

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ABBOTT LABORATORIES and
ABBOTT DIABETES CARE INC.,
Petitioner,

v.

ALTIVERA, LLC,
Patent Owner.

IPR2024-00425
Patent 7,969,307 B2

**DECLARATION OF MAJID SARRAFZADEH
IN SUPPORT OF PETITIONER'S REPLY**

Table of Contents

I.	Introduction and Qualifications	2
II.	Summary Of Materials Reviewed And Considered	2
III.	Legal Understanding	6
IV.	Claim construction	6
V.	Ground 1: Claims 1, 2, 5, 9, and 10 are obvious over Bandy	11
A.	Dr. Bandy's contribution to cited portions of the Bandy reference was significant.	11
B.	Bandy renders obvious the "unique ID" of the remote wireless device.	13
C.	Bandy renders obvious the authentication limitation.	15
VI.	Ground 2: Claim 3 is obvious over Bandy in view of Heller	17
VII.	Ground 3: Claims 1-3, 5, 9, and 10 are obvious over Beck in view of Heller and Lovejoy	18
A.	A POSITA would have been motivated to combine Beck and Heller	18
B.	A POSITA would have been motivated to combine Beck and Lovejoy	21
C.	The combination renders obvious a "unique identification ID number"	26
D.	The combination renders obvious a wireless device having a unique ID	28
E.	The combination renders obvious the authentication limitation	29
F.	The combination renders obvious geolocation means	32
G.	The combination renders obvious a "sensor interface having an analog to digital converter."	33
VIII.	CONCLUSION	35

I. Introduction and Qualifications

1. I have been retained by Abbott Laboratories and Abbott Diabetes Care Inc. (“Petitioner”) in the above-captioned *inter partes* review (“IPR”) concerning the validity of claims 1-3, 5, 9, and 10 of U.S. Patent No. 7,969,307 (“the ’307 patent”) (Ex. 1001).

2. I previously provided a declaration dated January 15, 2024, with my opinions related to the level of skill of ordinary artisans, the state of the art described in the ’307 patent at the time of the effective filing date, and the disclosure of the prior art relative to the claims of the ’307 patent. I understand that my original declaration was submitted as Exhibit 1003. I hereby incorporate Exhibit 1003 into this declaration by reference.

3. My experience and qualifications are set forth in Exhibit 1003 and in my curriculum vitae, which I understand was submitted as Exhibit 1004.

4. I have been asked to provide additional expert opinions regarding these matters in response to certain arguments in the Patent Owner Response and certain opinions of Patent Owner’s witness, Dr. Steven Warren.

II. Summary Of Materials Reviewed And Considered

5. All of the opinions contained in this Declaration are based on the documents I reviewed and my knowledge and professional judgment. In forming

the opinions expressed in this Declaration, while drawing on my experience in the field of wireless power transfer, I reviewed the following documents:

Ex. No.	Description
Paper 10	Institution Decision
Paper 17	Patent Owner's Response to Petition
1001	U.S. Patent No. 7,969,307 B2 ("307 patent")
1002	File History of U.S. Patent No. 7,969,307 B2 ("307 FH")
1005	U.S. Patent No. 7,148,803 B2 ("Bandy")
1006	U.S. Utility Patent Application Transmittal for U.S. Patent No. 7,148,803 B2 ("As-Filed Bandy Application")
1007	U.S. Patent Application Publication No. US 2002/0178126 A1 ("Beck")
1009	U.S. Patent No. 6,031,454 ("Lovejoy")
1015	U.S. Patent No. 6,987,965 B2 ("Ng")
1016	World Intellectual Property Organization, International Publication No. WO 02/058537 A2 ("Heller")
1017	Third Report & Order, <i>In re Revision of the Comm'n's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Sys.</i> , CC Docket No. 94-102, 14 FCC Rcd. 17388, 1999 WL 795989 (FCC adopted Sept. 15, 1999; released Oct. 6, 1999), http://standards.tiaonline.org/gov_affairs/fcc_filings/documents/e911rando.pdf ("FCC Report")
1018	U.S. Patent No. 6,002,344 ("Bandy-344")
1019	U.S. Patent No. 7,797,367 B1 ("Gelvin")
1020	U.S. Patent No. 6,416,471 B1 ("Kumar")

Ex. No.	Description
1021	U.S. Patent No. 6,978,182 B2 (“Mazar”)
1022	U.S. Patent No. 6,720,887 B1 (“Zunti”)
1023	U.S. Patent Application Publication No. 2003/0229723 A1 (“Kangas”)
1024	U.S. Patent Application Publication No. 2002/0165443 A1 (“Mori”)
1026	NEWTON’S TELECOM DICTIONARY (18th ed. 2002) (excerpted)
1027	U.S. Patent No. 7,446,646 B2 (“Huomo”)
1028	U.S. Patent No. 6,989,750 B2 (“Shanks”)
1029	U.S. Patent No. 7,844,505 B1 (“’505 patent”)
1030	Transcript of the Deposition of William Bandy, Ph.D., taken December 18, 2024 (“Bandy Dep.”)
1031	Transcript of the Deposition of Steven Warren, Ph.D., taken December 19, 2024 (“Warren Dep.”)
1032	Transcript of the Deposition of John P. Peeters, Ph.D., taken January 8, 2025 (“Peeters Dep.”)
2001	Declaration of William Bandy, Ph.D.
2002	Declaration of John P. Peeters, Ph.D.
2006	Aug. 19, 2003 email from John Peeters
2008	Nokia 1100 User Guide
2009	Declaration of Steven Warren, Ph.D.
2010	Curriculum Vitae of Steven Warren, Ph.D.
2011	Transcript of the Deposition of Majid Sarrafzadeh, Ph.D.
2012	Nokia 1100 full phone specifications (https://www.gsmarena.com/nokia_1100-512.php)

