



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/190,756	08/13/2008	Akihiko Toyoshima	50P4257.09	9420
36738	7590	02/04/2013	EXAMINER	
ROGITZ & ASSOCIATES 750 B STREET SUITE 3120 SAN DIEGO, CA 92101			TORRES, MARCOS L	
			ART UNIT	PAPER NUMBER
			2645	
			NOTIFICATION DATE	DELIVERY MODE
			02/04/2013	ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

John@rogitz.com  
Jeanne@rogitz.com  
Jennifer@rogitz.com

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

*Ex parte* AKIHIKO TOYOSHIMA

---

Appeal 2010-008513  
Application 12/190,756  
Technology Center 2600

---

Before SCOTT R. BOALICK, BARBARA A. BENOIT,  
and DAVID C. McKONE, *Administrative Patent Judges*.

McKONE, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellant appeals under 35 U.S.C. § 134(a) from a Final Rejection of claims 26-45, which constitute all the claims pending in this application.

*See* App. Br. 2.<sup>1</sup> Claims 1-25 are cancelled. *See id.* We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

---

<sup>1</sup> Throughout this opinion, we refer to the Appeal Brief filed February 16, 2010 (“App. Br.”), the Examiner’s Answer mailed May 12, 2010 (“Ans.”), and the Reply Brief filed May 17, 2010 (“Reply Br.”).

STATEMENT OF THE CASE

Appellant's invention relates to security systems for wireless devices. *See Spec. 3:1-13.* Claim 26, which is illustrative of the invention, reads as follows:

26. A system for rendering difficult the use of a wireless module with an unauthorized peripheral device, comprising:

at least one wireless module including a wireless transceiver, the wireless module including at least one security code; and

at least one peripheral device communicating with the wireless module only if a human user provides the security code to the peripheral device and the security code provided to the peripheral device matches the security code provided to the wireless module, the peripheral device being a portable computing device;

wherein the wireless module is automatically deactivated in the event that the wireless module is lost and/or stolen, wherein when the module is deactivated no access to the module by the peripheral device is granted.

THE REJECTION

The Examiner relies on the following prior art in rejecting the claims:

Wang	US 5,765,027	June 9, 1998
Helle	US 6,662,023 B1	Dec. 9, 2003 (filed July 6, 2000)
Kawashima	US 6,804,730 B1	Oct. 12, 2004 (filed Nov. 17, 1999)

Claims 26-45 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Wang, Kawashima, and Helle. *See Ans. 4-7.*

## ISSUE

Appellant argues claims 26-45 as a group. *See App. Br. 4-5.* Regarding claim 26, the Examiner finds that Wang teaches a wireless transceiver and at least one peripheral device. *See Ans. 4.* The Examiner further finds that Kawashima teaches a system for rendering difficult the use of a module with an unauthorized peripheral device; the module including a security code; using the module only if a security code provided by a human user to the peripheral device matches the security code provided to the module; and the peripheral device being a portable computing device. *See id.* The Examiner concedes that Wang and Kawashima do not teach that a wireless module that is automatically deactivated in the event that the wireless module is lost and/or stolen. *See id.* However, the Examiner finds this limitation taught by Helle. *See Ans. 4-5.*

Appellant argues that according to Helle, even in the case where the module is deactivated, it still remains accessible for emergency purposes (e.g., 911 calls). *See App. Br. 4.* The issue is whether Wang, Kawashima, and Helle teach or suggest that, “when the module is deactivated *no access* to the module by the peripheral device is granted.” *App. Br. 5* (emphasis Appellant’s).

## ANALYSIS

Helle teaches a mobile phone that requires a user to input a security code to activate the phone when an unknown subscriber identification module (“SIM”) card is put into the phone. *See Helle, col. 3, ll. 16-24.* If the user inputs an incorrect security code, the mobile phone goes into a “secure mode” which “is a state where the usage of the mobile phone 10 is

prohibited, except for emergency calls and calls to one other number.” Helle, col. 3, ll. 19-21, 42-45. According to the Examiner, Helle makes this exception to comply with Federal Communications Commission (“FCC”) requirements for 911 calls. *See* Ans. 5 (citing 47 C.F.R. § 20.18). The Examiner concludes that emergency calls “should not be constru[ed] as access to the module” because the exception is made to comply with Federal law. *See id.*

Appellant contends that, for 911 calls, Helle’s “deactivated module remains accessible,” and thus Helle does not teach “wherein when the module is deactivated *no access* to the module by the peripheral device is granted,” as recited in claim 26. App. Br. 4-5 (emphasis Appellant’s). As to whether an emergency call is “access,” Appellant argues that “[a]ccess is access, and simply because access might be mandated by agency rules does not transform it into its opposite, namely, non-access.” App. Br. 5. According to Appellant, “the claims limit access exceptions by clearly stating that *none* are permitted.” (emphasis in original). *Id.*

