i.e.*, the next time phone 172

provides car 170's Device ID to server 174 and receives an unlocking key in return). Bucuk, [0170] (repeating the disclosed cycle for further security).

84. Bucuk explains that the above system uses a “static’ list of unlocking numbers” and associated Device IDs that are known to the server and pre-programmed to the device (car 170). Bucuk, [0171]-[0172]; *see also* [0157] and [0168] (the unlocking keys are programmed into car 170 during initialization or registration with the server). That is, car 170 has initialized itself with the server and so “codes... change in a sequence which is known to the authentication server,” thus triggering a *predetermined event coordinated with said central server* each time car 170's Device ID is used and then changed for the next cycle. Bucuk, [0160]. This coordination between car 170 and server 174, with regard to the sequence of Device IDs/unlocking keys and their change after use, facilitates implementation of a user-friendly unlocking process while still providing security benefits. Bucuk, [0160].

(6) [1.B.II] “within a specific application on the second wireless device,”

85. Bucuk discloses that car 170's functions (including those claimed in [1.B]-[1.C]) are performed *within a specific application on the second wireless device* (for example, within installed software). *See* [1.PRE]; Bucuk, [0071]-[0072], [0305]-[0307], [0333] (functions are performed by executing software

applications); *see also* [0147], [0155], [0157], [0168], [0170] (devices/car 170 initialised by installing software and registering with the server).

(7) [1.B.III] “providing modified identification information over the first, direct, short range local wireless link in place of the initial identification information,”

86. Bucuk discloses *providing modified identification information* (for example, providing a changed Bluetooth name with a changed Device ID) *over the first, direct, short range local wireless link* (for example, over the short-range link) *in place of the initial identification information* (for example, rather than providing the initial Bluetooth name that was already used to unlock car 170).

87. Bucuk discloses that after car 170 provides its initial identification information to phone 172 over the short-range link (see [1.A.I]) and phone 172 unlocks car 170 with an unlocking key received from server 174, car 170 changes its Bluetooth name with a new Device ID, thus creating modified identification information. See [1.B.I]; Bucuk, [0170]. Further discussed for [1.B.I], car 170’s Device ID is “change[d]... according to a pre-arranged scheme” and “in a sequence... known to the authentication server,” “guaranteeing [that] only one device ID (unlocking key) at the time can unlock [car 170].” Bucuk, [0157], [0160], [0168], [0170]-[0171]. Accordingly, car 170’s Device ID is changed according to a sequence of Device IDs and will not use the initial (or previous)

Device ID in subsequent exchanges of identification information.

88. “[C]ycles of exchanging unique Device IDs” are “repeated” (Bucuk, [0170]), and so the next time phone 172 wants access to car 170, car 170 will provide its modified Bluetooth name (with changed Device ID) *over the first, direct, short range local wireless link (e.g., over the short-range link when “new values are [passed] to the authentication server”)* *in place of its initial* Bluetooth name (with initial Device ID). Bucuk, [0160].

89. Note that even if the initial Device ID and changed Device ID use the same value (a low but non-zero probability if the sequence was generated by a simple random process), phone 170 still goes through the process of changing its Device ID and creating *modified identification information*. Bucuk, [0170]. That is, the changing steps/functions are still performed, but the new Device ID could coincidentally have the same value as the previous Device ID. However, in most cases, the changed Device ID would be expected to have a different value since Bucuk describes that there may be as many as 100,000 Device IDs/unlocking keys to use. Bucuk, [0171]-[0173]. For example, Bucuk’s example uses a 4-digit hexadecimal number of “1f1f,” which Bucuk describes as “hex decimal,” suggesting at least 65,536 values. Bucuk, [0165], [0168].

(8) [1.C] “at the first wireless device, collecting said modified identification information.”

90. Bucuk discloses, *at the first wireless device, collecting said modified identification information* (for example, phone 172 receives the modified Bluetooth name).

91. Bucuk discloses that “cycles of exchanging unique Device IDs” are “repeated” (Bucuk, [0170]), which includes search for and receiving Bluetooth names of nearby devices (Bucuk, [0166]). Thus, phone 172 will collect car 170’s modified Bluetooth name the next time it searches for devices (for example, the next time the user of phone 172 wants access to car 170). Bucuk, [0166], [0170].

ii) Claim 2

(1) “The method of claim 1 wherein the predetermined event is one or more of: an elapsed time; a number of uses of the identifier; and/or a step in a process.”

92. Bucuk discloses that *the predetermined event is one or more of: an elapsed time; a number of uses of the identifier; and/or a step in a process.*

93. As discussed for [1.A.I], [1.A.III], and [1.B.I], car 170 changes its Bluetooth name (which includes its Device ID) each time car 170’s Device ID is used by phone 172 to contact server 174 and server 174 issues an unlocking key. Bucuk, [0160], [0167]-[0170].

94. The *predetermined event* of issuing an unlocking key based on car 170’s Device ID is *a number of uses of the identifier* because a single successful

use of car 170's Device ID that results in issuing an unlocking key causes car 170 to change its Bluetooth name. The *predetermined event* is also *a step in a process* because the step of car 170's changing its Bluetooth name is only performed when the step of issuing an unlocking key is performed first, as discussed above, and both steps together are part of an overall process.

iii) *Claim 3*

(1) “The method of claim 1 wherein the step of changing the user or entity identification information at said second wireless device is further: effected by a rule-based generation local to the application, downloaded from the server directly, or synchronized such that it is coordinated with predetermined receiving and transmitting times.”

95. I have been informed that because this claim recites “the step of changing...,” which does not refer to a previously introduced “a step of changing the user or entity identification information” (either in this claim or its parent claim), it is likely a typographical error that should be read as “a step of changing,” which I had done.

96. Bucuk discloses that *changing is effected by a rule-based generation local to the application*. For example, the change is carried out by car 170's *local application* (for example, installed software, *see* [1.B.II]) that follows a “pre-arranged scheme” set at initialisation, such that the next Bluetooth name used for identification information is the next in a “sequence” “pre-programmed” in car 170

and coordinated with server 174. Bucuk, [0160], [0170]-[0171]. Each subsequent Bluetooth name generated is therefore based on a *rule* of taking the next identification information in a sequence.

iv) ***Claim 13***

(1) “The method of claim 1 wherein the user or entity identification information is changed to protect the privacy of the identity of the a user or entity associated with the second wireless device.”

97. Bucuk discloses that both car 170’s and phone 172’s identification information are changed once for every iteration of the unlocking process. Bucuk, [0169]-[0170]. A POSITA would have recognized that changing identification information such that each identifier can only be used once before being changed *protects the privacy of the identity of the user or entity associated with the second wireless device* (for example, protects the privacy of user(s) unlocking their car; Bucuk, [0153]). For example, if car 170’s identification information did not change over time, an observer would be able to see car 170’s same identification information broadcast over time and correlate it with the identity of nearby persons (for example, the user(s) unlocking the car time after time) and devices (for example, the user(s)’s devices used to unlock the car).

v) **Claim 17**

(1) “The method of claim 1 wherein the first wireless device further performs the step of providing modified identification information to said central server, as collected by the first wireless device from the second wireless device.”

98. Bucuk discloses that *the first wireless device further performs the step of providing modified identification information to said central server, as collected by the first wireless device from the second wireless device* (for example, phone 172 provides car 170’s modified Bluetooth name to server 174 to unlock car 170 at a subsequent time).

99. Bucuk discloses the process of phone 172 unlocking car 170 once, as discussed for [1.A.I]-[1.B.I], is a “cycle[] of exchanging unique Device IDs [that] could be repeated.” Bucuk, [0170]. Thus, after phone 172 collects car 170’s modified identification information (*see* [1.C]), it will provide the modified identification information to server 174 to unlock car 170 a subsequent time. The modified identification information must be provided to the server because the initial identification information would no longer be valid for unlocking car 170. Bucuk, [0170]-[0171].

vi) **Claim 18**

(1) “The method of claim 1 wherein the initial identification information, if re-sent to the central server following said pre-determined event, is processed by said central server in a manner different from which it was processed prior to said pre-determined event.”

