

Demonstratives of Petitioner Fitbit, Inc.

Inter Partes Review of U.S. Patent Nos. 7,088,233

IPR2020-00783

Oral Hearing: July 29, 2020

IPR2020-00783 – Instituted Grounds

Jacobson Grounds

- **Ground 1:** Claims 1, 7-10, 14 are unpatentable as anticipated by *Jacobsen*
- **Ground 3:** Claims 1, 7-10, 14 are unpatentable as obvious over *Jacobsen* in view of *Say*
- **Ground 4:** Claim 13 is unpatentable as obvious over *Jacobsen* in view of *Say* and *Quy*
- **Ground 5:** Claims 24-25 are unpatentable as obvious over *Jacobsen* in view of *Say* and *Geva*
- **Ground 6:** Claim 26 is unpatentable as obvious over *Jacobsen* in view of *Say* and *Reber*

Say Grounds

- **Ground 2:** Claims 1, 7-10, 14 are unpatentable as obvious over *Say*
- **Ground 7:** Claims 15-16, 22 are unpatentable as obvious over *Say* in view of *Gabai*

Inst. Dec. at 8, 48

2

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

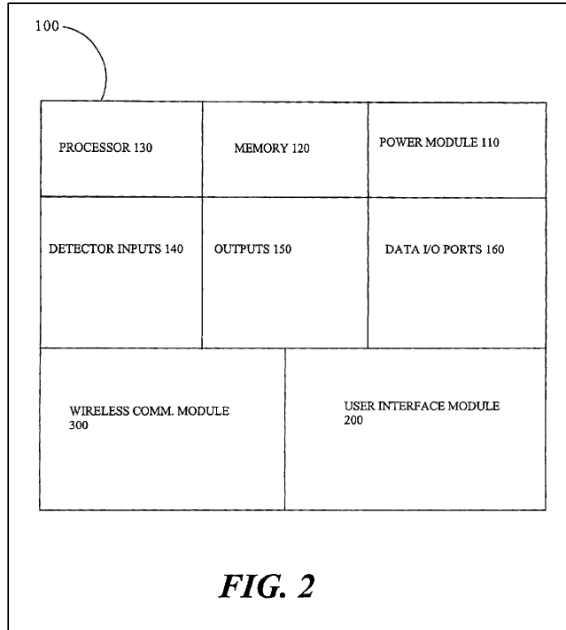
Agenda

- Security Mechanism
 - Use of passwords govern information transmitted
 - Use of encryption govern information transmitted
- *Jacobsen* and *Say* (alone or in combination) discloses and/or suggests the claimed “security mechanism” under any reasonable interpretation/construction
 - *Jacobsen*
 - *Say*
- Dependent claims
 - Claim 13 (BLUETOOTH)
 - Claims 24-25 (GPS)
 - Claim 26 (powered-down to powered-up state)
 - Claims 15-16, 22 (central communications base station / Internet)
 - Claim 14 (data I/O ports)

Agenda

- **Security Mechanism**
 - Use of passwords govern information transmitted
 - Use of encryption govern information transmitted
- *Jacobsen* and *Say* (alone or in combination) discloses and/or suggests the claimed “security mechanism” under any reasonable interpretation/construction
 - *Jacobsen*
 - *Say*
- Dependent claims
 - Claim 13 (BLUETOOTH)
 - Claims 24-25 (GPS)
 - Claim 26 (powered-down to powered-up state)
 - Claims 15-16, 22 (central communications base station / Internet)
 - Claim 14 (data I/O ports)

'233 Patent: Personal Medical Devices (PMD)



Ex. 1001 at FIG. 2

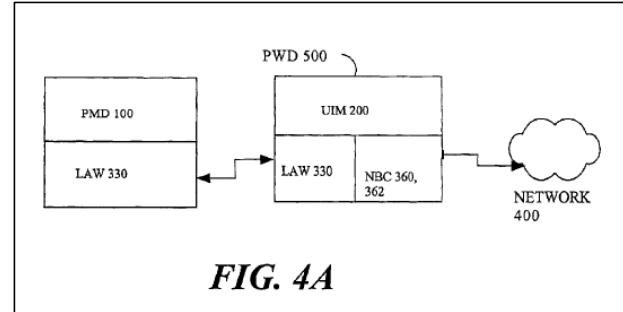


FIG. 4A

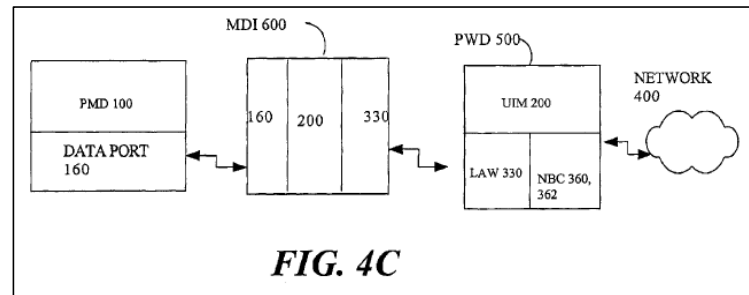


FIG. 4C

Ex. 1001 at FIGS. 4A, 4C

Ex. 1001, 3:18-59, 4:10-5:3

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Claim 1 of the '233 Patent

1. A bi-directional wireless communication system comprising:
 - (a) a first personal device, the first personal device further comprising:
 - (i) a processor;
 - (ii) a memory;
 - (iii) a power supply;
 - (iv) at least one detector input; and
 - (v) a short-range bi-directional wireless communications module;
 - (b) a second device communicating with the first device, the second device having a short-range bi-directional wireless communications module compatible with the short-range bi-directional wireless communications module of the first device; and
 - (c) a security mechanism governing information transmitted between the first personal device and the second device.

Ex. 1001 at 14:62-15:11 (Claim 1)

6

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

'233 Patent: Security

'233 Patent: Some level of Security

Security

The system and method of the present invention may also include various types of security arrangements.

It will be appreciated that the ability of various entities spread around a network to receive and/or transmit to and control the personal device 100 requires some measure of security. Only authorized agents should be allowed access to the device 100. For example, in the example shown in FIG. 5, only responding personnel RP (such as trained paramedics) who are on the scene of the event may be allowed to send a command to the personal device 100 causing the personal device 100 to dispense medication to the victim. Certainly, the bystander B should not be allowed this level of access, even though the bystander B's personal wireless device 600 may be acting as an intermediary in communication from the personal device 100 to the dispatcher D.

Ex. 1001 at 13:24-40

Ex. 1001, 13:24-40; Petition at 8; Reply 12; Ex. 1002 ¶¶40, 43

7

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Security Mechanism

'233 Patent: Password

In embodiments where the user employs standard or adapted paging or cell phones as their personal wireless device **500** or medical device interface **600**, security passwords may be entered by using numeric or other keys on a phone. In another embodiment, the security password may be entered by speaking words. In this embodiment, the system may use word recognition, voice recognition or a combination of these technologies. In the embodiment of a pager, a distinct order of pressing certain keys could provide the equivalent of a security code. For example, 3 short and 1 long on a certain key; or once on key 'a', once on key 'b', and once more on key 'a'.

Ex. 1001 at 8:11-22

3. The system of claim 1, wherein the security mechanism employs authorization by the first personal device.

4. The system of claim 1, wherein the security mechanism employs a key held by an agent and transmitted to the second device or wherein the security mechanism employs a key entered by a user of the first personal device.

Ex. 1001 at 15:14-19 (Claims 3-4)

The following are possible embodiments of security and not meant to be exclusive.

First, data transmitted to and from the personal device **100** may be encrypted by standard encryption algorithms, making it essentially impossible for the unsophisticated interceptor to interpret the data.

Second, voice and visual channels of transmission may be controlled for activation by the personal device **100** or by an authorized entity, but may not necessarily be encrypted.

Third, security keys may be held by a central agency and provided to the responding personnel RP.

Fourth, the user of the personal device **100** may have a security key that he can enter to release information or access to authorized parties.

Ex. 1001 at 13:41-54

Security Mechanism

'233 Patent: Encryption

The following are possible embodiments of security and not meant to be exclusive.

First, data transmitted to and from the personal device 100 may be encrypted by standard encryption algorithms, making it essentially impossible for the unsophisticated interceptor to interpret the data.

Ex. 1001 at 13:41-46

2. The system of claim 1, wherein the security mechanism encrypts the information.

Ex. 1001 at 15:12-13 (Claim 2)

Second, a public/private key system can be used in which access to both keys is required for decoding an encrypted message. Each party that wishes to participate in secure communications must create a key set for encrypting and decrypting messages. One key is private and the other is public. The public key is for exchanging with other parties with whom you who wish to participate in secure communication sessions. Each individual owner must keep the

Ex. 1001 at 13:60-66

Petition at 36-38; Ex. 1002, ¶ 87[1h] (p. 93); Reply at 10-13

9

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Security Mechanism

Board: Security Mechanism and Passwords / Encryption

We are not persuaded by this argument. The '233 patent explicitly discloses that the use of passwords or encryption can be used to secure information transmitted between personal device 100 and other points on the network to restrict access to authorized persons. Ex. 1001, 8:12–22, 13:25–67. The use of passwords or security keys certainly provides a form of “governing” or “control” falling within the ambit of the “security mechanism” of claim 1. We note that the Court in the *Garmin* case has concluded likewise, finding that “Dr. Martin’s conclusory opinion should not be afforded any weight.” Ex. 2023, 14. For present purposes, we see no need to construe the phrase at issue, and do not agree that such techniques as the use of passwords or encryption fall outside of the scope of claim 1.

Institution Decision at 15

Patent Owner argues that such password mechanisms do not “govern” or “control” the information transmitted between the first and second devices, and therefore are not a “security mechanism” under the proper construction of the claim. Prelim. Resp. 25–26. However, as discussed above in Section B.3, we are not persuaded that the claim language should be interpreted so narrowly as to exclude the use of passwords to control the transmission of information between the devices, particularly given that the '233 patent explicitly describes such use of passwords. Ex. 1001, 8:11–22.

Institution Decision at 36

Institution Decision at 13-15, 36, 42

10

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Security Mechanism

Patent Owner Preliminary Response

Sections E.2 and F.2 below, Patent Owner would narrow this claim requirement to exclude the use of passwords, or encryption techniques such as security keys and public/private key to protect information, which Patent Owner contends does not “govern” or “control” information. *Id.* at 25–26, 29–30.

particular, Dr. Martin relies on a statement in the Abstract providing for “**multiple levels** of prioritization, authentication of a person (task, step, process or order), and confirmation via interrogation of person, device, or related monitor.” *Id.* at ¶ 28. In addition, Dr. Martin relies on the

13:30–41). Dr. Martin further relies on a dictionary, which defines “governing” as “controlling.” *Id.* at ¶ 35. From this, Dr. Martin opines that one of ordinary skill would not consider security measures such as encryption to satisfy the claim requirement of “governing” transmission of information. *Id.* at ¶¶ 33–34.

