

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE BOARD OF PATENT APPEALS  
AND INTERFERENCES

---

*Ex parte* KATHERINE G. AUGUST and JOSEPH M. CANNON

---

Appeal 2008-3065  
Application 10/125,443  
Technology Center 2600

---

Decided: February 28, 2008

---

Before KENNETH W. HAIRSTON, MAHSHID D. SAADAT,  
and SCOTT R. BOALICK, *Administrative Patent Judges*.

HAIRSTON, *Administrative Patent Judge*.

**DECISION ON APPEAL**

Appellants appeal under 35 U.S.C. § 134 from a final rejection of claims 1 to 3, 5 to 11, 13 to 19, 21 to 43, and 46. We have jurisdiction under 35 U.S.C. § 6(b).

We will sustain the rejections.

**STATEMENT OF THE CASE**

Appellants have invented a system and method for a computer to remotely access a portable wireless device (e.g., a cellular telephone) to obtain user personal configuration information associated with the portable wireless device. The remote computer obtains the personal configuration information from the portable wireless device via the Internet. In the event

the portable wireless device is no longer accessible to the user, the remote computer can transfer the personal configuration information to a second portable wireless device (Figure 1; Specification 1, 6 and 7).

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

1. A system for remotely accessing a portable wireless device to store user personal configuration information associated with said portable wireless device, said system comprising:

a remote computer configured to access said portable wireless device over an Internet connection and to obtain said user personal configuration information associated with said portable wireless device over said Internet connection for archiving said user personal configuration information;

wherein said user personal configuration information is information that a user desires to transfer to a second portable wireless device in an event said portable wireless device is no longer accessible to said user.

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

Parker	US 5,864,757	Jan. 26, 1999
Mandahl	US 2002/0102965 A1	Aug. 1, 2002 (filed Jan. 26, 2001)
Aoyama	US 2002/0160760 A1	Oct. 31, 2002 (filed Mar. 29, 2001)
Moles	US 6,615,038 B1	Sep. 2, 2003 (filed Apr. 28, 2000)

The Examiner rejected claims 1 to 3, 5, 8 to 11, 13, 16 to 19, 21, 24 to 27, 30 to 33, 36 to 40, 43, and 46 under 35 U.S.C. § 103(a) based upon the teachings of Aoyama and Moles.

The Examiner rejected claims 6, 14, 22, 34, and 41 under 35 U.S.C. § 103(a) based upon the teachings of Aoyama, Moles, and Parker.

The Examiner rejected claims 7, 15, 23, 35, and 42 under 35 U.S.C. § 103(a) based upon the teachings of Aoyama, Moles, and Mandahl.

The Examiner rejected claims 28 and 29 under 35 U.S.C. § 103(a) based upon the teachings of Aoyama, Moles, and well-known prior art.

## ISSUE

Appellants contend *inter alia* that Aoyama and Moles, whether considered alone or in combination, do not provide for obtaining personal configuration information from a portable wireless device over an Internet connection (Br. 8 to 11). Therefore, the issue before us is does the applied prior art teach or would the applied prior art have suggested to the skilled artisan obtaining personal configuration information from a portable wireless device over an Internet connection?

## FINDINGS OF FACT

1. Appellants describe a system and a method for using an Internet connection to back up personal configuration information from a portable wireless device to a remote computer.
2. Aoyama describes a system for remotely accessing a portable wireless device 10 to store/archive user personal configuration information associated with the device 10 on a remote computer<sup>1</sup> at the data backup equipment 14 in the host office 12 (Figure 1; Abstract; paragraphs 0049; 0057).

---

<sup>1</sup> Appellants have not challenged the Examiner's finding (Final Rejection 6) that Aoyama uses a remote computer in the data backup equipment. Instead, Appellants agree with the Examiner's finding (Final Rejection 7) that Aoyama fails to disclose a remote computer "configured to access said

3. Notwithstanding the Examiner's erroneous finding that Aoyama does not access the portable wireless device over an Internet connection to obtain user personal configuration information (Final Rejection 7), we find that Aoyama expressly states that the radio signals transmitted between the portable wireless device 10 and the host office 12 may be "in the form of a packet signal, a TCP/IP<sup>2</sup> radio signal, and so on" (paragraph 0053).
4. The user personal configuration information in Aoyama is information that a user desires to transfer to a second portable wireless device in an event the portable wireless device is no longer accessible to the user (paragraphs 0014; 0058; 0062).
5. Aoyama uses a PIN to gain access to the user personal configuration information stored in the portable wireless device (paragraphs 0018; 0058; 0079).
6. The Examiner relied on the teachings of Moles because the wireless network "discloses the MSC serving mobile stations (111-114) communicates with mobile station configuration server (160) over the Internet (column 6, lines 17-19), reading on claimed 'over an Internet connection'" (Final Rejection 7).
7. The Examiner relied on the teachings of Parker because Parker uses a PIN to gain access to a handset 20 (col. 11, ll. 47 to 59) (Final Rejection 24).

