

US Patent & Trademark Office

Patent Public Search | Text View

United States Patent	12386931
Kind Code	B2
Date of Patent	August 12, 2025
Inventor(s)	Sweeney; Michael F. et al.

Systems and methods for age restricted product activation

Abstract

Embodiments of devices and methods for restricting access to certain age related devices are disclosed, including an accessory for an aerosol delivery device comprising an interface that is configured to provide access to age restricted material within the aerosol delivery device; and authentication circuitry that is configured to receive an age verification of a user, wherein the access is not provided to the aerosol delivery device without the age verification.

Inventors: Sweeney; Michael F. (Winston-Salem, NC), Stopyra; Thomas J. (Winston-Salem, NC)

Applicant: Integrated Solutions International, LLC (Winston-Salem, NC)

Family ID: 1000008749785

Assignee: Integrated Solutions International, LLC (Winston-Salem, NC)

Appl. No.: 18/545320

Filed: December 19, 2023

Prior Publication Data

Document Identifier	Publication Date
US 20240311455 A1	Sep. 19, 2024

Related U.S. Application Data

continuation parent-doc US 17467654 20210907 US 11880438 child-doc US 18545320
continuation parent-doc WO PCT/US2019/055337 20191009 PENDING child-doc US 17225192
continuation-in-part parent-doc US 17225192 20210408 US 11886952 child-doc US 17467654
us-provisional-application US 62815147 20190307
us-provisional-application US 62746675 20181017

Publication Classification

Int. Cl.: G06K7/10 (20060101); G06F21/31 (20130101); G06K7/14 (20060101)

U.S. Cl.:

CPC G06F21/31 (20130101); G06K7/10722 (20130101); G06K7/1413 (20130101);

Field of Classification Search

CPC: G06K (19/06037); G06K (7/10821); G06K (7/1404); G06K (7/1408); G06K (7/1417); G06K (7/10); G06K (7/14); G06F (31/31); G06Q (20/40)

References Cited

U.S. PATENT DOCUMENTS

Patent No.	Issued Date	Patentee Name	U.S. Cl.	CPC
7734779	12/2009	Piccionelli	N/A	N/A
8392975	12/2012	Raghunath	N/A	N/A
8485440	12/2012	Arora et al.	N/A	N/A
8967460	12/2014	Baykal et al.	N/A	N/A
9558387	12/2016	Sweeney et al.	N/A	N/A
9721147	12/2016	Kapczynski	N/A	N/A
9734377	12/2016	Sevier et al.	N/A	N/A
9984266	12/2017	Sweeney et al.	N/A	N/A
10257052	12/2018	Lønborg	N/A	H04L 41/50
10339351	12/2018	Sweeney et al.	N/A	N/A
10726226	12/2019	Sweeney et al.	N/A	N/A
10867143	12/2019	Sweeney et al.	N/A	N/A
10867144	12/2019	Sweeney et al.	N/A	N/A
11074603	12/2020	Smith	N/A	N/A
11880438	12/2023	Sweeney et al.	N/A	N/A
11886952	12/2023	Sweeney et al.	N/A	N/A
2003/0037075	12/2002	Hannigan et al.	N/A	N/A
2003/0061172	12/2002	Robinson	N/A	N/A
2003/0132292	12/2002	Gomez et al.	N/A	N/A
2003/0152947	12/2002	Crossman et al.	N/A	N/A
2004/0181749	12/2003	Chellapilla et al.	N/A	N/A
2005/0059339	12/2004	Honda et al.	N/A	N/A
2005/0080649	12/2004	Alvarez et al.	N/A	N/A
2006/0157559	12/2005	Levy et al.	N/A	N/A
2006/0252055	12/2005	Francis et al.	N/A	N/A
2006/0256388	12/2005	Erol et al.	N/A	N/A
2006/0280364	12/2005	Ma et al.	N/A	N/A
2007/0005173	12/2006	Kanitz et al.	N/A	N/A
2007/0047818	12/2006	Hull et al.	N/A	N/A
2007/0138260	12/2006	Keys	N/A	N/A
2008/0191035	12/2007	Cheon	N/A	N/A
2008/0207296	12/2007	Lutnick et al.	N/A	N/A

2008/0247363	12/2007	Lee et al.	N/A	N/A
2009/0001173	12/2008	Sevier et al.	N/A	N/A
2009/0036405	12/2008	Kennedy	N/A	N/A
2009/0039146	12/2008	Seo	N/A	N/A
2009/0092578	12/2008	Su et al.	N/A	N/A
2009/0108057	12/2008	Mu et al.	N/A	N/A
2009/0307232	12/2008	Hall	N/A	N/A
2010/0251336	12/2009	Allen, Jr. et al.	N/A	N/A
2012/0166309	12/2011	Hwang et al.	N/A	N/A
2013/0018794	12/2012	Ungerland et al.	N/A	N/A
2013/0112746	12/2012	Krell et al.	N/A	N/A
2014/0039932	12/2013	Walton	N/A	N/A
2014/0136012	12/2013	Tam	N/A	N/A
2014/0136223	12/2013	Phillips	N/A	N/A
2014/0222948	12/2013	Terasawa	N/A	N/A
2014/0246035	12/2013	Minskoff et al.	N/A	N/A
2014/0279526	12/2013	Jackson	N/A	N/A
2014/0279540	12/2013	Jackson	N/A	N/A
2014/0289107	12/2013	Moshal	N/A	N/A
2015/0076225	12/2014	Sweeney et al.	N/A	N/A
2015/0081460	12/2014	Chong et al.	N/A	N/A
2015/0106291	12/2014	Robinson et al.	N/A	N/A
2015/0120529	12/2014	Faaborg	N/A	N/A
2015/0124791	12/2014	Mazandarany et al.	N/A	N/A
2015/0181945	12/2014	Tremblay	N/A	N/A
2015/0245668	12/2014	Memari et al.	N/A	N/A
2016/0021930	12/2015	Minskoff et al.	N/A	N/A
2016/0098581	12/2015	Ascencio et al.	N/A	N/A
2016/0100111	12/2015	Atkinson	N/A	N/A
2016/0143361	12/2015	Juster et al.	N/A	N/A
2016/0342970	12/2015	Horn et al.	N/A	N/A
2016/0380774	12/2015	Lovelock et al.	N/A	N/A
2017/0098108	12/2016	Sweeney et al.	N/A	N/A
2017/0116450	12/2016	Sevier et al.	N/A	N/A
2017/0124587	12/2016	White	N/A	N/A
2017/0295014	12/2016	Baras et al.	N/A	N/A
2018/0018659	12/2017	Bolton	N/A	G06Q 20/3821
2018/0020720	12/2017	Matischek et al.	N/A	N/A
2018/0043114	12/2017	Bowen et al.	N/A	N/A
2018/0068105	12/2017	Shapiro et al.	N/A	N/A
2018/0197263	12/2017	Pearson et al.	N/A	N/A
2018/0263283	12/2017	Popplewell et al.	N/A	N/A
2018/0296777	12/2017	Terry et al.	N/A	N/A
2019/0050921	12/2018	Ryner et al.	N/A	N/A
2019/0095665	12/2018	Sweeney	N/A	G06K 7/1417
2019/0158938	12/2018	Bowen et al.	N/A	N/A
2019/0167922	12/2018	Cole	N/A	N/A
2019/0258838	12/2018	Sweeney	N/A	G06Q 30/04
2019/0272359	12/2018	Popplewell et al.	N/A	N/A

2019/0295353	12/2018	Cipriano	N/A	N/A
2020/0000143	12/2019	Anderson et al.	N/A	N/A
2020/0001027	12/2019	Jackson et al.	N/A	N/A
2020/0019920	12/2019	Durkee	N/A	G06Q 10/087
2020/0140256	12/2019	Setchell et al.	N/A	N/A
2020/0175802	12/2019	Crawford et al.	N/A	N/A
2021/0174417	12/2020	Kawamoto	N/A	G06Q 20/20
2021/0209204	12/2020	Flokos	N/A	N/A
2021/0350374	12/2020	Keen	N/A	N/A
2021/0350446	12/2020	D'Haenens et al.	N/A	N/A
2021/0358285	12/2020	Schorey et al.	N/A	N/A
2021/0390556	12/2020	Bermudez	N/A	N/A
2021/0401061	12/2020	Davis et al.	N/A	N/A
2021/0403239	12/2020	Patel	N/A	B65G 1/1371
2021/0405602	12/2020	Patel	N/A	G06K 7/1095
2021/0406970	12/2020	Patel et al.	N/A	N/A
2022/0071299	12/2021	Patel	N/A	G07F 11/00
2022/0256930	12/2021	Thomas et al.	N/A	N/A
2022/0264956	12/2021	Kim et al.	N/A	N/A
2023/0322487	12/2022	Patel	700/206	G06K 7/1413
2024/0311595	12/2023	Sweeney et al.	N/A	N/A