Institution Decision at 14 (citing POPR at 11, 25-26, 29-30; Ex. 2007, ¶¶ 28, 33-34)

11

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Security Mechanism

Patent Owner Response

As discussed above, the specification discusses “security” generally in the context of establishing restrictions on the information that is transmitted between a first personal device (e.g., a victim’s PMD) and a second device (e.g., a bystander B’s device). As set forth in the specification, this may be accomplished with or without encrypting the information. Ex. 1001, 13:47-49. Examples of mechanisms that govern information transmitted between the first personal device and the second device are those that establish authorization for a user of a device to access certain types of data over a preexisting channel. Ex. 2026, ¶29. Such mechanism could be implemented by a user having a password that provides a particular level of access to information that is transmitted. *Id.*

POR at 8

POR at 8-11

12

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Security Mechanism

Patent Owner Response

To be clear, it is not Patent Owner's position that some form of encryption could not be used to govern information that is transmitted between a first device and a second device. For example, the specification states that "a public/private key system can be used in which access to both keys is required for decoding an encrypted message." Ex. 1001, 13:60-62. Such encryption of the content of a communications signal would provide a way to validate the authenticity of a user to have a certain level of access or authorization to information transmitted. But encryption of the *contents* of the signal and using it to govern access by a particular device is different from encryption of signals on an established network, such as used with BLUETOOTH or disclosed in Say for purposes of avoiding cross-talk

POR at 11

POR at 8-11

13

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Security Mechanism

Patent Owner Sur-Reply

Petitioner purports to agree with the Board’s institution decision declining construction of this term, yet repeatedly advocates for a meaning that ignores the fact that the claimed “security mechanism” must govern **information** transmitted between devices. Petitioner’s Reply is replete with arguments as to how the use of encryption, as a concept, might constitute a “security mechanism,” without acknowledging that the claims require significantly more. Ex. 1001, claim 1.

Sur-Reply at 1

Sur-Reply at 1-10

14

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Security Mechanism

Patent Owner Sur-Reply

Despite Petitioner’s focus on the construction for this term advanced in Patent Owner’s Preliminary Response, neither Patent Owner’s Response (“POR”) nor Dr. Martin’s declaration rely on that originally proposed construction to distinguish the prior art. *See* POR at 20, 28-29, 34-37; Ex. 2026 at 16-17; *see also* Ex. 1076, 91:5-17. Both the POR and Dr. Martin’s declaration rely solely on the plain meaning of the words used in the claim, while pointing out that Petitioner’s unreasonably broad construction renders much of the claim language superfluous. *See* POR at 21-23.

Sur-Reply at 2

Sur-Reply at 1-10

15

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Security Mechanism

Patent Owner Sur-Reply

discussing the context of the invention, neither Patent Owner nor Dr. Martin have advocated for a construction of the term that requires multiple levels of authorization nor is that a basis on which the POR or Dr. Martin distinguish any prior art.

Sur-Reply at 10

Sur-Reply at 1-10

16

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Security Mechanism

Patent Owner's Expert, Dr. Martin

39. I understand that the PTAB declined to construe the term “governing information transmitted between the first personal device and the second device” as recited in claim 1 and declined to adopt Philips’ construction of that term as “controlling the transmission of information between the first personal device and the second device.” Dec., 13–15. My opinions herein do not rely on Philips’s original proposed construction for this term. Instead, I rely on what I regard as how a POSITA would understand this term according to its plain and ordinary meaning when understood in the context of the specification.

Ex. 2026 ¶39

Let's go to your declaration, Exhibit 2026, paragraph 39. Are you there?

A. Yes. I'm at paragraph 39.

Q. Here you state at kind of halfway down to the paragraph at the top of page 17. "My opinions herein do not rely on Philips' original proposed construction for this term"; is that correct?

A. Yes. That's correct.

Q. Instead, you rely on what you regard as how a POSITA would understand this term according to its plain and ordinary meaning when understood in the context of the specification; is that correct?

A. Yes. That's correct.

Ex. 1076, 91:2-17

Reply at 2

17

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Security Mechanism

Patent Owner's Expert, Dr. Martin

Q. And so is it your opinion that the ordinary meaning of the phrase "security mechanism" that you applied in your declaration is dependent or changes depending on the threat that you're trying to protect against?

MR. RODRIGUES: Objection to form.

THE WITNESS: Yes. I think the security mechanism depends. And, again, it's in the specification. As we talked about, there's the example of Figure 5, but there's also the example of transmitting information unencrypted but with authorization.

And then as -- there's the whole list of possible embodiments of the security mechanism, the embodiments of security -- sorry, let me look back at it -- in Column 13 that we've walked through before.

Ex. 1076 at 97:8-98:3

Q. And when you say the security mechanism depends, you're saying the ordinary meaning of security mechanism depends on the threat you're trying to protect against?

MR. RODRIGUES: Objection to form.

THE WITNESS: Yes. That's correct.

Ex. 1076 at 98:5-13

Q. So the opinions on which you base your declaration -- strike that.

So you can't tell me today sitting here today what the plain and ordinary mean of the phrase "security mechanism governing information transmitted between the first personal device and the second device" is until I tell you what you're trying to protect against?

MR. RODRIGUES: Objection to form.

THE WITNESS: Yes. That's correct. The form of the security mechanism is going to depend upon, you know, what the threats are that you're trying to protect against.

Ex. 1076 at 98:15-99:5

Reply at 2

18

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Security Mechanism

Patent Owner's Expert, Dr. Martin

Q. What is the plain and ordinary meaning of the phrase "security mechanism governing information transmitted between the first personal device and the second device"?

MR. RODRIGUES: Objection to form.

THE WITNESS: So, again, as I've said, the security mechanisms depend upon what you're trying to protect against. And so -- and so you have to take that into account as part of the meaning.

And then the -- there also needs to be information that's transmitted between the first personal device and the second device.

Ex. 1076 at 95:14-96:1

Q. So is it your opinion that the ordinary meaning of the phrase "security mechanism governing information transmitted between the first personal device and the second device" changes depending upon what you're trying to protect against?

MR. RODRIGUES: Objection to form.

THE WITNESS: So, you know, as I've said, the security mechanisms depend upon what your threat model is. And so depending upon, you know, what you're trying to accomplish and what the threats are to that would determine what security mechanisms you would have in place.

Ex. 1076 at 96:7-22

Reply at 2

19

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Security Mechanism

Patent Owner's Expert, Dr. Martin

Q. In -- so going back to what you said about the security mechanism, you said the security mechanism described in the '233 patent involves multiple levels of authorization, authentication and -- sorry.

You said the security mechanism, you know, in the '233 patent involves authentication and multiple levels of authorization and prioritization; is that correct?

A. Right. That's correct. I was referring to the way it's described in the abstract of the patent.

Q. And that's what you -- and that's the understanding that you rely on to support your opinions in your declaration; is that correct?

MR. RODRIGUES: Objection to form.

THE WITNESS: Yes. That's correct. The way the abstract describes it and, for instance, the example that we just discussed that's later in the specification.

Ex. 1076, 58:4-59:2

Q. And so the way the abstract describes multiple levels of prioritization, authentication and authorization is how -- as well as Figure 5 is how you have relied on -- is what you rely on to interpret the security mechanism in the '233 patent?

MR. RODRIGUES: Objection to form.

THE WITNESS: Those will be the main things, yes, that's correct.

Ex. 1076, 59:4-14

Reply at 5, 11

20

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Agenda

- Security Mechanism
 - Use of passwords govern information transmitted
 - Use of encryption govern information transmitted
- *Jacobsen and Say* (alone or in combination) discloses and/or suggests the claimed “security mechanism” under any reasonable interpretation/construction
 - *Jacobsen*
 - *Say*
- Dependent claims
 - Claim 13 (BLUETOOTH)
 - Claims 24-25 (GPS)
 - Claim 26 (powered-down to powered-up state)
 - Claims 15-16, 22 (central communications base station / Internet)
 - Claim 14 (data I/O ports)

Jacobsen: Security Mechanism

Patent Owner: *Jacobsen*

2. Jacobsen Does Not Anticipate Claims 1, 7-10, and 14

(a) Claim 1

The Petition and Dr. Paradiso assert that Jacobsen discloses a “first personal device,” i.e., Jacobsen’s “wrist sensor/display unit 18” (Pet., 24), in short-range bi-directional communication with a “second device,” i.e., Jacobsen’s “vest/harness” with “soldier unit 50” (Pet. 33). Jacobsen, however, does not disclose “a security mechanism governing information transmitted between the first personal device and the second device,” i.e., information transmitted between the wrist

sensor/display unit 18 (what the Petition characterizes as the “first personal device”) and the soldier unit 50 (what the Petition characterizes as the relevant “second device”). Ex. 2026, ¶70.

POR at 18

A. Claims 1, 7-10

1. *Jacobsen*

For *Jacobsen*, PO’s only argument is that *Jacobsen* does not disclose the “security mechanism.” (POR, 18-29.) But as discussed in section II.A, PO’s position hinges on an effective construction unsupported by the ’233 patent’s claims or specification, and does not rebut Petitioner’s evidence of unpatentability.

Reply at 10

POR at 18-29; Reply at 10-17

22

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Jacobsen: Security Mechanism

Jacobsen

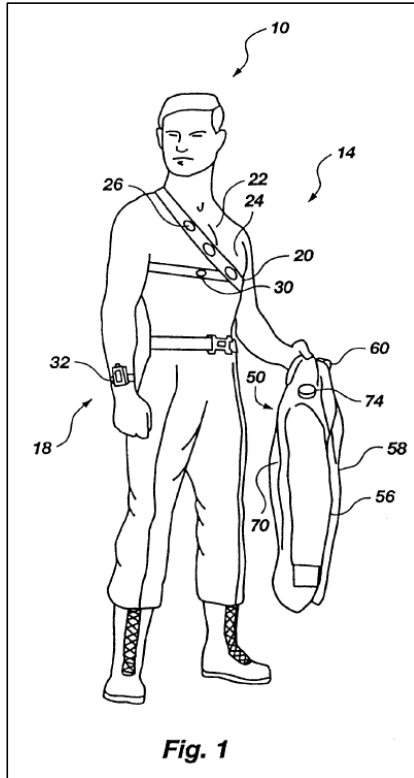


Exhibit 1005, FIG. 1

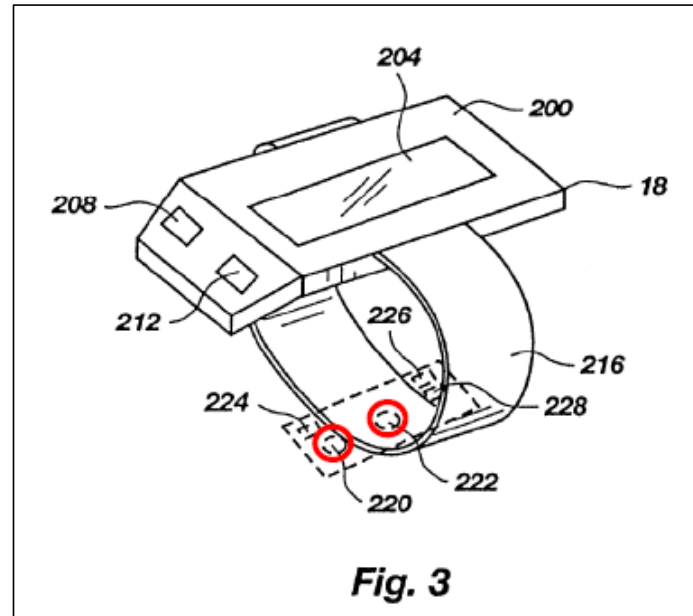


Exhibit 1005, FIG. 3

Ex. 1005, FIGS. 1, 3; Petition 8-11, 22-44; Ex. 1002 ¶¶ 51-58, 87-92

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Jacobsen: Security Mechanism