Ex. No.	Description
2013	Robert Triggs, A little history of Bluetooth, dated Sept. 1, 2023 (https://www.androidauthority.com/history-bluetooth-explained-846345/)
2014	Len Ott, The Evolution of Bluetooth In Wireless Medical Devices, Socket Mobile (July 2010)
2015	Wikipedia, Near-Field Communication
2016	Nathan Lawrentschuk & Damien M. Bolton, SYSTEMATIC REVIEW, Mobile phone interference with medical equipment and its clinical relevance: a systematic review, Vol. 181, No. 3 (Aug. 2004)
2017	A.A. Klein & G. N. Djaiani, JAPI, Mobile Phones in the hospital – past, present and future, Anesthesia (2003)
2018	ME YEOLEKAR & A SHARMA, Use of Mobile Phones in ICU – Why Not Ban?, Vol. 51 (Apr. 2004)
2019	Hiroshi Furuhata, JIKEI UNIV. SCHOOL OF MEDICINE TOKYO, JP, Electromagnetic Interferences of Electric Medical Equipment from hand-held radiocommunication Equipment
2020	P Gilligan, et al., THE BRITISH JOURNAL OF RADIOLOGY, GSM cellphones can interfere with ionizing radiation dose monitoring equipment (2000)
2021	Werner E. Irnich & Rolf Tobisch, Mobile Phones in Hospitals
2022	Greg Knell, SureCall Cell Phone Signal Booster Blog (Feb. 2022), https://surecall.com/surecall-cell-phone-signal-boosterblog/cellular-phone-frequency-bands-guide-2022/

6. My opinions are additionally guided by my appreciation of how a person of ordinary skill in the art would have understood the claims of the '307

patent at the time of the alleged invention, which I have been asked to assume is January 27, 2004.

III. Legal Understanding

7. I am not an attorney. However, I have been informed by counsel of certain legal standards and have applied those standards, described in Exhibit 1003, in formulating my opinions.

IV. Claim construction

8. Dr. Warren asserts that the phrase “the remote server authenticates said unique sensor ID associated with said unique wireless device ID” in claim 1 means “the remote server authenticates the unique sensor ID *and* the associated unique wireless device ID.” Warren Decl., ¶ 54. I disagree.

9. The plain language of this phrase does not require authentication of the wireless device ID, but only authentication of the unique sensor ID, which is associated with the wireless device ID. Dr. Warren agrees. Warren Decl., ¶ 55.

10. Nothing in the claims, the specification, or the prosecution history requires authenticating the wireless device ID in claim 1. Dr. Warren does not cite to anything in the specification to support his interpretation of the claim. Warren Decl., ¶¶ 54-60.

11. In fact, claim 18 of the '307 patent would have informed a POSITA's understanding that claim 1 does *not* require authentication of the

wireless device ID. Specifically, claim 18 (unlike claim 1) explicitly requires authentication of both IDs by saying just that: “wherein the remote server authenticates remotely said unique sensor tag ID *and* said unique wireless device ID.” ’307 patent, 21:8-9. Thus, claim 18 reinforces to a POSITA that if the inventor intended to require authentication of the wireless device ID, he would have said so explicitly. Claim 1 does not require such authentication.

12. Aside from the claims, the specification of the ’307 patent does not discuss or mention a wireless device ID, let alone associating such an ID with a sensor ID, or authenticating such an ID. The discussion of unique IDs in the ’307 patent’s specification focus on unique IDs on the RFID tag. *See* ’307 patent 7:43-47 (“Since the RFID tag provides a unique ID to the wireless device this ID identifies uniquely the type of sensor used.”); 16:50-56 (“a patient can either download data to computer 400 or upload into the cell phone the necessary information to conduct any given test by matching the ID of the RFID sensor with given software and data tables stored remotely on computer 400 via link 392”); 18:20-23 (“the ID of the RFID sensor is matched to a given class of sensor (e.g. a glucose sensor) and the software and/or instructions for the analyses are downloaded into the reader 2 as shown in function 738”).

13. Dr. Warren asserts that the association of IDs recited in claim 1 requires that the wireless device ID be authenticated by the remote server.

Warren Decl., ¶¶ 56-57. I disagree. For example, although Dr. Warren asserts that “the unique sensor ID could not be authenticated... without reference to the unique wireless device ID,” the only possible authentication in the '307 patent (i.e., matching the ID of the RFID sensor to a given class of sensor in column 18) performs the matching without reference to the wireless device ID. This is shown in Figure 22, reproduced below, where the “ID Match” (730) that enables downloading software (738) only relates to the Tag's ID (700, 708). *See* '307 patent 18:20-24.

