Attachment #33

Angel Lopez, 9/18/19 material

Testimony of Angel Lopez, *Resident of Providence* – *Delivered on 9/18/19*

§ 9-1-28.1. Right to privacy – Action for deprivation of right.

(a) *Right to privacy created.* It is the policy of this state that every person in this state shall have a right to privacy which shall be defined to include any of the following rights individually:

(1) The right to be secure from unreasonable intrusion upon one's physical solitude or seclusion;

http://webserver.rilin.state.ri.us/Statutes/TITLE9/9-1/9-1-28.1.HTM

Privacy in the most basic sense is the right to secure personal experiences, personal feelings, and possessions that are solely and exclusively my own. It is my choice if my feelings and experiences are shared. They are my possessions like my voice, face, eyes, fingerprints, DNA, and the vibratory frequencies of all my organs working in conjunction as I walk, exercise, or sleep. I am the exclusive owner of my experiences, feelings and biometrics, they are my gifts of life and that is what sets me apart from you and each of you from each other. None of these should be gathered or captured without my consent or knowledge and should never be shared, sold, or grouped within criminal or terrorist databases without my knowledge just because of my origins, culture, race, class, or religious beliefs.

I would like to bring to your attention US Patent US 10,020,004 B2 titled "Listening to the Frontend". This patent was submitted by Wal-Mart Stores, Inc. and approved on July 10, 2018. This patent in my view is the data input for an automated manager that will receive and decipher sounds, for the purpose of indicating an employee and a guest of a store to determine the performance metric of an employee. Please view the following 6 figures from the patent. I will begin with figure 6 then go from 1-5 in order to express my data input to an automated manager claim.

Fig. 1 shows all the devices including sensors on the ceiling and electronics at the point of sale. Figure 2 shows the frequencies of sound emitted by devices guests use (shopping carts in this case). Figures 3 and 4 illustrate two different set of frequencies that after analyzed will show the length of the line, the zone, and the location of each customer. All these sounds get switch over to frequencies illustrated as 500s in figure 5 for proper categorization and analytics. I don't know your thoughts here if you are only thinking profit or of a superior management system, but I see an excessive use of additional radio frequencies being placed near children, elderly, infants, disabled, our families and ourselves with-out considering the cellular, radio, television, other electro-magnetic or soon to be 5G frequencies that already surround us. Would any of you seriously be willing to expose your new-born infant to all these frequencies knowingly. Are all doctors in this state aware of the potential health effects of being exposed to this many radio frequencies for the long periods of time that the cashiers working in this environment will be exposed to. We are reaching the point where if we don't protect our privacy, we are putting our health at risk.

Now lets' look at US Patent US 10,108,984 B2 title "Detecting Body Language Via Bone Conduction". This patent was submitted by AT&T Intellectual Property and approved on

US010020004B2

(12) **United States Patent**
Jones et al.

(10) **Patent No.: US 10,020,004 B2**
(45) **Date of Patent: Jul. 10, 2018**

(54) **LISTENING TO THE FRONTEND**

(71) Applicant: **Wal-Mart Stores, Inc.**, Bentonville, AR (US)

(72) Inventors: **Nicholaus A. Jones**, Fayetteville, AR (US); **Aaron J. Vasgaard**, Rogers, AR (US); **Robert J. Taylor**, Rogers, AR (US); **Matthew A. Jones**, Bentonville, AR (US)

(73) Assignee: **WALMART APOLLO, LLC**, Bentonville, AR (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **15/492,608**

(22) Filed: **Apr. 20, 2017**

(65) **Prior Publication Data**

US 2017/0309290 A1 Oct. 26, 2017

Related U.S. Application Data

(60) Provisional application No. 62/325,589, filed on Apr. 21, 2016, provisional application No. 62/334,796, filed on May 11, 2016.

(51) **Int. Cl.**

G10L 21/02	(2013.01)
G10L 21/0208	(2013.01)
G10L 19/02	(2013.01)
G10L 25/18	(2013.01)

(52) **U.S. Cl.**

CPC ***G10L 21/0208*** (2013.01); ***G10L 19/02*** (2013.01); *G10L 25/18* (2013.01)

(58) **Field of Classification Search**

CPC G10L 21/0208; G10L 19/02; G10L 25/18
USPC 340/7.4–7.45
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,044,353	A	3/2000	Pugliese
7,309,965	B2	12/2007	Dowling
8,462,212	B1	6/2013	Kundu
8,706,555	B2	4/2014	Argue
2002/0178048	A1	11/2002	Huffman
2003/0164398	A1	9/2003	Walker
2007/0186515	A1	8/2007	Ruetten
2009/0265258	A1	10/2009	Regard

(Continued)

FOREIGN PATENT DOCUMENTS

WO	2014185883	11/2014

OTHER PUBLICATIONS

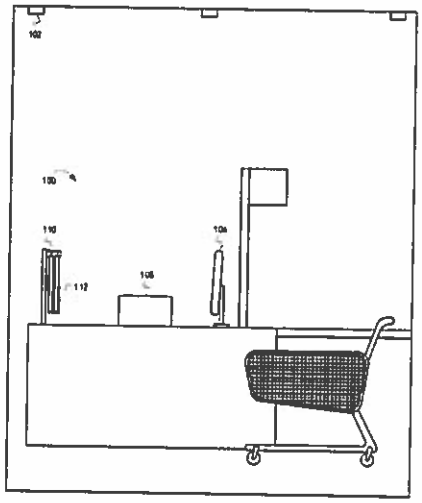
PCT, App. No. PCT/US2017/028823; International Search Report and Written Opinion dated Jul. 13, 2017.