FOREIGN PATENT DOCUMENTS

Patent No.	Application Date	Country	CPC
2924503	12/2021	CA	N/A
10334012	12/2004	DE	N/A
1548664	12/2004	EP	N/A
1811472	12/2006	EP	N/A
3047423	12/2015	EP	N/A
2786254	12/2019	ES	N/A
2010031110	12/2009	WO	N/A
2011147433	12/2010	WO	N/A
2015042060	12/2014	WO	N/A
2019162157	12/2018	WO	N/A
2020081316	12/2019	WO	N/A
2020081317	12/2019	WO	N/A
2020176898	12/2019	WO	N/A

OTHER PUBLICATIONS

Office Action, dated Sep. 27, 2024, by the USPTO, re U.S. Appl. No. 18/545,695. cited by applicant

Advisory Action, dated Jul. 21, 2016, by the USPTO, re U.S. Appl. No. 14/487,952. cited by applicant

Advisory Action, mailed Jun. 2, 2020, by the USPTO, re U.S. Appl. No. 16/205,809. cited by applicant

CA Office Action, mailed Apr. 8, 2022, by the CIPO, re Application No. 3,115,293. cited by applicant

CA Office Action, mailed Mar. 28, 2022, by the CIPO, re Application No. 3, 115,275. cited by applicant

EP Exam Report, dated Jan. 19, 2023, by the European Patent Office, in connection with EP

Application No. 19797866.2. cited by applicant
EP Exam Report, dated Jan. 19, 2023, by the European Patent Office, in connection with EP Application No. 19797867.9. cited by applicant
Final Office Action, dated Jun. 6, 2023, by the USPTO, re Application No. 17/225, 192. cited by applicant
Final Office Action, dated Mar. 13, 2020, by the USPTO, re U.S. Appl. No. 16/205,809. cited by applicant
Final Office Action, dated May 18, 2016, by the USPTO, re U.S. Appl. No. 14/487,952. cited by applicant
Final Office Action, dated Oct. 13, 2015, by the USPTO, re U.S. Appl. No. 14/487,952. cited by applicant
Final Office Action, dated Oct. 18, 2022, by the USPTO, re U.S. Appl. No. 17/225,192. cited by applicant
International Search Report and Written Opinion, dated Dec. 3, 2014, by the ISA/EP, regarding PCT/US2014/055916. cited by applicant
International Search Report, dated Jan. 20, 2020, by the ISA/EP, regarding PCT/US2019/055334. cited by applicant
International Search Report, dated Jan. 20, 2020, by the ISA/EP, regarding PCT/US2019/055337. cited by applicant
Notice of Allowance, dated Dec. 13, 2016, by the USPTO, re U.S. Appl. No. 14/487,952. cited by applicant
Notice of Allowance, dated Feb. 20, 2018, by the USPTO, re U.S. Appl. No. 15/382,319. cited by applicant
Notice of Allowance, dated Mar. 15, 2019, by the USPTO, re U.S. Appl. No. 15/954,909. cited by applicant
Notice of Allowance, dated Mar. 26, 2020, by the USPTO, re U.S. Appl. No. 16/418,285. cited by applicant
Notice of Allowance, dated Sep. 18, 2023, by the USPTO, re U.S. Appl. No. 17/225,192. cited by applicant
Notice of Allowance, dated Sep. 29, 2020, by the USPTO, re U.S. Appl. No. 16/205,809. cited by applicant
Notice of Allowance, dated Sep. 3, 2020, by the USPTO, re U.S. Appl. No. 16/403,785. cited by applicant
Notice of Allowance; mailed Sep. 18, 2023; by the USPTO; re Application No. 17/225, 192. cited by applicant
Notice of Allowance; mailed Sep. 20, 2023; by the USPTO; re U.S. Appl. No. 17/467,654. cited by applicant
Office Action, dated Apr. 27, 2023, by the USPTO, regarding U.S. Appl. No. 17/467,654. cited by applicant
Office Action, dated Dec. 13, 2018, by the USPTO, re U.S. Appl. No. 15/954,909. cited by applicant
Office Action, dated Dec. 28, 2016, by the CIPO, re CA App No. 2,924,503. cited by applicant
Office Action, dated Feb. 1, 2023, by the USPTO, re U.S. Appl. No. 17/225,192. cited by applicant
Office Action, dated Jan. 5, 2016, by the USPTO, re U.S. Appl. No. 14/487,952. cited by applicant
Office Action, dated Jul. 13, 2017, by the EPO, re EP App No. 14777999.5. cited by applicant
Office Action, dated Jun. 8, 2022, by the USPTO, re U.S. Appl. No. 17/225,192. cited by applicant
Office Action, dated May 22, 2020, by the USPTO, re U.S. Appl. No. 16/403,785. cited by applicant
Office Action, dated May 29, 2015, by the USPTO, re U.S. Appl. No. 14/487,952. cited by applicant

Office Action, dated Nov. 24, 2017, by the CIPO, re CA App No. 2,924,503. cited by applicant
Office Action, dated Nov. 25, 2019, by the USPTO, re U.S. Appl. No. 16/418,285. cited by applicant

Office Action, dated Oct. 2, 2019, by the USPTO, re U.S. Appl. No. 16/205,809. cited by applicant

Office Action, dated Sep. 12, 2017, by the USPTO, re U.S. Appl. No. 15/382,319. cited by applicant

Written Opinion, dated Jan. 20, 2020, by the ISA/EP, regarding PCT/US2019/055334. cited by applicant

Written Opinion, dated Jan. 20, 2020, by the ISA/EP, regarding PCT/US2019/055337. cited by applicant

Notice of Allowance, dated Apr. 15, 2025, by the USPTO, re U.S. Appl. No. 18/545,695. cited by applicant

Primary Examiner: Le; Thien M

Background/Summary

CROSS REFERENCE TO RELATED APPLICATIONS (1) This application is a continuation of U.S. application Ser. No. 17/467,654, filed Sep. 7, 2021, entitled “Systems and Methods for Age Restricted Product Activation,” which is a continuation-in-part of U.S. application Ser. No. 17/225,192 filed on Apr. 8, 2021 entitled “Systems and Methods for Point of Sale Age Verification,” which is a continuation of International Application No. PCT/US2019/055337, filed Oct. 9, 2019, and entitled “Systems and Methods for Point of Sale Age Verification,” which claims priority to Provisional Application No. 62/815,147, filed on Mar. 7, 2019, entitled “Systems and Methods for Point of Sale Age Verification,” and claims priority to Provisional Application No. 62/746,675, filed on Oct. 7, 2018 entitled “Systems and Methods for Age-Restricted Product Registration.” The disclosures of which are all incorporated by reference for all purposes. (2) This application is also commonly owned with the following U.S. patent applications: U.S. patent application Ser. No. 15/954,909, filed on Apr. 17, 2018, and entitled “Systems and Methods For Decoding And Using Data On Cards,” now U.S. Pat. No. 10,339,351, issued Jul. 2, 2019, which is a continuation of U.S. patent application Ser. No. 15/382,319, filed on Dec. 16, 2016, and entitled “Systems and Methods For Decoding And Using Data On Cards,” now U.S. Pat. No. 9,984,266, issued on May 29, 2018, which is a continuation of U.S. patent application Ser. No. 14/487,952, filed on Sep. 16, 2014, and entitled “Systems and Methods for Decoding and Using Data on Cards,” now U.S. Pat. No. 9,558,387, issued on Jan. 31, 2017, which claims priority to U.S. Provisional Application No. 61/878,823, filed on Sep. 17, 2013, and entitled “Systems and Methods for Decoding and Using Data on Cards.” The disclosures of which are all incorporated by reference for all purposes.

BACKGROUND INFORMATION

(1) Electronic devices that dispense age-restricted material are available. These electronic devices do not include systems for restricting access to users who are too young to consume the age-restricted material. Identification cards, such as government issued identification cards, increasingly include some form of machine-readable data. Often many different entities (e.g., corporations, states, or government organizations) use different encoding for this machine-readable data.

