

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte SCOTT SINA ABEDI, ROGER KENNETH ABRAMS, RYAN
CHARLES CATHERMAN, JAMES PATRICK HOFF, and JAMES
STEPHEN RUTLEDGE

Appeal 2008-1726
Application 11/018,274
Technology Center 2600

Decided: September 19, 2008

Before MAHSHID D. SAADAT, JOHN A. JEFFERY, and KARL D.
EASTHOM, *Administrative Patent Judges*.

EASTHOM, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants appeal under 35 U.S.C. § 134 from a final rejection of claims 1-8. (App. Br. 1). No other claims are pending. (Final Office Action, mailed Nov. 30, 2006). We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

STATEMENT OF THE CASE

Appellants' invention is related to a data processing method and system for determining whether a wireless shopping device is within a secured zone and has been subjected to unauthorized data alteration. (Spec. ¶¶ 0002, 0004, 0015, 0016). The system detection of such data alteration prevents unauthorized stealing of confidential information within the security zone (Spec. ¶ 0019). If the system determines that the wireless device has not been subjected to unauthorized alteration, the system device allows the device to continue its normal shopping functions; otherwise, the device activates an alarm or is disabled. (Spec. ¶¶ 0034-38).

Claim 1 is representative of the claims on appeal, and it reads as follows:

1. A system for securing data, comprising:
 - a boundary sensor defining a secured zone;
 - at least one wireless device storing data; and
 - a data processing system, coupled to said boundary sensor and said wireless device, wherein said data processing system includes:
 - a boundary controller for determining whether said at least one wireless device has entered said secured zone;
 - if said at least one wireless device has entered said secured zone:
 - a security controller queries said at least one wireless device to determine whether said data has been

subjected to an unauthorized alteration; and

in response to determining said data has not been subjected to an unauthorized alteration, said security controller enables said wireless device for operating within said secured zone.

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Zicker	US 5,046,082	Sept. 3, 1991
Vodin	US 2003/0071734 A1	Apr. 17, 2003
Schlieffers	US 2004/0111320 A1	Jun. 10, 2004
Muthuswamy	US 2004/0137893 A1	July 15, 2004

Claims 1- 3 and 5-8 stand rejected under 35 U.S.C. § 103(a) based upon the collective teachings of Schlieffers, Vodin, and Zicker.¹

Claim 4 stands rejected under 35 U.S.C. § 103(a) based upon the collective teachings of Schlieffers, Zicker, Vodin and Muthuswamy.

ISSUE

Appellants dispute the Examiner's determination that the collective teachings of Schlieffers, Vodin and Zicker teach "*in response to determining said data has not been subjected to an unauthorized alteration, said security controller enables said wireless device for operation within said secured zone,*" as recited in claim 1. (App. Br. 5-6, emphasis by Appellants). Independent claims 5 and 7 recite similar limitations.

¹ Appellants incorrectly included claim 4 as rejected within this group of claims. (App. Br. 4).

Appellants do not present separate arguments for the claims. Thus, the issue before us is whether the collective teachings of the art noted above teach or render obvious the determining/enabling function as set forth in representative claim 1.

PRINCIPLES OF LAW

Appellants have the burden on appeal to the Board to demonstrate error in the Examiner's position. *See In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006) ("On appeal to the Board, an applicant can overcome a rejection [under § 103] by showing insufficient evidence of *prima facie* obviousness or by rebutting the *prima facie* case with evidence of secondary indicia of nonobviousness.") (quoting *In re Rouffet*, 149 F.3d 1350, 1355 (Fed. Cir. 1998)). During examination, the Examiner bears the initial burden of presenting a *prima facie* case. *In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992).

The Examiner's articulated reasoning in the rejection must possess a rational underpinning to support the legal conclusion of obviousness. *In re Kahn*, 441 F.3d at 988.

ANALYSIS

Claims 1-3 and 5-8

Regarding the disputed limitation of claim 1 noted above, Appellants summarize their position as follows:

In view of the disparate teachings of *Zicker and Vodin*, nothing in the combination of *Schlieffers, Zicker, and Vodin* teaches or suggests *any* sort of causative relationship between the determination that the data has not been subjected to an unauthorized alteration *and* enabling the wireless device for

operation within a wireless zone. In *Zicker*, in response to the detection of an unauthorized alteration, the system dials a phone number to contact an administration system, as opposed to enabling a wireless device for operation within a wireless zone. In *Vodin*, the system enables a wireless device upon entry into a secured area by passing through an electronic gateway, but not in response to detection of no unauthorized alteration. Clearly, the combination of *Schlieffers*, *Zicker*, and *Vodin* does not teach or suggest "*in response to determining said data has not been subjected to an unauthorized alteration, said security controller enables said wireless device for operation within said secured zone,*" as recited in exemplary Claim 1.

(App. Br. 5-6).

We disagree with Appellants' characterization of *Schlieffers*, *Zicker* and *Vodin* because it fails to account for the references' collective teachings as a whole. Accordingly, we disagree with Appellants' conclusion that the collective teachings of the references fail to teach the causal relationship of enabling a wireless device in response to a determination of unauthorized data alteration.