Primary Examiner — Allen T Cao
(74) *Attorney, Agent, or Firm* — Fitch, Even, Tabin & Flannery, LLP

(57) **ABSTRACT**

In some embodiments, apparatuses, and methods are provided herein pertaining to sound analysis in a shopping facility. In some embodiments, a system comprises one or more sound sensors distributed throughout at least a portion of a shopping facility and configured to receive at least sounds resulting from activity in the shopping facility and a control circuit, the control circuit configured to receive, from at least one of the one or more sound sensors, audio data, receive an indication of an employee, correlate the audio data and in the indication of the employee, and determine, based at least in part on the audio data and the indication of the employee, a performance metric for the employee.

20 Claims, 6 Drawing Sheets



Lopez Pg. 2 of 15

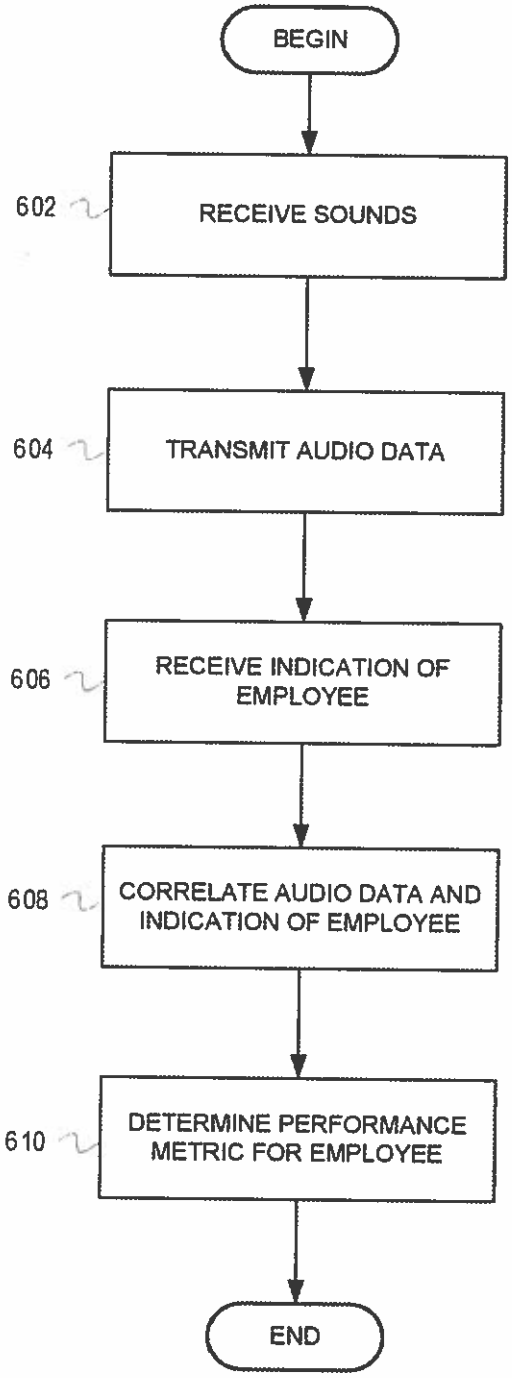

BEGIN
602
RECEIVE SOUNDS
604
TRANSMIT AUDIO DATA
606
RECEIVE INDICATION OF EMPLOYEE
608
CORRELATE AUDIO DATA AND INDICATION OF EMPLOYEE
610
DETERMINE PERFORMANCE METRIC FOR EMPLOYEE
END