---

portable wireless device over *an Internet connection* and to obtain said user personal configuration information associated with said portable wireless device *over said Internet connection* for archiving said user personal configuration information" (Br. 9).

<sup>2</sup> TCP/IP is an abbreviation for Transmission Control Protocol/Internet Protocol.

8. The Examiner relied on the teachings of Mandahl for a teaching of the use of encryption for secure data transmission between wireless devices 36 and another location 34 (paragraph 0039) (Final Rejection 25).

9. The Examiner took “Official Notice that it was old and well known in the art for a server to possess a hard drive to store data either for daily access by users or for back-up by the system or network it is serving” (Final Rejection 26).

#### PRINCIPLES OF LAW

The Examiner bears the initial burden of presenting a *prima facie* case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992). If that burden is met, then the burden shifts to the Appellant to overcome the *prima facie* case with argument and/or evidence. *See id.*

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 977, 988 (Fed. Cir. 2006).

“The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results.” *KSR International Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1739 (2007).

During ex parte prosecution, claims must be interpreted as broadly as their terms reasonably allow since Applicants have the power during the administrative process to amend the claims to avoid the prior art. *In re Zletz*, 893 F.2d 319, 321-22 (Fed. Cir. 1989).

#### ANALYSIS

As indicated *supra* in findings of fact 2 to 4, Aoyama describes a system and a method for using an Internet connection to back up personal configuration information from a portable wireless device to a remote

computer. The Internet teachings of Moles (finding of fact 6) are merely cumulative to the Internet teachings already present in Aoyama. Thus, both Aoyama and Moles describe the use of an “Internet connection” between portable wireless devices and a serving source (Br. 10).

Appellants’ argument that the data backup equipment in Aoyama is in a “telephone network” is without merit since the broadly claimed system on appeal does not preclude the use of such a network for data backup purposes (Br. 9 and 10).

Accordingly, we are of the opinion that the system limitations of claim 1 would have been obvious to the skilled artisan based on the teachings of Aoyama when considered alone or in combination with Moles. The same holds true for claims 2, 3, 5, 8 to 11, 13, 16 to 19, 21, 24 to 27, 30 to 33, 36 to 40, 43, and 46 which are grouped with claim 1 (Br. 8 to 11).

Turning to claims 28 and 29, we agree with the Examiner that it would have been manifestly obvious to the skilled artisan to use a hard drive or a tape drive as a permanent storage device for the user personal configuration information (Ans. 22 and 23). We note that Appellants never challenged the Examiner’s taking of Official Notice (finding of fact 9).

Turning next to claim 6, finding of fact 5 described a PIN used by Aoyama. Even if Aoyama did not use a PIN, we agree with the Examiner’s contention that it would have been obvious to the skilled artisan to use a PIN in Aoyama as taught by Parker “to enable activation or access of a handset remotely by only the designated operator or one of its designated providers” (Ans. 21). Thus, claim 6, and the claims grouped with claim 6 (i.e., claims 14, 22, 34, and 41), would have been obvious to the skilled artisan based upon the teachings of Aoyama, Moles, and Parker.

Appeal 2007-3065  
Application 10/125,443

Turning lastly to claims 7, 15, 23, 35, and 42, we agree with the Examiner that it would have been manifestly obvious to the skilled artisan to use the encryption teachings of Mandahl in Aoyama to secure the transfer of user personal configuration information from the portable wireless device 10 to the data backup equipment 14 (Ans. 21 and 22).

#### CONCLUSION OF LAW

The Examiner has established the obviousness of claims 1 to 3, 5 to 11, 13 to 19, 21 to 43, and 46.

#### ORDER

The obviousness rejections of claims 1 to 3, 5 to 11, 13 to 19, 21 to 43, and 46 is affirmed.

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

AFFIRMED

gvw

MANELLI DENISON & SELTER PLLC  
2000 M Street NW  
7<sup>th</sup> Floor  
Washington, DC 20036-3307