We turn first to *Vodin*. We find that *Vodin* discloses enabling an armband sensor 1 (i.e., "wireless device") after it passes through a security zone gateway in response to determining that the armband data has not been altered. (*Vodin*, Abstract, ¶¶ 0017-0019, 0021, 0025, 0026). Appellants acknowledge in the passage quoted above that *Vodin*'s system enables the wireless device upon entry through an electronic gateway to a secured zone. In addition, within such secured zone, we find that *Vodin* discloses querying for unauthorized altered data such as data transmitted from conductivity or temperature sensors on an armband: "for example conductivity sensors 11

may detect changes in the users skin surface moisture levels and provide a redundant continuity check that the armband 1 remains in place” (§ 0017). The system also prevents data isolation rendered by an unauthorized shield placed between the armband and user’s arm (*id.*). In other words, the sensors receive and transmit an unauthorized altered set of moisture level or temperature sensor data due either to armband removal or an isolating shield.

Such sensor data, stored and monitored in the armband “CPU/logic/memory,” is transmitted to the central console 200 (i.e., “data processing system”) (Vodin, §§ 0018, 0019). Console 200 regularly queries the wireless armband device, and as long as the armband data remains within preselected states (i.e., the “security controller” implicit in the console 200 “queries said at least one wireless device to determine whether said data has been subjected to unauthorized alteration”),² the system enables the armband to perform its intended function of monitoring – i.e., the armband locking system is not deactivated, the locking system is not disabled, the alarm is not activated, and the drug is not injected (Vodin, §§ 0022, 0025-0026).

Hence, we are not persuaded by Appellants’ argument that neither Vodin, nor the collective teachings of the references, suggest enabling a wireless device in response to an unauthorized alteration of data (App. Br. 5-6). We also are not persuaded by Appellants’ related argument that the collective teachings of the references do not suggest that the unauthorized determination “causes” the wireless device to be enabled (App. Br. 4-5,

² Claim 1 does not preclude the detection of unauthorized data that has been altered prior to its being stored by the wireless device as occurs in Vodin.

Reply Br. 2). As indicated above, Vodin's system queries a wireless armband device, and thereafter causes the device to be enabled by rendering a decision not to disable it. We note that Appellants similarly disclose that Appellants' wireless device is "enabled" because the system fails to disable it (*see* App. Br. 3, *citing* Spec. ¶¶ 0036 *et seq* as supporting the enabling feature of the claim, *see also* our description above of Appellants' disclosed invention ("Statement of the Case")). Accordingly, our interpretation of the term "enabling" is consistent with Appellants' use of the term. Thus, Vodin, like Appellants, teaches a causal enablement as constituted by a decision not to disable a wireless device after the system renders a determination that no unauthorized data alteration has occurred.

We also find that Vodin's console 200 and electronic gateway described above (*see also* Appellants' quote above at page 5 of our Decision) constitute the claimed data processing system coupled to a boundary sensor, and includes the claimed boundary controller and security controller. As we indicated above, the console 200 determines if the wireless armband device has entered a secured zone, and if so, enables it, if it has not been subjected to unauthorized alteration.

Furthermore, Vodin's console 200 performs the dual functions of monitoring and control of a secured zone for boundary entry and exit and security violations due to unauthorized exiting and tampering (*see also* Fig. 5, ¶¶ 0025-0026). The system also disables and enables the wireless armband based on transmitted and monitored data, and/or activates a triggered drug release in the armband, based on such sensed data and position, and thereby includes a data processing system which comprises a

security and a boundary controller as set forth in the claim. (*See* Abstract, ¶¶ 0008, 0018-22, 0025-0027, and 0029). That is, such controllers and boundary sensors (*see e.g.* ¶ 21- RFID gateway detection, ¶ 21 – antennas and “radio gateway barriers”) are at least implicitly suggested, if not explicit, in Vodin.

We also determine, consistent with Appellants’ disclosure, (*see* Spec. ¶¶ 0020-0022, 0043, Fig. 2A), that the claimed “controllers” are met by mere software as suggested or implicit within Vodin’s console software system, or they are implicit or suggested as separate hardware components in Vodin’s system. While the Examiner’s unchallenged findings rely on Schlieffer to teach the boundary sensor, the wireless device, and the data processing system (Ans. 4), our discussion above makes it apparent that Vodin also discloses these claimed elements.

In other words, we find that Vodin not only suggests claim 1, but also anticipates claim 1. *See In re Meyer*, 599 F.2d 1026, 1031 (CCPA 1979) (noting that obviousness rejections can be based on references that happen to anticipate the claimed subject matter). Accordingly, Appellants’ arguments, based on the contention that Vodin is limited to teaching that “the system enables a wireless device upon entry into a secured area by passing through an electronic gateway” (Reply Br. 5), must fail.