FIG. 6

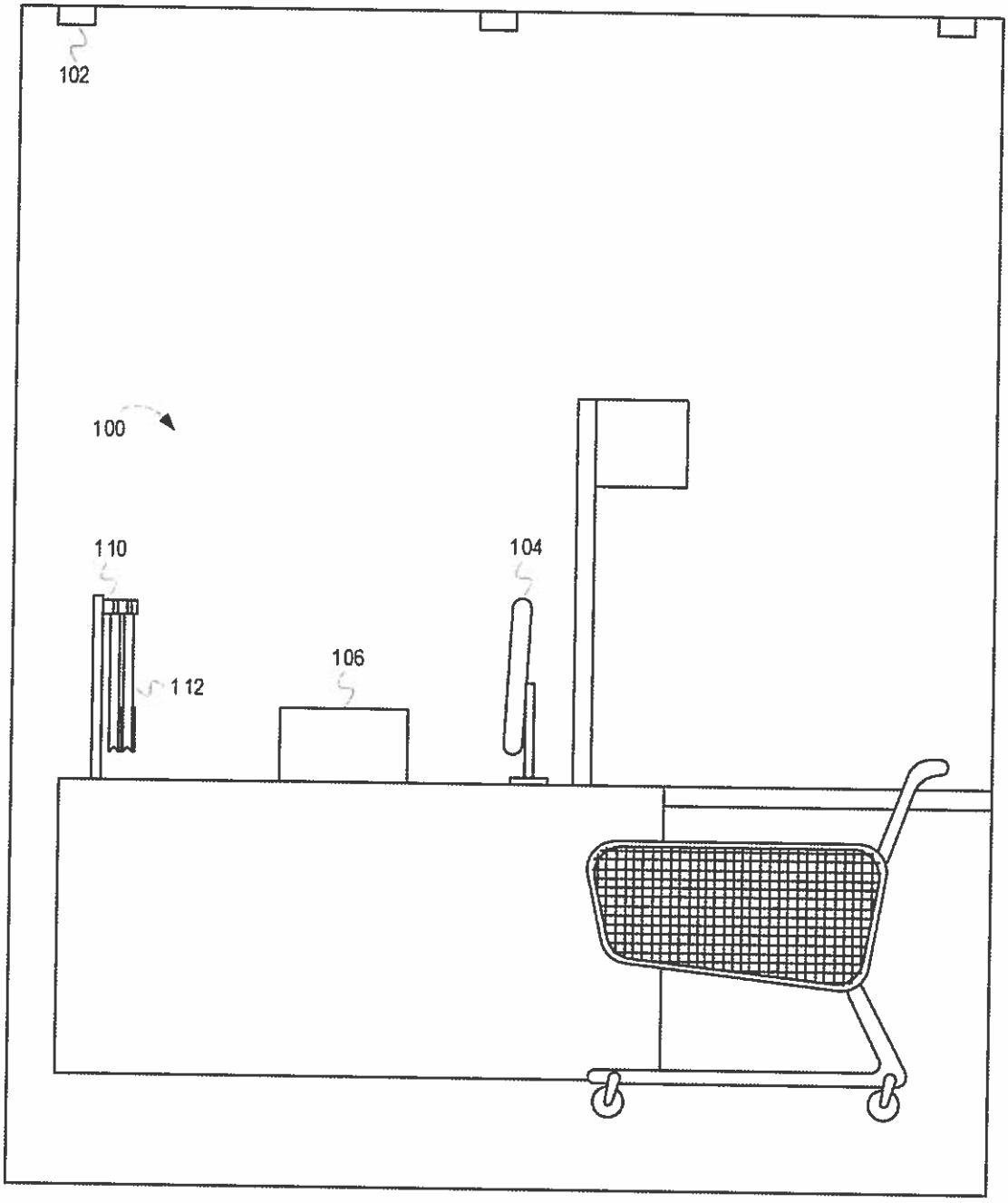


FIG. 1

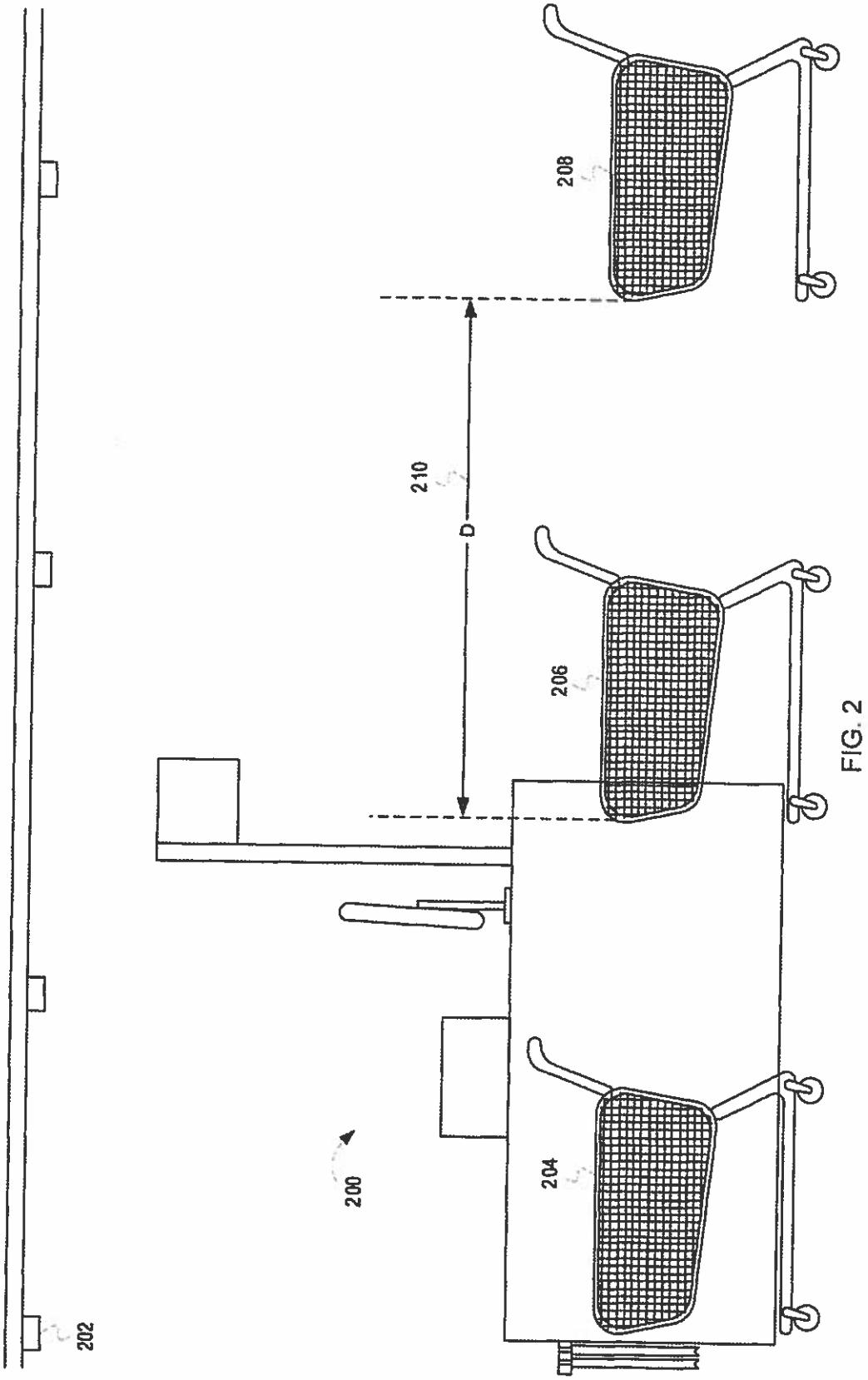


FIG. 2

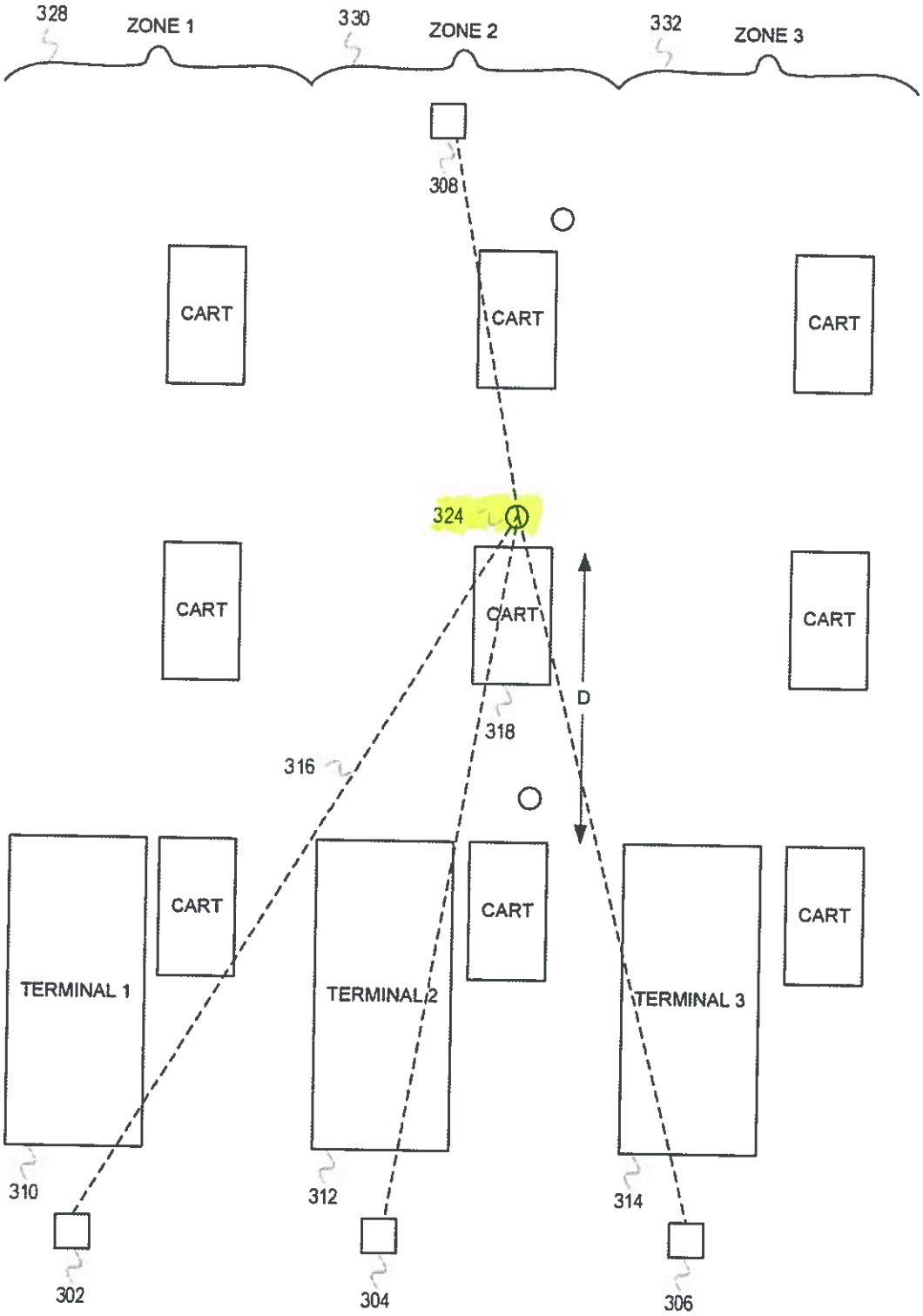

328
ZONE 1
330
ZONE 2
332
ZONE 3
308
CART
CART
CART
324
CART
CART
CART
D
318
316
CART
CART
CART
TERMINAL 1
TERMINAL 2
TERMINAL 3
310
312
314
302
304
306