100. Bucuk discloses that car 170’s Device ID is used to verify a link to phone 172 at server 174 (for unlocking car 170. Bucuk, [0166]-[0169]; *see* [1.A.I]-[1.B.I]. The Device ID that represents car 170 is changed after every use (Bucuk, [0169]-[0170]) and is a “single use code” that changes in a sequence. Bucuk, [0160]. Accordingly, if car 170’s initial identification information were re-sent to server 174 after being used to unlock car 170, server 174 will no longer recognize it as valid identification information for unlocking car 170 and will not provide an unlocking code to phone 172, therefore *processing it in a manner different from which it was processed prior to said pre-determined event*. Bucuk, [0170] (“only one device ID (unlocking key) at the time can unlock [car 170]”).

vii) **Claim 19**

(1) “The method of claim 17 wherein the modified identification information is used by the central server to verify the legitimacy, identity or authenticity of the first wireless device.”

101. Bucuk discloses that authentication server 174 uses the Device IDs (both initial and modified) to determine whether phone 172 and its user are associated with the car 170 in server 174’s database, wherein an authorized link

between the two results in granting an unlocking key to unlock car 170. *See* [1.B.I]-[1.B.III]; Bucuk, [0164], [0167]-[0168]. In this way, Bucuk discloses that *the modified identification information is used by the central server to verify the legitimacy, identity or authenticity of the first wireless device* (for example, authentication server 174 uses the changed Device ID to verify phone 172's legitimacy and identity as an entity authorized to unlock car 170).

viii) Claim 20

(1) “The method of claim 17 wherein the modified identification information is used by the central server to verify the legitimacy, validity, or authenticity of a transaction associated with one of (a) the first wireless device or (b) a user or entity associated with the first wireless device.”

102. Bucuk discloses that *the modified identification information is used by the central server to verify the legitimacy, validity, or authenticity of a transaction* (for example, authentication server 174 uses the changed Device ID to verify the legitimacy and validity of phone 172's request to unlock car 170) *associated with one or (a) the first wireless device or (b) a user or entity associated with the first wireless device* (for example, the request is initiated by phone 172 and its associated). *See* discussion of claim 19; Bucuk, [0153] (user of phone 172 requests access from car 170), [0166]-[0169]. The user's request to unlock the car is a *transaction associated with phone 172* (used to communicate with the car 170 and

server 174) and its user.

**B. GROUND 2: BUCUK IN VIEW OF NORDMAN RENDERS
OBVIOUS CLAIMS 1-3, 7-9, 13, 15, AND 17-26**

a. Overview of Bucuk (EX1051)

103. *See* Overview of Bucuk in Ground 1.

104. Bucuk also describes other variations of systems with devices in short-range communication, including, for example, systems with devices registered to, and communicating with, the same authentication server. Bucuk, [0188]. In such systems, one device or both devices in short-range communication may provide the other's identification information to the server to gain access to desired information and objects. Bucuk, [0188].

105. Bucuk also describes that identification information (or "Unique IDs") take many forms including device names and addresses, numbers/strings, changing numbers/strings that are periodically generated according to an algorithm, etc. Bucuk, [0100]-[0108], [0259], [0324]-[0325]. UIDs are generated "by the system on the server... side" and "periodically changed and updated to the mobile phone device... and all authentication servers... to provide greater privacy." Bucuk, [0108], [0259], [0325].

b. Overview of Nordman (EX1011)

106. U.S. Patent Application Publication No. 2002/0174364 to Nordman et al. ("Nordman," EX1011), titled "METHOD FOR PROTECTING PRIVACY

WHEN USING A BLUETOOTH DEVICE,” was filed on May 21, 2001 and was published on November 21, 2002.

107. Nordman is directed to a method for protecting the privacy of a Bluetooth device by preventing the correlation of a user’s identity, routes, and activities with their device’s address through use of a pseudonym address instead of a device’s real Bluetooth device address (BD_ADDR). Nordman, Abstract, [0005]-[0006], [0051], [0095]. That is, when a mobile device is freely sharing its identification information to the public—such as in the case of a BD_ADDR that is provided to Bluetooth inquiries, a “user’s routes and activities can be tracked by logging the times and locations of the observance of his/her device’s Bluetooth Device Address,” and that may allow “sinister observers... [to] compromise the use’s privacy and possibly the user’s safety.” Nordman, [0004]. The use of pseudonym addresses alleviates those concerns. Nordman, [0005].

108. Furthermore, a device’s pseudonym address is changed periodically to further enhance privacy because “[t]he anonymity of the user would otherwise be undermined if the same pseudonym address were to be used indefinitely.” Nordman, [0010]. Nordman therefore illustrates several options for changing addresses based on elapsed time, use counts, connections made, location information, and others. Nordman, [0010]-[0011], [0043]-[0051].

109. The generation of addresses is accomplished by, for example,

randomizing parts of a real address, selecting an address from previously computed values, and/or downloading addresses from a server. Nordman, [0057]-[0066], [0073], [0094].

c. Overview of Bucuk's and Nordman's combined teachings

110. Bucuk and Nordman are analogous art and their combined teachings renders obvious claims of the '749 patent.

111. The '749 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, 2:34-54 (including, for example, concerns of fraud, identity discovery and/or spoofing, and personal safety and privacy).

112. Bucuk and Nordman are each analogous to the '749 patent, as they are in the same field of wireless communications and/or reasonably pertinent to the problems identified above. Bucuk, [0001], [0019] (establishing relationships between devices in short-range communication, aided by a server), [0160], [0172], [0325]-[0326] (describing features that enhance privacy and security); Nordman, Abstract, [0004]-[0005], [0013], [0095]-[0096] (protecting the privacy of a user's identity, routes, and activities that could be tracked through wireless technologies).

113. Bucuk teaches that embodiments of "system could be designed so that

the unique number... is periodically changed and updated to the mobile phone device... and all authentication servers... to provide greater privacy to the user of the system from malicious monitoring of the [UID].” Bucuk, [0325]; see also [0108], [0259] (UIDs “generated by the system” are generated “on the server”); [0100]-[0107] (exemplary UIDs include BD_ADDRs and changing numbers). In embodiments implementing changes, Bucuk describes that periodic changes occur when UIDs can be “used only once” and/or are “time expiring.” Bucuk, [0161]-[0162], [0172]-[0173], [0259].

114. To the extent Patent Owner argues that embodiments of Bucuk relied upon in Ground 2 (such as those described in [0188] and [0325]) do not explicitly describe detailed mechanisms for changing a device’s identification information in accordance with a “predetermined event” (as in claims 1 and 7), such as using an “elapsed time” (one option in claims 2 and 8), Bucuk nonetheless leaves it to the discretion of a POSITA regarding the methods for implementing and triggering “periodically chang[ing]” UIDs, a concept that is taught by Nordman.

115. Like Bucuk, Nordman explains that a device (and its user) using the same identifier over time is susceptible to tracking, which may be “exploited... by market researchers, and possibly by more sinister observers, ...compromising the user’s privacy and... safety.” Nordman, [0004]; Bucuk, [0325]. Furthermore, these privacy/safety concerns were not limited to Bluetooth communications but were

also applicable to other types of wireless communications. Nordman, [0096].

Indeed, privacy and security concerns in short-range wireless devices that use fixed identifying information were well-known, as were techniques for changing identification information to address those concerns. EX1010, [0002]-[0004] (temporary and/or randomly generated identification numbers mitigates threats to security and privacy); EX1012, [0002]-[0008] (preventing tracking through a randomly generated Bluetooth address); EX1013, [0008]-[0011] (same).

116. Nordman thus teaches to program conditions and functions to prevent tracking by periodically changing identifiers based upon, for example, time, use counts, connections made, and/or locations. Nordman, [0010]-[0011], [0043]-[0051], [0060]-[0085]. It would have been obvious to a POSITA to modify Bucuk's servers to generate periodically changing UIDs based on Nordman's teachings of various predetermined events. Modifications to processes for periodically changing UIDs according to Nordman's described system design options would have been accomplished through coding techniques known to a POSITA, such as by modifying the software applications executed for server functions. Bucuk, [0335]-[0338].