SUMMARY OF EXAMPLE EMBODIMENTS

(2) Embodiments of the present disclosure include devices comprising input devices for scanning

- passive data-sources, and processing ability to decode machine-readable data stored in the passive data-source. This information is then used to verify the age of a user. Once the user's age has been verified an activation signal is sent to an electronic device that dispenses age-restricted material (e.g., an e-cigarette or “vape” device).
- (3) One illustrative system according to the present disclosure comprises a system for activating an age-restricted device, the system comprising: a scanner configured to scan a passive data source on an identification card; and a processor coupled to the scanner, the processor configured to: receive a scanner signal from the scanner; verify an age of a user based on the scanner signal; and transmit a verification signal to an age-restricted device.
- (4) According to another embodiment, an illustrative system of the present disclosure comprises a system for activating an age-restricted device, the system comprising: a processor configured to receive an age verification signal and activate the age-restricted device based on the age verification signal; and a network interface configured to receive a verification signal from a remote device, wherein the remote device comprises: a scanner configured to scan a passive data source on an identification card; and a processor coupled to the scanner, the processor configured to: receive a scanner signal from the scanner; verify an age of a user based on the scanner signal; and transmit the verification signal to the age-restricted device.
- (5) According to another embodiment, a method according to the present disclosure comprises: receiving a scanner signal from a scanner configured to scan a passive data source on an identification card; verifying an age of a user based on the scanner signal; and transmitting a verification signal to an age-restricted device.
- (6) According to yet another embodiment, a method according to the present disclosure comprises: receiving an age verification signal from a remote device, wherein the remote device comprises: a scanner configured to scan a passive data source on an identification card; and a processor coupled to the scanner, the processor configured to: receive a scanner signal from the scanner; verify an age of a user based on the scanner signal; transmit the verification signal to the age-restricted device; and activating the age-restricted device based on the age verification signal.
- (7) According to yet another embodiment of the present disclosure a non-transitory computer readable medium may comprise program code, which when executed by a processor is configured to cause the processor to: receive a scanner signal from a scanner configured to scan a passive data source on an identification card; verify an age of a user based on the scanner signal; and transmit a verification signal to an age-restricted device.
- (8) According to yet another embodiment of the present disclosure a non-transitory computer readable medium may comprise program code, which when executed by a processor is configured to cause the processor to: receive an age verification signal from a remote device, wherein the remote device comprises: a scanner configured to scan a passive data source on an identification card; and a processor coupled to the scanner, the processor configured to: receive a scanner signal from the scanner; verify an age of a user based on the scanner signal; transmit the verification signal to an age-restricted device; and activate the age-restricted device based on the age verification signal.
- (9) This illustrative embodiment is mentioned not to limit or define the limits of the present subject matter, but to provide an example to aid understanding thereof. Illustrative embodiments are discussed in the Detailed Description, and further description is provided there. Advantages offered by various embodiments may be further understood by examining this specification and/or by practicing one or more embodiments of the claimed subject matter.

Description

BRIEF DESCRIPTION OF THE DRAWINGS

- (1) A full and enabling disclosure is set forth more particularly in the remainder of the specification. The specification makes reference to the following appended figures.
- (2) FIG. 1 shows an illustrative system for age-restricted product registration according to one embodiment of the present disclosure;
- (3) FIG. 2A shows another illustrative system for age-restricted product registration according to one embodiment of the present disclosure;
- (4) FIG. 2B shows another illustrative system for age-restricted product registration according to one embodiment of the present disclosure;
- (5) FIG. 3 shows another illustrative system for age-restricted product registration according to one embodiment of the present disclosure;
- (6) FIG. 4A shows yet another illustrative system for age-restricted product registration according to one embodiment of the present disclosure;
- (7) FIG. 4B shows yet another illustrative system for age-restricted product registration according to one embodiment of the present disclosure;
- (8) FIG. 4C shows yet another illustrative system for age-restricted product registration according to one embodiment of the present disclosure;
- (9) FIG. 4D shows yet another illustrative system for age-restricted product registration according to one embodiment of the present disclosure;
- (10) FIG. 5 shows a flow chart of method steps for implementing a method for age-restricted product registration according to one embodiment of the present disclosure; and
- (11) FIG. 6 shows a flow chart of method steps for implementing a method for age-restricted product registration according to one embodiment of the present disclosure.

DETAILED DESCRIPTION

(12) Reference will now be made in detail to various and alternative illustrative embodiments and to the accompanying drawings. Each example is provided by way of explanation and not as a limitation. It will be apparent to those skilled in the art that modifications and variations can be made. For instance, features illustrated or described as part of one embodiment may be used on another embodiment to yield a still further embodiment. Thus, it is intended that this disclosure include modifications and variations as come within the scope of the appended claims and their equivalents.

(13) Illustrative Example of a Device for Age-Restricted Product Registration

(14) Turning now to FIG. 1, which shows one illustrative embodiment of the present disclosure **100**. As shown in FIG. 1, the system **100** comprises an age-restricted device **112**, such as an electronic cigarette (e-cigarette), which are sometimes referred to as vaping devices. An e-cigarette dispenses a vapor that contains nicotine, and which a user inhales. An e-cigarette is not authorized for use for people under the age of eighteen. An illustrative embodiment herein provides systems and methods for restricting the use of an e-cigarette by people under the age of eighteen.

(15) The illustrative embodiment further comprises a mobile device **106** (e.g., a wearable device, smartphone, tablet, portable music device, or laptop). In the embodiment shown in FIG. 1, the mobile device **106** comprises a scanner **108** for reading data from an identification card **102** comprising a passive data source **104**. In some embodiments, the identification card may include, e.g., a State Issued Driver License, State Issued Real ID Compliant Driver License, State issued identification card, Federally issued Passport or Military Identification. In some embodiments, the identification card **102** may comprise an electronic identification card, e.g., an electronic ID stored in an application on, e.g., the user's mobile device.

(16) In the embodiment shown in FIG. 1, the scanner **108** comprises a digital camera configured to capture images. In the illustrative embodiment, this camera comprises a standard camera found on mobile devices, without any specialized hardware. The illustrative embodiment further comprises a

network connection, such as a wired or wireless internet connection. The illustrative embodiment further comprises a network interface **110** (e.g., Bluetooth, Near Field Communication (“NFC”), or RFID) to connect to a similar network interface **114** on the age-restricted device **112**.

(17) In the illustrative embodiment the user accesses an application configured to verify the user's age by capturing an image of the user's identification card **102**. For example, the user captures an image of either the front or back face of a driver's license. For example, the user may load a mobile application that includes a widget to execute an age-verification application.

(18) In such an embodiment, this widget may appear as a button, switch, graphical user interface, or other user interface available for use with the mobile application. After the user accesses this functionality, e.g., by interacting with the widget, the mobile device **106** may be configured to enter an image capture mode.

(19) In the image-capture mode, the mobile device **106** may access a digital camera coupled to the mobile device and display the output on a display of the mobile device **106**. The user may then direct the camera toward the user's identification card **102** (such as a driver's license). Specifically, the user may direct the camera toward passive data source **104**, which may comprise machine-readable data (e.g., a barcode encoded in PDF-417 appearing on the back of the identification card). Examples of PDF-417 are shown in FIGS. **4A** and **4B** below. When the camera captures an image of the machine-readable data at sufficient resolution to extract the data encoded therein, the application may exit the image capture screen, and return to another screen of the mobile application.

(20) Once the image has been captured, a processor on the mobile device **106** may process the image to extract encoded data. In some embodiments, this processing may comprise cropping and compressing the data contained on the image. The mobile device **106** may then use a network interface (e.g., a wired or wireless network interface) to transmit the image data to a server.

(21) In some embodiments, the server may comprise algorithms developed to quickly process and determine information associated with the cards. In some embodiments, these algorithms may have been developed utilizing a database of data associated with identification cards. Currently, in the United States, there are more than 1,000 different formats of encoded data associated with identification cards issued by various entities (e.g., corporations, states, government organizations, military, or post office). For example, some states change the encoding used on their drivers licenses every few years. However, those states may leave the older drivers licenses in rotation. Thus, these identification cards may comprise out of date encoding. Further, some states may use multiple different types of encryption. Similarly, multiple states use different encoding and encryption, thus, an algorithm associated with, e.g., Georgia may not be useful for decoding data associated with another state's identification cards. In some embodiments, the remote database may comprise data associated with a large number of these entities. Algorithms developed based on the data in this database may enable the server to quickly process and parse the data on an identification card. Further, in some other embodiments, data comparison software or string searches may enable the database to be quickly searched to determine information about the received data.