Jacobsen

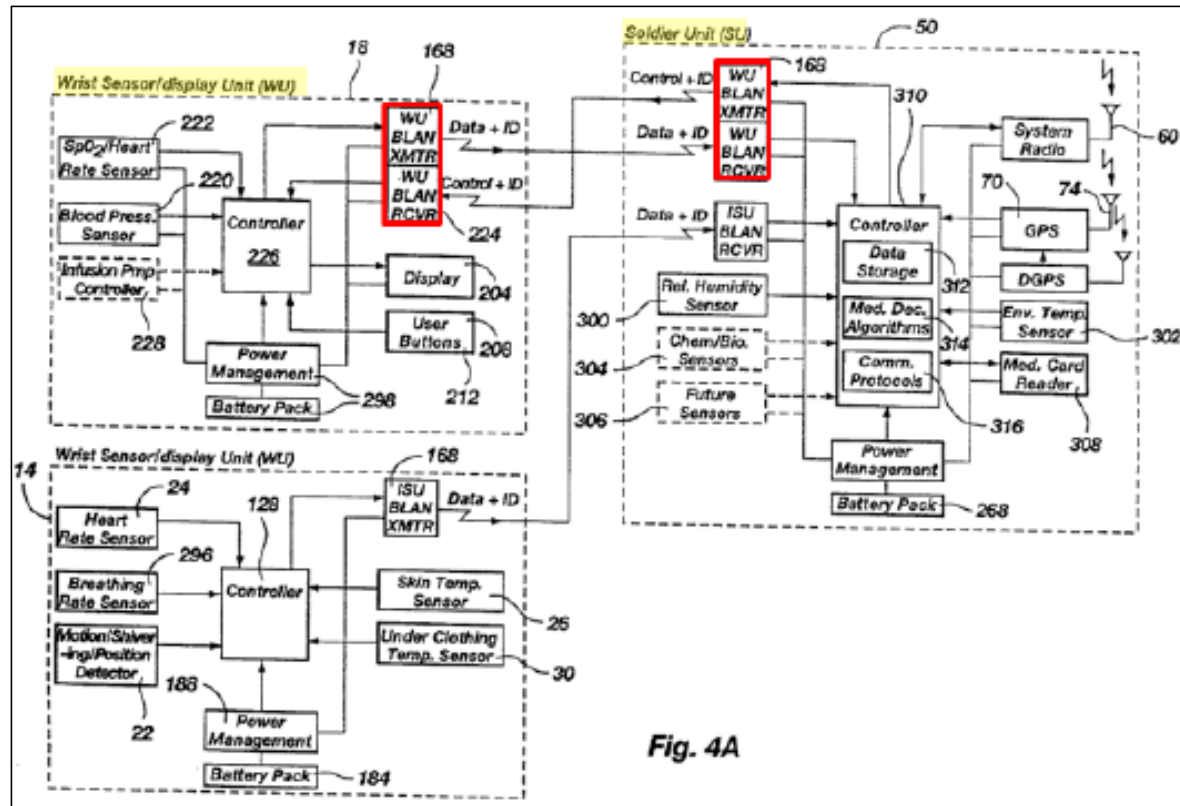


Fig. 4A

Petition at 11; Exhibit 1005, FIG. 4A

Ex. 1005, Fig. 4A; Petition 8-11, 22-44; Ex. 1002 ¶¶ 51-58, 87-92; Reply at 10

24

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Jacobsen: Security Mechanism

Petition

¶87[1h]. To begin, the specification and claim 4 of the '233 patent describe that the claimed "security mechanism" can employ "a key entered by a user of the first personal device." Ex. 1001, 15:17-20; *see also id.*, 13:52-54; Ex. 1002, ¶87[1h]. Similarly, *Jacobsen* discloses the wrist sensor/display unit 18 and soldier unit 50 operating only when users enter the correct password: "each device may contain a self-disabling means, such as software which requires the entry of a password or some other code. If the wrong password is entered for more than one attempt, the device will automatically disable itself." Ex. 1005, 15:5-10.

Petition at 37

Jacobsen

To ensure that none of the devices may be used against the soldiers if captured by the enemy, each device may contain a self-disabling means, such as software which requires the entry of a password or some other code. If the wrong password is entered for more than one attempt, the device will automatically disable itself. While disablement will not be critical for soldier units, it is important that leader/medic control units and command units not be usable by an enemy to track the position of the soldiers which are monitored by those units.

Ex. 1005, 15:5-14

Petition 36-38; Ex. 1002 ¶87[1h]

25

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Jacobsen: Security Mechanism

'233 patent

In embodiments where the user employs standard or adapted paging or cell phones as their personal wireless device 500 or medical device interface 600, security passwords may be entered by using numeric or other keys on a phone. In another embodiment, the security password may be entered by speaking words. In this embodiment, the system may use word recognition, voice recognition or a combination of these technologies. In the embodiment of a pager, a distinct order of pressing certain keys could provide the equivalent of a security code. For example, 3 short and 1 long on a certain key; or once on key 'a', once on key 'b', and once more on key 'a'.

Ex. 1001 at 8:11-22

The following are possible embodiments of security and not meant to be exclusive.

Fourth, the user of the personal device 100 may have a security key that he can enter to release information or access to authorized parties.

Ex. 1001 at 13:25-26, 13:52-54

4. The system of claim 1, wherein the security mechanism employs a key held by an agent and transmitted to the second device or wherein the security mechanism employs a key entered by a user of the first personal device.

Ex. 1001 at 15:16-19 (Claim 4)

Ex. 1001, 8:11-22, 13:25-26, 13:40-54, 15:16-19; Petition at 36-38; Ex. 1002 ¶87[1h]; Reply at 1-2, 10-17

Board

Patent Owner argues that such password mechanisms do not “govern” or “control” the information transmitted between the first and second devices, and therefore are not a “security mechanism” under the proper construction of the claim. Prelim. Resp. 25–26. However, as discussed above in Section B.3, we are not persuaded that the claim language should be interpreted so narrowly as to exclude the use of passwords to control the transmission of information between the devices, particularly given that the '233 patent explicitly describes such use of passwords. Ex. 1001, 8:11–22.

Institution Decision at 36

Jacobsen: Security Mechanism

Patent Owner: Sur-Reply

transmitted between the first personal device and the second device,” Petitioner now argues—for the first time in reply—that the term “information transmitted” does not require that information actually be transmitted and points to the specification of the ’233 Patent’s reference to “security keys” and “biometrics. **First**, this is a new claim construction argument raised for the first time in reply and has thus been waived. **Second**, the examples cited to, while concerning authorization, also require the actual transmission of information. **Third**, to the extent the specification did describe some semblance of self-disabling means akin to that of Jacobsen, that is not what was claimed in the claims at issue—which requires information transmitted.

Sur-Reply at 13

Sur-Reply at 11-14

27

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Jacobsen: Security Mechanism

Patent Owner's Expert, Dr. Martin

But it seems to me that the way this is described, you're also -- the patent's also talking about controlling the access to the device, and in that case, encryption would be a part of -- would likely be a part of what you're doing, but it wouldn't be enough to provide access.

And so controlling that -- if you didn't want that information to be received at all, perhaps there's information that you don't want to be transmitted at all, then encryption wouldn't be enough to prevent that.

Ex. 2025 at 134:12-22

Reply at 14-15

28

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Jacobsen: Security Mechanism

Patent Owner: Sur-Reply

Petitioner goes on to argue that Jacobsen’s “self-disabling means” does govern information transmitted between the first personal device and the second device because if a user enters a password incorrectly once, they would have another opportunity to do so before the device is disabled. However, even this feature of Jacobsen is untethered to any information transmitted between the devices. To the contrary, this “first password” scenario only further demonstrates how such a password is focused on the device itself and not the information transmitted.

Sur-Reply at 13

Sur-Reply at 11-14

29

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Jacobsen: Security Mechanism

Jacobsen

To ensure that none of the devices may be used against the soldiers if captured by the enemy, each device may contain a self-disabling means, such as software which requires the entry of a password or some other code. **If the wrong password is entered for more than one attempt, the device will automatically disable itself.** While disablement will not be critical for soldier units, it is important that leader/medic control units and command units not be usable by an enemy to track the position of the soldiers which are monitored by those units.

Ex. 1005 at 15:5-14

Reply at 15

Dr. Martin

You would agree that Jacobsen contemplates someone entering the wrong password once and then entering the right password on the second try, correct?

MR. RODRIGUES: Objection to form.

THE WITNESS: So, yeah, yes. At line 8 it says if the wrong password is entered for more than one attempt. So it looks like you get one shot at it based upon that reading.

BY MR. OKANO:

Q. So if Jacobsen, if someone enters a wrong password once, they are not able to access device -- the device, correct?

A. That's correct. They're not able to access the device.

Q. And then on their second attempt they entered the correct password, and they are able to access the device and the information available to the device, correct?

A. Correct. Because they entered the correct password, the device is functioning.

Q. So when they entered -- in that scenario when they entered the incorrect password the first time, there's still the possibility that data can be transmitted, correct?

MR. RODRIGUES: Objection to form.

THE WITNESS: That's correct. After the first incorrect password, the device is not yet disabled.

Ex. 1076 at 214:25-216:9

30

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Jacobsen: Security Mechanism

Dr. Martin: Multiple Levels of Access / Layers of Security

Q. Yeah. And my question is to tie that to the Claim 1 security mechanism. In that hypothetical, multiple levels of access would not be required to meet Claim 1's security mechanism; is that your opinion?

MR. RODRIGUES: Objection to form.

THE WITNESS: Again, if I'm just trying to find -- find the person and want to broadcast out their identity, then multiple levels aren't required in that case.

Ex. 1076, 153:6-18

You know, yes or no: If a security mechanism cannot accomplish Figure 5, does it meet Claim 1?

MR. RODRIGUES: Objection to form.

THE WITNESS: There might be security mechanisms that cannot accomplish Figure 5 that could meet Claim 1.

Ex. 1076, 86:17-25

embodiments.”). Further, PO’s expert, who provides the only evidence supporting PO’s position (POR 20 (citing only Ex.2026 ¶¶72-73)), conceded (1) this additional layer of security “would not necessarily be required” (Ex.1076, 150:2-153:18; *id.*, 86:14-25 (“There might be security mechanisms that cannot accomplish Figure 5 that could meet Claim 1.”), 88:2-21) and (2) is not described in Figure 5 (*id.*, 104:4-105:5 (admitting additional layer of security “is not shown as an explicit element of Figure 5”)). In district court, PO’s expert has conceded “that patent’s also talking about controlling the access to the *device*.” (Ex.2025, 134:8-22 (emphasis added)).

Reply at 11

Reply at 11

31

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Jacobsen: Security Mechanism

Patent Owner's Expert, Dr. Martin

Q. Would a POSITA have understood -- at the relevant time frame, would a POSITA have understood multiple levels to mean -- to include full authorization and no authorization?

MR. RODRIGUES: Objection to form.

THE WITNESS: So you're saying I either have access or I don't have access? Is that what you're asking?

BY MR. OKANO:

Q. That's correct.

A. I mean, that would be one option.

Q. So the option of -- a POSITA would have understood multiple levels of authorization to include full access and no access to a device?

MR. RODRIGUES: Objection to form.

THE WITNESS: Yeah, so you either have access or you don't. So that's multiple levels.

Ex. 1076, 62:8-63:4

Reply at 4

32

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Jacobsen: Security Mechanism

Patent Owner

contrary, this “first password” scenario only further demonstrates how such a password is focused on the device itself and not the information transmitted.

Sur-Reply at 13

Patent Owner’s Expert, Dr. Martin

But it seems to me that the way this is described, you're also -- the patent's also talking about controlling the access to the device, and in that case, encryption would be a part of -- would likely be a part of what you're doing, but it wouldn't be enough to provide access.