117. This modification would have been further obvious as it is the application of a known technique (Nordman's variations of periodically changing identifiers) to a known device ready for improvement (Bucuk's server that

periodically change device identifiers) to yield predictable results (periodically changing those identifiers based on different events such as time and use counts).

118. A POSITA would have also had a reasonable expectation of success in modifying Bucuk with the teachings of Nordman. For example, Nordman teaches how to implement steps for monitoring events, such as elapsed times and identifier use, utilizing counters and conditional logic. Nordman, [0059]-[0085]. A POSITA would have required no more than ordinary software coding skills to modify and/or add to Bucuk's software applications so that they monitor and act on the various conditions for periodically changing UIDs, as known in the art.

d. The '749 Patent Claims

i) Claim 1

(1) [1.PRE] “A method for exchange of information between one or more applications executing on at least a first wireless device and a second wireless device, the method comprising the steps of:”

119. Bucuk discloses *a method for exchange of information* (for example, exchanging identification information and other data) *between one or more applications executing on at least a first wireless device and a second wireless device* (for example, between software executing on devices communicating via short-range communications).

120. Bucuk that “two devices” (*i.e., a first wireless device and a second wireless device*) “exchange their [UIDs] via a short range communication

connection between the two devices.” Bucuk, [0188]. An authentication server may authorize a link/bond between the first and second device that grants the devices access to information, data, services, resources, etc. associated with the other device. Bucuk, [0188], [0191], [0329], [0332]; *see also* [0042], claims 23 and 28 (example sending a data object from the first device to a linked second device), [0184]-[0185] (example of bonding between two devices that permits each device to access selected data of the other). These are *exchanges of information*.

121. Bucuk further discloses that devices in its system perform disclosed methods by executing installed software applications. Bucuk, [0333]; *see also* Bucuk, [0071]-[0072], [0089], [0118], [0147], and [0305]-[0307] (describing executing stored software to perform functions). That is, when devices exchange information based on functions described by Bucuk, it is the applications on those devices causing that information to be transmitted and/or received.

(2) [1.A.I] “at the first wireless device, providing initial identification information to a central server, said initial identification information having been collected by the first wireless device from the second wireless device via a first, direct, short range local wireless link between the second and first wireless devices,”

122. Bucuk discloses *at the first wireless device, providing initial identification information to a central server* (for example, the first device sends the second device’s UID to an authentication server), *said initial identification*

information having been collected by the first wireless device from the second wireless device via a first, direct, short range local wireless link between the second and first wireless devices (for example, the first device received the second device's UID via short-range communications).

123. As discussed for [1.PRE], Bucuk discloses that the two devices “exchange their [UIDs] via a short range communication connection between the two devices.” Bucuk, [0188]. Examples of short-range communications include Bluetooth, WiFi, NFC, etc. Bucuk, [0009], [0312]-[0315].

124. After the exchange, “[a]t least one device... sends the other device's [UID] to the authentication server...,” thus *providing initial identification information to a central server*. Bucuk, [0188].

(3) [1.A.II] “wherein the initial identification information is associated at the central server with an identity of a user or entity associated with the second wireless device, and”

125. Bucuk discloses that *the initial identification information (for example, the second device's UID) is associated at the central server with an identity of a user or entity associated with the second wireless device (for example, the server associates the second device's UID with a user and Unique Entity ID of the device).*

126. A UID, such as the second device's UID (*the initial identification*

information), is information that, “for a particular server or database,” “directly or indirectly identify an Entity (which could be a User..., an object...)” Bucuk, [0324]. Therefore, because the second device is registered with the authentication server (Bucuk, [0188]) and the second device’s UID information “will resolve [to identify a] Unique Entity ID and/or identify an Entity, for example through prior registration or login information” (Bucuk, [0324]), the second device’s UID is *associated at the central server with an identity of a user or entity associated with the second wireless device.*

(4) [1.A.III] “wherein the initial identification information is provided to the central server, by the first wireless device, over a second wireless link;”

127. Bucuk discloses that *the initial identification information is provided to the central server, by the first wireless device, over a second wireless link* (for example, the first device provides the second device’s UID to the authentication server over a long-range communication connection).

128. Bucuk discloses that the first device “sends the [second] device’s [UID] to the authentication server via its own long range communication connection,” which is different from the short-range connection between the two devices. Bucuk, [0188]. Examples of long-range communications include internet connections and GSM, GPRS, and UMTS cellular connections. Bucuk, [0002], [0135], [0333].

(5) [1.B.I] “at the second wireless device, upon an occurrence of a predetermined event coordinated with said central server,”

129. Bucuk-Nordman teaches performing additional actions (for example, *see [1.B.III]-[1.C]) at the second wireless device, upon an occurrence of a predetermined event coordinated with said central server* (for example, at the second device, on the occurrence of a periodic changing of the second device’s UID).

130. As discussed above, Bucuk-Nordman teaches that the second device’s UID is “periodically changed” (Bucuk, [0325]) upon the *occurrence of a predetermined event* based on known criteria such as an identifier’s expiration and/or one-time use (Bucuk, [0161]-[0162], [072]-[0173], [0259]), which Nordman teaches in detail (Nordman, [0010]-[0011], [0043]-[0051], [0060]-[0085]).

131. Bucuk further teaches that changed UIDs are “updated to the mobile phone device... and all authentication servers.” Bucuk, [0325]. Therefore, the *predetermined event* that causes the second device’s UID to be changed is *coordinated with said central server*. This coordination of UIDs between relevant devices and servers is an obvious, if not necessary, step for facilitating Bucuk’s system, as the relevant devices and servers must be aware of updated UID values before they are used and exchanged, so that appropriate bonds/links may be made

between devices based on those UIDs.

(6) [1.B.II] “within a specific application on the second wireless device,”

132. Bucuk discloses that the second device’s functions (including those claimed in [1.B]-[1.C]) are performed *within a specific application on the second wireless device* (for example, within installed software). *See* [1.PRE].

(7) [1.B.III] “providing modified identification information over the first, direct, short range local wireless link in place of the initial identification information,”

133. Bucuk discloses *providing modified identification information* (for example, providing the second device’s changed UID) *over the first, direct, short range local wireless link* (for example, over the short-range communication link between the first and second device) *in place of the initial identification information* (for example, rather than providing the UID that existed before the change).

134. Bucuk discloses that when the first and second device “come into close proximity, they exchange their [UIDs] via a short range communication connection between the two devices.” Bucuk, [0188]; *see* [1.A.I]. Bucuk further discloses that the system process of exchanging UIDs to access services and objects is “repeated” between devices. Bucuk, [0123], [0129], [0170], [0296]; *see also* [0208]-[0209] (example where nearby devices “constantly” transmit/receive

identification information to unlock a door and where authorizations change over time). Accordingly, after the second device changes its UID (*see* [1.B.I]), the initial identification information has since been changed, so subsequent exchanges of UIDs will include *providing modified identification information in place of the initial identification information* to the first device.

(8) [1.C] “at the first wireless device, collecting said modified identification information.”

135. Bucuk discloses, *at the first wireless device, collecting said modified identification information* (for example, first device receives the modified UID). *See* [1.B.III].

ii) Claim 2

(1) “The method of claim 1 wherein the predetermined event is one or more of: an elapsed time; a number of uses of the identifier; and/or a step in a process.”

136. Bucuk-Nordman teaches that *the predetermined event is one or more of: an elapsed time; a number of uses of the identifier; and/or a step in a process.*

137. Bucuk-Nordman teaches the occurrence of the predetermined event for changing identifiers (or UIDs), for example, a predetermined time. *See* [1.B.I]. Other examples of predetermined events track use counts and/or location changes. Nordman, [0010], [0029]-[0051], [0054], claims 13-18.

138. For example, the identifier changes after a “predetermined time or count,” which changes identifiers after a certain amount of time elapses. Nordman,

Fig. 3 (steps 304 and 320-332), [0048], [0060]-[0070]. A change based on a predetermined time/count is therefore based on *an elapsed time*.