(22) Further, in some embodiments, the server may track whether the user has recently activated a different age-restricted device or bought more than a certain number of age-restricted devices. The server may be configured to deny access to a user that has activated another age-restricted device within a certain time period (e.g., one day or one-week), thus ensuring that one user who is of age (e.g., over eighteen or twenty-one) cannot activate multiple age-restricted devices for users that are not of age. In still other embodiments, the server may be configured to compare information associated with the user to a no sell list. If the user is on the no sell list the server may send information to the mobile device **106** to prevent the mobile device **106** from activating the age-restricted device **112**.

(23) Once the data is decoded, the server may use a network connection to transmit the decoded

data back to the mobile device **106**. Once the mobile device receives this data, it will confirm that the user is over an age required to access the age-restricted device. If the user is over the age required to access the age-restricted device, the computing device will transmit an activation signal to the age-restricted device **112**. Once the age-restricted device receives this activation signal, it will be activated and allow users to access the age-restricted material **116**. In some embodiments, the age-restricted material **116** may comprise one or more of e.g., a nicotine or a cannabinoid such as THC or CBD containing substance, or some controlled medication (e.g., anxiety or depression medication), opioids, or some other controlled substance, which may be configured to be vaporized or otherwise dispensed by age-restricted device **112**.

(24) This illustrative embodiment is mentioned not to limit or define the limits of the present subject matter, but to provide an example to aid understanding thereof. Illustrative embodiments are discussed in the Detailed Description, and further description is provided there. Advantages offered by various embodiments may be further understood by examining this specification and/or by practicing one or more embodiments of the claimed subject matter.

(25) Illustrative Systems for Age-Restricted Product Registration

(26) FIG. 2A shows an illustrative system **200** for age-restricted product registration. Particularly, in this example, system **200** comprises a computing device **201** such as, e.g., a wearable device, smartphone, tablet, portable music device, laptop, desktop, kiosk, or dedicated computer terminal. As shown in FIG. 2A, computing device **201** has one or more processor(s) **202** interfaced with other hardware via bus **206**. A memory **204**, which can comprise any suitable tangible (and non-transitory) computer-readable medium such as RAM, ROM, EEPROM, or the like, embodies program components that configure operation of the computing device. In this example, computing device **201** further includes one or more network interface devices **210**, input/output (I/O) interface components **212**, and additional storage **214**.

(27) Network device **210** can represent one or more of any components that facilitate a network connection. Examples include, but are not limited to, wired interfaces such as Ethernet, ETSB, IEEE 1394, and/or wireless interfaces such as IEEE 802.11, Bluetooth, Near Field Communication, RFID, and/or radio interfaces for accessing cellular telephone networks (e.g., transceiver/antenna for accessing a CDMA, GSM, UMTS, or other mobile communications network(s)).

(28) I/O components **212** may be used to facilitate connection to devices such as one or more user interfaces **216** (e.g., keyboards, mice, speakers, microphones, and/or other hardware used to input data or output data) and display **220** (e.g., a display such as a plasma, liquid crystal display (LCD), electronic paper, cathode ray tube (CRT), light emitting diode (LED), or some other type of display known in the art). In some embodiments, user interfaces **216** and display **220** may comprise a single component, e.g., a touch screen display. In some embodiments, I/O components **212** may include speakers configured to play audio signals provided by processor **202**. Storage **214** represents nonvolatile storage such as magnetic, optical, or other storage media.

(29) Scanner **218** comprises a sensor configured to detect a passive data-source, such as data encoded in a multidimensional code. For example, in one embodiment, scanner **218** may comprise an optical sensor such as a digital camera. In such an embodiment, processor **202** may use scanner **218** to take an image of a passive data-source, e.g., a matrix barcode such as a QR code, bar code, or multidimensional bar code encoded in PDF-417. In some embodiments, the digital camera may comprise no specialized hardware capability, for example, in some embodiments, the digital camera may be a standard digital camera found on mobile devices such as smartphones and tablets. Further, in some embodiments, the digital camera may comprise an auto-focus capability that enables the camera to capture an image of the multidimensional code at sufficient resolution to reliably extract the encoded data. In such an embodiment, processor **202** may use software stored in memory **204** (discussed below) to determine data encoded in the multidimensional bar code. In other embodiments, scanner **218** may comprise another component, such as a laser scanner, CCD, reader, video camera reader, or other type of scanner configured to scan a passive data-source such

as a multidimensional bar code. In still other embodiments, scanner **218** may comprise a scanner configured to detect data from a magnetic code (e.g., a magnetic strip), an RFID, NFC, a SmartCard, an Integrated Circuit Card (ICC) or some other type of passive data. Turning to memory **204**, exemplary program components **224** and **226** are depicted to illustrate how a device may be configured to decode data on identification cards. In this example, an image detection module **224** configures processor **202** to monitor the input from scanner **218** to detect an image comprising machine-readable data. For example, module **224** may configure processor **202** to enter an image capture mode in which display **220** shows the output from scanner **218**. Further, in some embodiments, image detection module **224** may be configured to determine the quality of data received from scanner **218**. For example, in one embodiment, this may comprise measuring the resolution and focus of the received image. In some embodiments, image detection module **224** may further comprise software to enable processor **202** to determine that the image is of sufficient quality, and therefore capture the image.

(30) Image-parsing module **226** represents a program component that analyzes image data received from scanner **218**. In one embodiment, image-parsing module **226** may comprise software configured to enable processor **202** to crop and/or compress the captured image for transmission via network **210** to a remote server. In further embodiments, image-parsing module **226** may comprise program components configured to enable processor **202** to perform an image comparison between the captured image and data stored on a local database. In some other embodiments, image-parsing module **226** may comprise algorithms that enable the processor **202** to quickly determine the data encoded in a label, e.g., the name, date of birth, address, driver's license number, height, weight, state, county, race, organ donor status, issue date, expiration date, driver restriction, class of vehicle, passport information, criminal record information, or any other information stored in the encoded data. In some embodiments, some of this information may be withheld, e.g., due to privacy concerns. Thus, in some embodiments, information such as a person's height, weight, race, organ donor status, driver restrictions, or class of vehicle may be withheld.

(31) In other embodiments, program components **224** and **226** may be comprise software components configured to enable processor **202** to process other types of passive data-sources, e.g., magnetic strips, RFIDs, NFC, SmartCards, or Integrated Circuit Cards (ICC).

(32) In other embodiments, computing device **201** may comprise additional components, such as motion detectors, accelerometers, or GPS receivers that processor **202** may use to determine other information, such as the movements or orientation of computing device **201**.

(33) Turning now to FIG. 2B, which shows an illustrative system **250** for age-restricted product registration. Particularly, in this example, system **250** comprises an age-restricted device **251**, e.g., an e-cigarette device. As shown in FIG. 2B, the system **250** has one or more processor(s) **252** interfaced with other hardware via bus **256**, age-restricted material **254** (e.g., a nicotine or a cannabinoid such as THC or CBD containing substance, or some controlled medication (e.g., anxiety or depression medication), opioids, or some other controlled substance, which may be configured to be vaporized or otherwise dispensed by age-restricted device **251**), a network interface **260**, and input/output (I/O) interface components **262**.

(34) Network device **260** can represent one or more of any components that facilitate a network connection. Examples include, but are not limited to, wired interfaces such as Ethernet, USB, microUSB, Firewire, IEEE 1394, and/or wireless interfaces such as IEEE 802.11,

(35) Bluetooth, Near Field Communication, RFID, and/or radio interfaces for accessing cellular telephone networks (e.g., transceiver/antenna for accessing a CDMA, GSM, UMTS, or other mobile communications network(s)). In some embodiments, network interface **260** is configured to receive an activation signal from computing device **201**, described above with regard to FIG. 2A, transmit this activation signal to processor(s) **252**, which then activate the age-restricted device **251** based on the activation signal.

(36) I/O components **262** may be used to facilitate connection to devices such as one or more user

interfaces **266** (e.g., keyboards, mice, speakers, microphones, and/or other hardware used to input data or output data) and display **220** (e.g., a display such as a plasma, liquid crystal display (LCD), electronic paper, cathode ray tube (CRT), light emitting diode (LED), or some other type of display known in the art). In some embodiments, I/O components **262** may include speakers configured to play audio signals provided by processor **262**.

(37) FIG. **3** illustrates another illustrative system for age-restricted product registration **300**. As shown in FIG. **3**, system **300** comprises a computing device **310**, comprising a processor **311**, memory **312** comprising instructions **313**, and a network interface **314**. In some embodiments, computing device **310**, and its components may operate similarly to the components of computing device **201** described above with regard to FIG. **2A**. Thus, in some embodiments, the components of computing device **310** may enable the computing device to scan a passive data-source, process the data, and transmit the processed data via access network **330**.