FIG. 3

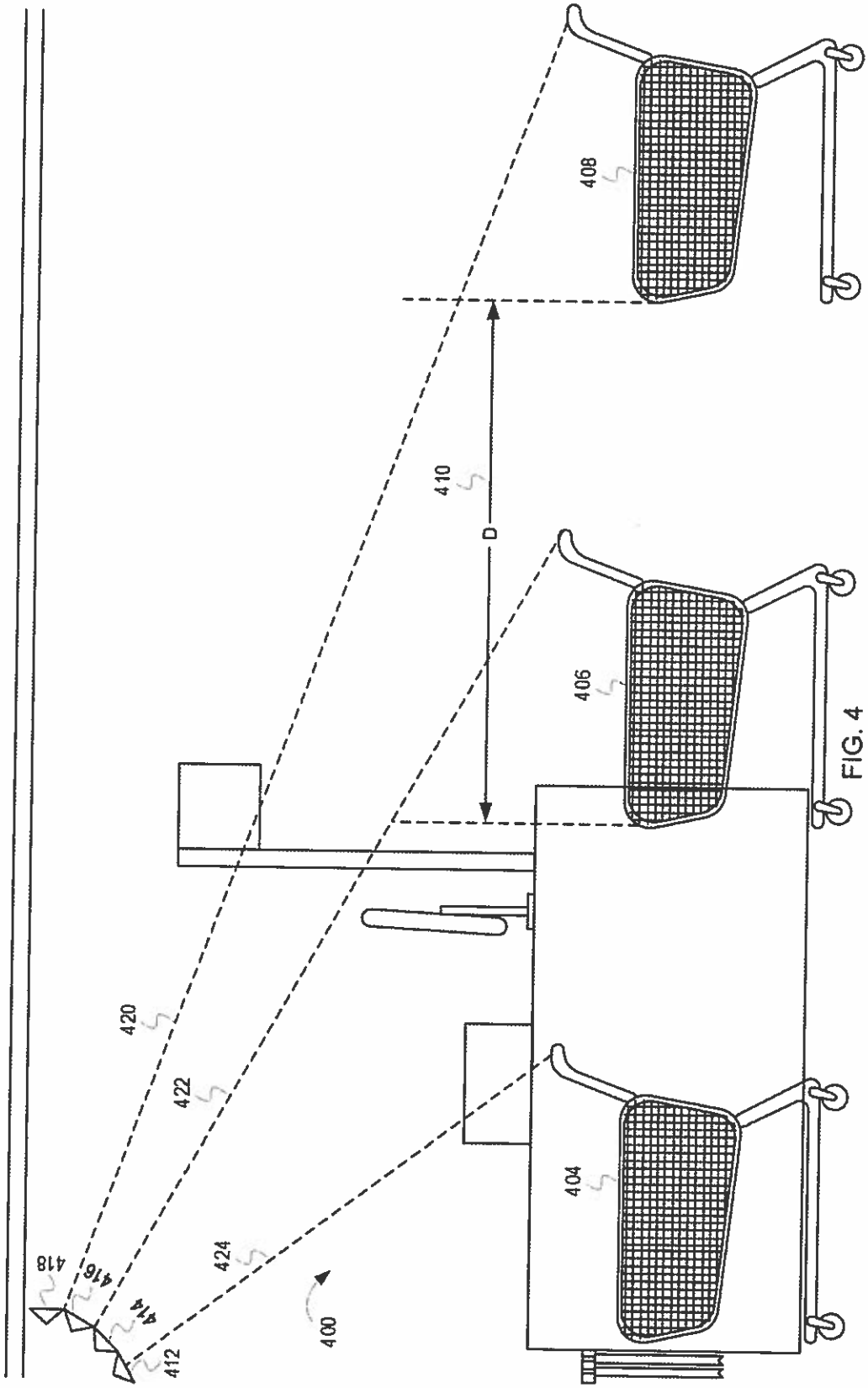


FIG. 4

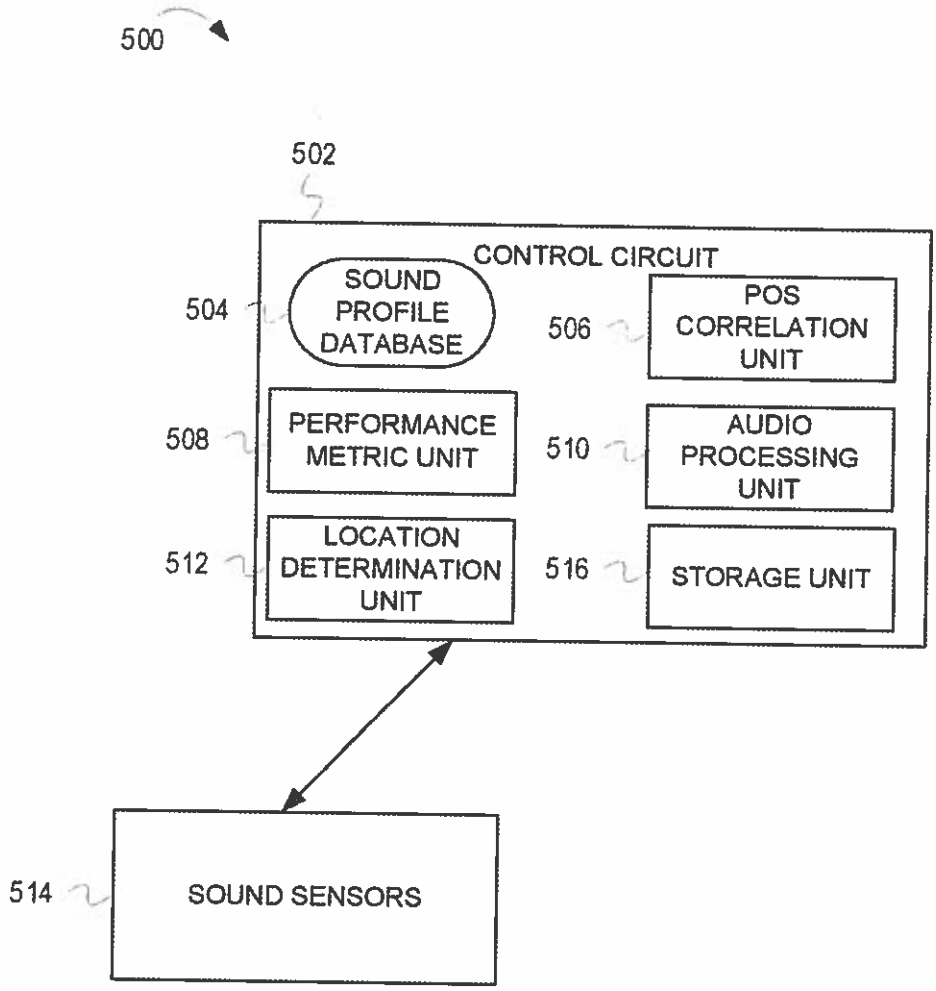

500
502
CONTROL CIRCUIT
504
SOUND PROFILE DATABASE
506
POS CORRELATION UNIT
508
PERFORMANCE METRIC UNIT
510
AUDIO PROCESSING UNIT
512
LOCATION DETERMINATION UNIT
516
STORAGE UNIT
514
SOUND SENSORS

FIG. 5

October 23,2018. This patent shows a device that can detect the body language of an individual and generate a signal to send to a network connected to the individual. Figure 1 in this diagram clearly depicts the use of the internet of things (5G capabilities). Even the definition of a Noun in the English language separates a person from a thing, but in the case of the internet of things there is no distinction.

Now, the purpose of detecting body language via bone conduction in US patent 10,108,984 is for the purpose of sending ads or marketing to an individual to meet the needs based on their mood. If you are thinking profit, is it far fetched that a new set of frequencies will be added near or at the same check out area for the purpose of sending an additional advertisement to the consumer for something they forgot to buy or something that will make them feel better?

We all know that consumer credit information is not as safe or secure as it should be. Equifax breach in 2017 (148 Million affected), GOP Data firm Deep Root Analytics data breach of 2017 (198 Million affected), the recent Capital One data breach in 2019 (100 Million affected).

GOP Data Firm Accidentally Leaks Personal Details of Nearly 200 Million American Voters, written on 6/19/2017
https://gizmodo.com/gop-data-firm-accidentally-leaks-personal-details-of-ne-1796211612

198 Million Affected

Along with home addresses, birthdates, and phone numbers, the records include advanced sentiment analyses used by political groups to predict where individual voters fall on hot-button issues such as gun ownership, stem cell research, and the right to abortion, as well as suspected religious affiliation and ethnicity.

Deep Root Analytics, a conservative data firm that identifies audiences for political ads, confirmed ownership of the data to Gizmodo on Friday.

The Equifax Data Breach: What to Do, written on 9/8/2017
https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

143 Million Consumers affected. "The breach lasted from mid-May through July. The hackers accessed people's names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers."

Information on the Capital One Cyber Incident, updated on 8/4/2019
https://www.capitalone.com/facts2019/

100 Million US individuals affected 6 Million in Canada