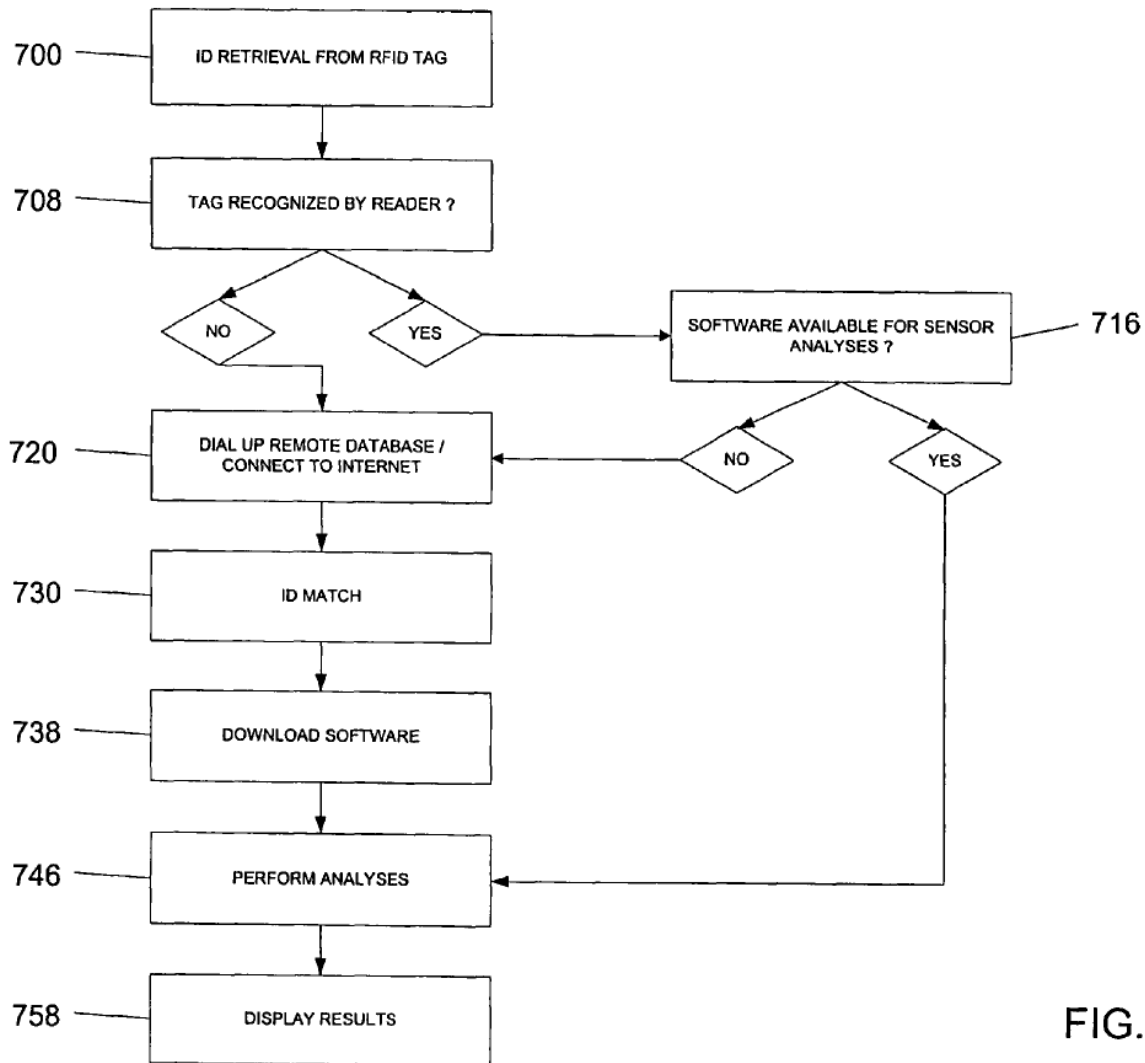


FIG. 22

14. The phrase “associated” has no special technical meaning in this context—it does not require authentication or anything beyond conventional association (e.g., relation or connection). *See* ’307 patent 12:33-36 (discussing biomarkers “associated with a given condition”), 14:44-47 (discussing “smells associated with the aging or degradation of [] cheese”), 17:30-33 (discussing “storage of RFID tables and associated software”).

15. Dr. Warren also states that authenticating the wireless device ID is necessary for security and privacy of the system. Warren Decl., ¶¶ 57-58. I disagree because (1) the claim does not recite security or privacy, and (2) security and privacy can be accomplished in other ways. For example, unlike the '307 patent, Beck explicitly discloses a concern for protecting patient data, and allows for authentication based not only on wireless device ID (i.e., "client computing device network address") and sensor ID ("medical device serial number") but also based on "username/password." Beck [0051].

16. Additionally, the prosecution history does not support Dr. Warren's interpretation, either. Dr. Warren states that this passage "supports the requirement that both the sensor ID and the wireless device ID are transmitted to the remote server." Warren Decl., ¶ 59 (citing Exhibit 1002 at 65). Based on this, he concludes that "both the Applicant and Examiner clearly understood that [the authentication limitation]... meant that the wireless device was transmitting both" IDs "to the remote server." Warren Decl., ¶ 59. However, as I noted during my deposition, the cited passage does not mention authentication (Ex. 2011 59:21-60:5), and Dr. Warren does not appear to assert that the passage requires authentication of the wireless device ID, but instead mere transmission to the remote server.

V. Ground 1: Claims 1, 2, 5, 9, and 10 are obvious over Bandy

17. In my first declaration, I showed that Bandy renders claims 1-2, 5, 9, and 10 obvious. Ex. 1003 ¶¶ 120-218. Below, I address different issues raised by Dr. Warren and/or Patent Owner.

A. Dr. Bandy's contribution to cited portions of the Bandy reference was significant.

18. As part of my original analysis, I was informed and understood that Bandy is prior art to the '307 patent. Ex. 1003 ¶ 99.

19. I further understand that, after my first declaration was filed in this case, the named inventors of Bandy (William R. Bandy and John P. Peeters) submitted declarations relating to inventorship of the Bandy reference. *See* Ex. 2001 (Bandy Declaration) and Ex. 2002 (Peeters Declaration). I have also reviewed the deposition transcripts of Dr. Bandy (Ex. 1030) and Dr. Peeters (Ex. 1032).

20. Drs. Bandy and Peeters agree that Dr. Bandy contributed at least an interrogation protocol. Ex. 1030 21:13-15 ("The other important technology I was involved in developing was our interrogation protocol."), 85:8-86:2 ("That is our contribution" in relation to the binary tree traversal protocol"); 24:13-25:11 (contributed interrogation protocol includes "tree-walking" algorithm); Ex. 1032 45:12-20 (the binary tree traversal protocol was "one of the Bandy contributions, yes"). Dr. Bandy explained that his contributions included "interrogating the one

or more RF addressable sensors to isolate an individual RF addressable sensor.”

See Ex.1030 77:22-78:7; *see also* Ex.1030 86:21-88:18 (Bandy column 5 disclosures relate to Dr. Bandy’s contributions).

21. In my declaration, I cited Bandy’s disclosures relating to interrogation, including in paragraphs 103 (citing Bandy 5:1-5, 5:19-22, 5:6-9), 169 (citing Bandy 5:6-9, 5:19-23), 190 (citing Bandy 16:41-42, 16:47-51), and 191 (citing Bandy 13:1-3). I also annotated Figure 7A, highlighting step 780 (“Communicate Sensor Data”). Ex. 1003 ¶ 190.