139. In another example, the identifier changes after “inquiries/connections,” which changes identifiers after every connection—for example, if an inquiry is received but no connection is made, or if a connection is terminated. Nordman, Fig. 3 (steps 304, 306-318), [0049], [0071]-[0085]. A change based on a number of inquiries/connections is therefore based on *a number of uses of the identifier*.

140. In another example, the identifier changes after a location change, which follows steps to change an identifier after determining that a device changes physical location by a predetermined distance (for example, 10m). Nordman, Fig. 3 (steps 304, 306-318), [0050], [0071]-[0085]. A change based on a location change is therefore based on *a step in a process*.

iii) ***Claim 3***

(1) “The method of claim 1 wherein the step of changing the user or entity identification information at said second wireless device is further: effected by a rule-based generation local to the application, downloaded from the server directly, or synchronized such that it is coordinated with predetermined receiving and transmitting times.”

141. I have been informed that because this claim recites “the step of changing...,” which does not refer to a previously introduced “a step of changing

the user or entity identification information” (either in this claim or its parent claim), it is likely a typographical error that should be read as “a step of changing.”

142. Bucuk as modified by Nordman teaches that *changing identification information may be downloaded from the server directly*. For example, Bucuk describes that the changed UID is generated by the system (for example, the server; Bucuk, [0108], [0259]) and “updated to the mobile phone device” (Bucuk, [0325]), which a POSITA would have recognized as obviously including a download from the server (which generated the UID) to the second device (which is updated with the generated UID). *See also* Bucuk, [0115], [0328] (UIDs are transferred through SMS, MMS, email, WAP push, etc.); Nordman, [0094] (known technique of a server computing an identifier that is “downloaded” to a wireless device).

143. To the extent Patent Owner argues that Bucuk does not describe that the server generating the changed UID is the authentication server, it would have been obvious to a POSITA to utilize one or many servers to carry out system functionality in Bucuk-Nordman, choosing a balance between costs (for example, constructing and maintaining multiple servers compared to a single server) and benefits, such as distributing loads (for example, providing multiple servers in different locations to address regional communication latency, multiple servers to increase processing capacity, scaling, etc.) and providing failure redundancies. The

integration, division, and/or distribution of functions in one or more “server” units would have been no more than an obvious configuration design choice for a POSITA and was well-known in prior art server implementations. *See* Bucuk, [0025] (servers associated with devices are the same), [0126] (“server” as software on shared hardware), [0251]-[0252] (same server for multiple devices and services); EX1052, [0144] (separate servers having separable, combinable, and/or distributed functionality); EX1053, 6:8-13 (server elements may be separated, combined, and connected as desired); EX1054, [0063] (server functions may be combined and/or separated and/or dispersed in different servers).

iv) ***Claim 7***

(1) [7.PRE] “A server for exchanging information between one or more applications executing on at least two wireless devices, the server comprising:”

144. Bucuk discloses *a server for exchanging information* (for example, a server generates Unique UIDs for devices that are exchanged to authorize further exchanges of information) *between one or more applications executing on at least two wireless devices* (for example, between software executing on devices communicating via short-range communications).

145. As discussed for [1.PRE], Bucuk discloses a system including a first device executing software, a second device executing software, and an authentication server that facilitates exchanges of information between the two

devices by authorizing links/bonds between them.

146. Additionally, as discussed for [1.A.I], [1.B.I], and claim 3, Bucuk-Nordman teaches that the server provides the periodically changed UIDs that are exchanged between the devices. Accordingly, the server further facilitates the exchange of identification information between the devices.

(2) [7.A.I] “a receiver, for receiving initial identification information having been collected by a first wireless device from a second wireless device via a, first, direct, short range local wireless link between the first and second wireless devices,”

147. Bucuk discloses the server function of *receiving initial identification information...* for the same reasons discussed for [1.A.I].

148. Furthermore, the server receives the initial identification information over a long-range communication connection such as the Internet (*see* [1.A.III]), and Bucuk discloses that the server includes a *receiver* such as “a network card or modem” for communications over the Internet. Bucuk, [0336].

(3) [7.A.II] “wherein the initial identification information is associated at the server with an identity of a user or entity associated with the second wireless device, and”

149. *See* [1.A.II].

(4) [7.A.III] “wherein the initial identification information is received by the server from the first wireless device over a second wireless link distinct from the first wireless link; and”

150. See [1.A.III].

151. Furthermore, the second wireless link (for example, cellular or Internet connection; see [1.A.III]) is *distinct* from the first wireless link (for example, Bluetooth; see [1.A.I]) because, for example, they are separate and different links used to connect different devices (for example, the server and first device versus the first and second device) using different communications standards (for example, cellular GSM versus Bluetooth).

(5) [7.B.I] “a transmitter for, upon an occurrence of a predetermined event coordinated with the second wireless device,”

152. See [1.B.I].

153. Bucuk further discloses the server including *a transmitter* (for example network card or modem) for the same reasons it includes a receiver—to communicate information with wireless devices over the long-range communication connection (see [7.PRE]-[7.A.I]).

(6) [7.B.II] “sending a message to the second wireless device to change the identification information within a specific application on the second wireless device and”

154. Bucuk-Nordman teaches the transmitter *sending a message to the second wireless device to change the identification information* (for example,

updating the second device to change UID) *within a specific application on the second wireless device* (for example, UIDs are used within the second device's installed software).

155. Bucuk-Nordman teaches changing the second device's UID from an initial UID to a modified UID. *See* [1.B.I]-[1.B.III]. Bucuk further teaches that UIDs are generated by the system on the server and "updated to the mobile phone device" (*i.e.*, the second device) through, for example, a download from the server to the second device using a known technology such as SMS, MMS, email, WAP push, etc. Bucuk, [0115], [0328]; Nordman, [0094]; *see* discussion of claim 3. A POSITA would have recognized that a UID update using one of these types of communications would have included a *message* that causes the second device to *change its identification information*. For example, "SMS" stands for Short Message Service (aka text messaging), and "MMS" stands for Multimedia Messaging Service, each of which function by sending *messages*. Email, WAP push, and other similar technologies are also used to convey information from one device to another by sending *messages* through communication channels.

156. Furthermore, Bucuk's second device uses the modified UID in at least its exchange of information with the first device. *See* [1.B.III]. Because the second device executes a software application to perform that function and other functions related to UIDs (*see* [1.PRE]), *the identification information is changed within a*

specific application on the second wireless device.

(7) [7.B.III] “for subsequently providing modified identification information over the first, direct, short range local wireless link in place of the initial identification information, and”

157. See [1.B.III].

(8) [7.B.IV] “such that the modified identification information is associated at the server with said identity of a user or entity associated with the second device.”

158. See [1.B.IV].

v) Claim 8

(1) “The server of claim 7 wherein the predetermined event is one or more of: an elapsed time; and/or a number of uses of the identifier; and/or a step in a process.”

159. See claim 2.

vi) Claim 9

(1) “The server of claim 7 wherein the change of user or entity identification information is further: effected by a rule-based generation local to the application, downloaded from the server directly, or synchronized such that it is coordinated with predetermined receiving and transmitting times.”

160. See claim 3.

vii) **Claim 13**

(1) “The method of claim 1 wherein the user or entity identification information is changed to protect the privacy of the identity of the a user or entity associated with the second wireless device.”

161. Bucuk discloses that periodically changing a UID “provide[s] greater privacy to the user of the system from malicious monitoring of the [UID].” Bucuk, [0325]. Since UIDs identify associated users and devices, changing the second device’s UID *protects the privacy of the identity of the user or entity associated with the second device.*

viii) **Claim 15**

(1) “The method of claim 7 wherein the user or entity identification information is changed to protect the privacy of the identity of a user or entity associated with the second wireless device.”

162. See claim 13.

ix) **Claim 17**

(1) “The method of claim 1 wherein the first wireless device further performs the step of providing modified identification information to said central server, as collected by the first wireless device from the second wireless device.”