Data Compromised:

- About 140,000 Social Security numbers of our credit card customers.
- About 80,000 linked bank account numbers of our secured credit card customers.

Even RI's Consumer Empowerment and Identity Theft Protection Act of 2006 aims to put the consumer in further control of their identity and credit data by allowing the consumer to call for a security freeze if personal data is being used for purposes other than their own. Do you know what companies are interested in the biometric information of everyone including children? Are you 100% sure that those corporations intend to protect your privacy and your biometric information when devices that capture biometric information are popping up in residential buildings in New York City, neighborhoods in Detroit, and quite possibly in neighborhoods of Providence. See colored pictures. They were taken over the last 30 days in the same neighborhood of Providence.

These pictures also show how far this state has allowed corporations to abuse certain populations of its residents. However, while the topic around Congress is Facial Recognition the state of RI is debating biometric information without considering the impact it will have on all residents of the State. Biometric capturing technology will not empower residents or promote economic growth within the state. Instead it will commodify that which exclusively belongs to ourselves for the purpose of profit which given the recent data breaches I mentioned security will not ~~have~~ play a role. We never needed biometric verification to surf the net, make purchases, or use an app over the internet. This is not a time to begin demanding that we the residents give up our privacy to use the internet so that inadequate and misleading corporations profit off our data. Allowing biometric data capturing is an investment in artificial, secondary intelligence and not the natural superior intelligence that all residents of RI possess.

The fact that the internet of things(5G)makes no distinction between people and things, is forbidding us of our privacy. Illinois implemented Biometric Information Protection Act (BIPA) in 2008 and residents are suing Facebook for violating it.

These are a couple of the legislative findings of BIPA.

http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004 **not the full Bill**

Biometric Information Protection Act (BIPA) – 2008 State of Illinois

Section 5: Legislative Findings Section

(c) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

(g) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.
(Source: P.A. 95-994, eff. 10-3-08.)

