UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,

Petitioner,

v.

PROXENSE, LLC,

Patent Owner.

Case No. IPR2024-00233
U.S. Patent No. 8,886,954

DECLARATION OF STEPHEN GRAY

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

TABLE OF CONTENTS

I. INTRODUCTION 1

II. SUMMARY OF OPINIONS 2

III. QUALIFICATIONS AND BACKGROUND 2

IV. MATERIALS CONSIDERED 6

V. LEGAL STANDARDS 8

A. Level of Ordinary Skill 9

B. Prior Art 10

C. Anticipation 10

D. Obviousness 11

VI. THE '954 PATENT 16

A. Overview 16

VII. CLAIM CONSTRUCTION 18

VIII. LEVEL OF ORDINARY SKILL IN THE ART 20

IX. THE PRIOR ART 21

A. Ludtke (U.S. Patent No. 7,188,110) 22

B. Kon (U.S. Patent Application Publication No. 2002/0046336) 25

X. GROUNDS OF UNPATENTABILITY 30

XI. THE CHALLENGED CLAIMS ARE UNPATENTABLE BASED ON THE PRIOR ART 31

A. Ground 1: Claims 1, 2, 4-7, 10, 12, 13, 15, 16, 18, 19, and 22-27 Are Obvious in View of Ludtke. 31

1. Independent claim 1 31

a. [1preamble]: "A method comprising:" 31

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

b. [1ai]: "persistently storing biometric data of a user [in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered] and"....32

c. [1aii]: "[persistently storing] a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device [in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered] and"....35

d. [1aiii]: "[persistently storing] a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered;"....37

e. [1b]: "responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;"....44

f. [1c]: "comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;"....45

g. [1d]: "responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes from the plurality of codes and the other data values for authentication to a third party that operates a trusted authority, wherein the one or more codes and other data values include[] the device ID code; and"....45

h. [1e]: "receiving, at an application, an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values sent to the third party and allowing the user access to the application....51

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

2. Claim 2: "The method of claim 1, wherein the one or more codes and the other data values are transmitted to the trusted authority over a network." 55

3. Claim 4: "The method of claim 1, wherein the one or more codes and the other data values indicate that the biometric verification was successful." 55

4. Claim 5: "The method of claim 1, wherein the biometric data includes one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition."....57

5. Claim 6: "The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob."....57

6. Claim 7: "The method of claim 1, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account." 59

7. Claim 10: "The method of claim 1, further comprising establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication."....60

8. Independent Claim 12 60

   a. [12preamble]: "An integrated device comprising:" 60

   b. [12ai]: "a persistent storage media that stores biometric data of a user, and"....60

   c. [12aii]: "a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device, and" 60

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

d. [12aiii]: "a secret decryption value in a tamper proof format written to the memory that is unable to be subsequently altered;".....61

e. [12b]: "a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends one or more codes and other data values from the plurality of codes and other data values for authentication by a third party that operates a trusted authority, wherein the one or more codes and other data values includes the device ID code; and".....61

f. [12c]: "a radio frequency communication module that receives an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values to the third party and allowing the user access to an application.".....63

9. Claim 13: "The integrated device of claim 12, wherein the one or more codes and the other data values are transmitted to the trusted authority over a network." 64

10. Claim 15: "The integrated device of claim 12 comprising: an LED to be activated for requesting the biometric scan." 64

11. Independent Claim 16 66

a. [16preamble]: "A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:" 66

b. [16a]: "wirelessly receiving one or more codes and other data values from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and other data values comprises the device ID code uniquely identifying an integrated device associated with a

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.