163. Bucuk-Nordman teaches that *the first wireless device further performs the step of providing modified identification information to said central server, as collected by the first wireless device from the second wireless device* (for example, the first device receives the changed UID from the second device and provides it to

the authentication server).

164. Bucuk discloses that the system's process of exchanging UIDs is repeated, such that the devices exchange initial UIDs (as in [1.A.I]) and, later, modified UIDs (as in [1.C]). Thus, following the same process for the initial UID, the first device will provide the modified UID, as received from the second device, to the authentication server (as similarly discussed for [1.A.I]).

165. For example, as applied to an embodiment in which an automatic door (a first device) receives a mobile phone's (a second device's) UIDs to unlock the door, the door will provide the phone's received UID to the authorization server even after changing/modifying. That is because the modified UID will appear to the door as a "new" UID (having been changed) and/or the modified UID is not recognized as an authorized UID after the user loses access (for example, no longer an employee of a company, based on non-payment of fees), each situation requiring verification with the server. Bucuk, [0208]-[0209].

x) Claim 18

(1) "The method of claim 1 wherein the initial identification information, if re-sent to the central server following said pre-determined event, is processed by said central server in a manner different from which it was processed prior to said pre-determined event."

166. Bucuk as modified by Nordman teaches that the second device's initial identification information is changed to the modified identification

information after the predetermined event, and this change is synchronized across devices and servers. *See* [1.B.I]; Bucuk, [0325] (changing UID to protect user privacy). Accordingly, because the second device and its user are no longer associated with the initial UID after the predetermined event, *if* the initial UID were to be *re-sent* to the authentication server, the *initial identification information* will be *processed* by the authentication server *in a manner* (for example, not identifying an entity associated with the second device) *different from which it was processed prior to said pre-determined event* (for example, prior to the predetermined event, the initial UID would have identified an entity associated with the second device). Bucuk, [0324].

xi) Claim 19

(1) “The method of claim 1 wherein the initial identification information, if re-sent to the central server following said pre-determined event, is processed by said central server in a manner different from which it was processed prior to said pre-determined event.”

167. Bucuk explains that the authentication server may authorize a link/bond between the first and second devices and/or entities based on received UIDs, which includes the modified UID after the pre-determined event. Bucuk, [0188]; *see* [1.C], discussion of claim 17. An authorized link/bond is used, for example, to “verify an identity or authenticity of an entity.” Bucuk, [0191], [0330]. Discussed below, Bucuk describes different applications of its system that render

claim 19 obvious.

Police ID Example

168. In one example, the first device and the second device are the mobile phone devices of a resident and a police officer, respectively, and the officer wants to “verify the identity of [the] mobile phone device user.” Bucuk, [0228]. Through bonding (which includes exchanging UIDs and the modified UID as discussed above), aided by the common police authentication server, the officer is able to see details about the identity of the resident and verify the resident’s identity. Bucuk, [0228]-[0229].

169. Accordingly, *the modified identification information* (for example, the officer device’s modified UID) *is used by the central server* (for example, by bonding the officer device’s modified UID with the resident device’s UID at an authentication server) *to verify the legitimacy, identity or authenticity of the first wireless device* (for example, bonding of the UIDs is part of a process to verify the identity or authenticity of the resident).

170. Additionally, while the “entity” being verified in this example is the user/resident, Bucuk teaches that “entity” also refers to devices. Bucuk, [0320]. Accordingly, it would have been obvious to a POSITA that this exemplary use not only verifies the identity and authenticity of the user (the resident) but may also be used to verify the user/resident’s mobile device that exchanges UIDs (*i.e.*,

verifying *the first wireless device*).

Web Access Example

171. In another example, the first device and the second device are a desktop computer and a mobile phone device, respectively, and the user of the mobile phone device wants to log into the desktop computer (for example, to access a secure bank website). Bucuk, [0231]-[0234]. The mobile phone device collects the UID of the desktop computer of interest and sends that information to its authentication server. Bucuk, [0233]. The desktop computer similarly collects the Bluetooth names and UIDs of devices in its proximity, including the mobile phone device, and sends that information to a bank authentication server. Bucuk, [0234]. The bank authentication server uses the UIDs “to positively identify [the] mobile phone device[] as being in close proximity of the desktop[] and having [the particular UID].” Bucuk, [0234].

172. Accordingly, *the modified identification information* (for example, the mobile phone’s modified UID) *is used by the central server to verify the legitimacy, identity or authenticity of the first wireless device* (for example, used by the bank authentication server to verify that the desktop computer is identified as legitimately in proximity of the mobile phone).

173. Additionally, while this example makes use of one other server in addition to the bank authentication server 314 (*see* [0233]-[0234], describing an

authentication server 316 associated with the mobile phone), Bucuk makes clear that the server configurations used in the various different embodiments and systems are obvious design choices for a POSITA. *See* Bucuk, [0025] (server associated with a first device and server associated with a second device may be the same server), [0126] (“server” may refer to software that can operate on shared hardware), [0251]-[0252] (same server serving multiple devices and providing multiple services). Accordingly, to the extent Patent Owner argues that the Web Access example described above is not representative of server functions in this claim because it includes two servers, it would have been obvious to a POSITA to consolidate those functions as an obvious design choice to, for example, minimize the amount of hardware required. *See* discussion of claim 3 above—implementations with one or many servers were well-known in the art; EX1052, [0144] (separate servers having separable, combinable, and/or distributed functionality); EX1053, 6:8-13 (server elements may be separated, combined, and connected as desired); EX1054, [0063] (server functions may be combined and/or separated and/or dispersed in different servers).

xii) Claim 20

(1) “The method of claim 17 wherein the modified identification information is used by the central server to verify the legitimacy, validity, or authenticity of a transaction associated with one of (a) the first wireless device or (b) a user or entity associated with the first wireless device.”

174. Bucuk as modified by Nordman teaches that *the modified identification information* (for example, the second device’s modified UID) *is used by the central server to verify the legitimacy, validity, or authenticity of a transaction* (for example, the authentication server receives the modified UID to verify the legitimacy and validity of a money transfer request) *associated with one or (a) the first wireless device or (b) a user or entity associated with the first wireless device* (for example, the money transfer is from the second device and user to a first device and user).

175. Bucuk explains that the authentication server may authorize a link/bond between the first and second devices and/or entities based on received UIDs, which includes the modified UID after the pre-determined event. Bucuk, [0188]; *see* [1.C], discussion of claim 17. An authorized link/bond is used, for example, to trigger an event or action, execute code, perform a business process, verify an identity or authenticity of an entity, etc. Bucuk, [0191], [0330].

176. For example, the first device and second device are devices of users

that exchange UIDs to conduct a currency transfer (a *transaction*)—for example, corresponding to a “newspaper[] seller” collecting money from a “newspaper reader.” Bucuk, [0222]-[0224]. The first device collects the modified UID information from the second device and transmits that information to a bank authentication server, which looks up the “respective [UIDs] collected during the bonding procedure” to authorize a “one off money transfer.” Bucuk, [0224]; *see also* [0223] (devices “enable currency transfer” by first making themselves available for bonding at the authentication server), [0225] (both devices deal with the bank authentication server).

177. Accordingly, because the requested money transfer is only authorized by the authentication server if the two devices made themselves available for bonding, which the server determines by looking up received UIDs as discussed above, the authentication server uses UIDs (including the modified UID) *to verify the legitimacy or validity of a transaction* as being authorized between two *devices* and *users* that have made themselves available for bonding and currency transfer.

xiii) Claim 21

(1) “The method of claim 1 wherein upon the [occurrence] of the predetermined event, further notifying the second wireless device of the modified identification information via a wireless configuration message or an instruction to change communication state.”

178. Bucuk-Nordman teaches that *upon the occurrence of the predetermined event* (for example, after the predetermined time), *further notifying the second wireless device of the modified identification information via a wireless configuration message* (for example, the server transmits a message to the second device to change its UID).