SEP 14 '05 10:1

Article about Illinois Facebook user's lawsuit

https://www.theguardian.com/technology/2019/aug/09/facebook-facial-recognition-lawsuit-can-proceed-us-court

1st two paragraphs. Article written on 8/9/2019 Illinois users' lawsuit against Facebook can move forward 3-0 vote from San Francisco Circuit Court.

A US federal appeals court has rejected Facebook's effort to undo a class action lawsuit alleging it illegally collected and stored biometric data for millions of users without their consent using facial recognition technology.

In 2019 San Francisco, Oakland, and Somerville, MA have banned or are in process of banning biometric capturing and even stop police from using it. If you are unaware of what protection of Privacy looks like read H.R. 4008 the "No Biometric Barriers to Housing Act of 2019". I will summarize 3 definitions in the bill that describe biometric data capturing technology appropriately unlike RI Bills H5930 and S234 that were presented to the General Assembly of RI during 2019.

Facial Recognition Technology – technology that identifies an individual based on physical characteristics of the individuals face, or that logs characteristics of an individual's face, head, or body to infer emotion, associations, activities, or location.

Physical Biometric Recognition Technology – technology that identifies an individual or captures information about an individual based on DNA, fingerprints, palm prints, iris, or retina.

Remote Biometric Recognition Technology – Identifies an individual or captures information about the characteristics of an individual based on gait (walk) voice, or other immutable characteristic made for certain from a distance. It logs characteristics to infer emotion, associations, activities, or location of the individual.

In order to properly describe "other immutable characteristic(s)", I will repeat statements made earlier in my testimony "vibratory frequencies of all my organs working in conjunction as I walk, exercise, or sleep" I stated this earlier when I described possessions that are exclusively my own, and revisit the illustrations of Figure 3 from US Patent 10,020,004 "Listening to the Frontend" Signal 324 and Figure 1 from US Patent 10,108,984 "Detecting Body Language Via Bone Conduction" Signals 102 and 104.

Given these three definitions, if I am around such technologies because of where I shop, exercise, or even sleep my person is being subjected to unwarranted searches and seizures via invasive radio frequencies. I am not a lawyer, but I think this violates my 4th Amendment Rights. This also violates my right to privacy and puts my health at risk. I look forward to discussing further how we can protect the privacy of all residents in this state. Children face the biggest risk here from classified and or targeted health impacts to biometric theft leading to the loss of self-ownership.
-END

US010108984B2

(12) **United States Patent**
Baldwin et al.

(10) **Patent No.: US 10,108,984 B2**
(45) **Date of Patent: Oct. 23, 2018**

(54) **DETECTING BODY LANGUAGE VIA BONE CONDUCTION**

(71) Applicant: **AT&T Intellectual Property I, L.P.**, Atlanta, GA (US)

(72) Inventors: **Christopher Baldwin**, Crystal Lake, IL (US); **Brian S. Amento**, Morris Plains, NJ (US)

(73) Assignee: **AT&T Intellectual Property I, L.P.**, Atlanta, GA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 338 days.

(21) Appl. No.: **14/065,663**

(22) Filed: **Oct. 29, 2013**

(65) **Prior Publication Data**

US 2015/0120465 A1 Apr. 30, 2015

(51) **Int. Cl.**

G06F 21/32	(2013.01)
H04W 12/10	(2009.01)
H04L 29/06	(2006.01)
G06Q 30/02	(2012.01)
H04W 12/12	(2009.01)
G06K 9/00	(2006.01)

(52) **U.S. Cl.**

CPC ***G06Q 30/0269*** (2013.01); ***H04L 63/0853*** (2013.01); ***H04L 63/0861*** (2013.01); ***H04L 63/1416*** (2013.01); ***H04L 63/1466*** (2013.01); ***H04W 12/12*** (2013.01); *G06K 2009/00939* (2013.01); *H04L 2463/121* (2013.01)

(58) **Field of Classification Search**

None

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

3,629,521	A	12/1971	Puharich et al.
4,048,986	A	9/1977	Ott
4,340,778	A	7/1982	Cowans et al.
4,421,119	A	12/1983	Pratt
4,720,607	A	1/1988	de Moncuit
4,754,763	A	7/1988	Doemland
4,799,498	A	1/1989	Collier

(Continued)

FOREIGN PATENT DOCUMENTS

AU	2003257031	2/2004
AU	2007200415	8/2007

(Continued)

OTHER PUBLICATIONS

U.S. Office Action dated Mar. 8, 2010 in U.S. Appl. No. 11/586,142.

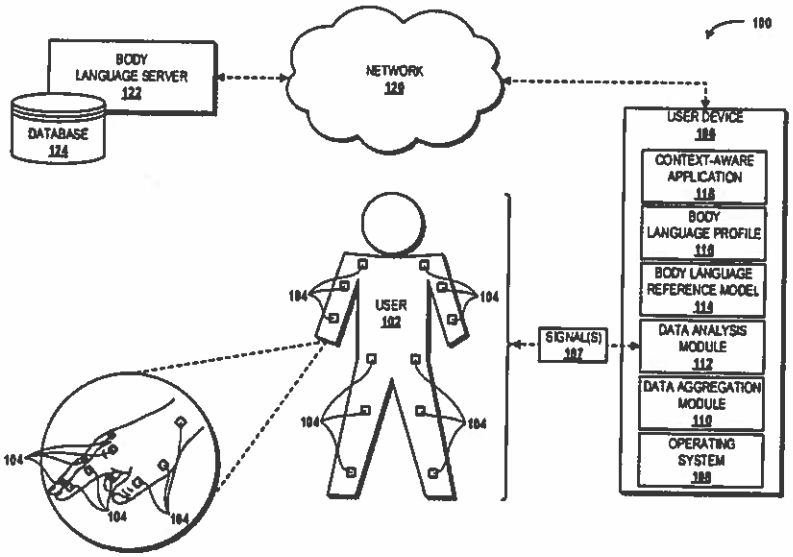
(Continued)