22. It is my opinion, based on my review of the Bandy reference, and the testimony from Drs. Bandy and Peeters, that Dr. Bandy’s contribution to the cited passages relating to interrogation was significant when measured against the full disclosure of Bandy. For example, Dr. Bandy described the interrogation protocol as an “important technology.” Ex. 1030 21:13-15. Dr. Bandy describes that the state of the art could interrogate “a few tags per second” but that with his contribution “we increased that to 1,000 tags per second.” Ex. 1030 21:19-22:2. The binary tree traversal protocol appears to be the only interrogation protocol disclosed in Bandy, including in relation to step 780 of Figure 7A. Bandy 16:41-51 (“The details of this communication are dependent upon the protocol.... In an embodiment..., the protocol used is a binary tree traversal protocol.”). Interrogation forms a specific step recited in claims 65, 81, and 83 of the Bandy

reference, which both inventors stated Dr. Bandy contributed to. Ex. 2001 ¶ 8; Ex. 2002 ¶ 18; Ex. 1030 72:21-74:2 (identifying the interrogation limitation of claim 81, including isolating a sensor, as his contribution), 77:22-78:19 (confirming his contribution related to the first two steps of claim 65); Ex. 1032 45:12-46:3 (Dr. Bandy's protocol "is specifically to isolate a tag..."). Dr. Peeters did not seem to have contributed to interrogation beyond his assertion that he possessed background knowledge. Ex. 1032 51:65-52:1 ("Q. So the only portion of claim 65 that Dr. Bandy contributed to was the isolation portion of step B and nothing else? A. ...I don't recall 22 years ago exactly we sat down and wrote this thing together....").

B. Bandy renders obvious the "unique ID" of the remote wireless device.

23. In my first declaration I showed that Bandy renders obvious the "unique ID" of the remote wireless device. Ex. 1003 ¶¶ 184-185.

24. I have reviewed Exhibit 2006 (August 19, 2003 email from John Peeters) and in my opinion it supports that a unique ID of a wireless device would have been obvious to a POSITA. Specifically, the "Patent Outline" shows that such a "Unique ID" was simply one of several "Technologies provided by a cell phone," alongside "Geolocation," "Two way communication," "Access to the Internet," "Battery/power," and "Microprocessing and programming capabilities." Ex. 2006 at 2. Additionally, Dr. Warren's testimony that a wireless

device having a unique ID was inherent to the specification of the '307 patent further supports that it would have been known and obvious to a POSITA based on Bandy. Ex. 1031 30:21-32:1 (“International RFID and tag standards would inherently incorporate unique IDs in such readers, and in such tags.”). For example, as I pointed out in my first declaration, Bandy’s server is able to provide the correct software for the correct sensor to the correct wireless reader. Ex. 1003 ¶¶ 195-196. Under Dr. Warren’s logic, Bandy therefore must include a wireless device ID (that is associated with the sensor ID). *Cf.* Ex. 2009 ¶ 95. To the extent Dr. Warren intended to assert that I did not identify an association of IDs, I disagree. *Cf.* Ex. 2009 ¶ 95. As I discuss below in Paragraph 51, the claimed association refers to, or at least encompasses, the association made by the claim, which occurs when the wireless device (having a unique ID) obtains the ID via the sensor interface. I showed that this occurs in my first declaration. Ex. 1003 ¶¶ 190-191. And the same unique ID associated with this ID is authenticated in Bandy’s system. Ex. 1003 ¶¶ 195-196. The remote server then communicates *to the wireless device* processed information relating to said sensor data and software *related to the unique sensor ID*. Ex. 1003 ¶ 197; *see also* ¶ 200 (“software related to the unique sensor ID necessary for the wireless device to interpret the sensor anywhere worldwide”). The '307 patent does not explicitly disclose a wireless device ID, let alone authenticating a wireless device ID. Dr.

Warren asserted that these disclosures are inherent and necessary in the '307 patent. Ex. 1031 49:17-51:18. Under Dr. Warren's logic, because Bandy's system provides the correct software related to the unique sensor ID to the wireless reader, the association is also necessary in Bandy.

25. Additionally, Dr. Peeters's testimony that unique IDs in wireless devices was "completely standard" at the time of the Bandy reference further supports that a unique ID would have been obvious to a POSITA based on Bandy. Ex.1032 73:22-75:15 ("a unique ID is now found almost anywhere in any chip that is made but specifically in wireless communication technologies.... [an] everyday example of this is cell phones and wireless communication.").

C. Bandy renders obvious the authentication limitation.

26. In my first declaration I discussed how Bandy renders obvious "wherein the remote server authenticates said unique sensor ID associated with said unique wireless device ID and communicates to said wireless device processed information relating to said sensor data and software related to the unique sensor ID, thereby allowing said wireless device to interpret said sensor anywhere worldwide." Ex. 1003 ¶¶ 194-201. For example, the sensor "identifies itself (e.g., by providing its identification number)" to the cell phone reader. Ex. 1003 ¶ 195. When the necessary processing and analysis information is downloaded to the cell phone from a remote location, "only the ID of the RFID-

sensor is necessary.” Ex. 1003 ¶ 196 (quoting Bandy at 10:37-41). I observed that this passage of Bandy confirms that the unique ID of the RFID sensor is used to identify and download the software and other information needed to process the sensor data. Ex. 1003 ¶ 196. Thus, Bandy’s system authenticates the unique sensor ID (tag identification number) associated with the unique wireless device ID (i.e., the tag identification number obtained by the cell phone reader possessing the wireless device ID).

27. Dr. Warren asserts that these passages of Bandy “relate only to what is communicated from the server” and not “sending anything to the server.” Ex. 2009 ¶ 99. I disagree. Bandy discloses that the sensor “provides the cell phone reader with the necessary information for analyzing the sensor output.” Bandy 10:19-24. In some cases, this means that the sensor provides sensor handling information and a testing protocol to the reader. Bandy 10:19-29. “Software may also be downloaded directly and transparently into the cell phone or reader.” Bandy 10:33-35. In the event that “necessary processing and analysis information is downloaded from a remote location, only the ID of the RFID-sensor is necessary, providing a highly streamlined solution for universal sensor analyses for wireless devices such as cell phones.” 10:37-41. In the context of column 10, it would have been clear to a POSITA that Bandy discloses that the ID of the RFID-sensor is used by the cell phone to obtain the necessary processing and

analysis information from the remote location, and thus sent to the remote location to obtain the relevant information.