179. Bucuk-Nordman teaches using a predetermined event, such as an elapsed time or use count, as a basis for changing the second device’s UID, which is generated at the server and updated to the second device. *See* discussions of Bucuk and Nordman’s combined teachings and claims 1-3 above. The server updates the second device with a message (for example, SMS, MMS, email, WAP push) that causes the second device to change its UID. *See* [7.B.II].

180. A POSITA would have recognized that the message to the second device that causes the second device to thereafter use the modified UID is a *wireless configuration message* because it is a message that the second device receives and recognizes as containing data that alters the second device’s wireless

behavior—*i.e.*, by providing the modified UID in subsequent transmissions instead of the initial UID.

xiv) Claim 22

(1) “The server of claim 7 wherein the central server further receives modified identification information, as collected by the first wireless device from the second wireless device.”

181. See claim 17.

xv) Claim 23

(1) “The server of claim 7 wherein the initial identification information, if re-sent to the central server following said pre-determined event, is processed by said central server in a manner different from which it was processed prior to said pre-determined event.”

182. See claim 18.

xvi) Claim 24

(1) “The method of claim 23 wherein the modified identification information is used by the central server to verify the legitimacy, identity or authenticity of the first wireless device.”

183. See claim 19.

xvii) Claim 25

(1) “The server of claim 7 wherein the modified identification information is used by the central server to verify legitimacy, validity, or authenticity of a transaction associated with one of (a) the first wireless device or (b) a user or entity associated with the first wireless device.”

184. See claim 20.

xviii) Claim 26

(1) “The server of claim 7 wherein upon the [occurrence] of the predetermined event, the server further notifies the second wireless device of the modified identification information via a wireless configuration message or an instruction to change communication state.”

185. See claim 21.

**C. GROUND 3: BUCUK IN VIEW OF NORDMAN AND KALLIO
RENDERS OBVIOUS CLAIMS 4-6 AND 10-12**

186. Bucuk and Nordman were introduced in Grounds 1 and 2 above.

187. U.S. Patent Application Publication No. 2003/0224756 to Kallio, titled “SYSTEM AND METHOD FOR SERVICES ACCESS,” was filed on May 30, 2002 and published on December 4, 2003.

188. Kallio is in the same field of endeavor (*see* Kallio, [0001]-[0003], [0011]-[0017] (facilitating access to services from, for example, a Bluetooth base station with managing servers), [0024] (communicating device and service identifiers)) and teaches that a wireless device terminal identifying itself to a server

may use an identifier such as “a MAC (media access control) address... or a Bluetooth device address.” Kallio, [0020]. MAC addresses and Bluetooth device addresses are “MAC addresses” as discussed for [1.A.II] above. Kallio further teaches that using a different MAC address in the form of a “randomly generated” “48-bit address similar in form to a Bluetooth hardware address, but whose composition [bears] no relation to any identifier corresponding to [the] terminal,” provides anonymity to the terminal and/or its user. Kallio, [0020], [0024]-[0026]. The 48-bit addresses may be generated according to rules or constraints (for example, ensuring uniqueness among devices, having values in certain ranges, etc.) and/or in several different ways (for example, generated one by one or assigned from a bank of addresses). Kallio, [0024]-[0027].

189. As discussed above, Bucuk-Nordman teaches a system including devices that exchange identifiers (UIDs) via short-range communications and an authentication server that facilitates further communication between those devices based on their UIDs. Bucuk-Nordman further teaches enhancing privacy and safety by periodically changing a device’s UIDs. *See* discussion of Ground 2.

190. To the extent Patent Owner argues that Bucuk-Nordman does not describe server functions in detail, such as taking an identifier from a pool of identifiers (as in claims 4 and 10 of the ’749 patent) or using an identity manager within a server to assign identifiers (claims 5-6 and 11-12 of the ’749 patent), those

server functions would have been obvious to a POSITA, as taught by Kallio.

191. It would have been obvious to modify Bucuk's server to generate the periodically changing UUIDs with enhancements taught by Kallio. Bucuk teaches that UUIDs take the form of names, addresses, numbers, strings, codes, etc. Bucuk, [0100]-[0108], [0324]-[0325]. Nordman and Kallio both express concern over the possibility of generating duplicate identifiers that may conflict with the existing identifiers of nearby wireless devices. Nordman, [0012], [0066], [0076] (performing extra steps to generate an address "because of other duplicate addresses in the vicinity"); Kallio, [0024]-[0025] ("constraint that no other terminal be currently assigned the particular address"), [0026] ("constraint that a created address not be identical to an actual and/or existing Bluetooth hardware address, MAC address or other identifier"). Kallio addresses this concern by, for example, generating a "bank" (or *pool*) of identifiers from which a server assigns identifiers. Kallio, [0026]. Thus, by implementing a centralized source to assign identifiers from a pool (thus functioning as an *identity manager*), the server advantageously avoids extraneous processing and ensures that no two devices use the same identifier. These modifications would have been accomplished through software coding techniques known to a POSITA, such as by modifying the server software for generating UUIDs. Bucuk, [0335]-[0338] (servers include installed "software drivers and applications" for functionality); Kallio, [0039]-[0043].

192. Accordingly, the combined teachings of Bucuk-Nordman-Kallio would have resulted in wireless devices periodically changing their UIDs by receiving modified UIDs that a server selects from a pool of identifiers. This modification would have been further obvious as an application of a known technique (Kallio's assignment of identifiers from a pool) to a known device ready for improvement (Bucuk-Nordman's server generates identifiers) to obtain predictable results (assigning non-duplicative identifiers to devices from a centralized server) to ensure duplicate addresses are avoided.

193. A POSITA would have also had a reasonable expectation of success in modifying server functions to generate/assign addresses and coordinate the same with participating devices. For example, the generation of a "bank" of identifiers would have required no more than ordinary software coding skills to modify and/or add to the server software so that it generates, stores, selects, and communicates those values, as known in the art.

a. The '749 Patent Claims

i) Claim 4

(1) "The method of claim 1 further comprising: at said second wireless device, receiving a user or entity identifier from a central server, the user or entity identifier taken from a pool of identifiers determined by the central server."

194. It is unclear whether claim 4's "a central server" is a new recitation of

a central server or references the central server already introduced in parent claim

1. Nevertheless, it would have been obvious to a POSITA to utilize one or many servers to carry out system functionality in Bucuk-Nordman-Kallio such that the integration, division, and/or distribution of functions in one or more “server” units would have been no more than an obvious design choice for a POSITA. *See* discussion of claim 3 in Ground 2 above.

195. Bucuk-Nordman-Kallio teaches, *at said second wireless device, receiving a user or entity identifier from a central server* (for example, the second device receives a modified UID from a server), *the user or entity identifier taken from a pool of identifiers determined by the central server* (for example, the modified UID is selected from a bank of identifiers at the server).

196. As discussed above, a POSITA would have been motivated to use a central server to distribute to devices UIDs (identifying users and devices; Bucuk, [0324]), thereby avoiding duplicate values across a plurality of devices.

197. For example, Kallio describes a server assigning identifiers by generating a “bank” of acceptable identifiers (*i.e., a pool of identifiers*) and randomly selecting an identifier from that bank for assignment, thereby ensuring that the identifier is not identical to an actual and/or existing identifier. Kallio, [0024]-[0026].

i) *Claim 5*

(1) “The method of claim 1 further comprising: using an identity manager within a server to assign user or entity identifiers to devices by sending the same over a WWAN cellular data link to said second wireless device; and wherein the user or entity identifiers are changed over time.

198. Bucuk-Nordman-Kallio teaches *using an identity manager within a server to assign user or entity identifiers to devices* (for example, a server assigns identifiers to devices using software applications) *by sending the same over a WWAN cellular data link to said second wireless device* (for example, server-device communications are over cellular links); *and wherein the user or entity identifiers are changed over time* (for example, see claims [1.B.I] and 2).