(38) In some embodiments the access network **330** may be a 3 GPP network, a 3GPP2 network, a WiMAX network, 4G LTE, HSPA+, UMTS, a Wi-Fi network (e.g., a network that operates in accordance with an IEEE 802.11 standard), or some other wireless access network.

(39) In other embodiments, access network **330** may comprise a wired network such as Ethernet, USB, microUSB, Firewire, IEEE 1394, cable, or telephone networks. In some embodiments, access network **330** may comprise a plurality of different types of wired and/or wireless networks configured to transmit data between computing device **310** and server **320**.

(40) As shown in FIG. **3**, the access network **330** is further coupled to a server **320**. Server **320** is configured to receive data sent from computing device **310** via access network **330** using network interface **323**. Network interface **323** may comprise a wired and/or wireless network interface configured to receive data using access network **330**.

(41) Server **320** further comprises a processor **321** coupled to a database **322**. Database **322** may comprise a database of data associated with identification cards. In some embodiments, the database **322** may comprise data associated with identification cards issued by one or more of corporations, states, and government organizations. Processor **321** may be configured to use data comparison software to compare data received from computing device **310** to data stored in database **322** to determine the type of encoding associated with an image and then quickly decode the data, e.g., by parsing the data to determine the stored information, e.g., the name, date of birth, address, driver's license number, height, weight, state, county, or any other information stored in the encoded data.

(42) In other embodiments, rather than performing a full lookup of database **322**, processor **321** may instead comprise algorithms configured to determine information about a passive data source without having to search database **322**. In some embodiments, these algorithms may have been developed using the data available in database **322**. Further, in some embodiments, these algorithms may enable the processor **321** to quickly determine the jurisdiction that issued a card, e.g., by determining the Issuer Identification Number (“UN Number”) associated with the card, or the type of encryption used in the card. Once this is determined, processor **321** may access an algorithm associated with that IIN number to quickly determine data associated with the passive data source. In some embodiments, processor **321** may be configured to determine the stored data in 2 seconds or less.

(43) Further, in some embodiments, processor **321** and database **322** may be configured to adapt to new data types. For example, in some embodiments, the administrators of database **322** may periodically update database **322** with new data associated with new entities (e.g., states, government organizations, or corporations). In other embodiments, processor **321**, may be configured to update database **322** based on new data received from entities as the entities post new information (e.g., as a state releases a new type of identification card).

(44) In other embodiments, processor **321** and database **322** may be configured to analyze received data that is not associated with a known type, and based on patterns of other received data, make a

determination about the received data. For example, in one embodiment, processor **321** and database **322** may be configured to compare the encoding to known encoding types and thus determine that the encoded data is associated with North Carolina. The processor **321** and database **322** may be configured to further determine that some component of the encoding or encryption is incorrect, for example, because the person who set up the multidimensional code for the drivers' licenses in a jurisdiction (e.g., a state or county) used the wrong type of encoding. Based on this determination processor **321** may update database **322** with new information about this jurisdiction (e.g., the state or county), to thus enable processor **321** to use database **322** to determine data associated with that jurisdiction in the future. In still other embodiments, computing device **310** and server **320** may comprise additional components, such as additional memory and processing components or network components configured to provide faster or more convenient access via access network **330**.

(45) In some embodiments, the parsed data may be stored on the server **320**. In some embodiments, this information may be used for future processing and authentication. For example, in some embodiments, a user may not be able to authenticate more than one device within a set time period (e.g., one-day, one-week, one-month) to prevent a user from authenticating multiple age-restricted devices and distributing them. Further, in some embodiments, the server **320** may store the total amount of an age-restricted substance purchased by the user. In some embodiments, this information may be used to restrict the user's access to additional amounts of an age restricted substance. For example, one user may not be able to purchase over a certain quantity of the age-restricted substance in a set time period. In still other embodiments, the user's age, the total amount of a substance the user has purchased, and the time since the user's last purchased may all be used together to determine whether the user can purchase more of the age-restricted substance. In still other embodiments, the server may be configured to determine whether the user is on a no sell list, and, if so, prevent the user from being able to activate the age-restricted device.

(46) Further, in some embodiments, the user may be able to deactivate an age-restricted device, e.g., if the user loses the age-restricted device. In such an embodiment, users may verify their identity by scanning an ID card as described above and sending data to the server **320** indicating that an age-restricted device should be deactivated. In such an embodiment, the server **320** may send a signal to the age-restricted device or to a computing device associated with the age-restricted device to deactivate the age-restricted device so it cannot be operated.

(47) Turning now to FIGS. **4A** and **4B**, FIGS. **4A** and **4B** comprise images **400** and **450** of data encoded on the back of drivers licenses from two different states. As shown in FIGS. **4A** and **4B**, the data is encoded using PDF-417. As discussed above, PDF-417 is a stacked linear barcode format. PDF stands for Portable Data File. The 417 signifies that each pattern in the code consists of 4 bars and spaces, and that each pattern is 17 units long. In some embodiments, data encoded using PDF-417 may further comprise some type of compression or encryption. These types of encryption and compression are applied irregularly amongst jurisdictions such as Federal and State organizations. The present disclosure comprises a database that takes into account these differences and is usable for all jurisdictions (e.g., using a prior technology a Georgia government body may be able to scan identification cards issued by Georgia but cannot effectively scan cards issued by other states). Further, in some embodiments, additional data may be encoded into the identification card. For example, in Florida some information associated with the driver may be embedded into the driver's license number. Thus, in some embodiments, a database associated with Florida driver's licenses may be useful only if it is designed to store this information.

(48) Turning to FIG. **4C**, FIG. **4C** illustrates an example embodiment of the front face of an identification card **460**. As shown in FIG. **4C**, the identification card is an example similar to many states' driver's licenses and includes a picture as well as written information identifying the holder of the driver's license. FIG. **4D** shows the reverse side **470** of the identification card **460**. As shown in FIG. **4D**, the identification card includes a PDF-417 label (e.g., labels **400** or **450** described

above). In some embodiments, this label may comprise all or some part of the data on the front of the identification card. Further, in some embodiments, rather than being on the back of the card, the label may instead be located on the front. For example, some military identification cards (e.g., CAC cards) include a label on the front of the card. Some of these cards further include additional passive data-sources, such as ICC, SmartCards, RFIDs, NFCs, magnetic strips, or QR Codes. In some embodiments, rather than a PDF-417 label, the driver's license may instead comprise one of these other types of passive data-sources. Embodiments of the present disclosure may use similar technology to capture and decode data stored in these additional types of passive data sources. Further, In some embodiments, the identification card may comprise an electronic identification card, e.g., an electronic ID stored in a computer associated with the user, e.g., stored in an application on the user's mobile device.

(49) Illustrative Methods for Age-Restricted Product Registration

(50) FIG. 5 is a flowchart showing an illustrative method **500** for age-restricted product registration. In some embodiments, the steps in flow chart **500** may be implemented in program code executed by a processor, for example, the processor in a general purpose computer, mobile device, or server. In some embodiments, these steps may be implemented by a group of processors. In some embodiments the steps shown in FIG. 5 may be performed in a different order. Alternatively, in some embodiments, one or more of the steps shown in FIG. 5 may be skipped or additional steps not shown in FIG. 5 may be performed. The steps below are described with reference to components described above with regard to the systems described above with regard to FIGS. 2A, 2B, and 3.

(51) The method **500** is described with regard to image capture of a passive data source (e.g., of an image of a multidimensional bar code). However, the steps below are equally applicable to processing data extracted from other types of passive data sources. For example, these method steps may be applied to capturing data from a magnetic code (e.g., a magnetic strip), an RFID, NFC, a SmartCard, an Integrated Circuit Card (ICC) or some other type of passive data. Further, in some embodiments, the methods described below may be used to extract data appearing as printed text on the front of an identification card. In such an embodiment the processor **202** may be configured to perform an optical character recognition (OCR) of this text. The method **500** begins at step **502** when processor **202** receives a scanner signal from scanner **218**. As discussed above, scanner **218** may comprise one of a plurality of devices configured extract data from a passive data source (e.g., a barcode or other information printed on an identification card). In one embodiment, scanner **218** may comprise a camera configured to capture an image of the front or the back of an identification card. In some embodiments, the image may comprise an image of machine-readable data encoded in an identification card (e.g., on the back of the identification card). In some embodiments, the machine-readable data may comprise a multidimensional encoding, such as data encoded using PDF-417. In other embodiments, the image may comprise an image of text printed on the front or the back of the identification card. In still other embodiments the scanner **218** may comprise a scanner configured to scan other types of passive data sources, e.g., a magnetic code (e.g., a magnetic strip), an RFID, NFC, a SmartCard, an Integrated Circuit Card (ICC) or some other type of passive data.

