

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. IPR2022-00602

U.S. Patent No. 9,665,705

DECLARATION OF DR. ANDREW SEARS

IPR2022-00602

TABLE OF CONTENTS

I.	INTRODUCTION	10
A.	MATERIALS CONSIDERED.....	14
II.	LEGAL FRAMEWORK.....	16
A.	ANALOGOUS ART	17
B.	OBVIOUSNESS.....	17
C.	SECONDARY CONSIDERATIONS OF NON-OBVIOUSNESS	23
III.	CLAIM CONSTRUCTION	24
A.	NON-CONSTRUED CLAIM TERMS.....	24
B.	CONSTRUED CLAIM TERMS.....	24
IV.	BACKGROUND OF TECHNOLOGY	27
A.	BIOMETRIC ACCESS SYSTEMS	27
B.	HARDWARE COMPONENTS OF A BIOMETRIC ACCESS SYSTEM	36
C.	SECURE ACCESS SIGNAL	40
D.	INPUTTING A SERIES OF ENTRIES FOR INVOKING FUNCTIONS IN A BIOMETRIC ACCESS SYSTEM	43
E.	PROVIDING DIFFERENT TYPES OF ACCESS	47
V.	OPINIONS REGARDING THE '705 PATENT AND PRIOR ART	54
A.	DESCRIPTION OF THE ALLEGED INVENTION OF THE '705 PATENT	55
B.	OPINIONS REGARDING <i>MATHIASSEN</i>	59
C.	OPINIONS REGARDING <i>MCKEETH</i>	65
D.	OPINIONS REGARDING <i>ANDERSON</i>	68
E.	BRIEF OVERVIEW OF THE OPINIONS ON THE '705 PATENT	73
VI.	OVERVIEW OF <i>MATHIASSEN'S</i> ARCHITECTURE.....	76
VII.	GROUND 1: OPINIONS REGARDING THE COMBINATION OF <i>MATHIASSEN</i>, <i>MCKEETH</i>, AND <i>ANDERSON</i>	79

A.	CLAIM 1	79
1.	<i>Claim 1(Pre): “A system for providing secure access to a controlled item, the system comprising:”</i>	79
2.	<i>Claim 1(a): “a memory comprising a database of biometric signatures;”</i>	84
3.	<i>Claim 1(b): “a transmitter sub-system comprising:”</i>	88
4.	<i>Claim 1(b1): “a biometric sensor configured to receive a biometric signal;”</i>	91
5.	<i>Claim 1(b2): “a transmitter sub-system controller configured to match the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute;”</i>	92
6.	<i>Claim 1(b3): “a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute”</i>	118
7.	<i>Claim 1(c)-1(c1)</i>	127
	<i>Claim 1(c): “a receiver sub-system comprising: a receiver sub-system controller configured to”</i>	127
	<i>Claim 1(c1): “receive the transmitted secure access signal”</i>	127
8.	<i>Claim 1(c2): “provide conditional access to the controlled item dependent upon said information”</i>	133
9.	<i>Claim 1(d): “wherein the transmitter sub-system controller is further configured to”</i>	135
10.	<i>Claim 1(d1): “receive a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry”</i>	135
11.	<i>Claim 1(d2): “map said series into an instruction”</i>	156
12.	<i>Claim 1(d3): “populate the database according to the instruction”</i>	160
13.	<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>	173

B.	CLAIM 4	174
	CLAIM 4: “THE SYSTEM ACCORDING TO CLAIM 1, WHEREIN THE BIOMETRIC SENSOR IS RESPONSIVE TO ONE OF VOICE, RETINAL PATTERN, IRIS PATTERN, FACE PATTERN, AND PALM CONFIGURATION, AND/OR THE DATABASE OF BIOMETRIC SIGNATURES IS LOCATED IN AT LEAST ONE OF THE TRANSMITTER SUB-SYSTEM AND THE RECEIVER SUB-SYSTEM.”.....	174
C.	CLAIM 6	175
	1. <i>Claim 6(a): “The system as claimed in claim 1, wherein the biometric sensor is further configured to authenticate the identity of a user;”</i>	175
	2. <i>Claim 6(b): “wherein the transmitter is further configured to transmit information capable of granting access to the controlled item using a secure wireless signal dependent upon a request from the user and the authentication of the user identity;”</i>	176
	3. <i>Claim 6(c): “the system further comprising a control panel configured to receive the information and provide the secure access requested.”</i>	178
D.	CLAIM 10	180
	1. <i>Claim 10(Pre): “A transmitter sub-system for operating a system for providing secure access to a controlled item, wherein the transmitter sub-system comprises:”</i>	180
	2. <i>Claim 10(a): “a biometric sensor configured to receiving a biometric signal;”</i>	180
	3. <i>Claim 10(b): “a controller configured to match the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute;”</i>	181
	4. <i>Claim 10(c): a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute;”</i>	181
	5. <i>Claim 10(d): “wherein the controller is further configured to:”</i>	181
	6. <i>Claim 10(d1): “receive a series of entries of the biometric signal, said series being characterized according to at least one</i>	

of the number of said entries and a duration of each said entry;” 181

7. *Claim 10(d2): “map said series into an instruction;”* 181

8. *Claim 10(d3): “populate the database according to the instruction;”* 181

9. *Claim 10(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.”* 181

E. CLAIM 11 181

1. *Claim 11(Pre1): “A method for providing secure access to a controlled item in a system comprising”* 182

2. *Claim 11(Pre2): “a database of biometric signatures;”* 182

3. *Claim 11(Pre3): “a transmitter sub-system comprising a biometric sensor configured to receive a biometric signal, and a transmitter configured to emit a secure access signal capable of granting access to the controlled item;”* 182

4. *Claim 11(Pre4): “a receiver sub-system comprising a receiver sub-system controller configured to receive the transmitted secure access signal, and provide conditional access to the controlled item dependent upon information in said secure access signal;”* 189

5. *Claim 11(a): “the method comprising: populating the database of biometric signatures by:”* 191

6. *Claim 11(a1)-(a2) “receiving a series of entries of the biometric signal;” and “determining at least one of the number of said entries and a duration of each said entry.....* 191

7. *Claim 11(a3): “mapping said series into an instruction;”* 191

8. *Claim 11(a4): “populating the database according to the instruction;”* 191

9. *Claim 11(b): “receiving the biometric signal;”* 192

10. *Claim 11(c): “matching the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute;”* 192

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.