Ex. 2025 at 134:12-17

Reply at 11; Sur-Reply at 13

33

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Agenda

- Security Mechanism
 - Use of passwords govern information transmitted
 - Use of encryption govern information transmitted
- *Jacobsen* and *Say* (alone or in combination) discloses and/or suggests the claimed “security mechanism” under any reasonable interpretation/construction
 - *Jacobsen*
 - *Say*
- Dependent claims
 - Claim 13 (BLUETOOTH)
 - Claims 24-25 (GPS)
 - Claim 26 (powered-down to powered-up state)
 - Claims 15-16, 22 (central communications base station / Internet)
 - Claim 14 (data I/O ports)

Say: Security Mechanism

Patent Owner: *Say*

2. Claims 1, 7-10, and 14 Are Patentable Over Say

a. Claim 1

The Petition relies on two aspects of Say's disclosure as meeting the requirements of "a security mechanism governing information transmitted between the first personal device and the second device." Pet., 60. The first is a "unique identification code," while the second is a form of device-to-device encryption designed to avoid cross talk. *Id.* (citing Ex. 1006, 49:15-37 and 49:38-67); Ex. 2026, ¶88. Yet neither is tied to the information transmitted from one device to the other, and therefore fails to provide a security mechanism that governs information transmitted between Say's sensor d

POR at 34-35

Reply at 17

2. *Say*

Similar to *Jacobsen*, PO's only argument for *Say* is failure to disclose the claimed "security mechanism." (POR, 34-42.) For reasons similar to those explained above in Sections II.A/III.A.1, PO's argument relies on an effective construction for the term that is unsupported by the claims or specification, and does not rebut Petitioner's evidence of unpatentability.

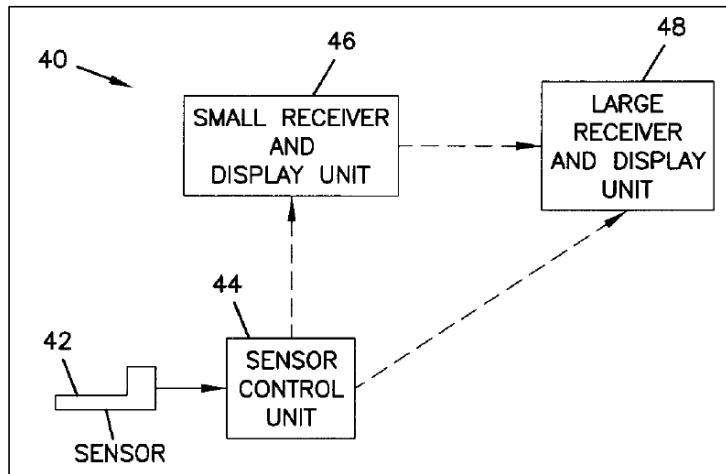
POR at 34-41; Reply at 17-20

35

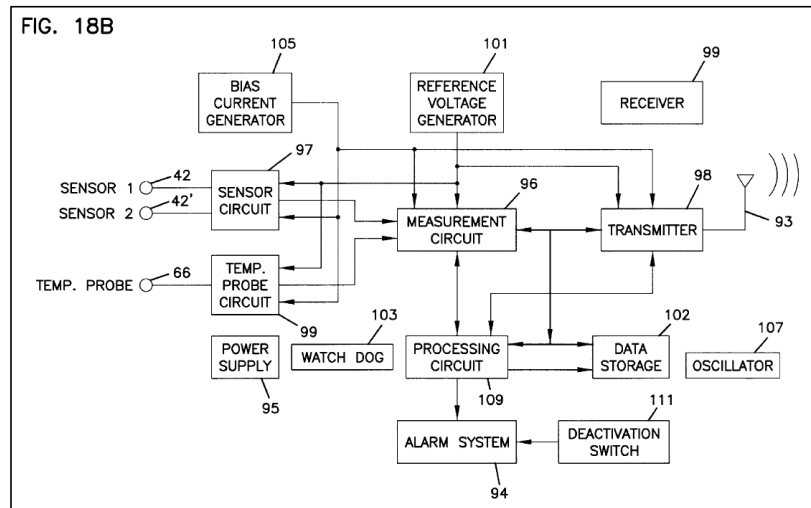
DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Say: Security Mechanism

Say



Ex. 1006 at Fig. 1



Ex. 1006 at Fig. 18B

Ex. 1006, Figs. 1, 18B; Petition at 11-12, 45-66; Ex. 1002 ¶¶ 59-70, 94-99

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Say: Security Mechanism

Petition

ix. Claim element [1h]

Say discloses a security mechanism governing information transmitted between the “sensor control unit 44” and the “receiver/display unit 46, 48.” Ex. 1002, ¶94[1h]. The ’233 patent’s specification and dependent claims 2 and 4 state that the claimed “security mechanism governing information transmitted” includes encryption or a “key entered by a user of the first personal device.” Ex. 1001, 15:13-14, 15:17-20; *see also id.*, 13:41-67. Say discloses both of these security and the receiver/display unit 46, 48. Ex. 1002, ¶94[1h]. Say discloses that sensor control unit 44’s transmitter may “transmit a code to indicate, for example, the beginning of a transmission and/or to identify, preferably using a unique identification code, the particular on-skin sensor control unit 44” and that this “identification code may be selected by the patient and communicated to the sensor control unit 44 via [] an input device coupled to” the unit. Ex. 1006, 49:15-37.

Say also discloses that the sensor control unit 44’s transmitter “may use encryption techniques to encrypt the datastream from the transmitter” and the “receiver/display unit 46, 48 contains a key to decipher the encrypted data signal.” *Id.*, 49:38-67. Thus, Say’s communications between the sensor control unit 44 and receiver/display unit 46, 48 involve encryption and/or a “key entered by a user of the first personal device,” just like the ’233 patent’s “security mechanism.” Ex. 1002, ¶94[1h]. As such, Say’s bi-directional wireless communication system (the analyte monitoring system 40 depicted in Figure 1) includes a security mechanism as claimed. *Id.*

Petition at 59-60

Petition at 59-60; Ex. 1002, ¶¶ 59-70, 94[1h] (Pages 137-139)

37

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Say: Security Mechanism

Say: Unique Code

The presence of other devices, including other on-skin sensor control units, may create noise or interference within the frequency band of the transmitter 98. This may result in the generation of false data. To overcome this potential difficulty, the transmitter 98 may also transmit a code to indicate, for example, the beginning of a transmission and/or to identify, preferably using a unique identification code, the particular on-skin sensor control unit 44 in the event that there is more than one on-skin sensor control unit 44 or other transmission source within range of the receiver/display unit 46, 48. The provision of an identification code with the data may reduce the likelihood that the receiver/display unit 46, 48 intercepts and interprets signals from other transmission sources, as well as preventing “crosstalk” with different on-skin sensor control units 44. The identification code may be provided as a factory-set code stored in the sensor control unit 44. Alternatively, the identification code may be randomly generated by an appropriate circuit in the sensor control unit 44 or the receiver/display unit 46, 48 (and transmitted to the sensor control unit 44) or the identification code may be selected by the patient and communicated to the sensor control unit 44 via a transmitter or an input device coupled to the sensor control unit 44.

Ex. 1006 at 49:15-37

Ex. 1006, 49:15-37; Petition at 59-60; Ex. 1002 ¶94[1h]

38

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Say: Security Mechanism

Say: Encryption

Other methods may be used to eliminate “crosstalk” and to identify signals from the appropriate on-skin sensor control unit 44. In some embodiments, the transmitter 98 may use encryption techniques to encrypt the datastream from the transmitter 98. The receiver/display unit 46, 48 contains the key to decipher the encrypted data signal. The receiver/display unit 46, 48 then determines when false signals or “crosstalk” signals are received by evaluation of the signal after it has been deciphered. For example, the analyzer 152 in the one or more receiver/display units 46, 48 compares the data, such as current measurements or analyte levels, with expected measurements (e.g., an expected range of measurements corresponding to physiologically relevant analyte levels). Alternatively, an analyzer in the receiver/display units 46, 48 searches for an identification code in the decrypted data signal.

Ex. 1006 at 49:38-53

Ex. 1006, 49:38-53; Petition at 59-60; Ex. 1002 ¶94[1h]

39

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Say: Security Mechanism

'233 Patent

Encryption

The following are possible embodiments of security and not meant to be exclusive.

First, data transmitted to and from the personal device 100 may be encrypted by standard encryption algorithms, making it essentially impossible for the unsophisticated interceptor to interpret the data.

Ex. 1001 at 13:41-46

2. The system of claim 1, wherein the security mechanism encrypts the information.

Ex. 1001 at 15:12-13 (Claim 2)

Security Key

The following are possible embodiments of security and not meant to be exclusive.

Fourth, the user of the personal device 100 may have a security key that he can enter to release information or access to authorized parties.

Ex. 1001 at 13:41-54

4. The system of claim 1, wherein the security mechanism employs a key held by an agent and transmitted to the second device or wherein the security mechanism employs a key entered by a user of the first personal device.

Ex. 1001 at 15:17-20 (Claim 4)

Say: Security Mechanism

Dr. Martin: “Encryption Alone” Can Meet “Security Mechanism”

Q. Yes. And my question is by preventing eavesdropping in that circumstance, that encryption alone would meet Claim 1 security mechanism limitation, correct?

MR. RODRIGUES: Objection to form.

THE WITNESS: Sorry. I'm clearly not understanding something, because I feel like I've answered that -- if all you're worried about is -- is eavesdropping, then, yes, encryption would be a security mechanism that would prevent eavesdropping.

BY MR. OKANO:

Q. Yeah, what I'm asking is the next step which is then -- so encryption alone would satisfy the security mechanism of Claim 1; is that correct?

MR. RODRIGUES: Objection to form.

THE WITNESS: If the application that you're applying Claim 1 to was just worried about eavesdropping, then, yes, that would satisfy.

Ex. 1076, at 157:20-158:19

Reply at 3

41

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Say: Security Mechanism

Dr. Martin: “Encryption Alone” Can Meet “Security Mechanism”

Q. And so any one of these approaches would -- in your opinion, a POSITA would understand any of the listed approaches, as the specification describes them, as possible embodiments of security to meet Claim 1 security mechanism?

MR. RODRIGUES: Objection to form.

THE WITNESS: Again, you're saying anyone, but it -- it's going to depend upon what the -- what the threat that you're worried about is.

So, for example, if you're just worried about somebody eavesdropping on the communication, you might use encryption. But just encryption alone is not going to provide the capabilities to perform the example of the -- of the victim, the bystander and the responding personnel.

So if I were to build such a system, that the only thing I was worried about was eavesdropping, then, you know, I might just use encryption. If I'm worried about more than eavesdropping, I'm going to need additional things.

Q. The spec does not say that multiple embodiments of security are required; is that correct?

MR. RODRIGUES: Objection to form.

THE WITNESS: I don't think it says multiple are required. But it certainly describes like this list that we just walked through and like I said earlier in the -- in the abstract, the multiple levels of -- how did they put it?

I'm sorry. Let me jump back to the abstract -- you know, the multiple levels of prioritization, authentication of person tasks that process order and confirmation via interrogation of personal device or related monitor.

Ex. 1076 at 68:19-70:15

Reply at 3-4

42

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Say: Security Mechanism

Dr. Martin in District Court: “Encryption Alone” Can Meet “Security Mechanism”

Q. So does the Claim 1(c) of the '233 patent as written allow the security mechanism to only include encryption?

MR. RODRIGUES: Objection to form, vague.

THE WITNESS: It could only be encryption.

Ex. 2025 at 132:25-133:4

Reply at 3

43

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Say: Security Mechanism

Dr. Martin: Say's Unique ID Code Used To Provide Access to Transmitted Information

Q. And would it be fair to say that if the identification code is the one, you know, that matches the identification -- selected by the patient is the one that matches the expected identification code at the receiver display 46, 48, that the receiver display will -- will have access to all the data transmitted -- not just have access, but to receive all -- and have access to all the data transmitted by the sensor control unit?

MR. RODRIGUES: Objection to form.

THE WITNESS: Yes. It would receive all the data that's transmitted for it, but that's just because that identification code is saying you're the intended recipient. Like I said in the report, that ID code, whether selected by the user or not, is really just a network address.