(52) Next processor **202** determines a type of encryption associated with the scanner signal **504**. In some embodiments, determining the type of encryption may comprise determining a type of encoding associated with the scanner signal or determining that the scanner signal is not encoded or encrypted. For example, in some embodiments, determining a type of encryption may comprise determining how data is encoded, e.g., encoded in a matrix barcode such as a QR code, bar code, or multidimensional bar code encoded in PDF-417. Further, in some embodiments, determining a type of encoding may comprise determining a type of scanner, e.g., determining that the scanner signal is received from one or more different types of scanners **218**, e.g., scanners configured to detect information embedded in one or more of an image, a magnetic code (e.g., a magnetic strip), an

RFID, NFC, a SmartCard, an Integrated Circuit Card (ICC) or some other type of passive data. In still other embodiments, the type of encryption may be determined by processor **321** on a server connected to computing device **201** via a network connection.

(53) At step **506** the processor **202** extracts known data elements from the scanner signal. For example, the processor may be configured to extract data elements such as e.g., the name, date of birth, address, driver's license number, height, weight, state, county, race, organ donor status, issue date, expiration date, driver restriction, class of vehicle, passport information, criminal record information, or any other information stored based on the scanner signal. The processor **202** may extract this information by comparing the scanner signal to data stored in a local data store.

Alternatively, the processor **202** may execute algorithms to extract certain encoded data from the scanner signal. In still other embodiments, known data elements may be determined by processor **321** on a server connected to computing device **201** via a network connection.

(54) Then at step **508** processor **202** transmits data associated with the scanner signal to a server **320**. In some embodiments, processor **202** may compress data prior to transmission, e.g., the processor **202** may perform one or more compression algorithms to reduce network overhead and upload time in transmitting data associated with the scanner signal. Processor **202** may use network **210** to transmit the data. As discussed above, network **210** may comprise any type of wired and/or wireless network available to computing device **201**. In other embodiments, processing the image data may comprise extracting known elements from the image. For example, in some embodiments, the image may comprise non-encrypted PDF-417. In such an embodiment, processor **202** may extract available known data from the image. For example, in some embodiments, the processor **202** may resize the image to 640×480 pixels, transform the image to 24-bit grayscale with a quality of 80%, and convert the image to Base64 string representation.

(55) Processor **321** on server **320** may process the scanner signal to extract data from the scanner signal. Alternatively, in some embodiments, the processing may occur on processor **202** local to computing device **201**. In some embodiments, processing the scanner signal may comprise determining information about the scanner signal, e.g., a type of encoding or encryption type associated with the scanner signal. In some embodiments, processing the data may comprise comparing the data to a database. In other embodiments, rather than performing a line-by-line comparison to a database, the server may instead use a series of algorithms developed based on previous cards to determine the data. For example, the server may comprise a database **322** of data associated with identification cards. The server may further comprise a series of algorithms configured to determine information about identification cards.

(56) In some embodiments, these algorithms may have been developed using the data stored in database **322**. In some embodiments, these algorithms may enable the server to quickly determine identification data. For example, the server may use algorithms and logic to quickly determine the IIN Number associated with the card. Further, once the IIN number is identified, the server may use low overhead string functions to perform a lookup in a specially formatted string that contains all of the applicable values. In some embodiments, this may comprise using a Supertanker String Lookup technique during the data discovery process. These may comprise low overhead string functions to perform a lookup in a specially formatted string that contains all of the applicable values. For example, enclosing the ID Issue State/Province in dashes and looking for the index of its position in the following string: “-BC-, -MB-, -NF-, -PO-, -SK-, -ON-, -NS-, -NB-, -PE-”. In some embodiments, if the index is greater than zero, then the country of origin is Canada. Another example, putting a dash in front of the IIN and looking for the index of its position in a string like the following would return the corresponding state if valid: “-636033AL, -636059AK, -636026AZ, -636021AR”. In both of the above examples, the resources required to find the position of a string within another are much lower than doing a lookup in a table or other data structure.

(57) Further, in some embodiments, processing the image data comprises determining that there is enough captured data to start the process. In some embodiments, processing may also determine

whether the data was extracted from a magnetic stripe (e.g., via swiping a reader rather than a captured image) or a barcode. In some embodiments, processing the data may further comprise replacing any invalid binary characters and standardizing on the Track Sentinels. In some embodiments, processing the data may further comprise checking binary data points to determine if any information is encrypted (e.g., if the data comprises an encrypted driver's license or identification card). In some embodiments, the processing may further comprise replacing any invalid binary characters and determining the type of data (e.g., driver's license, military identification, passport, or some other data type).

(58) In some embodiments, the parsed data may be stored on the server **320**. In some embodiments, this information may be used for future processing and authentication.

(59) For example, in some embodiments, a user may not be able to authenticate more than one device within a set time period (e.g., one-day, one-week, one-month) to prevent a user from authenticating multiple age-restricted devices and distributing them. Further, in some embodiments, the server **320** may store the total amount of an age-restricted substance purchased by the user. In some embodiments, this information may be used to restrict the user's access to additional amounts of an age restricted substance. For example, one user may not be able to purchase over a certain quantity of the age-restricted substance in a set time period. In still other embodiments, the user's age, the total amount of a substance the user has purchased, and the time since the user's last purchased may all be used together to determine whether the user can purchase more of the age-restricted substance.

(60) Then at step **508**, server **320** transmits a data signal associated with the data extracted from the scanner signal. In some embodiments, this data signal comprises information associated with the age or identity of the user who scanned the identification card. Further, in some embodiments, this data includes whether the user is authorized to activate an age-restricted device **251**, e.g., the user is over a certain age and had not activated an age-restricted device within a certain time period.

(61) At step **510**, the computing device **201** receives the data signal from the server **320**. Then at step **512**, the computing device **201** transmits an activation signal to the age-restricted device **251**. The activation signal may be transmitted via either a wired or wireless network connection, e.g., via one or more of a Ethernet, USB, microUSB, Firewire, IEEE 1394, and/or wireless interfaces such as IEEE 802.11, Bluetooth, Near Field Communication, RFID, and/or radio interfaces for accessing cellular telephone networks (e.g., transceiver/antenna for accessing a CDMA, GSM, UMTS, or other mobile communications network(s)). The activation signal causes a processor **252** on the age-restricted device to activate the device and enable a user to access age-restricted material **254** on the device. For example, if the age-restricted device **251** is an e-cigarette, the activation signal will enable the user to use the e-cigarette. In some embodiments, the age-restricted device **251** is required to be activated only once. In other embodiments, the age-restricted device **251** must be activated each time a user attempts to use the device, or must be activated within a certain set period, e.g., every day, week, month, etc.

(62) Turning now to FIG. **6**, which is a flowchart showing an illustrative method **600** for age-restricted product registration. In some embodiments, the steps in flow chart **600** may be implemented in program code executed by a processor, for example, the processor in a general purpose computer, mobile device, or server. In some embodiments, these steps may be implemented by a group of processors. In some embodiments the steps shown in FIG. **5** may be performed in a different order. Alternatively, in some embodiments, one or more of the steps may be skipped or additional steps may be performed. The steps below are described with reference to components described above with regard to the systems described above with regard to FIGS. **2A**, **2B**, and **3**.

(63) At step **602** an age-restricted device **251** receives a verification signal from computing device **201**. The verification signal was determined based on scanning a passive data source and extracting data from the passive data source as described in the embodiments above.

(64) At step 604 a processor 252 activates the age-restricted device based on the verification signal. In some embodiments, the activation signal causes a processor 252 on the age-restricted device to activate the device and enable a user to access age-restricted material 254 on the device. For example, if the age-restricted device 251 is an e-cigarette, the activation signal will enable the user to use the e-cigarette. In some embodiments, the age-restricted device 251 is required to be activated only once. In other embodiments, the age-restricted device 251 must be activated each time a user attempts to use the device, or must be activated within a certain set period, e.g., every day, week, month, etc.