VI. Ground 2: Claim 3 is obvious over Bandy in view of Heller

28. In my first declaration I expressed my opinion that claim 3 of the '307 patent is obvious over Bandy in view of Heller. Ex. 1003 ¶¶ 219-223. As part of that analysis, I discussed Bandy's disclosure of a smart card or badge 1103 "is affixed to a person (or animal) such that the sensor elements of the RF addressable sensor are proximate to the surface of the skin." Ex. 1003 ¶ 220 (quoting Bandy 20:4-9). I explained that for such affixing, a POSITA would have understood that the sensor elements would be integrated with some sort of adhesive material, and that such details are disclosed in Heller. Ex. 1003 ¶¶ 221-222. I observed that Heller provides "a variety of methods for affixing its on-skin sensor control unit to a patient's skin" including "adhesive patch." Ex. 1003 ¶ 222 (quoting Heller 54:29-32). I showed that a POSITA would have been motivated to apply Heller's approach to Bandy "as doing so would have been nothing more than applying a known technique to a known device ready for improvement to yield predictable results." Ex. 1003 ¶ 223.

29. Dr. Warren asserts that "Petitioner fails to demonstrate that a POSITA would have been motivated to use Heller's implantable sensors in Bandy's unrelated system directed to external cards or badges." Ex. 2009 ¶ 103. I

disagree that Bandy's system is "unrelated" or the implication that "external cards or badges" prevents or teaches away from combination with Heller's adhesive patch. For example, Bandy discloses that its "RF addressable sensor 1110 may include low power sensors to monitor certain conditions or characteristics such as the *individual's vital functions*." Bandy 20:6-9. Bandy even explicitly contemplates "medical institution application[s]" where a patient's vital function data would be collected. Bandy 20:16-21. Heller's solutions for affixing sensors (which collect patient vital function data) to the skin of patients is perfectly compatible with Bandy, which expresses the goal of affixing sensors to a body to collect vital function data.

VII. Ground 3: Claims 1-3, 5, 9, and 10 are obvious over Beck in view of Heller and Lovejoy

30. In my first declaration, I showed that Beck in view of Heller and Lovejoy renders claims 1-3, 5, 9, and 10 obvious. Ex. 1003 ¶¶ 224-357. Below, I address different issues raised by Dr. Warren and/or Patent Owner.

A. A POSITA would have been motivated to combine Beck and Heller

31. In my first declaration I addressed why a POSITA would have been motivated to combine Beck and Heller. Ex. 1003 ¶¶ 225-238. I discussed that Beck and Heller both relate to glucose meters, and Heller provides technical details relating to such systems as well as techniques for improving sensor

devices. Ex. 1003 ¶¶ 225, 228-231. I opined that a POSITA would have been motivated to modify Beck to add a temperature probe/sensor as disclosed in Heller to improve accuracy of sensor readings as temperature changed. Ex. 1003 ¶ 233. I also opined that a POSITA would have recognized Heller's disclosure of implementing test device electrodes on a substrate was a known way to implement or improve Beck's medical device that measures blood glucose or other analytes. Ex. 1003 ¶ 234. I also opined that a POSITA would have been motivated and/or found it obvious to integrate Heller's adhesive patch into Beck's medical device so as to attach it to the skin of a person. Ex. 1003 ¶ 234.

32. Dr. Warren asserts that "[t]he medical devices of Beck are... large and bulky—far from disposable wireless skin patches." Ex. 2009 ¶ 105. He asserts that "Petitioner's suggestion that it would have been obvious to a POSITA to transition from Beck's collection of bulky, stand-alone medical devices to a disposable patch is nonsensical." Ex. 2009 ¶ 105. Dr. Warren seems to ignore Beck's disclosures of using radio frequencies and a cellular phone to communicate with the medical device, describing Beck's client computing device as "a computer-based host that incorporates standard operating-system support and built-in network communication interfaces" that would use, e.g., a wired serial cable for communication. Ex. 2009 ¶¶ 109, 106-107.

33. Dr. Warren states that “a POSITA would have considered Heller’s system antithetical to—not compatible with—Beck’s system.” Ex. 2009 ¶ 112. I disagree. For the reasons I discussed in my first declaration, which Dr. Warren does not directly address, the references not only do not teach away from each other, but motivate integrating Heller’s adhesive patch into Beck’s medical device (e.g., glucose meter) so as to attach it to the skin of a person. Ex. 1003 ¶ 234. Heller’s discussion of “large, bulky, and/or inflexible” devices relates to “devices [that] use electrochemical sensors which are directly implanted into a blood vessel or in the subcutaneous tissue of a patient,” and Heller specifically motivates its own solution to such devices. Heller 1:30-2:6. Thus, Heller further motivates its application to Beck with disclosure of “a small, compact device that can operate the sensor and provide signals to an analyzer without substantially restricting the movements and activities of a patient.” Heller 2:13-15; *see also* 2:19-21.

34. Dr. Warren also asserts that “the proposed combination of Beck and Heller necessarily involves a connection to a bulky device in a hospital setting.” Ex. 2009 ¶ 111. I disagree. Beck is not limited to hospital settings, but discloses that a “user” of a client computing device can be “a patient.” Beck [0052]. *See also* Beck [0002] (“*Patients* commonly use medical devices to monitor various biological and/or physiological conditions.”). Nothing in Beck limits the

disclosure to a hospital or other controlled medical facility. *See* Ex.1031 68:22-69:4

35. Dr. Warren also asserts that “[t]he entire purpose of Heller was to provide a system that could be ‘used effectively outside of a controlled medical facility.’” Ex. 2009 ¶ 111. But Heller’s disclosure can be used in controlled medical facilities, too. Ex. 1031 68:4-10. Both references can be used within or external to a controlled medical facility.