Ex. 1076 at 249:12-250:7

Reply at 19

44

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Say: Security Mechanism

Patent Owner: Levels of Access

Say's use of encryption simply does not **govern information transmitted** between devices and is instead solely focused on establishing a communications scheme that avoids crosstalk, regardless of the **information** that may be transmitted using that scheme. Ex. 2026, ¶91. Full access to the sensor information transmitted is provided at the receiving device. There is no connection

POR at 36-37

POR at 36-38

45

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Say: Security Mechanism

Patent Owner: Levels of Access

As with Jacobsen, any attempt to apply the specific encryption technique disclosed by Say to implement the system described in Figure 5 of the '233 patent would not work. *See id.*, ¶94. In the context of Fig. 5, one might rely on Say to

to avoid crosstalk. *See Ex. 2026*, ¶94. This approach, however, would provide no security mechanism governing the information actually transmitted between these devices because it is solely focused on encrypting the transmission at each link, but not providing any form of security to the information itself. *Id.* Using Say's encryption, there would be no way of accomplish the goal of allowing or disallowing B's access to information (such as a sensitive command to administer medicine sent from RP to Personal Device 100) with Say's encryption. *Id.* Instead, B would simply have access to all information upon receiving information over a communications link (even where the link was itself utilized Say-like encryption). *Id.*

POR at 38-39

POR at 36-39

46

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Say: Security Mechanism

Patent Owner: Levels of Access

As explained by Dr. Martin, the type of transmission-focused encryption provided by Say is similar to the type of encryption provided by the BLUETOOTH protocol, which the '233 patent acknowledges to have been known in the field. *Id.*, ¶95. Just like the encryption scheme disclosed by Say, BLUETOOTH only provides device-to-device encryption focused on establishing secure communications links, and has no security mechanism to govern information transmitted thereby providing access to various levels of the information that may be transmitted over those communication links that may be established by BLUETOOTH—even where BLUETOOTH encrypts those links. *Id.* As

POR at 39

It is not until Plaintiff's Responsive Brief that the issue critical to the parties' dispute (which is allegedly relevant to an issue of patent invalidity) takes center stage. Plaintiff initially argued that "[w]hile the specification may describe other forms of security that do not control the transmission of information (such as, for example, encryption), that is not what was intended by the language actually used in the claim." (Dkt. No. 77 at 13.) Through this assertion and as further elaborated in its Responsive Brief, Plaintiff appears to take the position that the claims require the security mechanism to be capable of fully preventing transmission of information for there to be "control." Plaintiff supports its position by citing to its expert, Dr. Martin. Dr. Martin opines that "encryption is a technique that may protect information, but it does not govern or control its transmission." (Dkt. No. 77-6 at ¶ 33.) However, Dr. Martin does not provide any further explanation or cite to any evidence for this aspect of his opinion. (*Id.*) Moreover, the specification expressly discloses "standard encryption algorithms" as a "possible embodiment of security." '233 Patent at 13:41-44. Based on the disclosure in the specification, the Court finds Dr. Martin's conclusory opinion should not be afforded any weight. *See SkinMedica, Inc. v. Histogen Inc.*, 727 F.3d 1187, 1209 (Fed. Cir. 2013)

Ex. 2023 at 13-14
(Judge Birotte CDCA DCT
Markman order)

POR at 36-39; Institution Decision at 13-14; Reply at 3

47

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Agenda

- Security Mechanism
 - Use of passwords govern information transmitted
 - Use of encryption govern information transmitted
- *Jacobsen and Say* (alone or in combination) discloses and/or suggests the claimed “security mechanism” under any reasonable interpretation/construction
 - *Jacobsen*
 - *Say*
- Dependent claims
 - Claim 13 (BLUETOOTH)
 - Claims 24-25 (GPS)
 - Claim 26 (powered-down to powered-up state)
 - Claims 15-16, 22 (central communications base station / Internet)
 - Claim 14 (data I/O ports)

Ground 3: *Jacobsen* in view of *Say*

Petition: A POSITA Would Have Been Motivated to Configure *Jacobsen*'s System to Use Encryption

Given the disclosure of *Jacobsen* and *Say*, and the knowledge of a POSITA, a POSITA would have been motivated to configure *Jacobsen*'s security features implemented in its system to include mechanisms that use encryption to govern information transmitted between the wrist sensor/display unit 18 and soldier unit 50, similar to the mechanisms disclosed by *Say*. Ex. 1002, ¶¶104-10; KSR, 550 U.S. at 415-21.

A POSITA would have been motivated to implement such features in *Jacobsen*'s system because it would have improved the security of communications between the two units by encrypting the data transmitted over the short-range wireless channels, thus minimizing opportunities for nefarious entities from intercepting and interpreting the transmitted data. Ex. 1002, ¶105. A

Petition at 67; see also Ex. 1002 ¶¶ 104-10

Petition at 66-70; Ex. 1002 ¶¶100-110

49

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 3: *Jacobsen* in view of *Say*

Dr. Martin: “Encryption Alone” Can Meet “Security Mechanism” to Prevent “Eavesdropping”

Q. Yes. And my question is by preventing eavesdropping in that circumstance, that encryption alone would meet Claim 1 security mechanism limitation, correct?

MR. RODRIGUES: Objection to form.

THE WITNESS: Sorry. I'm clearly not understanding something, because I feel like I've answered that -- if all you're worried about is -- is eavesdropping, then, yes, encryption would be a security mechanism that would prevent eavesdropping.

BY MR. OKANO:

Q. Yeah, what I'm asking is the next step which is then -- so encryption alone would satisfy the security mechanism of Claim 1; is that correct?

MR. RODRIGUES: Objection to form.

THE WITNESS: If the application that you're applying Claim 1 to was just worried about eavesdropping, then, yes, that would satisfy.

Ex. 1076, at 157:20-158:19

Reply at 3

50

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 3: *Jacobsen* in view of *Say*

Patent Owner

previously discussed, requiring additional power for needless encryption of short range signals would detract from Jacobsen's communications capabilities. Ex. 2026, ¶109.

POR at 44

Jacobsen does not identify any need to encrypt the sensor data or GPS location data of a single soldier that is communication between the wrist unit and the soldier unit mounted on the soldier. *Id.* Indeed, why would Jacobsen have such a already be able to determine the captured soldier's location and physiological condition without having to resort to intercepting data between the wrist unit and soldier unit? *Id.*

POR at 44-45

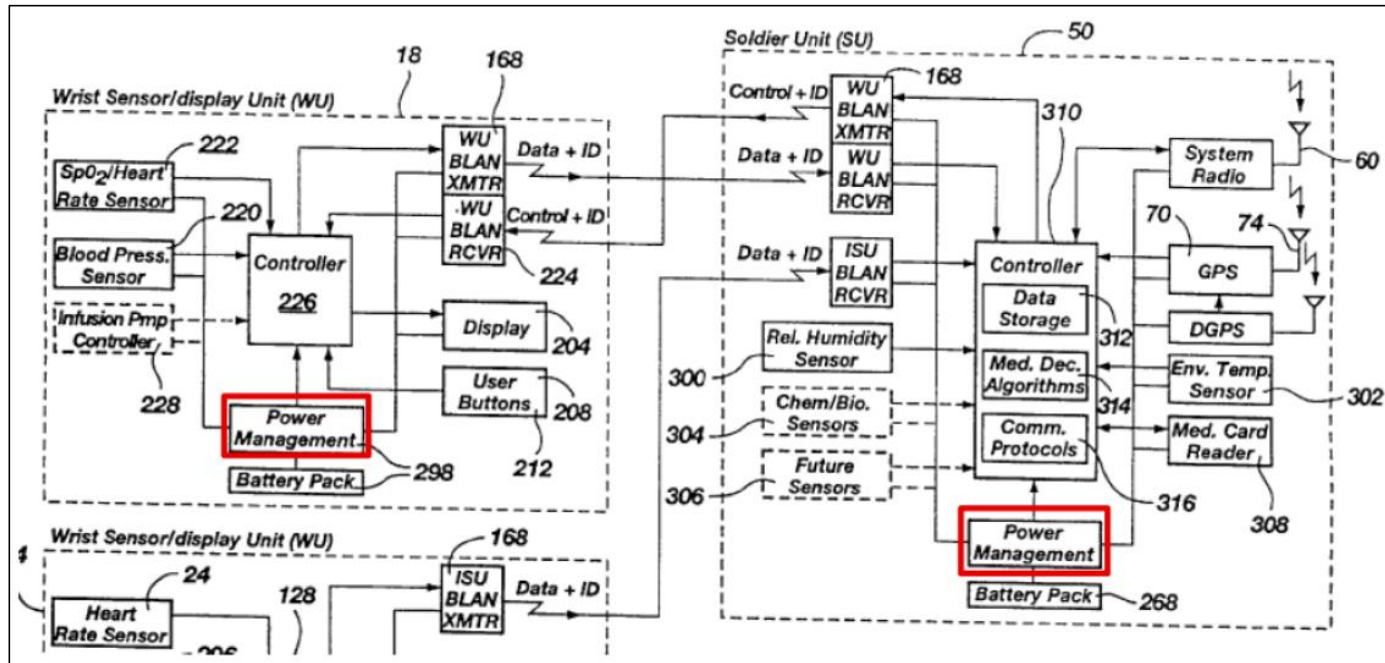
POR at 42-46

51

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 3: *Jacobsen* in view of *Say*

Jacobsen



Ex. 1005 at Fig. 4A (cropped, annotated in Reply at 22)

Reply at 20-23

52

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 3: *Jacobsen* in view of *Say*

Dr. Martin

Q. So you would agree that *Jacobsen* discloses that communications between the soldier unit 50 and the wrist sensor/display unit, could include information about the location of other soldiers, correct?

A. Yes. That's correct. It says here that it could – it could have the position or physiological status of the other soldiers.

Q. So if a soldier were captured, you would agree it would be important to prevent an enemy combatant from learning the location of other soldiers, right?

MR. RODRIGUES: Objection to form.

THE WITNESS: Yes. It would be important to not give away the position of other soldiers.

Ex. 1076 at 178:24-179:17

Jacobsen

Referring now to FIG. 3, there is shown a perspective view of the wrist sensor/display unit 18 shown in FIG. 1. The wrist sensor/display unit 18 includes a body 200 with a display screen 204 contained therein. Typically the display screen 204 will be an LCD screen, although other types of displays may be used. The display screen 204 is used to display information regarding time and geolocation, and could even be used to communicate instructions to a soldier regarding his physiological status, or the position or physiological status of other soldiers. A pair of control buttons 208 and 212 are provided to enable the soldier to chose what information is displayed, and to control the LCD illumination when necessary.

Ex. 1005 at 9:21-32

Reply at 21-23; Petition at 10; Ex. 1002 ¶¶ 55, 105-109

53

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Agenda

- Security Mechanism
 - Use of passwords govern information transmitted
 - Use of encryption govern information transmitted
- *Jacobsen* and *Say* (alone or in combination) discloses and/or suggests the claimed “security mechanism” under any reasonable interpretation/construction
 - *Jacobsen*
 - *Say*
- **Dependent claims**
 - **Ground 4: Claim 13 (BLUETOOTH)-*Jacobsen* in view of *Say* and *Quy***
 - Claims 24-25 (GPS)
 - Claim 26 (powered-down to powered-up state)
 - Claims 15-16, 22 (central communications base station / Internet)
 - Claim 14 (data I/O ports)

Ground 4: Claim 13 Obvious Over *Jacobsen, Say, and Quy*

'233 Patent: Claim 13

13. The system of claim 1, wherein the short-range wireless communications further comprises BLUETOOTH technology.

Ex. 1001, Claim 13

Petition

Given the disclosure of *Jacobsen, Say, and Quy*, and the knowledge of a POSITA, a POSITA would have been motivated to configure the combined *Jacobsen-Say* system to use Bluetooth technology to provide short-range wireless communications between the wrist sensor/display unit 18 and soldier unit 50.

KSR, 550 U.S. at 415-21; Ex. 1002, ¶113.