The Examiner responds that Kawashima is also cited for teaching preventing access to a module by a peripheral device if a user incorrectly enters a password. *See* Ans. 7-8 (citing Kawashima, col. 10, ll. 40-44); *see also* Ans. 4 (citing Kawashima, col. 10, ll. 25-61). According to the Examiner, Helle is cited to show “automatic deactivation when the device is lost or stolen.” Ans. 8 (citing Helle, col. 1, ll. 53-55). Thus, the Examiner explains, regardless of whether Helle discloses “no access,” “the combination of the references only requires bringing from Helle the automatic method to activate the secure mode of the combination of Wang and Kawashima . . . .” Ans. 8.

Appellant admits that Kawashima teaches “use [of] a password to prohibit access,” but argues that “Helle is the only reference used for automatic deactivation in the event that the module is lost or stolen,” and that combining these references in accordance with their teachings would arrive at a device that would still grant access in the event of loss or theft. Reply Br. 1. Appellant contends that the Examiner is “attempting to divorce the lost/stolen aspect of Helle from Helle’s insistence that even when lost or stolen, the phone can still be used for emergency calls.” *Id.* According to Appellant, Helle’s emergency exception is “a manifest teaching away . . . .” App. Br. 4.

We are not persuaded by Appellant’s arguments. As the Examiner finds, Kawashima teaches that when a user enters an incorrect password into a peripheral device (Kawashima’s computer 2), the peripheral device cannot access a module (Kawashima’s memory card 1). *See* Ans. 4; Kawashima, col. 10, ll. 50-54. Wang’s wireless module can be modified to incorporate Kawashima’s security feature. *See* Ans. 4 (“[I]t would have been obvious to one of the ordinary skills in the art at the time of the invention to add the security features of Kawashima to the mobile module of Wang to protect access to the module from unauthorized use, thereby enhancing security.”). Adding in Helle’s teaching, a person of ordinary skill in the art would contemplate a wireless module, per Wang, automatically deactivated when lost or stolen, as in Helle, in communication with a peripheral device, wherein no access to the module by the peripheral device is granted, per Kawashima. *See* Ans. 8 (“[T]he combination of Wang and Kawashima brings a wireless module with the use [a] password to lock/unlock the module. Helle discloses automatic deactivation when the device is lost or

stolen.”). Thus, regardless of Helle’s teaching, Kawashima teaches a module and peripheral device where “no access to the module by the peripheral device is granted,” as recited in claim 26. Unlike Helle, Kawashima describes no exceptions to its prohibition of access. *See* Ans. 9.

We also do not agree that Helle teaches away from “no access to the module by the peripheral device.” “A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant.” *In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994). Helle’s emergency exception is an “additional step . . . to comply with the 47 CFR 20.18 FCC rule . . . ,” Answer page 8, not a technical requirement for limiting access when a device is lost or stolen. Appellant has not persuasively explained why Helle’s emergency exception would also be imposed upon Kawashima when Helle’s teaching of automatic deactivation is followed. In other words, Appellant has not shown why a person of ordinary skill, following Helle’s teaching, would be discouraged from omitting Helle’s additional emergency exception feature. *See Gurley*, 27 F.3d at 553. Thus, the Examiner’s conclusion of obviousness is not “classic impermissible picking and choosing of some aspects of the references to meet a claim while ignoring related aspects of the references that manifestly render a claim patentable,” Reply Br. 1-2.

As to whether Helle itself teaches the recited “no access,” the Examiner finds that Helle’s exception for 911 calls “is directed to the function of [the] wireless module itself,” rather than to access to a module by a peripheral device. Ans. 8. Thus, the Examiner finds that, while

Helle's emergency exception may allow the wireless module itself access to make an emergency call, this is not access to the module "by the peripheral device," as recited in claim 26. *See id.* Appellant does not adequately explain why this finding is erroneous. In any case, omitting the emergency access exception, an extra feature, in the absence of a Federal regulation requiring that feature, would have been a predictable design choice, and therefore obvious. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 421 (2007) ("When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp.").

Appellant does not separately argue claims 27-45. *See* App. Br. 4-5.

Accordingly, we sustain the rejection of (1) independent claim 26; (2) independent claim 36, which includes a recitation substantially the same as claim 26; (3) claims 27-35, which depend on claim 26; and (4) claims 37-45, which depend on claim 36.

#### ORDER

The decision of the Examiner to reject claims 26-45 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). *See* 37 C.F.R. § 1.136(a)(1)(iv) (2010).

AFFIRMED

kis