

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner

v.

CPC Patent Technologies PTY, LTD.,
Patent Owner

Inter Partes Review Case No. IPR2022-00601

U.S. Patent No. 9,269,208

DECLARATION OF DR. ANDREW SEARS

IPR2022-00601

TABLE OF CONTENTS

I.	INTRODUCTION	9
A.	BACKGROUND AND QUALIFICATIONS	10
B.	MATERIALS CONSIDERED.....	13
II.	LEGAL FRAMEWORK.....	15
A.	ANALOGOUS ART	16
B.	OBVIOUSNESS.....	16
C.	SECONDARY CONSIDERATIONS OF NON-OBVIOUSNESS	22
III.	CLAIM CONSTRUCTION.....	23
A.	NON-CONSTRUED CLAIM TERMS.....	23
B.	CONSTRUED CLAIM TERMS.....	24
1.	<i>Non Means-Plus Function Terms</i>	24
2.	<i>Means-Plus-Function Limitations</i>	24
3.	<i>Mathiasen’s Teaching of “computer program product”</i>	27
IV.	BACKGROUND OF TECHNOLOGY.....	30
A.	BIOMETRIC ACCESS SYSTEMS	31
B.	HARDWARE COMPONENTS OF A BIOMETRIC ACCESS SYSTEM	40
C.	SECURE ACCESS SIGNAL	44
D.	INPUTTING A SERIES OF ENTRIES FOR INVOKING FUNCTIONS IN A BIOMETRIC ACCESS SYSTEM.....	47
E.	PROVIDING DIFFERENT TYPES OF ACCESS	51
V.	OPINIONS REGARDING THE ’208 PATENT AND PRIOR ART	58
A.	DESCRIPTION OF THE ALLEGED INVENTION OF THE ’208 PATENT	59
B.	OPINIONS REGARDING <i>MATHIASSEN</i>	63
C.	OPINIONS REGARDING <i>MCKEETH</i>	69
D.	OPINIONS REGARDING <i>ANDERSON</i>	72

E. BRIEF OVERVIEW OF THE OPINIONS ON THE '208 PATENT 77

**VI. GROUND 1: OPINIONS REGARDING THE COMBINATION
OF MATHIASSEN, MCKEETH, AND ANDERSON 80**

A. CLAIM 10 80

1. *Claim 10(Pre1): “A method for providing secure access to a controlled item in a system comprising”* 80

2. *Claim 10(Pre2): “a database of biometric signatures”* 85

3. *Claim 10(Pre3): “a transmitter subsystem comprising a biometric sensor for receiving a biometric signal, and means for emitting a secure access signal capable of granting more than two types of access to the controlled item”* 89

4. *Claim 10(Pre4): “a receiver sub-system comprising means for receiving the transmitted secure access signal, and”*..... 121

5. *Claim 10(Pre5): “means for providing conditional access to the controlled item dependent upon information in said secure access signal”* 124

6. *Claim 10(a): “the method comprising the steps of: populating the database of biometric signatures by”* 133

7. *Claim 10(a1): “receiving a series of entries of the biometric signal”* 134

8. *Claim 10(a2): “determining at least one of the number of said entries and a duration of each said entry”*..... 139

9. *Claim 10(a3): “mapping said series into an instruction”* .. 153

10. *Claim 10(a4): “populating the database according to the instruction”*..... 156

11. *Claim 10(b): “receiving a biometric signal”* 167

12. *Claim 10(c): “matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute”* 168

13.	<i>Claim 10(d): “emitting a secure access signal conveying information dependent upon said accessibility attribute” ..</i>	181
14.	<i>Claim 10(e): “providing conditional access to the controlled item dependent upon said information” ..</i>	184
15.	<i>Claim 10(f): “wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device” ..</i>	186
B.	CLAIM 11	187
	CLAIM 11: “THE METHOD ACCORDING TO CLAIM 10, WHEREIN THE STEP OF POPULATING THE DATABASE OF BIOMETRIC SIGNATURES FURTHER COMPRISES THE STEP OF ENROLLING A BIOMETRIC SIGNATURE INTO THE DATABASE OF BIOMETRIC SIGNATURES COMPRISING THE STEPS OF: RECEIVING A BIOMETRIC SIGNAL; AND ENROLLING THE BIOMETRIC SIGNAL AS AN ADMINISTRATOR SIGNATURE IF THE DATABASE OF BIOMETRIC SIGNATURES IS EMPTY.”	187
C.	CLAIM 13	189
	CLAIM 13: “A NON-TRANSITORY COMPUTER READABLE STORAGE MEDIUM FOR STORING A COMPUTER PROGRAM COMPRISING INSTRUCTIONS, WHICH WHEN EXECUTED BY PROCESSORS CAUSES THE PROCESSORS TO PERFORM THE STEPS OF THE METHOD OF CLAIM 10”	189
D.	CLAIM 1	191
1.	<i>Claim 1(pre): “A system for providing secure access to a controlled item, the system comprising” ..</i>	191
2.	<i>Claim 1(a): “a database of biometric signatures” ..</i>	191
3.	<i>Claim 1(b): “a transmitter subsystem comprising:” ..</i>	191
4.	<i>Claim 1(b1): “a biometric sensor for receiving a biometric signal” ..</i>	192
5.	<i>Claim 1(b2): “means for matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute” ..</i>	192

6.	<i>Claim 1(b3): “means for emitting a secure access signal conveying information dependent upon said accessibility attribute”</i>	194
7.	<i>Claim 1(c): “a receiver subsystem comprising”</i>	194
8.	<i>Claim 1(c1): “means for receiving the transmitted secure access signal”</i>	194
9.	<i>Claim 1(c2): “means for providing conditional access to the controlled item dependent upon said information”</i>	194
10.	<i>Claim 1(d): “wherein the transmitter subsystem further comprises means for populating the data base of biometric signatures, the population means comprising:”</i> .	195
11.	<i>Claim 1(d1): “means for receiving a series of entries of the biometric signal, said series being characterized according to at least one of the number of entries and a duration of each said entry:”</i>	196
12.	<i>Claim 1(d2): “means for mapping said series into an instruction”</i>	199
13.	<i>Claim 1(d3): “means for populating the data base according to the instruction”</i>	201
14.	<i>Claim 1(e): “wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device”</i>	202
E.	CLAIM 3	202
1.	<i>Claim 3(a): “The system according to claim 1, wherein the database of biometric signatures comprises signatures in at least one of a system administrator class, a system user class, and a duress class”</i>	202
2.	<i>Claim 3(b): “the accessibility attribute preferably comprising: an access attribute if the biometric signal matches a member of the database of biometric signatures”</i>	207

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.