36. Patent Owner asserts that “Beck does not disclose that a client computing device...is mobile.” POR at 43. I disagree. Beck discloses that a client computing device can be an “Internet enabled cellular phone[.]” Beck [0027]. A POSITA would have understood that such devices were mobile, even in the early 2000s. Dr. Warren agrees. Ex. 1031 65:5-66:13.

B. A POSITA would have been motivated to combine Beck and Lovejoy

37. In my first declaration I addressed why a POSITA would have been motivated to combine Beck and Lovejoy. Ex. 1003 ¶¶ 239-247. For example, I explained that Beck’s disclosure of a portable handheld computing device such as a cellular phone intended for use in monitoring various biological/physiological parameters and conditions of patients motivates including geolocation in Beck’s system, e.g., in the cellular phone as client computing device. Ex. 1003 ¶¶ 240-242. I also explained that Lovejoy discloses known implementation techniques

for implementing geolocation functionality including GPS and non-GPS geolocation features in mobile devices for effective intervention in dangerous events. Ex. 1003 ¶ 245. I also explained that cellular phones before 2003 commonly included geolocation features and noted that in 1999 the FCC had already begun a concerted effort to require cell phone carriers to outfit cell phones with automated location identification through GPS or non-GPS geolocation features. Ex. 1003 ¶ 246. As such, inclusion of such features on a phone in 2003 would have been nothing more than implementation of features normally found on conventional phones at the time. Ex. 1003 ¶ 246.

38. After I submitted my declaration, Patent Owner submitted Exhibit 2006, which bears a date of August 19, 2003, and describes “geolocation” as a “Technolog[y] provided by a cell phone.” Ex. 2006 at 2. I agree. Additionally, Dr. Peeters testified that he was not the first person to conceive of geolocation in cell phones and that “the geolocation part was inherited from the earlier work that was done with Mike [Lovejoy] in the six years before.” Ex. 1032 83:15-20. According to Dr. Peeters, “at the time of the finding these were standard things that were available out there that we referenced because we knew that geolocation was very important.” Ex. 1032 83:15-24. Both GPS and non-GPS technologies (e.g., “time of flight”) were “completely standard” and “well known in the art.” Ex. 1032 84:5-9. I agree, and Dr. Peeters’s testimony is consistent

with what a POSITA would have understood by January 2004 when the '307 patent was filed.

39. Patent Owner asserts that Beck only discloses cell phones “in the context of *connecting a cell phone to a client computing device*.” POR 43. I disagree. Beck explicitly discloses that the client computing device can be implemented as a cellular phone or handheld mobile device. Beck [0027], [0049]. Additionally, Dr. Warren’s assertion that Beck’s client computing device is not mobile is inconsistent with Beck’s explicit disclosure of a portable handheld device or cellular phone, which Dr. Warren agrees is mobile. Ex. 1003 ¶ 124; Ex. 1031, 65:5-66:13 (“Beck discloses that the client-computing device can be implemented with a cellular phone, which describes the idea that the care provider in this case might be mobile....”).

40. Dr. Warren’s discussion of the FCC Report misses the point, and does not seem to address the knowledge of a POSITA as evidenced by the Report (and admitted by, e.g., Dr. Peeters). See Ex. 2009 ¶¶ 138-142.

41. Dr. Warren asserts that I could not, in deposition, “distinguish between network-based geolocation and handset-based geolocation” and that such “distinction is key.” Ex. 2009 ¶ 139. I disagree on both points. First, I was asked the difference between network-based and handset-based geolocation solutions without context. Ex. 2011 65:9-18 (“Q. Without looking at your

report....”). I responded by noting that these terms are used differently in different contexts, and stated: “Generally speaking, anything that is network-based, you do it based on the network. If you are doing it with a handset, like a cell phone, you do it with a handset phone, such as a cell phone.” Ex. 2011 65:20-25. Notably, although Dr. Warren states the “distinction is key” (Ex. 2009 ¶ 139), the only distinction he seems to assert is the timelines of the two geolocation technologies. Ex. 2009 ¶¶ 140-141. As I noted in my first declaration, Phase II rules were initially adopted in 1996, when it was believed that “location information could only effectively provided by technologies based in or overlaid on carrier networks, using approaches such as triangulation of the handset’s signal.” Ex. 1003 ¶ 96 (quoting Ex. 1017 at 4). This describes non-GPS geolocation, including network-based geolocation. However, after 1996, “advancements in location technologies that employ new or upgraded handsets have demonstrated important progress.” Ex. 1003 ¶ 96 (quoting Ex. 1017 at 4). I also cited various pages “requiring carriers to begin selling location-capable handsets no later than March 1, 2001, and provide network-based location (triangulation) coverage by October 1, 2001.” Ex. 1003 ¶ 96; *see also id.* pp. 80-81 (footnote 3), p. 96 (footnote 4), p. 98 (footnote 5), ¶ 246 (citing Ex. 1017 at 48-50). Similar deadlines apply to “Wireless carriers who employ a Phase II location technology that requires new, modified or upgraded handsets (such as

Global Positioning System (GPS)-based technologies.” FCC at 006. I further identified Lovejoy’s disclosure of “Time-of-arrival with a triangulation algorithm” as an example “non-GPS radar-responsive tag geolocation.” Ex. 1003 ¶¶ 118, 245-246, 314-315, 356. Dr. Warren’s citation to “December 31, 2004” (Ex. 2009 ¶ 141) relates to the FCC Report’s requirement of “achiev[ing] **100 percent penetration** of ALI-capable handsets in its total subscriber base” and further demonstrates that a POSITA would have found it obvious to incorporate GPS and/or non-GPS geolocation into a cellular phone. Ex. 1017 at 006. Thus, although network-based and handset-based geolocation technologies had different timelines, the FCC Report is evidence that geolocation in a cell phone was well-known and obvious to a POSITA by January 2004.