Petition at 72-73; Ex. 1002 ¶ 113

Quy

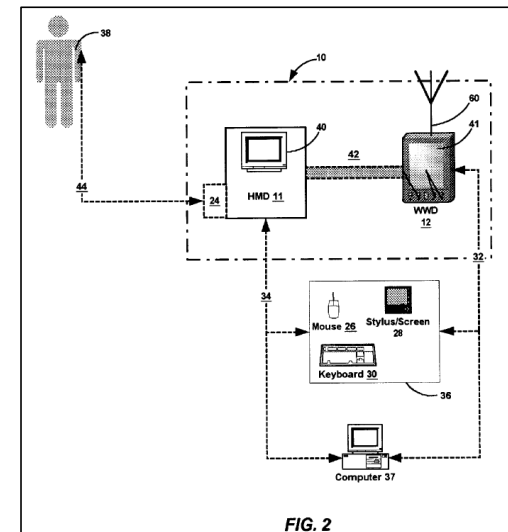


FIG. 2

Ex. 1007 at Fig. 2

Petition at 13-14, 71-75; Reply at 24; Ex. 1002 ¶¶ 113

55

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 4: Claim 13 Obvious Over *Jacobsen, Say, and Quy*

BLUETOOTH: Known Low Power Standard

To find and connect different BLUETOOTH™ units and form an ad-hoc network is not trivial. BLUETOOTH™ units do not broadcast information when they are in standby. Instead, they periodically scan the spectrum for a very short duration. The low-duty cycle scan is important to keep power consumption to a minimum. By default, a BLUETOOTH™ device scans one hop channel for about 11 ms every 1.28 seconds. Therefore, every 1.28 seconds a different hop channel is selected and scanned. The interval of 1.28 seconds can be increased up to 3.84 seconds in very low-power devices. This means that during 3.84 second intervals, the unit is in a sleep mode and cannot be reached by other BLUETOOTH™ units. Since the BLUETOOTH™ units do not routinely broadcast signals, another mechanism has been implemented to discover which units are in range. In this

Ex. 1079, 5:20-32

In a preferred implementation of the multiplexing mode, if an IEEE 802.11 packet must be transmitted, all Bluetooth data connections are placed in the so-called PARK mode. The interoperability device 106 will issue one HLC_Park_Mode primitive per active ACL (Asynchronous Connectionless data) connection to the Bluetooth transceiver, to put all ACL connections in PARK mode. The PARK mode of the Bluetooth radio system will be familiar to one skilled in the art. In this way, the Bluetooth radio system is deactivated whilst an IEEE 802.11 transmission takes place.

Ex. 1080, 7:64-8:6

demands. POR at 47-48. This is so despite the fact that Bluetooth may have been a “comparatively” lower power standard at the time. Patent Owner and Dr. Martin’s

Sur-Reply at 20

Reply at 24; Ex. 1079, 5:20-32; Ex. 1080, 7:64-8:6; Sur-Reply at 20

56

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 4: Claim 13 Obvious Over *Jacobsen, Say, and Quy*

Jacobsen: Civilian Medical Applications

Jacobsen

By continually monitoring the location and status of the soldiers, significant decreases in casualty rates can be achieved. Additionally, the technology used in the present invention can be modified slightly to maintain high levels of care in civilian medical applications while significantly decreasing the costs.

Ex. 1005 at 5:1-6

Dr. Martin

Q. So you would agree that Jacobsen's system is not limited to combat environments only?
MR. RODRIGUES: Objection to form.
THE WITNESS: Yes, I would agree with that. He describes these medical applications.

Ex. 1076, 174:2-9

Ex. 1005 at 1:8-14, 2:25-30, 2:37-39, 5:1-6; Reply at 24

57

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Agenda

- Security Mechanism
 - Use of passwords govern information transmitted
 - Use of encryption govern information transmitted
- *Jacobsen* and *Say* (alone or in combination) discloses and/or suggests the claimed “security mechanism” under any reasonable interpretation/construction
 - *Jacobsen*
 - *Say*
- **Dependent claims**
 - Claim 13 (BLUETOOTH)
 - **Ground 5: Claims 24-25 (GPS)-*Jacobsen* in view of *Say* and *Geva***
 - Claim 26 (powered-down to powered-up state)
 - Claims 15-16, 22 (central communications base station / Internet)
 - Claim 14 (data I/O ports)

Ground 5: Claims 24-25 Obvious over *Jacobsen, Say, and Geva*

'233 Patent: Claims 24-25

24. The system of claim **1**, wherein the first personal device further comprises a location determination module that determines the geographical location of the first personal device.

25. The system of claim **24**, wherein the location determination module further comprises a GPS receiver.

Ex. 1001 at Claims 24-25

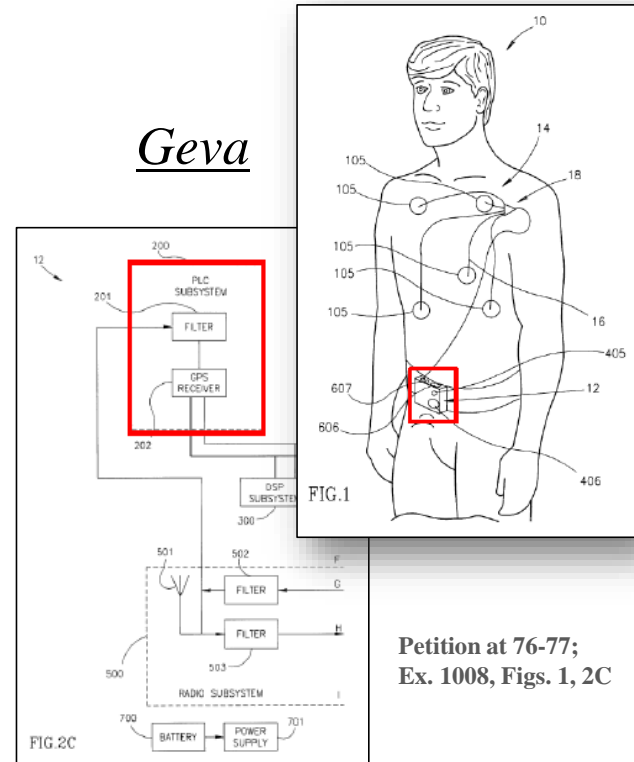
Ground 5: Claims 24-25 Obvious over *Jacobsen, Say, and Geva*

Petition

Given the disclosures of *Jacobsen, Say, and Geva*, and the knowledge of a POSITA, a POSITA would have been motivated to configure the wrist sensor/display unit 18 (“first personal device”) in the combined *Jacobsen- Say* system to further include a module for determining the location of the wrist sensor/display unit 18 (and thus user) similar to the features disclosed by *Geva*.
Ex. 1002, ¶115; *KSR*, 550 U.S. at 415-21.

Petition at 77

Geva



Petition at 76-77;
Ex. 1008, Figs. 1, 2C

Petition at 14-15, 75-82; Ex. 1002 ¶¶ 115-116; Reply at 25-26

60

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 5: Claims 24-25 Obvious over *Jacobsen, Say, and Geva*

Petition

Ex. 1005, FIGS. 1, 4, 7:24-39, 9:58-10:3, 18:8-15. So, the proposed combination would have merely involved using similar types of GPS components in another or different device (e.g., wrist sensor/display unit 18 and the vest/harness, or wrist sensor/display unit 18 alone) in *Jacobsen*'s system. Ex. 1002, ¶115. A POSITA would not have been deterred from implementing such a configuration despite the existing use of GPS on the vest/harness because the vest/harness may be separated from the soldier, whereas the wrist sensor/display unit 18 may stay with the soldier. *Id.* Indeed, Figure 1 above illustrates this separation. *Id.*

Petition at 79

Jacobsen

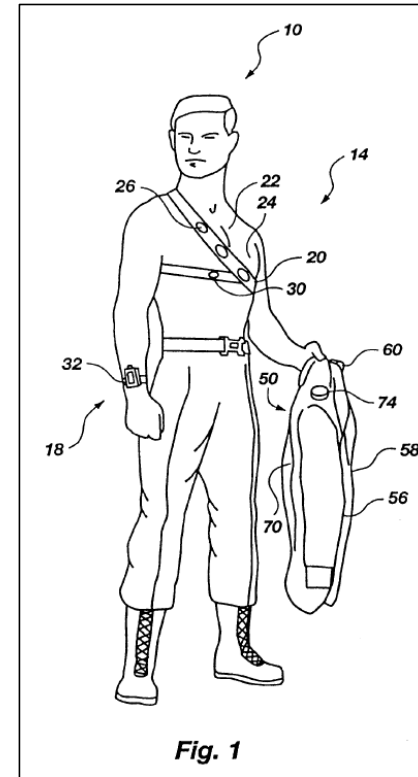


Exhibit 1005, FIG. 1

Petition at 14-15, 75-82; Ex. 1002 ¶¶ 115-116; Reply at 25-26

61

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Agenda

- Security Mechanism
 - Use of passwords govern information transmitted
 - Use of encryption govern information transmitted
- *Jacobsen* and *Say* (alone or in combination) discloses and/or suggests the claimed “security mechanism” under any reasonable interpretation/construction
 - *Jacobsen*
 - *Say*
- **Dependent claims**
 - Ground 4: Claim 13 (BLUETOOTH)
 - Claims 24-25 (GPS)
 - **Ground 6: Claim 26 (powered-down to powered-up state)- *Jacobsen, Say, Reber***
 - Claims 15-16, 22 (central communications base station / Internet)
 - Claim 14 (data I/O ports)

Ground 6: Claim 26 Obvious over *Jacobsen, Say, and Reber*

'233 Patent: Claim 26

26. The system of claim 1, wherein the bi-directional communications module has a powered-down state and a powered-up state, and further comprising a means for signaling the bi-directional communications module to transition from the powered-down state to the powered-up state.

Ex. 1001 at Claim 26

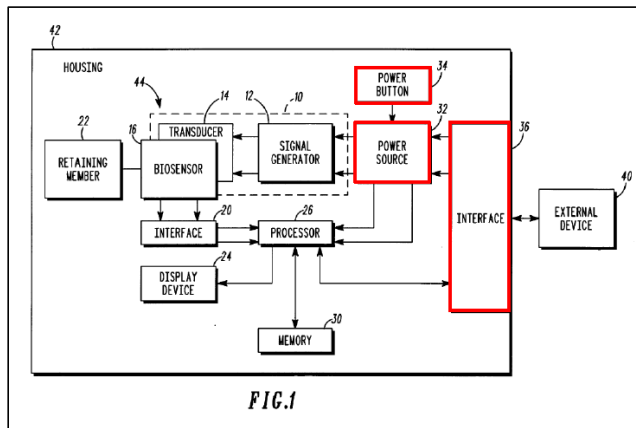
Ground 6: Claim 26 Obvious over *Jacobsen, Say, and Reber*

Petition

Given the disclosure of *Jacobsen, Say, and Reber*, and the knowledge of a POSITA, a POSITA would have been motivated to modify the combined *Jacobsen-Say* system to further include a power control mechanism (e.g., such as a button or similar mechanism) that would, when activated (e.g., pressed) enable *Jacobsen's* wrist sensor/display unit 18, including to its "communications mechanism 224," to transition from a powered-down state to a powered-up state. *KSR*, 550 U.S. at 415-21; Ex. 1002, ¶118. The powered-down state of the