(65) In some embodiments, the systems and methods described above may be provided to application developers on a software development kit (SDK) that enables the developer (e.g., the developer of the webpage or IOS, Android, or Windows application) to quickly plug the functionality into their application or web page as a module. In other embodiments, an application or web page development company may develop its own image capture software, but may be given access to image processing capability using the database and algorithms described herein. In other embodiments, the database of data associated with identification card data may be sold to application or web page development companies. In other embodiments, only portions of the database may be sold or made available, e.g., only the segment of the database associated with a state, region, or government entity. In other embodiments, algorithms developed to determine identification data associated only a certain region may be made available.

GENERAL CONSIDERATIONS

(66) The methods, systems, and devices discussed above are examples. Various configurations may omit, substitute, or add various procedures or components as appropriate.

(67) For instance, in alternative configurations, the methods may be performed in an order different from that described, and/or various stages may be added, omitted, and/or combined. Also, features described with respect to certain configurations may be combined in various other configurations. Different aspects and elements of the configurations may be combined in a similar manner. Also, technology evolves and, thus, many of the elements are examples and do not limit the scope of the disclosure or claims.

(68) Specific details are given in the description to provide a thorough understanding of example configurations (including implementations). However, configurations may be practiced without these specific details. For example, well-known circuits, processes, algorithms, structures, and techniques have been shown without unnecessary detail in order to avoid obscuring the configurations. This description provides example configurations only, and does not limit the scope, applicability, or configurations of the claims. Rather, the preceding description of the configurations will provide those skilled in the art with an enabling description for implementing described techniques. Various changes may be made in the function and arrangement of elements without departing from the spirit or scope of the disclosure.

(69) Also, configurations may be described as a process that is depicted as a flow diagram or block diagram. Although each may describe the operations as a sequential process, many of the operations can be performed in parallel or concurrently. In addition, the order of the operations may be rearranged. A process may have additional steps not included in the figure. Furthermore, examples of the methods may be implemented by hardware, software, firmware, middleware, microcode, hardware description languages, or any combination thereof. When implemented in software, firmware, middleware, or microcode, the program code or code segments to perform the necessary tasks may be stored in a non-transitory computer-readable medium such as a storage medium. Processors may perform the described tasks.

(70) Having described several example configurations, various modifications, alternative constructions, and equivalents may be used without departing from the spirit of the disclosure. For example, the above elements may be components of a larger system, wherein other rules may take precedence over or otherwise modify the application of the invention. Also, a number of steps may

be undertaken before, during, or after the above elements are considered.

(71) Accordingly, the above description does not bound the scope of the claims.

(72) The use of “adapted to” or “configured to” herein is meant as open and inclusive language that does not foreclose devices adapted to or configured to perform additional tasks or steps.

Additionally, the use of “based on” is meant to be open and inclusive, in that a process, step, calculation, or other action “based on” one or more recited conditions or values may, in practice, be based on additional conditions or values beyond those recited. Headings, lists, and numbering included herein are for ease of explanation only and are not meant to be limiting.

(73) Embodiments in accordance with aspects of the present subject matter can be implemented in digital electronic circuitry, in computer hardware, firmware, software, or in combinations of the preceding. In one embodiment, a computer may comprise a processor or processors. The processor comprises or has access to a computer-readable medium, such as a random access memory (RAM) coupled to the processor. The processor executes computer-executable program instructions stored in memory, such as executing one or more computer programs including a sensor sampling routine, selection routines, and other routines to perform the methods described above.

(74) Such processors may comprise a microprocessor, a digital signal processor (DSP), an application-specific integrated circuit (ASIC), field programmable gate arrays (FPGAs), and state machines. Such processors may further comprise programmable electronic devices such as PLCs, programmable interrupt controllers (PICs), programmable logic devices (PLDs), programmable read-only memories (PROMs), electronically programmable read-only memories (EPROMs or EEPROMs), or other similar devices. Such processors may comprise, or may be in communication with, media, for example tangible computer-readable media, that may store instructions that, when executed by the processor, can cause the processor to perform the steps described herein as carried out, or assisted, by a processor. Embodiments of computer-readable media may comprise, but are not limited to, all electronic, optical, magnetic, or other storage devices capable of providing a processor, such as the processor in a web server, with computer-readable instructions. Other examples of media comprise, but are not limited to, a floppy disk, CD-ROM, magnetic disk, memory chip, ROM, RAM, ASIC, configured processor, all optical media, all magnetic tape or other magnetic media, or any other medium from which a computer processor can read. Also, various other devices may include computer-readable media, such as a router, private or public network, or other transmission device. The processor, and the processing, described may be in one or more structures, and may be dispersed through one or more structures. The processor may comprise code for carrying out one or more of the methods (or parts of methods) described herein.

(75) While the present subject matter has been described in detail with respect to specific embodiments thereof, it will be appreciated that those skilled in the art, upon attaining an understanding of the foregoing may readily produce alterations to, variations of, and equivalents to such embodiments. Accordingly, it should be understood that the present disclosure has been presented for purposes of example rather than limitation, and does not preclude inclusion of such modifications, variations and/or additions to the present subject matter as would be readily apparent to one of ordinary skill in the art. For instance, in some embodiments, there may be a system for activating an age-restricted device, the system comprising: a scanner configured to scan a passive data source on an identification card; and a processor coupled to the scanner, the processor configured to: receive a scanner signal from the scanner; verify an age of a user based on the scanner signal; and transmit a verification signal to an age-restricted device.

(76) Other embodiments may include the above system wherein verifying an age of the user comprises: determining a type of encryption associated with the passive data source; and extracting one or more known data elements from the passive data source.

(77) Other embodiments may include the above system wherein extracting one or more known data elements comprises: transmitting data associated with the passive data source to a server configured to: extract a date of birth from the passive data source; and transmit the date of birth to a

device associated with the scanner.

(78) Other embodiments may include the above system wherein the server is further configured to: extract data comprising one or more of: a first name, a last name, an address, a city, a state, a zip code, an issue date, or an expiration date from the passive data source; and transmit the extracted data to a device associated with the scanner.

(79) Other embodiments may include the above system wherein the server is further configured to determine whether a user is an authorized user.

(80) Other embodiments may include the above system wherein determining whether the user is an authorized user comprises determining whether the user has activated another age-restricted device within a predefined time period.

(81) Other embodiments may include the above system wherein the age-restricted device is in communication with the processor via a network connection comprising one or more of: Bluetooth, RFID, or NFC.

(82) Other embodiments may include the above system wherein the scanner comprises a digital camera on a smartphone and wherein the processor is configured to crop an image of the passive data source.

(83) Other embodiments may include the above system wherein the passive data source comprises one or more of: data encoded in a Near Field Communication (NFC) device, a Radio-frequency identification (RFID) chip, a SmartCard, an Integrated Circuit Card (ICC), a magnetic strip, a quick response (QR) code, optical media, or PDF-417.

(84) Other embodiments may include the above system wherein the age-restricted device comprises an electronic cigarette.

(85) A system for activating an age-restricted device, the system comprising: a processor configured to receive an age verification signal and activate the age-restricted device based on the age verification signal; and a network interface configured to receive a verification signal from a remote device, wherein the remote device comprises: a scanner configured to scan a passive data source on an identification card; and a processor coupled to the scanner, the processor configured to: receive a scanner signal from the scanner; verify an age of a user based on the scanner signal; and transmit the verification signal to the age-restricted device.

(86) Other embodiments may include the above system wherein verifying an age of the user comprises: determining a type of encryption associated with the passive data source; and extracting one or more known data elements from the passive data source.

(87) Other embodiments may include the above system wherein extracting one or more known data elements comprises: transmitting data associated with the passive data source to a server configured to: extract a date of birth from the passive data source; and transmit the date of birth to a device associated with the scanner.

(88) Other embodiments may include the above system wherein the server is further configured to: extract data comprising one or more of: a first name, a last name, an address, a city, a state, a zip code, an issue date, or an expiration date from the passive data source; and transmit the extracted data to a device associated with the scanner.

(89) Other embodiments may include the above system wherein the server is further configured to determine whether a user is an authorized user.

(90) Other embodiments may include the above system wherein determining whether the user is an authorized user comprises determining whether the user has activated another age-restricted device within a predefined time period.

(91) Other embodiments may include the above system wherein the age-restricted device is in communication with the processor via a network connection comprising one or more of: Bluetooth, RFID, or NFC.

(92) Other embodiments may include the above system wherein the scanner comprises a digital camera on a smartphone and wherein the processor is configured to crop an image of the passive

data source.