Contrary to Appellants’ similar characterization of Zicker as limited to teaching dialing a phone number in response to the detection of unauthorized alteration (*id.*), we find that Zicker cumulatively teaches enabling a wireless device in response to a determination that no unauthorized data alteration occurs. That is, we find that Zicker teaches

enabling a wireless device by providing “almost no alteration in the normal outgoing call procedures” (col. 12, ll. 56-57), after the system queries a “checksum” routine to determine that no unauthorized data alteration has occurred (col. 12, ll. 25-58).³

Thus, we find that employing Vodin’s well known function of enabling, in a security zone, a wireless device determined to lack an unauthorized data alteration, with or without Zicker’s similar function of generally enabling, in any zone, a wireless device based on a determination of unauthorized data alteration, would have produced a predictable beneficial result of enhanced security in any secured zone employing a wireless communication system, such as that of either Vodin or Schlieffer.

We also find, contrary to Appellants’ assertion (Reply Br. 5), that Schlieffer’s system teaches activating an alarm if the wireless device “enter[s] or come[s] within close proximity” to the secured zone near the exits of the retail store to prevent wireless device theft (¶ 0083, emphasis added). The alarm activates if a transmitted device ID matches a stored ID within the computer monitoring/control system. On the other hand, the alarm does not activate if there is no such match, because the system infers the device is not an “in-store” device and/or otherwise belongs to the customer (*id.*). Therefore, as the Examiner generally reasoned, modifying Schlieffer’s system with Vodin’s and Zicker’s so that within such a secured zone, the system enables a wireless device if its data has not been altered in

³ On the other hand, Zicker’s wireless handset device is disabled as “UNIT BUSY” and “not available for use by the user” in process 700 if the data has been determined by the checksum algorithm to have been subjected to unauthorized alteration (col. 15, ll. 40-45, Fig. 7).

an unauthorized manner, would have enhanced security (*see* Ans. 8-9), thereby furthering Schlieffer's goal of theft prevention (*see* ¶ 0083).

In other words, as suggested by Zicker's unauthorized data detection system for enabling handsets as described above, and/or Vodin's similar system for armbands, the proposed system as modified would detect unauthorized data tampering in only the true "in-store" devices, and render those devices enabled or disabled, the latter to prevent an unauthorized ID data alteration from thwarting Schlieffer's alarm activation. After the alarm activation, the device would be disabled from its normal function as a shopping device, similar to the devices of Vodin (after activating an alarm and/or releasing an immobilizing drug dosage in response to device tampering, the armband no longer functions as a trigger releasing device – *see* discussion above, and Abstract), or Zicker (the disabled telephone can only perform "911" calls, col. 15, ll. 40-49).

On the other hand, notwithstanding an alarm activation due to sensed boundary exit encroachment of an in-store device based on an ID match, such a match determination, in combination with Zicker and Vodin, constitutes at least an indirect determination of no unauthorized tampering, as the Examiner generally reasoned (Ans. 8). As such, according to Schlieffer, the shopping device remains enabled for further shopping, and as modified by the collective teachings of the references, the modified system enables the device as set forth in the claim by rendering a decision not to disable it - based on the lack of an unauthorized ID alteration - in case for example, the shopper decides not to exit the store, and/or is browsing goods near the exit within the security zone.

Consequently, while we agree with Appellants that Schlieffer alone does not teach determining that a wireless device was subject to an unauthorized alteration because, as Appellants' assert, a plausible explanation for a lack of an ID match is that a device is not an in-store device and is thereby authorized for removal (Reply Br. 4-5), the explanation does not defeat the obviousness determination based on the collective teachings of the references as generally found by the Examiner, and as explained above. That is, an in-store device with an unauthorized altered ID or other altered data will not be authorized for removal based on the modified system as suggested by the collective teachings of the references, while a customer's device will be authorized for such removal.

In sum, Vodin either discloses or suggests all the claimed elements. Alternatively, Vodin and/or Zicker, at a minimum, suggest the disputed function in claim 1: "in response to determining said data has not been subjected to an unauthorized alteration, said security controller enables said wireless device for operating within said secured zone." As such, Appellants' arguments, based on the assertion that the references do not disclose or teach such a function (App. Br. 4-6, Reply Br. 2-4), and also those arguments based on the assertion that the references fail to support the Examiner's rationale or finding of a suggestion or motivation (App. Br. 6, Reply Br. 4-5), must fail, because the prior art directly discloses and/or teaches such a function, and its use yields the predictable beneficial result of enhanced security, as we found above.

For the reasons noted above, Appellants have failed to demonstrate error in the Examiner's rejection of independent claims 1, 5 and 7.

Appeal 2008-1726
Application 11/018,274

Therefore, we will sustain the Examiner's rejection of those claims. For the same reasons, we also will sustain the Examiner's rejection of dependent claims 2, 3, 6 and 8.

Claim 4

Appellants do not separately argue claim 4. For the reasons outlined above, we also will sustain the obviousness rejection of dependent claim 4.

CONCLUSION

The Examiner's decision rejecting claims 1-8 is affirmed

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv)(2006).

AFFIRMED

gvw

DILLON & YADELL LLP
8911 N. CAPITAL OF TEXAS HWY.
AUSTIN, TX 78759

Appeal 2008-1726
Application 11/018,274