199. As similarly discussed for claim 4, it would have been obvious to use a server to assign identifiers, selected from a pool of identifiers, to devices for use as UUIDs, as taught by Kallio. Kallio teaches that the server executes “software modules” to implement that functionality. Kallio, [0039]-[0043]; *see also* Bucuk, [0335]-[0338] (servers include “software drivers and applications”). The ’749 patent does not describe *identity manager* as necessarily requiring any particular structure—“identity manager” is the descriptive name for a functional block or application agent of the server. EX1001, Fig. 13, 16:58-17:1. Bucuk’s and Kallio’s server software applications and modules performing the same claimed functions

are at least equivalent to the claimed *identity manager*.

200. As discussed for [1.A.III], the server and devices communicate via long-range communications, for example, GSM, GPRS, or UMTS cellular connections—*i.e.*, *WWAN cellular data links*. Bucuk, [0002], [0135], [0333].

201. Further discussed above, UIDs identifying users and devices are “periodically changed” upon the occurrence of a predetermined event, such as an elapsed time, and are therefore *changed over time*. See discussion of Bucuk’s and Nordman’s combined teachings above (in Ground 2), [1.B.I], and claim 2.

i) *Claim 6*

(1) “The method of claim 5 wherein at least one of the user or entity identifiers are associated with a device identifier by the identity manager, and the device identifier is associated with one or more of the initial identification information or modified identification information, and wherein the device identifier is one or more of: a media access control (MAC) device address of a short range wireless network adapter; a SSID in an IEEE-802.11 network beacon; a BSSID of an IEEE802.11 network adapter; a IEEE802.15.1 Inquiry Response Message as a BD_ADDR associated with an inquiry response message; a device name in a Bluetooth name response packet; or one or more identifiers listed in a services list as provided in a LMP_features_req message or LMP_features_req_ext message for a Bluetooth device.”

202. Bucuk-Nordman-Kallio teaches that *at least one of the user or entity identifiers* (for example, one of the generated UIDs) *are associated with a device*

identifier by the identity manager (for example, the modified UID is associated with an Entity ID at the server), *and the device identifier is associated with one or more of the initial identification information or modified identification information* (for example, the Entity ID is associated with the initial UID prior to the predetermined event and with the modified UID after the predetermined event).

203. Bucuk teaches that the server, which includes the *identity manager* (*i.e.*, server software applications performing functions related to identification information; *see* discussion of claim 5), manages a database of user account information that associates various information about a user (for example, names, addresses, UIDs, etc.) to a unique “Entity ID.” Bucuk, [0109], [0155], [0254], [0320]. The Entity ID is different from the UID (though optionally the same), and in use, the UID identifies an entity user and/or device by resolving to its Entity ID at the server. Bucuk, [0324]; *see* [1.A.II]; *see also* Bucuk, [0160] (“code[s] which represent the same user/device/entity change[] whilst still representing the same user/device/entity”).

204. The Entity ID associated with the second device is therefore a *device identifier associated with the second device’s initial identification information* (second device’s initial UID) and *modified identification information* (second device’s modified UID) because the second device’s UID, whether it is the pre- or post-predetermined event UID, is configured to resolve to the Entity ID.

Additionally, because the value of the second device's modified identification information is taken from an assigned *user or entity identifier* generated by the server (*see* discussion of claim 5), the Entity ID associated with the modified identification information is also *associated with at least one of the user or entity identifiers*.

205. Furthermore, Bucuk discloses that *the device identifier is one or more of: a media access control (MAC) device address of a short range wireless network adapter; a BSSID of an IEEE802.11 network adapter; [and] a IEEE802.15.1 Inquiry Response Message as a BD_ADDR associated with an inquiry response message*. Like the UID, the Entity ID may comprise, for example, a Bluetooth *BD_ADDR*, WiFi *BSSID*, or network card *MAC address*. Bucuk, [0090], [0100]-[0103] (describing values used for unique identifiers), [0259] (*BD_ADDR*, *BSSID*, and other identification codes used for Unique Entity IDs).

i) Claim 10

(1) “The server of claim 7 further comprising: a receiver, for receiving a user or entity identifier from a central server, the identifier taken from a pool of identifiers determined by the central server.”

206. *See* [7.A.I] (server includes a receiver) and claim 4 (second device receives an identifier, from a pool of identifiers, from a central server).

Additionally, Bucuk discloses that the second device includes “a long range radio

transmitter and receiver” (*a receiver*) for communicating in GSM, GPRS, or UMTS systems and for *receiving a user or entity identifier* from the server. Bucuk, [0333]; *see* discussion of claim 5.

207. To the extent Patent Owner argues that claim 10 requires “the server of claim 7” to receive a user or entity identifier from another different server—a *central server* that is not *the server*—a POSITA would have recognized the use of multiple servers to be an obvious variation of Bucuk-Nordman-Kallio. As discussed for claim 4, it would have been obvious to a POSITA to configure servers and server functions in one server or a plurality of servers—combining, separating, and/or distributing functions as desired. Thus, where Kallio teaches that the server is “present[ed]... with a bank of acceptable anonymity addresses” (Kallio, [0026]) but does not explain in further detail the origin of the bank of addresses (for example, generated locally or remotely), it would have been an obvious design choice to include a separate central server for generating addresses. For example, Kallio describes that, in some embodiments, different servers serve different terminals, requiring servers to share lists of assigned addresses to avoid duplicate assignments. Kallio, [0025]; *see also* Bucuk, [0325] (periodically changing UID and updating “all authentication servers”). Using a central server (*i.e.*, consolidating servers’ address generation functions) would have limited the risk of those double assignments and avoided the need for additional

communications for verification.

208. Accordingly, it would have been further obvious to modify Bucuk-Nordman-Kallio to use a central server to generate banks of keys for the server.

i) Claim 11

(1) “The server of claim 7 further comprising: an identity manager, to assign user or entity identifiers to devices by sending the same over a WWAN cellular data link, and wherein the user identifiers are changed over time.”

209. See claim 5.

i) Claim 12

(1) “The server of claim 11 wherein the user or entity identifiers are associated with a device identifier by the identity manager, and the device identifier is selected from one of: a media access control (MAC) addresses of a short range wireless network adapter; a SSID in an IEEE-802.11 network beacon; a BSSID of an IEEE802.11 network adapter; a IEEE802.15.1 Inquiry Response Message as a BD_ADDR associated with an inquiry response message; a device name in a Bluetooth name response packet; or one or more identifiers listed in a services list as provided in a LMP_features_req message or LMP_features_req_ext message for a Bluetooth device.”

210. See claim 6.

D. GROUND 4: BUCUK IN VIEW OF NORDMAN AND PERTTILA RENDERS OBVIOUS CLAIMS 14 AND 16

211. Bucuk and Nordman were introduced in Grounds 1 and 2 above.

212. 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.

213. Perttala is in the same field of wireless communications and reasonably pertinent to objectives of facilitating the exchange of information and validating commercial transactions. EX1001, 1:58-2:7; Perttala, Abstract, [0001], [0006]-[0008], [0016], [0026], [0042]-[0043]. As shown in Fig. 1a (below), a system 20 according to Perttala 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). Perttala, [0026], [0037].