(93) Other embodiments may include the above system wherein the passive data source comprises one or more of: data encoded in a Near Field Communication (NFC) device, a Radio-frequency identification (RFID) chip, a SmartCard, an Integrated Circuit Card (ICC), a magnetic strip, a quick response (QR) code, optical media, or PDF-417.

(94) Other embodiments may include the above system wherein the age-restricted device comprises an electronic cigarette.

(95) Some alternative embodiments may include a method for activating an age-restricted device, the method comprising: receiving a scanner signal from a scanner configured to scan a passive data source on an identification card; verifying an age of a user based on the scanner signal; and transmitting a verification signal to an age-restricted device.

(96) Other embodiments may include the above method wherein verifying an age of the user comprises: determining a type of encryption associated with the passive data source; and extracting one or more known data elements from the passive data source.

(97) Other embodiments may include the above method wherein extracting one or more known data elements comprises: transmitting data associated with the passive data source to a server configured to: extract a date of birth from the passive data source; and transmit the date of birth to a device associated with the scanner.

(98) Other embodiments may include the above method wherein the server is further configured to: extract data comprising one or more of: a first name, a last name, an address, a city, a state, a zip code, an issue date, or an expiration date from the passive data source; and transmit the extracted data to a device associated with the scanner.

(99) Other embodiments may include the above method wherein the server is further configured to determine whether a user is an authorized user.

(100) Other embodiments may include the above method wherein determining whether the user is an authorized user comprises determining whether the user has activated another age-restricted device within a predefined time period.

(101) Other embodiments may include the above method wherein the scanner comprises a digital camera on a smartphone and wherein the method further comprises cropping an image of the passive data source.

(102) Other embodiments may include the above method wherein the passive data source comprises one or more of: data encoded in a Near Field Communication (NFC) device, a Radio-frequency identification (RFID) chip, a SmartCard, an Integrated Circuit Card (ICC), a magnetic strip, a quick response (QR) code, optical media, or PDF-417.

(103) Other embodiments may include the above method wherein the age-restricted device comprises an electronic cigarette.

(104) In yet certain embodiments there may be a method for activating an age-restricted device, the method comprising: receiving an age verification signal from a remote device, wherein the remote device comprises: a scanner configured to scan a passive data source on an identification card; and a processor coupled to the scanner, the processor configured to: receive a scanner signal from the scanner; verify an age of a user based on the scanner signal; transmit the verification signal to the age-restricted device; and activating the age-restricted device based on the age verification signal.

(105) Other embodiments may include the above method wherein verifying an age of the user comprises: determining a type of encryption associated with the passive data source; and extracting one or more known data elements from the passive data source.

(106) Other embodiments may include the above method wherein extracting one or more known data elements comprises: transmitting data associated with the passive data source to a server configured to: extract a date of birth from the passive data source; and transmit the date of birth to a device associated with the scanner.

(107) Other embodiments may include the above method wherein the server is further configured

to extract data comprising one or more of: a first name, a last name, an address, a city, a state, a zip code, an issue date, or an expiration date from the passive data source; and transmit the extracted data to a device associated with the scanner.

(108) Other embodiments may include the above method wherein the server is further configured to determine whether a user is an authorized user.

(109) Other embodiments may include the above method wherein determining whether the user is an authorized user comprises determining whether the user has activated another age-restricted device within a predefined time period.

(110) Other embodiments may include the above method wherein the age-restricted device is in communication with the processor via a network connection comprising one or more of: Bluetooth, RFID, or NFC.

(111) Other embodiments may include the above method wherein the scanner comprises a digital camera on a smartphone and wherein the processor is configured to crop an image of the passive data source.

(112) Other embodiments may include the above method wherein the passive data source comprises one or more of: data encoded in a Near Field Communication (NFC) device, a Radio-frequency identification (RFID) chip, a SmartCard, an Integrated Circuit Card (ICC), a magnetic strip, a quick response (QR) code, optical media, or PDF-417.

(113) Other embodiments may include the above method wherein the age-restricted device comprises an electronic cigarette.

(114) Any advantages and benefits described may not apply to all embodiments of the invention. When the word “means” is recited in a claim element, Applicant intends for the claim element to fall under 35 USC 112(f). Often a label of one or more words precedes the word “means”. The word or words preceding the word “means” is a label intended to ease referencing of claims elements and is not intended to convey a structural limitation. Such means-plus-function claims are intended to cover not only the structures described herein for performing the function and their structural equivalents, but also equivalent structures. For example, although a nail and a screw have different structures, they are equivalent structures since they both perform the function of fastening. Claims that do not use the word “means” are not intended to fall under 35 USC 112(f).

(115) The foregoing description of the embodiments of the invention has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many combinations, modifications and variations are possible in light of the above teaching. For instance, in certain embodiments, each of the above described components and features may be individually or sequentially combined with other components or features and still be within the scope of the present invention. Undescribed embodiments which have interchanged components are still within the scope of the present invention. It is intended that the scope of the invention be limited not by this detailed description, but rather by the claims.

Claims

1. A system comprising: an age verification system configured to verify an age of a user; an aerosol delivery device comprising: hardware that provides aerosol to the user; and an accessory configured to provide access to age restricted material of the aerosol delivery device when the accessory is unlocked, wherein the accessory is unlocked in response to the user being authenticated with the age verification system; wherein the accessory is initially unlocked in response to the user performing an initial age verification with the age verification system by providing an electronic identification card, and the accessory is subsequently unlocked in response to an authentication that comprises a verification of a user's identity without requiring evidence of age.

2. The system of claim 1, wherein the user is authenticated by the accessory communicating with

the age verification system.

3. The system of claim 2, wherein the accessory further comprises authentication circuitry configured for communication with the age verification system.

4. The system of claim 1, wherein the accessory couples a power supply with the aerosol delivery device.

5. The system of claim 4, further comprising a host device coupled with the accessory, wherein the host device provides communication with the age verification system over a network.

6. The system of claim 5, further comprising a network through which the age verification system is coupled with the host device.

7. An accessory for an aerosol delivery device comprising: an interface that is configured to provide access to age restricted material within the aerosol delivery device; and authentication circuitry that is configured to receive an age verification of a user, wherein the access is not provided to the aerosol delivery device without the age verification by providing an electronic identification card; subsequently transitioning from preventing the access from being provided to the aerosol delivery device to permitting the access to be provided to the aerosol delivery device in response to a subsequent authentication that comprises a verification of a user's identity without requiring the evidence of age.

8. The accessory of claim 7, wherein the interface comprises a switch configured to provide the access via an interface on the accessory to the aerosol delivery device upon the age verification, and further wherein the switch does not allow the access via the interface when the age verification fails.

9. The accessory of claim 7, wherein the age verification comprises an authentication that includes communicating with an age verification system over a network.

10. The accessory of claim 9, wherein the authentication is required and references the age verification of the user.

11. The accessory of claim 9, wherein an initial age verification operation is performed using identifying documentation.

12. The accessory of claim 7, wherein the age verification comprises an initial age verification for a user and comprises subsequent authentications of that user.

13. The accessory of claim 12, wherein the initial age verification comprises an association of a user with an age, such that the subsequent authentications comprise requests to authenticate the association with the user.

14. The accessory of claim 13, wherein the initial age verification occurs around a time of purchase.

15. The accessory of claim 12, further comprising I/O components to facilitate connection to one or more user interfaces.

16. The accessory of claim 12, wherein subsequent authentications comprises data for subsequent authentications to data stored from the initial age verification for the user.

17. The accessory of claim 7, further comprising a sensor configured to detect a passive data-source.

18. The accessory of claim 7, wherein the accessory is configured to be a host device.

19. The accessory of claim 18, wherein the host device is configured to communicate with an age verification system over a network regarding the age verification.

20. The accessory of claim 18, wherein the host device is configured to communicate with the accessory through electric pulses or data pulses.

21. The accessory of claim 7, wherein the aerosol delivery device comprises a bus for assisting with delivery of the age restricted material.

22. A method for operating a charging accessory with an age restricted device, the method comprising: receiving an initial age verification for a user by providing an electronic identification card; accessing, when the age verification is authenticated, the age restricted device; preventing

from accessing, when the age verification is not authenticated, the age restricted device; and subsequently transitioning from preventing the accessing to permitting the access to be provided to the age restricted device in response to a subsequent authentication that comprises a verification of a user's identity without requiring evidence of age.

23. The method of claim 22, further comprising: communicating, over a network, with an age verification system for receiving the age verification of the user.

24. The method of claim 23, wherein the age verification comprises information on whether the user has a verified age or not.