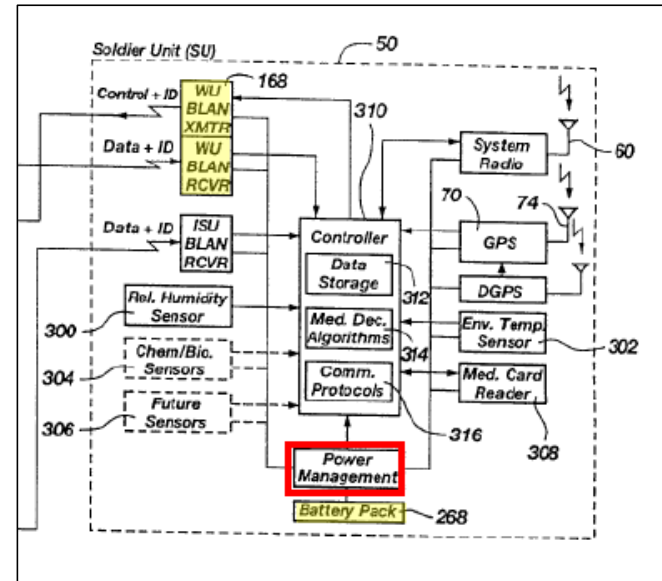
Reber

Petition at 85



Ex. 1020, Fig. 1

Jacobsen



Petition at 87; Ex. 1005, Fig. 4 (excerpted and annotated)

Petition at 15-16,, 82-90; Ex. 1002 ¶ 118; Reply at 26-27

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Agenda

- Security Mechanism
 - Use of passwords govern information transmitted
 - Use of encryption govern information transmitted
- *Jacobsen* and *Say* (alone or in combination) discloses and/or suggests the claimed “security mechanism” under any reasonable interpretation/construction
 - *Jacobsen*
 - *Say*
- **Dependent claims**
 - Ground 4: Claim 13 (BLUETOOTH)
 - Claims 24-25 (GPS)
 - Claim 26 (powered-down to powered-up state)
 - **Ground 7: Claims 15-16, 22 (central base station / Internet)- *Say* in view of *Gabai***
 - Claim 14 (data I/O ports)

Ground 7: Claims 15-16, 22 Obvious over *Say* in view of *Gabai*

'233 Patent: Claims 15, 16, 22

15. The system of claim 1, further comprising a central communications base station communicating with the first personal device using short-range wireless communications.

16. The system of claim 15, wherein the short-range wireless communications is selected from the group consisting of HomeRF™, BLUETOOTH, and wireless LAN.

Ex. 1001 at Claims 15-16

22. The system of claim 15, wherein the central communications base station further comprises a connection to the Internet.

Ex. 1001 at Claim 22

Ground 7: Claims 15-16, 22 Obvious over *Say* in view of *Gabai*

Petition

Given the disclosure of *Say* and *Gabai*, and the knowledge of a POSITA, a POSITA would have been motivated to configure *Say*'s system such that *Say*'s sensor control unit 44 engaged in short-range communications with a base station providing an Internet connection, such as the "radio base station 62" disclosed in *Gabai*. *KSR*, 550 U.S. at 415-21; Ex. 1002, ¶120.

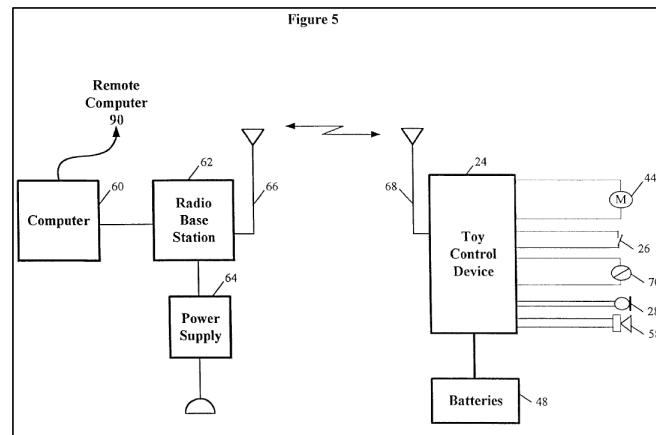
Petition at 94

For the same reasons discussed above for claim 15 (relevant and incorporated here), the combination of *Say* and *Gabai* discloses and/or suggests the system of claim 15, wherein the central communication base station further comprises a connection to the Internet. *See* section X.G.1; Ex. 1002, ¶22. Indeed, as discussed, the combined *Say-Gabai* system would have included *Say*'s sensor control unit 44 communicating with a central communications base station providing an Internet connection (such as *Gabai*'s base station 62, which provides a connection to the Internet through "computer 60." Ex. 1002, ¶122; Ex. 1040,

Petition at 98

Petition at 91-99; Ex. 1002 ¶¶ 120-122; Reply at 27-28

Gabai



Ex. 1040 at Fig. 5

Ground 7: Claims 15-16, 22 Obvious over *Say* in view of *Gabai*

Gabai

The present invention relates to computer systems and methods generally and more particularly to development of interactive constructs, to techniques for teaching such development, and to verbally interactive toys.

Ex. 1040 at 1:8-9

Petitioner's Expert, Dr. Paradiso

THE WITNESS: *Gabai* is an example of -- of many devices at the time that communicated with a base station. It's a -- it's a device that had wireless sensors in it. *Gabai* is full of sensors. It's really a wireless sensor platform.

At the media lab, we built such toys at the time and POSITAs were developing them. This is probably around the time Furby was developed, and others; but people were thinking about wireless connections from toys. Companies used to visit us at the media lab all the time to talk about this in those days.

Gabai is an example of a device. It happens to be a toy, but there are many classes and devices like this that has sensors and has a -- a wireless connection to a -- a base station, a bidirectional wireless connection to a base station which is connected to the Internet, very clearly disclosed.

Ex. 2030 at 100:3-19

Q If a POSITA in 2000 was working in the field of wireless communications as related to the '233 patent, would they more likely look to a toy like a Furby or would they more likely look to something closer to the other references that you've discussed?

A You have to remember that this was the beginning of the Internet of things. It was a very exciting time and lots of things would start to incorporate sensors and -- and put them on networks.

And I think a POSITA at the time -- if you look at the field of -- of the invention, wireless communications, you know, we have, of course, a sensor device. This is clearly in -- in the family; and, you know, I can see where a POSITA certainly would -- would look at this.

Ex. 2030 at 101:4-18

Petition at 91-99; Ex. 1002 ¶¶ 120-122; Reply at 27-28

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Agenda

- Security Mechanism
 - Use of passwords govern information transmitted
 - Use of encryption govern information transmitted
- *Jacobsen* and *Say* (alone or in combination) discloses and/or suggests the claimed “security mechanism” under any reasonable interpretation/construction
 - *Jacobsen*
 - *Say*
- **Dependent claims**
 - Ground 4: Claim 13 (BLUETOOTH)
 - Claims 24-25 (GPS)
 - Claim 26 (powered-down to powered-up state)
 - Claims 15-16, 22 (central base station / Internet)
 - **Grounds 1-3: Claim 14 (data I/O ports)**

Grounds 1-3: Claim 14 Disclosed By *Jacobsen and Say*

'233 Patent: Claim 14

14. The system of claim 1, wherein the first personal device further comprises a data input/output port, the second device further comprises a data input/output port, and wherein the second device communicates with the first personal device using the data input/output ports.

Ex. 1001 at Claim 14

Grounds 1-3: Claim 14 Disclosed By *Jacobsen and Say*

Institution Decision

However, the '233 patent draws a distinction between local area wireless communication and communication via data ports, as illustrated in Figures 4A and 4C, and explained as follows:

Optionally, [the personal medical device] has connections to data input/output ports 160. Data I/O ports 160 may include, but are not limited to: serial, parallel, USB, etc.

....

Optionally, [the personal medical device] includes a wireless communications module In one embodiment the wireless communications module includes systems and standards for Local Area Wireless 330.

....

FIG. 4A depicts one embodiment of the present system. [The personal medical device] communicates to Personal Wireless Device (PWD) 500 with local area wireless (LAW) 330.

....

FIG. 4C depicts another embodiment of the present system. [The personal medical device] communicates through data port 160 to Medical Device Interface (MDI) 600.

Ex. 1001, Figs. 4A, 4C, 3:47-49, 3:54-57, 4:14-16, 4:25-27

Institution Decision at 38-39; Reply at 6-10, 23

71

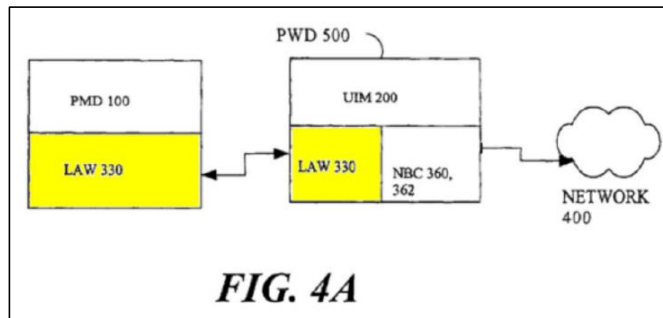
DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Grounds 1-3: Claim 14 Disclosed By *Jacobsen and Say*

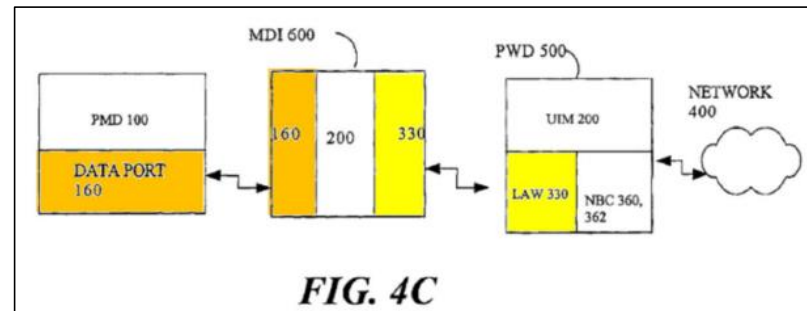
'233 Patent

14. The system of claim 1, wherein the first personal device further comprises a data input/output port, the second device further comprises a data input/output port, and wherein the second device communicates with the first personal device using the data input/output ports.

Ex. 1001 at Claim 14



Ex. 1001 at Fig. 4A (annotated in Reply at 8)



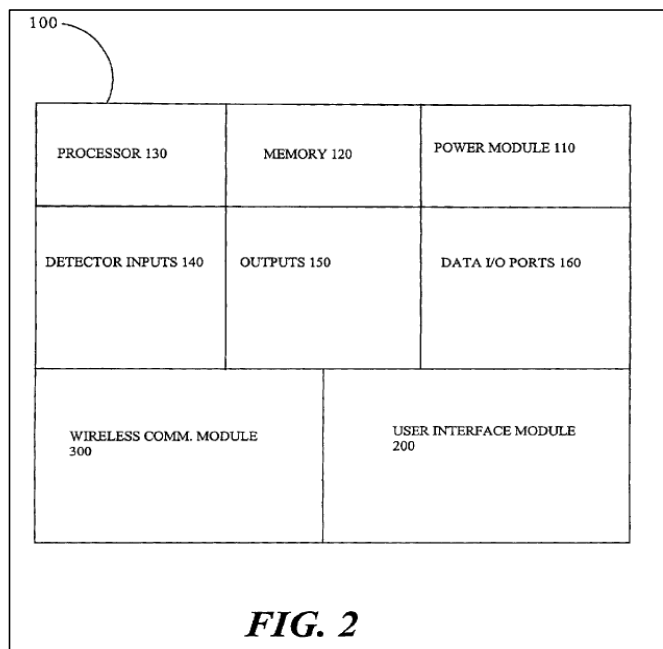
Ex. 1001 at Fig. 4C (annotated in Reply at 8)

Institution Decision at 38-39; Reply at 6-10, 23

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Grounds 1-3: Claim 14 Disclosed By *Jacobsen and Say*

'233 Patent



Ex. 1001 at FIG. 2

FIG. 2 is a block diagram depicting the components of one embodiment of a PMD 100. In one embodiment, the

Ex. 1001 at 3:18-19

Optionally, PMD 100 has connections to data input/output ports 160. Data I/O ports 160 may include, but are not limited to: serial, parallel, USB, etc.

