UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner,

v.

UNIVERSAL SECURE REGISTRY, LLC,

Patent Owner.

Case IPR2018-00810

U.S. Patent No. 9,100,826

REPLY TO PATENT OWNER'S RESPONSE

DOCKET ALARM

Find authenticated court documents without watermarks at docketalarm.com.

Contents

I. Introduction 1

II. Argument 1

A. USR's Proposed Claim Constructions Are Overly Narrow And Contravene BRI. 1

1. "Biometric Information" Is An Example Of "Authentication Information." 1

2. USR's Construction For "Enabling Or Disabling" A Device Is Unduly Narrow. 4

B. USR Fails To Overcome Petitioner's Showing That The Challenged Claims Are Obvious. 5

1. Maritzen's Biometric Key Is "First Authentication Information" Derived/Determined From A "First Biometric Information." 5

2. It Would Have Been Obvious To Combine Maritzen With Jakobsson To Determine The Recited "First Authentication Information" From "First Biometric Information." 7

3. Maritzen's "Biometric Information" Is The Claimed "Authentication Information." 14

4. It Would Have Been Obvious To Combine Maritzen With Jakobsson's Teachings That "Second Biometric Information" Is Retrieved From Memory By A Second Device. 14

5. Maritzen In View Of Jakobsson And Niwa Discloses A Second Processor "Configured To Receive A First Authentication Information." 16

6. Maritzen and Jakobsson Disclose Authenticating The First Entity "Based Upon The First Authentication Information And The Second Biometric Information." 17

7. Maritzen Discloses A "First Handheld Device." 19

8. Maritzen Discloses A Processor Configured To "Enable Or Disable" Use Of The First Handheld Device Based On The Result Of A Comparison. 21

9. Maritzen In View Of Niwa Discloses Storing "Respective Biometric Information For A Second Plurality Of Users." 21

10. USR Fails To Demonstrate Any Secondary Considerations of Non-Obviousness. 22

III. Conclusion 26

DOCKET ALARM

Find authenticated court documents without watermarks at docketalarm.com.

I. Introduction

USR's Patent Owner Response ("POR") repeats arguments that the Board already rejected, and fails to rebut Petitioner's showing that the challenged claims are unpatentable. First, USR proposes improperly narrow constructions that not only contravene the broadest reasonable interpretation standard but also are inconsistent with plain meaning and the intrinsic evidence. Second, USR mischaracterizes the express teachings of Maritzen, Jakobsson, and Niwa, and the testimony of Petitioner's expert, Dr. Shoup. Finally, USR fails to demonstrate any secondary considerations of non-obviousness whatsoever.

II. Argument

A. USR's Proposed Claim Constructions Are Overly Narrow And Contravene BRI.

1. "Biometric Information" Is An Example Of "Authentication Information."

Claiming that "biometric information" must be different from "authentication information," as USR does (POR, 12-13), is inconsistent with the intrinsic evidence and the BRI standard. "Authentication information" is a set of information items that can be used to authenticate a user, and can include PINs, passwords, and biometric information. Ex-1018, Shoup-Decl., ¶12.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

First, nothing in the claims requires that "authentication information" and "first biometric information" are mutually exclusive.[1] Moreover, the claims recite two different elements that should not be conflated, as USR does: "authentication information" (with no modifier) and "first authentication information." These are independent elements with no recited relationship. USR argues that "authentication information" (with no modifier) cannot be biometric information because the claims require determining "first authentication information" from the biometric information. POR, 14. However, the claims require that "***first*** authentication information" be determined from "biometric information." They do not require that "authentication information" (with no modifier) be determined from "biometric information." Because "first authentication information" and "authentication information" (with no modifier) are not related, there is no restriction on the relationship between "authentication information" (with no modifier) and "biometric information." Ex-1018, Shoup-Decl., ¶13.

The order of the claim steps does not support USR either, as it erroneously suggests (POR, 13-14). For example, system claim 1 only requires a processor that is configured to (a) "authenticate a user of the first handheld device based on

[1] For example, a dependent claim could have read: "wherein the authentication information comprises the first biometric information."

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

authentication information," and (b) "retrieve or receive first biometric information of the user of the first handheld device." The claim does not require the processor to perform these steps in any particular sequence. Ex-1018, Shoup-Decl., ¶15.

Moreover, method claims do not require any specific order of operations unless expressly set forth in the claim. *Interactive Gift Exp., Inc. v. Compuserve Inc.*, 256 F.3d 1323, 1342 (Fed. Cir. 2001). Here, method claims 10 and 30 do not require any specific sequence.

Second, the specification[2] expressly identifies "biometric information" as one example of "authentication information" used by the system to verify the identity of an individual. Ex-1001, '826 patent, 35:18-21 ("the act of receiving the first authentication information of the first entity comprises receiving biometric information of the first entity"). Ex-1018, Shoup-Decl., ¶16.

Third, those of ordinary skill in the art would have understood that "authentication information" means any information used to authenticate a user, including biometric information. Ex-1018, Shoup-Decl., ¶17. Accordingly, Petitioner's construction falls within the broadest reasonable interpretation of the phrase "authentication information."

---

[2] USR argues that the term "system" is ambiguous, but challenged claims 1 and 21 claim a "system for authenticating identities."

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.