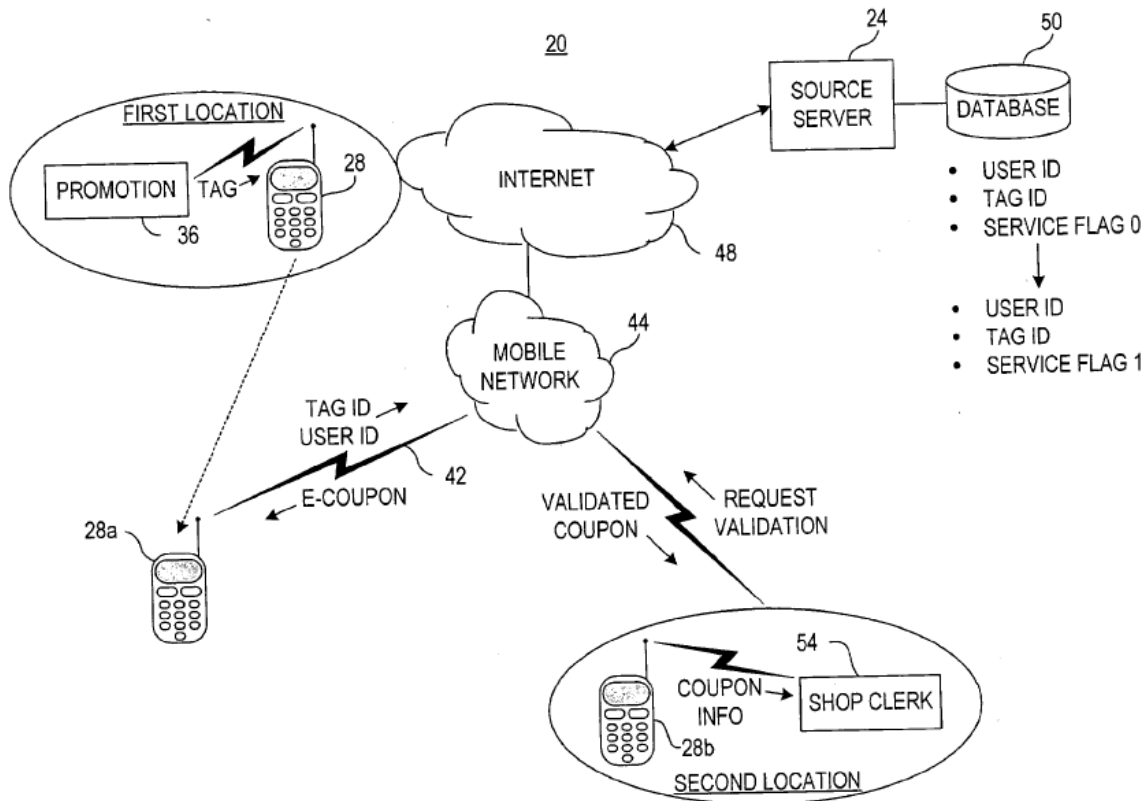


FIG. 1a

214. Bucuk explains that the authentication server may authorize a link/bond between the first and second devices and/or entities based on received UIDs, which includes the modified UID after the pre-determined event. Bucuk, [0188]; *see* [1.C], discussion of claim 17. An authorized link/bond is used, for example, to share data, trigger an event or action, execute code, perform a business process, verify an identity or authenticity of an entity, etc. Bucuk, [0191], [0330]. Applications of Bucuk's system of establishing relationships using identifiers and short-range communications are numerous, and a POSITA would have looked to known applications of short-range and long-range wireless systems, like Perttila's,

for implementation. Bucuk, Abstract, [0180].

215. 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 detects a Bluetooth beacon inside a store, notifies a server with its ID information and beacon information, and in return receives an electronic coupon for redemption. Perttila, [0011], [0028], [0031], [0037]-[0039]; EX1019, 13-14; EX1034, 6-7. The coupon may be a ticket to purchase or receive a "merchant offering," redeemed electronically by transferring and validating coupon information using ID information at the server. Perttila, [0005], [0031], [0041]-[0042], claims 17, 26. Through validation, used/expired coupons may be rejected, providing merchants control over offerings. Perttila, [0042]-[0043]; *see also* [0006] (describing coupons with time/location limitations).

216. A POSITA applying Bucuk's system for a "business process" (Bucuk, [0191], [0330]) would have been motivated to look towards known e-commerce solutions for implementation, and it would have been obvious to modify Bucuk-Nordman's server to alert devices (for example, the first device) of nearby offerings (for example, from the second device) with coupon data linked and redeemable with device IDs (for example, UIDs). Perttila's teachings advantageously "ensure that the user has rights" to offerings—permitting

merchants to control their offerings. Perttila, [0005]-[0015], [0043].

217. Moreover, the modification would have been no more than the application of a known technique (Perttila's proximity-based coupons) to a known device ready for improvement (Bucuk-Nordman's proximity-aware system that identifies nearby contacts and facilitates associations and links/bonds) to yield predictable results (controlling access to resources) with a reasonable expectation of success (techniques for transferring and analyzing data were within the skill of a POSITA).

a. The '749 Patent Claims

i) Claim 14

(1) "The method of claim 1 wherein the user or entity identification information is changed to provide for a confirmation of the identification information provided to the central server, or to provide a validation of the legitimacy of one or both of the first or the second wireless devices and respective applications."

218. Bucuk-Nordman-Perttila teaches that *the user or entity identification information is changed* (for example, the second device's initial UID to the modified UID) *to... provide a validation of the legitimacy of one or both of the first or the second wireless devices and respective applications* (for example, the authentication server uses the changing UIDs to validate the legitimacy of the first and second devices and their applications).

219. As discussed above, Bucuk-Nordman-Perttila teaches the server using

UIDs for coupon distribution and redemption. For example, a device (a terminal; for example, the first device) provides a server with its ID information (for example, the first device's UID) and merchant ID information (a merchant ID code from a "tag" or beacon; for example, the second device's modified UID) and receives coupon information in response. Perttila, [0037]-[0039]. To redeem the coupon at a later time, the first device provides information to the server, which attempts to validate the coupon by checking its database for device ID information (for example, the first device's UID) and merchant ID information ("tag" information; for example, the second Device's modified UID) to see if the coupon is valid. Perttila, [0041]-[0042].

220. Because the second device's identification information (UID) changes periodically, the server will therefore verify that the first device is in possession of, and attempting to redeem, a current and valid coupon. For example, Perttila teaches that ID codes identify coupon types, which are useful for identifying coupons with "expiration periods restrictions." Perttila, [0029]; *see also* Bucuk, [0161]-[0162], [0173] (validity of codes and IDs configured to expire). Thus, the second device may have had an initial UID associated with a coupon expiring in a first time period, and a modified UID associated with a coupon valid in a subsequent second time period. If the first device provides the second device's initial UID in the second time period (*i.e.*, after it expired), the server will not

validate the legitimacy of the first device (i.e., not a legitimate coupon holder). On the other hand, if the first device provides the second device's modified UID in the second time period (i.e., valid and not expired; after changing), the server will validate the legitimacy of the first device (i.e., as a legitimate coupon holder) and the legitimacy of the second device (i.e., as a distributor of legitimate unexpired coupons).

221. Additionally, because devices execute respective applications to perform functions in the system of Bucuk-Nordman-Kallio-Perttila (*see* [1.B.II]), the transmission, reception, and verification of data from those applications as being valid (for example, determined to have transmitted valid coupons) also *validates the legitimacy* of those *respective applications*. That is, the devices executing respective applications will only produce the right information (for example, UIDs) and communicate to the right devices and servers if they are executing legitimate applications for the communications system.

ii) Claim 16

(1) “The method of claim 7 wherein the user or entity identification information is changed to provide for a confirmation of the identification information provided to the central server, or to provide a validation of the legitimacy of one or both of the first or the second wireless devices and respective applications.”

222. I have been instructed to interpret this claim as being directed to the

“server of claim 7” instead of the “method of claim 7” because there is no “method of claim 7,” and this is likely a typographical error. Nevertheless, claim 16 is obvious for the same reasons discussed for claim 14 above.

IX. SECONDARY CONSIDERATIONS

223. The Challenged Claims of the '749 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.

224. I am not currently aware of any alleged objective indicia that Patent Owner has asserted specifically for the '749 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.

X. CONCLUSION

225. 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 '749 patent obvious.

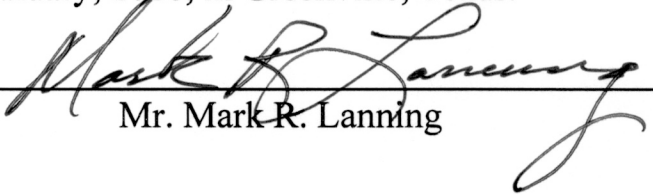
226. To the extent it is argued that any further disclosure is required for an element in the Challenged Claims that I have identified as being disclosed, a person of ordinary skill in the art would certainly have found that element obvious to include based on the sample explicit disclosure or inherent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

227. 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.

228. 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.

229. 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.

230. Executed this 8th day of January, 2026, in Greenville, Texas.


Mr. Mark R. Lanning