Ex. 1001 at 3:47-49

Optionally, PMD 100 includes a wireless communications module 300. In one embodiment the wireless communications module includes systems and standards for Local Area Wireless 330. In one embodiment the wireless communications are designed to be Network Based Communications (NBC) 360.

Ex. 1001 at 3:54-57

Institution Decision at 38-39; Reply at 6-10, 23

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Grounds 1-3: Claim 14 Disclosed By *Jacobsen and Say*

'233 Patent

14. The system of claim 1, wherein the first personal device further comprises a data input/output port, the second device further comprises a data input/output port, and wherein the second device communicates with the first personal device using the data input/output ports.

Ex. 1001 at Claim 14

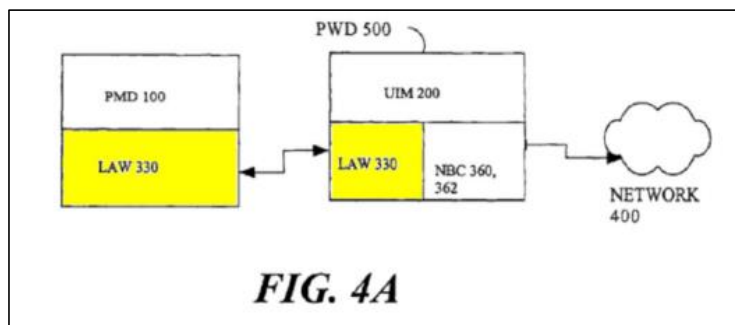


FIG. 4A

Ex. 1001 at Fig. 4A (annotated in Reply at 8)

FIG. 4A depicts one embodiment of the present system. PMD 100 communicates to Personal Wireless Device (PWD) 500 with local area wireless (LAW) 330. PWD 500 includes a LAW 330 compatible with LAW 330 in PMD 100. In one embodiment, PWD 500 includes a UIM 200. PWD 500 includes network based communications (NBC) 360. NBC 360 communicates information received from LAW 330 to long-range bi-directional network 400.

Ex. 1001 at 4:14-21

Institution Decision at 38-39; Reply at 6-10, 23

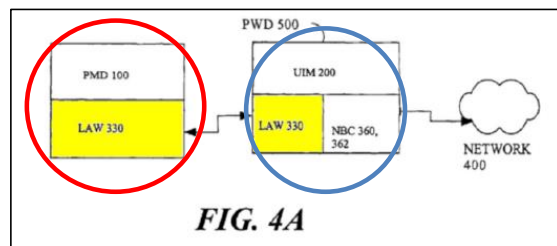
DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Grounds 1-3: Claim 14 Disclosed By *Jacobsen and Say*

'233 Patent

First Personal Device

Dr. Martin



Second Device

Dr. Martin

Ex. 1001 at Fig. 4A (annotated in Reply at 8)

Q. Sure. It's your opinion that -- I guess you would agree that -- I'm sorry. It's your opinion that this box on the left, PMD 100 and LAW 330 is an example of Claim 1's first personal device -- correct? -- in Figure 4A?

A. The personal medical device 100 is the personal medical device, and then the wireless -- then the LAW 330 in that diagram provides the wireless capability.

Q. And so it's your opinion that the PMD -- oh, sorry. Looking at your answer, when you say "personal medical device," are you talking about this Claim 1's first personal device, or are you talking about just a general medical device?

A. I'm talking about Claim 1's first personal device.

Ex. 1076 at 227:17-228:9

Q. And, in your opinion, is PWD 500 an example of a second device recited by Claim 1?

A. Yes. That's correct.

Q. And the LAW 333 of the second device, PWD 500 communicates with the LAW 330 of the first personal device in Figure 4A as represented by those bi-directional arrows?

A. Yes. That's correct. Except you said LAW 333, but I think you meant 330.

Q. 330, that's correct.

A. Yep.

Ex. 1076 at 229:1-13

Institution Decision at 38-39; Reply at 6-10, 23; Ex. 1076, 226:14-229:13

75

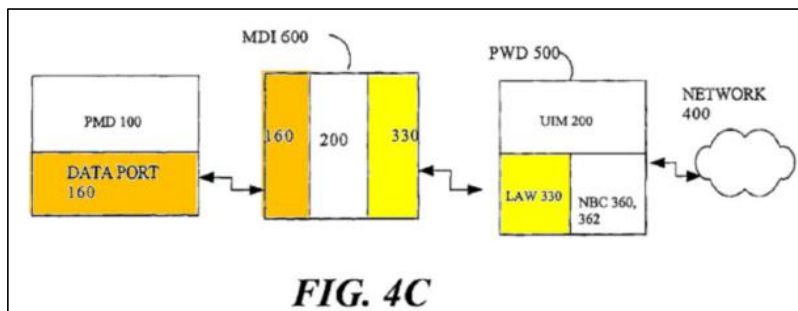
DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Grounds 1-3: Claim 14 Disclosed By *Jacobsen and Say*

'233 Patent

14. The system of claim 1, wherein the first personal device further comprises a data input/output port, the second device further comprises a data input/output port, and wherein the second device communicates with the first personal device using the data input/output ports.

Ex. 1001 at Claim 14



Ex. 1001 at Fig. 4C (annotated in Reply at 8)

FIG. 4C depicts another embodiment of the present system. PMD 100 communicates through data port 160 to Medical Device Interface (MDI) 600. In one embodiment, MDI 600 includes a UIM 200. In this embodiment, MDI 600 includes a LAW 330 and communicates to PWD 500 through LAW 330. PWD 500 includes a LAW 330 compatible with MDI 600. Preferably, PWD 500 includes UIM 200. Preferably, PWD 500 includes NBC 360 and communicates to long-range bi-directional 400 through NBC 360.

Ex. 1001 at 4:25-33

Institution Decision at 38-39; Reply at 6-10, 23

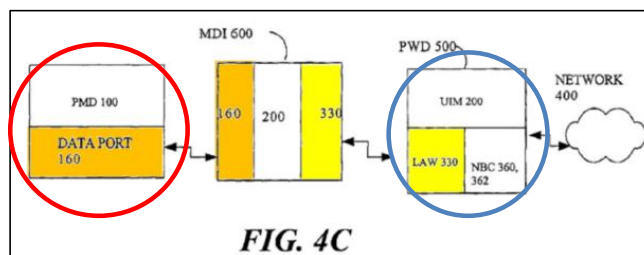
76

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Grounds 1-3: Claim 14 Disclosed By *Jacobsen and Say*

'233 Patent

First Personal Device



Second Device

Dr. Martin

Ex. 1001 at Fig. 4C (annotated in Reply at 8)

Dr. Martin

In Figure C, in your opinion, what is -- I'm sorry. In Figure 4C, in your opinion, what is Claim 1's first personal device?

MR. RODRIGUES: Objection to form.

THE WITNESS: The personal medical device 100.

BY MR. OKANO:

Q. And that is in Figure 4C, the box on the far left?

A. Yes. That's correct.

Ex. 1076 at 231:15-232:1

A. Yes. That's correct.

Q. In Figure 4C, in your opinion, what is the second device recited by Claim 1?

A. It's the -- the PWD 500.

Q. And so the second device in Figure 4C is the box on the right between the network cloud 400 and the MDI 600?

A. Yes. That's correct.

Ex. 1076 232:2-9


Institution Decision at 38-39; Reply at 6-10, 23; Ex. 1076, at 231:15-232:9

77

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Grounds 1-3: Claim 14 Disclosed By *Jacobsen and Say*

Patent Owner's Infringement Contentions For Claims 1 and 14

		U.S. Patent No. 7,088,233	Fitbit Versa
<p>Claim 14</p> <p>The system of claim 1, wherein the first personal device further comprises a data input/output port, the second device further comprises a data input/output port, and wherein the second device communicates with the first personal device using the data input/output ports.</p>	<p>The Accused Product provides a system with a port (a port for wireless communications), wireless communications), and wherein the data input/output ports:</p> <p>Wireless Technology</p> <p>Versa contains a Bluetooth 4.0 radio and contains an NFC chip.</p> <p>PNA-FB0001174</p> <p>Sync data to your Fitbit account</p> <p>Regularly sync Versa with the Fitbit app. The dashboard is where you'll track your progress, see exercise history, track your sleep patterns, log food and water, identify trends, participate in challenges, and much more. We recommend syncing at least once a day.</p> <p>The Fitbit app uses Bluetooth Low Energy technology to sync data with Versa and to update apps installed on your watch.</p> <p>Each time you open the Fitbit app, Versa syncs automatically when it's nearby. Versa also syncs with the app periodically if All-Day Sync is on. To turn on this feature:</p> <p>PNA-FB0001113-1114</p>	<p>Claim 1</p> <p>A bi-directional wireless communication system comprising:</p>	<p>The Accused Product provides a bi-directional wireless communication system as claimed:</p> 
	<p>(v) a short-range bi-directional wireless communications module:</p> <p>The first personal device of the system provided by the Accused Product comprises a short-range bi-directional wireless communications module:</p> <p>Sync data to your Fitbit account</p> <p>Regularly sync Versa with the Fitbit app to transfer data to your dashboard. The dashboard is where you'll track your progress, see exercise history, track your sleep patterns, log food and water, identify trends, participate in challenges, and much more. We recommend syncing at least once a day.</p> <p>The Fitbit app uses Bluetooth Low Energy technology to sync data with Versa and to update apps installed on your watch.</p>	<p>Ex. 1075 at 10, 17, 39</p>	

Institution Decision at 38-39; Reply at 6-10, 23

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Grounds 1-3: Claim 14 Disclosed By *Jacobsen and Say*

Patent Owner Drops Claim 14 After Dr. Martin Deposition

IPR2020-00783
Patent No. 7,088,233 B2

REMOTE EXAMINATION of THOMAS MARTIN, M.D.

TAKEN ON
MONDAY, APRIL 5, 2021

(Whereupon, a recess was taken at 6:30 p.m.)
MR. OKANO: Back on the record. No further questions. Pass the witness.
MR. RODRIGUES: We have no questions at this time. Philips has no questions at this time.
(Time noted: 6:36 p.m.)

Ex. 1076 at 1, 280

Ruben,

To be clear, your April 5 email was the first time Fitbit received notice that Philips is no longer asserting Claim 14 of the '233 Patent

Best,
Karim

Karim Z. Oussayef
DESMARAIS LLP
230 Park Avenue
New York, NY 10169
T: (212) 351-3427 | F: (212) 351-3401

From: RRodrigues@foley.com <RRodrigues@foley.com>
Sent: Monday, April 5, 2021 8:24 PM
To: Karim Oussayef <KOussayef@desmaraisllp.com>; Okano, David <davidokano@paulhastings.com>
Cc: BOSTFPhilipsFitbit@foley.com; Philips - Fitbit <Philips-Fitbit@paulhastings.com>; Fitbit Philips DC Service <FitbitPhilipsDCService@desmaraisllp.com>
Subject: [Ext] Philips v. Fitbit (D. Mass) - Claim 14 of the '233 Patent

****EXTERNAL EMAIL** This email originated from outside the company. Do not click on any link unless you recognize the sender and have confidence the content is safe.**

Hi Karim & David,

I was under the impression that we had formally withdrawn Claim 14 of the '233 Patent in the District of Massachusetts action as we did in the Central District of California action against Garmin. To clarify the record and for avoidance of doubt, I wanted to clarify that Philips no longer asserts Claim 14 of the '233 Patent against the Fitbit accused products in this action.

Regards,
-Ruben

Ruben J. Rodrigues
Foley & Lardner LLP
111 Huntington Ave, Suite 2600

Ex. 1077

Institution Decision at 38-39; Reply at 6-10, 23

79

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE