

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte CLAUDIO R. BALLARD, AMARISH PATHAK, MICHAEL T.
IMBRUCE, EDWARD H. CURRIE, and JAMES CASSATA

Appeal 2008-3753
Application 10/245,232
Technology Center 3600

Decided: September 10, 2008

Before HUBERT C. LORIN, ANTON W. FETTING, and
JOSEPH A. FISCHETTI, *Administrative Patent Judges*.

LORIN, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Claudio R. Ballard, et al. (Appellants) seek our review under 35
U.S.C. § 134 of the final rejection of claims 1, 3, 9, 11-13, 19, 45, 46, 49,

70-73, and 76. Claims 2, 4-8, 10, 14-18, 20-44, 47, 48, 50-69, 74, and 75 have been cancelled. We have jurisdiction under 35 U.S.C. § 6(b) (2002).

SUMMARY OF DECISION

We REVERSE.¹

THE INVENTION

“This invention relates generally to a private system to store and retrieve all types of information with the use of biometrics for authentication and encryption techniques for security.” Specification [0003]. “[T]here is a need for a system where any type of information may be stored securely and retrieved with anonymity, ease and convenience. Further, there is a need for a single, comprehensive, information storage system having reliability, privacy, authenticity, and accessibility.” Specification [0014]. “This invention involves the storage and retrieval of data with the full identification and verification of users through means of a biometric identifier. The biometric identifier identifies biometric data or biometrics that comprises a statistical analysis of biological data, for example: retina geometry prints, facial prints, DNA data, fingerprints, or voice patterns. Biometric data represents a unique personal identity marker, which is in possession of the user at all times. The use of biometrics ensures a private system due to its inherent characteristics. The Data TreasuryTM Repository System uses a biometric, as a unique identity marker. The usage of

¹ Our decision will make reference to the Appellants’ Appeal Brief (“App. Br.,” filed May 25, 2007) and Reply Brief (“Reply Br.,” filed Nov. 20, 2007), and the Examiner’s Answer (“Answer,” mailed Sep. 20, 2007).

biometrics effectuates creates an extremely secure method of authentication for access to data stores. Furthermore, as communication protocols have become increasingly sophisticated users can access data anywhere in the world.” Specification [0016].

Claims 1 and 45, reproduced below, are illustrative of the subject matter on appeal.

1. A system to provide a centralized, secured and authenticated storage of information comprising:
 - a client subsystem to receive and send transactional data comprising:
 - a biometric processing client subsystem for capturing biometric data; and a data capturing device to capture additional data;
 - a remote data management subsystem for receiving the transactional data from the client subsystem;
 - a remote data storage subsystem, connected to the remote data management subsystem over a communication network, to store transactional data at the direction of the remote data management subsystem;
 - a data processing subsystem, connected to the remote data management subsystem over the communication network, for processing transactions initiated by the remote data management subsystem, on encrypted subsystem identification information and encrypted transactional data provided by the client subsystem to the remote data management subsystem;
 - a biometric subsystem instantiated by the data processing subsystem to verify the identity of a user of the client subsystem, from the captured biometric data in the transactional

data; and

an encryption subsystem instantiated by the data processing subsystem for ensuring the security of the transactional data.

45. A method for central management, security, storage, biometric authentication, verification, and initiation of data transactions comprising the steps of:

capturing transactional data including an image of the biometric data of a user and additional data, at a remote location, and encrypting the transactional data, and sending encrypted transactional data to an object request broker;

verifying the authenticity of the user for access to an appropriate account by a sequence of operations comprising:

operating the object request broker to cause an application server to instantiate a biometric verification object;

operating the biometric verification object to extract characteristics from the biometric data; and

operating the object request broker to query a database for stored matches to the biometric data based on the extracted characteristics; and

operating the object request broker to cause an application server to instantiate an encryption object for encrypting the transactional data for transmission and storage in a database in a data storage subsystem, and for decrypting the transactional data upon processing for presentation to the authorized user.

THE REJECTION

The Examiner relies upon the following as evidence of unpatentability:

Pare, Jr.	US 5,870,723	Feb. 9, 1999
Yu	US 5,930,804	Jul. 27, 1999
Dulude	US 6,310,966 B1	Oct. 30, 2001

The following rejection is before us for review:

1. Claims 1, 3, 9, 11-13, 19, 45, 46, 49, 70-73, and 76 are rejected under 35 U.S.C. §103(a) as being unpatentable over Pare, Jr., Dulude, and Yu.

ISSUE

The issue before us is whether the Appellants have shown that the Examiner erred in rejecting claims 1, 3, 9, 11-13, 19, 45, 46, 49, 70-73, and 76 under 35 U.S.C. §103(a) as being unpatentable over Pare, Jr., Dulude, and Yu.

PRINCIPLE OF LAW

Obviousness

“Section 103 forbids issuance of a patent when ‘the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.’” *KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1734 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the

prior art, (2) any differences between the claimed subject matter and the prior art, and (3) the level of skill in the art. *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966). *See also KSR*, 127 S.Ct. at 1734 (“While the sequence of these questions might be reordered in any particular case, the [*Graham*] factors continue to define the inquiry that controls.”) The Court in *Graham* further noted that evidence of secondary considerations “might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented.” 383 U.S. at 17-18.

ANALYSIS

Claim 1

The Appellants make the following arguments in challenging the rejection:

- the cited prior art “do not teach the [claimed] remote data storage management system and remote data storage” (App. Br. 6-8);
- the cited prior art “do not teach [the claimed] data processing subsystem that processes transactions initiated by the remote data storage management system” (App. Br. 9-11); and,
- “[t]here is no suggestion from the prior art to modify the teachings of the applied references to reach the claim” (App. Br. 11-12).

We will address the first argument. The others are moot in view of our decision that the first argument is persuasive as to error in the rejection.

“remote data storage management system and remote data storage”

Claim 1 is drawn to a system comprising “a remote data management subsystem” and “a remote data storage subsystem.”

The function of the remote data management subsystem is, according to claim 1, “for receiving the transactional data from [a] client subsystem”; the client subsystem comprising (a) a biometric processing client subsystem for capturing biometric data” and (b) a “data capturing device to capture additional data.” Accordingly, the claimed remote data management subsystem has a structure such that it is capable of performing that function.

The function of the remote data storage subsystem is to store transactional data at the direction of the remote data management subsystem. Accordingly, the claimed remote data storage subsystem has a structure such that it is capable of performing that function.

Also, according to claim 1, the remote data storage subsystem is connected to the remote data management subsystem and the remote data management subsystem is connected to a data processing subsystem over a communication network; the data processing subsystem having the function of “processing transactions initiated by the remote data management subsystem, on encrypted subsystem identification information and encrypted transactional data provided by the client subsystem to the remote data management subsystem.”

We have a difficulty understanding the Examiner’s position with regard to these claimed elements and their corresponding functions.

In the Final Rejection, the Examiner took the position that “Pare, Jr et al (See abstract, Figs. 8-18, Col. 11, [lines] 5-57, Col. 14, lines 32-64, [Col.] 15, lines 20-35, Col. 18, lines 5-55, claim 1-66) disclose means for employing a network transaction having a biometric a biometric and additional data input including intermediaries and transmission of verification with encryption substantially as claimed.” Final Rejection 4. The

Examiner stated that the differences between Pare and the claimed system were “the use of specific transactional data and client system.” (Final Rejection 4.) Dulude was relied upon for “show[ing] biometric inputs at a transaction point encrypted and transmitted over a network.” (Final Rejection 4.) “Yu was relied upon for “show[ing] network server authentication of biometric data prior to a transaction.” (Final Rejection 4.) This position was repeated in the Answer (Answer 3).

It would appear that the Examiner is relying on Pare as the evidence to show that the claimed “remote data management subsystem” and “remote data storage subsystem” are known in the prior art. Since the Examiner cites to the abstract, Figs. 8-18, col. 11, ll. 5-57, col. 14, ll. 32-64, col. 15, ll. 20-35, col. 18, ll. 5-55, and claim 1-66, of Pare, it should be there that the claimed limitations “remote data management subsystem” and “remote data storage subsystem” are disclosed. However, the Appellants have had difficulty locating these limitations at those locations in Pare. (App. Br. 6-7.)

In response to the Appellants’ desire for more guidance (e.g., “Does the Examiner identify which component in or teaching of the reference corresponds to the remote data management subsystem of claim 1?” (App. Br. 7), the Examiner stated the following:

Examiner respectfully disagrees and directs attention to Pare, wherein "The DPC contains several databases and software execution modules as shown in (FIG. 2). In a preferred embodiment of the invention, the databases are backed up or "mirrored" in distinct physical locations for safety reasons. The Firewall Machine 5 is responsible for prevention of electronic intrusion of the system

while the Gateway Machine 6 is responsible for routing all requests from the user, including adding, deleting and otherwise modifying all databases. The Gateway Machine is also responsible for decryption and de-packaging of data that has arrived from the terminals using the MACM module 7, MDM module 8, and the SNM module 9. The PGL module 10, and the IML module 11 are used to locate the proper PIN code and biometric basket." (col. 9 ln 45-58). Further, Dulude et al (See Fig. 4, Col. 5, lines 50-65, Col. 6, lines 1-25) show biometric inputs at a transaction point encrypted and transmitted over a network. Thus, since the references are in the same field, it would have been obvious to one of ordinary skill in the art to combine the references because the biometric inputs are conventional functional equivalents with respect to the claim limitations and their employment and comparison is a necessary component of validation and use in a transaction system.

(Answer 6-7).

A claim chart attached to the Answer refers only to Dulude as evidence of prior art disclosing the claimed limitations "remote data management subsystem" and "remote data storage subsystem." The Appellants did not find the Examiner's additional statements helpful. (Reply Br. 2-3). We agree with the Appellants.

In rejecting claims under 35 U.S.C. § 103, the Examiner bears the initial burden of presenting a prima facie case of obviousness. *See In re Rijckaert*, 9 F.3d 1531, 1532 (Fed. Cir. 1993). A prima facie case of obviousness is established by presenting evidence that the reference teachings would appear to be sufficient for one of ordinary skill in the relevant art having the references before her to make the proposed

combination or other modification. *See In re Lintner*, 9 F.2d 1013, 1016 (CCPA 1972). “[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.” *KSR.*, 127 S. Ct. at 1741 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)). In the present case, it would have been helpful to the cause of establishing a prima facie case of obviousness had the Examiner provided a more detailed claim construction analysis. *Cf. Gechter v. Davidson*, 116 F.3d 1454, 1457-1460 (Fed. Cir. 1997) (“When the opinion explaining the decision lacks adequate fact findings, meaningful review is not possible, frustrating the very purpose of appellate review as well as this court's compliance with its statutory mandate. ... In the present case, the Board's opinion lacks a claim construction, makes conclusory findings relating to anticipation, and omits any analysis on several limitations.”)

If we understand the Examiner's position correctly, the Examiner is equating the claimed “remote data management subsystem” and “remote data storage subsystem” with the databases of Pare's Data Processing Center (DPC). The Pare databases can apparently communicate with each other and, in a preferred embodiment, may have distinct locations (i.e., can be remotely located). See Pare, col. 9, ll. 40-49. The Specification's discussion of databases in describing the “remote data management subsystem” and “remote data storage subsystem” (see e.g., Fig. 1 and [0068]-[0071]) would appear to support that equation. However, even if we construed the claimed “remote data management subsystem” and “remote data storage subsystem” as involving databases, there is still the matter of the structure of the systems such that they perform the functions claimed. It is not clear to us, nor has

the Examiner explained, how one of ordinary skill in the art given the Pare databases would be led to systems performing the functions claimed. For example, the function of the claimed “remote data storage subsystem” is to store transactional data *at the direction of the remote data management subsystem*. The Examiner does not explain how one of ordinary skill in the art given the Pare databases would have been led to a system that stores transactional data at the direction of the remote data management subsystem. A disclosure to a database, without more, is insufficient to meet the claimed “remote data storage subsystem,” even if we were to construe it as involving a database.

For the foregoing reasons, we will not sustain the rejection of claim 1. Since we do not sustain the rejection of claim 1, we do not sustain the rejection of the claims dependent on claim 1, namely claims 3, 9, 11-13, and 19. *Cf. In re Fritch*, 972 F.2d 1260, 1266 (Fed. Cir. 1992) (“[D]ependent claims are nonobvious if the independent claims from which they depend are nonobvious.”).

Claim 45

Claim 45 is a method claim. The issue here is whether the cited prior art discloses or suggest “operating [an] object request broker to cause an application server to instantiate an encryption object for encrypting the transactional data for transmission and storage in a database in a data storage subsystem, and for decrypting the transactional data upon processing for presentation to [an] authorized user”; where the object request broker is used in a sequence of operations for verifying the authenticity of the user for

access to an appropriate account. An object request broker is a type of data management subsystem (see Fig. 4).

The Examiner took the same position as the one taken with respect to claim 1. (See Final Rejection 6 and Answer 4-5). In response, the Appellants argued that “none of the applied references teach the verifying and operating steps that are expressly required by claim 1. Nor was the presence of these specific claim steps alleged to be taught by the prior art, in the making of the final rejection.” (App. Br. 15) In response, the Examiner stated:

Appellant [sic] argue, with respect to claim 45, that (t)he references do not teach the verifying and operating steps of claim 45". Examiner respectfully disagrees and directs attention to Yu et al (Figs. 1, 4 and 5) that show network server authentication of biometric data prior to a transaction. It would have been obvious to the person having ordinary skill in this art to provide a similar arrangement for Pare, Jr et al because the biometric inputs are conventional functional equivalents with respect to the claim limitations and their employment and comparison is a necessary component of validation and use in a transaction method. Further, KSR forecloses the argument that a specific teaching is required for a finding of obviousness. KSR, 127 S. Ct. at 1741, USPQ2d at 1396. Additionally, claim 1 recites combinations which merely unite old elements with no change in their respective functions and which yield predictable results.

(Answer 5-6).

We agree with the Appellants. We do not find that the Examiner has satisfied the initial burden of establishing a prima facie case of obviousness.

Notwithstanding our difficulties understanding the Examiner's reasoning, we are unable to find where in Pare and/or Yu, the claimed operation of the object request broker is disclosed as the Examiner has indicated. We are unable to discern how a disclosure of a network server authenticating biometric data prior to a transaction (i.e., Fu) meets the claimed "operating [an] object request broker to cause an application server to instantiate an encryption object for encrypting the transactional data for transmission and storage in a database in a data storage subsystem, and for decrypting the transactional data upon processing for presentation to [an] authorized user". At the very least, an application server is necessary; a claim limitation and one the Examiner did not treat.

Regarding the Examiner's view that "KSR forecloses the argument that a specific teaching is required for a finding of obviousness," KSR does not foreclose the Examiner's burden of showing in the first instance that the prior art exhibits all the claimed steps and their limitations with "a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does." *KSR* at 1741. A conclusory statement that "claim 1 recites combinations which merely unite old elements with no change in their respective functions and which yield predictable results" is insufficient as a basis for establishing a prima facie case of obviousness where the underlying factual findings in support of the premise that the claimed method is a combination of old elements operating according to their known functions to yield a predictable result have not been made.

For the foregoing reasons, we will not sustain the rejection of claim 45. Since we do not sustain the rejection of claim 45, we do not sustain the

Appeal 2008-3753
Application 10/245,232

rejection of the claims dependent on claim 45, namely claims 46, 49, 70-73, and 76.

CONCLUSION

We conclude that the Appellants have shown that the Examiner erred in rejecting claims 1, 3, 9, 11-13, 19, 45, 46, 49, 70-73, and 76 under 35 U.S.C. §103(a) as being unpatentable over Pare, Jr., Dulude, and Yu.

DECISION

The decision of the Examiner to reject claims 1, 3, 9, 11-13, 19, 45, 46, 49, 70-73, and 76 is reversed.

REVERSED

LV:

ANDERSON, LEVINE & LINTEL L.L.P.
14785 PRESTON ROAD
SUITE 650
DALLAS, TX 75254