42. Dr. Warren asserts that “the FCC Report does not teach ‘geolocation’ as taught in the ’307 Patent.” Ex. 2009 ¶ 142. I disagree. As an initial matter, nothing in the ’307 patent requires any specific precision for geolocation, let alone greater precision than what was already commercially available or required by the FCC. Further, Dr. Warren’s support for his assertion of imprecision seems to relate to situations where either no geolocation is implemented or a Phase I implementation where only “cell site or cell sector information” is provided. *Id.* (quoting Ex. 1017 at 2-3); *see id.* (“technology available to the public... could provide information regarding the general area of

a target (e.g., the zip code)...”). In other words, Dr. Warren’s assertions ignore disclosure of the FCC Report of implementing GPS and triangulation-based methods. Where he does address the revised precision standard, he simply concludes that they are not “precise geolocation.” Ex. 2009 ¶ 142. I disagree—there is no precision requirement in the ’307 patent, and the use of GPS and non-GPS geolocation would have been obvious to include in cell phones by 2004.

C. The combination renders obvious a “unique identification ID number”

43. In my first declaration I discussed that the Ground 3 combination renders obvious a “unique identification ID number” as recited in claim 1. Ex. 1003 ¶¶ 269-270. For example, Beck discloses that the client computing device 120 “identif[ies] the medical device without the need for the user to enter identifying information for the medical device” including through “identification codes” and “serial numbers” retrieved from the medical device. Ex. 1003 ¶ 270 (quoting Beck [0055]).

44. Dr. Warren asserts that “Beck discloses, at most, identification numbers for the entire medical device” and “merely identif[ying] a *type* of sensor, or the *medical device* used with that sensor... is insufficient to meet the claim limitation.” Ex. 2009 ¶ 145. According to Dr. Warren’s declaration, Beck’s serial numbers and identification codes are “for the medical device” and “not a sensor unit as required by the claim.” Ex. 2009 ¶ 145. I disagree. First, the claim

does not require that the “unique identification ID number” identifies any specific component, and Dr. Warren agreed in his deposition. When asked what the unique identification ID number identifies, Dr. Warren could only say that the sensor unit comprises the ID “which means it incorporates that number in some way.” Ex. 1031 55:8-56:3. He further stated that it would be “inconsistent...with the claim language” to require the unique identification ID number to identify the sensor unit because the claim only requires the sensor unit to incorporate such a number. Ex. 1031 56:5-14. I generally agree with this portion of Dr. Warren’s deposition, and in my opinion it undercuts his argument that Beck’s identification codes are distinguishable from the claim because they don’t identify the “sensor unit as required by the claim.” Ex. 2009 ¶ 145. Additionally, I showed in my first declaration that Beck’s medical device constitutes the claimed “sensor unit.” Ex. 1003 ¶ 251. Thus, identifying the medical device constitutes identifying the sensor unit recited in the preamble.

45. Further, by identifying the medical device, Beck’s unique ID identifies every component of the device. For example, an ID identifying a glucose meter also identifies sensors of the device as glucose sensors. *See* Ex. 1031 61:22-62:2 (“Q. You agree that lots of medical devices incorporate sensors? A. Yes, of course.”). This allows the system to determine the “type” of device, sensor unit, and sensors that are collecting and providing patient data. Beck’s

disclosure and use of the serial numbers/identification codes matches that of the '307 patent's sensor ID. In Beck, the unique IDs are used for authentication and to download software. Beck [0065], [0067]. This information tells the server about the "type of medical device," enabling the server to provide the correct "protocol component" (software) "to be used with the identified medical device." Beck [0069]; [0070]-[0072]. Likewise, in the '307 patent, the sensor ID "uniquely identifies the *type* of sensor used," which is then used by a remote server to provide software associated with that type. Ex.1001 7:43-45; *see id.* 18:18-23 (remote server matches "the ID of the RFID sensor... to a given *class of sensor* (e.g. a *glucose sensor*) and the software and/or instructions for the analyses are downloaded into the reader.").

D. The combination renders obvious a wireless device having a unique ID

46. In my first declaration I described that the combination renders obvious a wireless device having a unique ID. Ex. 1003 ¶¶ 317-319. For example, I noted that "Beck discloses that server 110 authenticates client computing device 120 based on 'the network address of the client computing device.'" Ex. 1003 ¶ 318 (quoting Beck [0065]). At least because of such use in authentication, the network address is a unique ID. Ex. 1003 ¶ 318.

47. Dr. Warren asserts that Beck "does not refer to any particular type of network address" and that "some network addresses might be unique, but others,

such as internal IP addresses... may not be unique.” Ex. 2009 ¶ 149. He does not dispute that its use by a server for authentication implies that it is unique. Nor does Dr. Warren cite anything in Beck that would suggest the network address is not unique. The existence of “internal IP addresses” is not relevant to Beck’s disclosure, which uses “the Internet to provide ubiquitous access” for server communication. Beck [0043]. Additionally, Patent Owner’s Exhibit 2006 includes a “Patent Outline” from 2003 that lists “Unique ID” as part of “Technologies provided by a cell phone.” Ex.2006 2. I agree that a unique ID was a standard feature provided by a cell phone before 2004.

48. Finally, to the extent Dr. Warren’s discussion of internal IP addresses identifying devices on a private network implies that the claim requires the ID to be a globally unique identifier, I disagree. For example, even on a private network, each device would have a unique IP address in the context of that network. Nevertheless, Beck is not limited to private networks as discussed above.

E. The combination renders obvious the authentication limitation

49. In my first declaration I discussed how the combination renders obvious “wherein the remote server authenticates said unique sensor ID associated with said unique wireless device ID and communicates to said wireless device processed information relating to said sensor data and software

related to the unique sensor ID, thereby allowing said wireless device to interpret said sensor anywhere worldwide.” Ex. 1003 ¶¶ 325-332. For example, I noted that “Beck teaches that ‘the server computing device 110 attempts to authenticate the user, the client computing device 120, and/or the medical device 130 via various authentication schemes.’” Ex. 1003 ¶ 326 (quoting Beck [0065]). The authentication is based “upon the network address of the client computing device 120, the serial number of the medical device 130,” etc. Ex. 1003 ¶ 326 (quoting Beck [0065]). I also described that the serial number of the medical device is obtained by the client computing device in order to identify the type of device. Ex. 1003 ¶ 323 (quoting Beck [0055]). Thus, Beck’s system authenticates the unique sensor ID (serial number of the medical device) associated with the unique wireless device ID (i.e., the serial number obtained by the client computing device possessing the wireless device ID).

50. The passages I quoted in my first declaration (and above) demonstrate that Beck discloses this limitation under Dr. Warren’s (incorrect) construction, which requires authenticating both sensor ID and wireless device ID. Specifically, paragraph 65 of Beck explicitly discloses authenticating both IDs. Ex. 1003 ¶ 326. Beck’s authentication of both IDs is further enabled by Beck’s server storing (and thus associating in another way) “authentication information” including “client computing device network address” and “medical

device serial number.” Beck [0051]. These disclosures of Beck are well beyond what the '307 patent discloses in relation to authentication. For example, the '307 patent does not explicitly disclose a wireless device ID, let alone authenticating a wireless device ID. Dr. Warren asserted that these disclosures are inherent and necessary in the '307 patent. Ex. 1031 49:17-51:18.

51. Dr. Warren asserts that “Petitioner [does not] provide any disclosure in the prior art of” the claim limitation requiring that “the unique sensor ID is ‘associated with the unique wireless device ID.’” Ex. 2009 ¶ 150. As I discussed above, this is not true. Dr. Warren seems to imply that the “associated” portion of the claim requires more than what’s recited in the claim itself. I disagree. The claim recites a “wireless device having... a unique ID” and “the wireless device communicates with the RF addressable sensor interface to obtain the [sensor] ID.” This step of obtaining the sensor ID associates the IDs. Notably, there is no explicit “associating” step in the claim or anywhere else in the '307 patent. Thus, when claim 1 recites “said unique sensor ID associated with said unique wireless device ID” the claim is referencing and encompassing the association made in the previous limitation to specify which sensor ID is being authenticated (i.e., the “said unique sensor ID obtained by the wireless device possessing the wireless device ID”).

F. The combination renders obvious geolocation means.

52. I discussed in my first declaration that the combination renders obvious “geolocation means.” Ex. 1003 ¶¶ 311-316.

53. As I discussed previously in Section VII.B, I have reviewed Exhibit 2006, which includes a page titled “Patent Outline” and a date of August 19, 2003, and describes “Geolocation” as a “Technolog[y] provided by a cell phone.” Ex. 2006 at 2. This is consistent with my opinion that geolocation in cell phones was obvious to a POSITA by January 2004. Additionally, Dr. Peeters testified that he was not the first person to conceive of geolocation in cell phones and that “the geolocation part was inherited from the earlier work that was done with Mike [Lovejoy] in the six years before.” Ex. 1032 83:15-20. According to Dr. Peeters, “at the time of the finding these were standard things that were available out there that we referenced because we knew that geolocation was very important.” Ex. 1032 83:15-24. Both GPS and non-GPS technologies (e.g., “time of flight”) were “completely standard” and “well known in the art.” Ex. 1032 84:5-9. I agree, and Dr. Peeters’s testimony is consistent with what a POSITA would have understood by January 2004 when the ’307 patent was filed. Further, Dr. Warren testified “[N]o, [Dr. Peeters] did not invent geolocation in cellular phones....” Ex. 1031 71:22-72:1. I agree.

54. Dr. Warren argues, however, that “adding a geolocation means to Beck’s reader would have been nonsensical, as such means would only indicate where the reader (or person performing the reading...) is located—not where the sensor (or the patient wearing such a sensor who may be remote from the reader) is located.” Ex. 2009 ¶ 157. I disagree. First, as I discussed above, Beck explicitly identifies a patient as a user of the reader (e.g., client computing device). Beck [0052]. At least in that scenario the location of the reader is the location of the patient. Second, Dr. Warren’s hypothetical seems to imply reading of the sensors from a significant distance from the patient. But in most if not all cases, a reader will be proximate to the sensor, such that the reader’s location provides sufficient information about the patient’s location, and Dr. Warren does not cite to anything in Beck that supports his assertion. Regardless, such a scenario would not teach away from incorporating “completely standard” components in a cell phone. Ex. 1032 84:5-9.

G. The combination renders obvious a “sensor interface having an analog to digital converter.”

55. In my first declaration, I opined that the combination renders obvious a “sensor interface having an analog to digital converter.” Ex. 1003 ¶¶ 271-279. For example, I observed that Beck discloses using “integrated analog/digital hybrid circuits,” and that sensors (such as glucose sensors) generate an analog signal, and use of such sensors in Beck’s medical device

“would require converting the analog signal to a digital signal by an interface that includes an analog to digital converter....” Ex. 1003 ¶¶ 274-275. I also noted that such converters were “conventional and in widespread use well-before the priority date of the '307 patent.” Ex. 1003 ¶ 276. I further relied on Heller’s disclosure of “converting an analog signal into a digital signal.” Ex. 1003 ¶ 276.

56. Dr. Warren does not address my discussion and reliance on Heller. Instead, he asserts that A/D converters were not inherent in Beck. Ex. 2009 ¶ 160. However, Dr. Peeters (the named inventor of the '307 patent) described that an analog to digital converter is “an essential component” and such that it is “just part of any, you know, any sensor component because you need to convert a continuous variable signal into a digital signal.” Ex. 1032 73:5-21. I agree with this portion of Dr. Peeters’s testimony. Dr. Warren asserts “there are ways to calculate a value based on... two sensors without first converting them to digital values” but provides no explanation and does not cite any evidence. Even though my analysis does not require inherency in Beck (due to my additional reliance on Heller), A/D converters are inherent to Beck.

VIII. CONCLUSION

All statements made herein of my own knowledge are true, and all statements made on information and belief are believed to be true. Further, I am aware that these statements are made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. § 1001. I declare under penalty of perjury that the foregoing is true and correct.

Executed on 1/20/2025, in Corona Del Mar, CA.



Majid Sarrafzadeh