Primary Examiner — Fonya M Long
Assistant Examiner — Rashida Shorter
(74) *Attorney, Agent, or Firm* — Hartman & Citrin LLC

(57) **ABSTRACT**

Concepts and technologies are disclosed herein for detecting body language via bone conduction. According to one aspect, a device can detect body language of a user. The device can generate a signal and send the signal to a sensor network connected to a user. The device can receive a modified signal from the sensor network and compare the modified signal to a body language reference model. The device can determine the body language of the user based upon comparing the modified signal to the body language reference model.

17 Claims, 11 Drawing Sheets



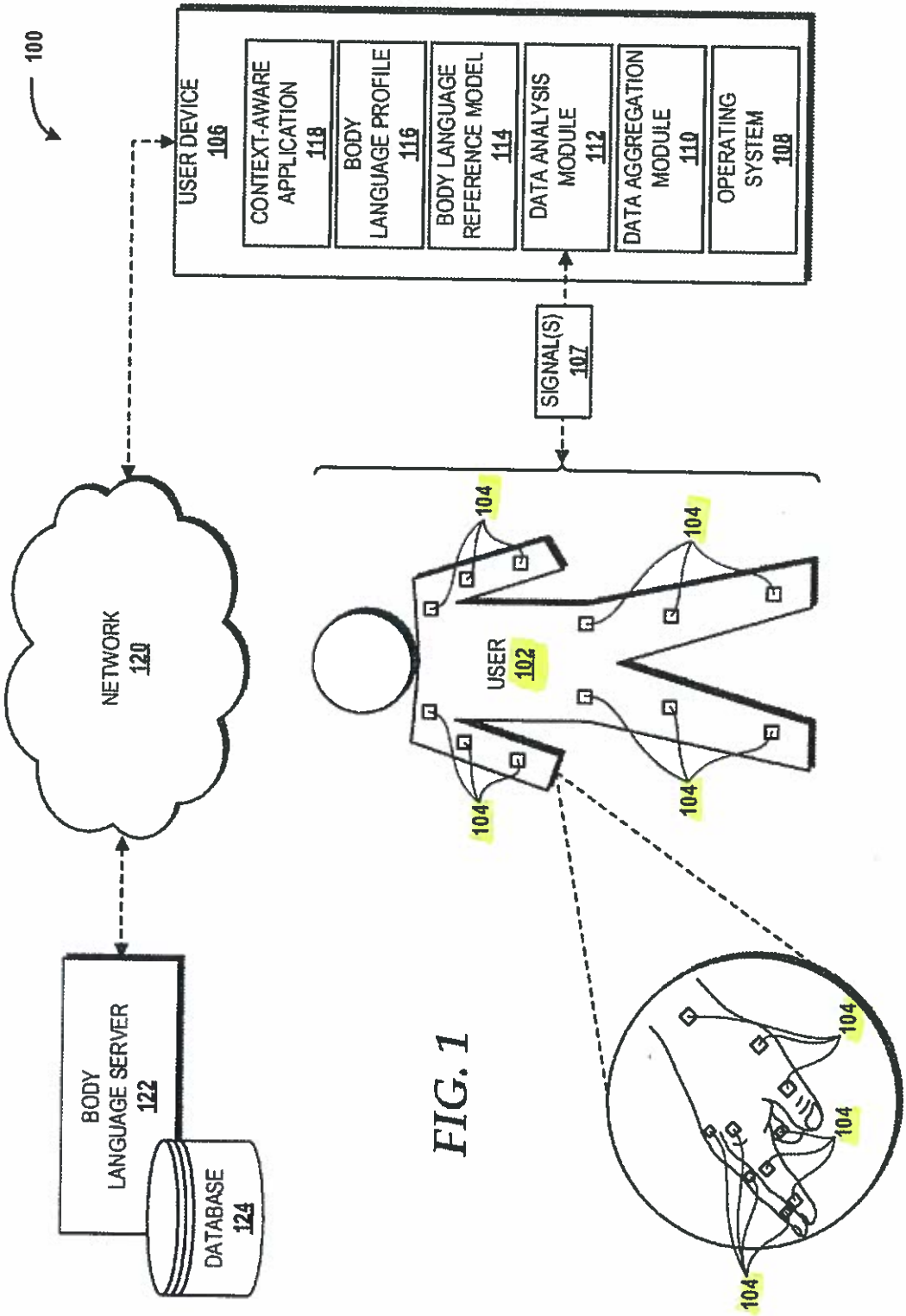

100
USER DEVICE 106
CONTEXT-AWARE APPLICATION 118
BODY LANGUAGE PROFILE 116
BODY LANGUAGE REFERENCE MODEL 114
DATA ANALYSIS MODULE 112
DATA AGGREGATION MODULE 110
OPERATING SYSTEM 108
SIGNAL(S) 107
NETWORK 120
USER 102
104
BODY LANGUAGE SERVER 122
DATABASE 124

FIG. 1

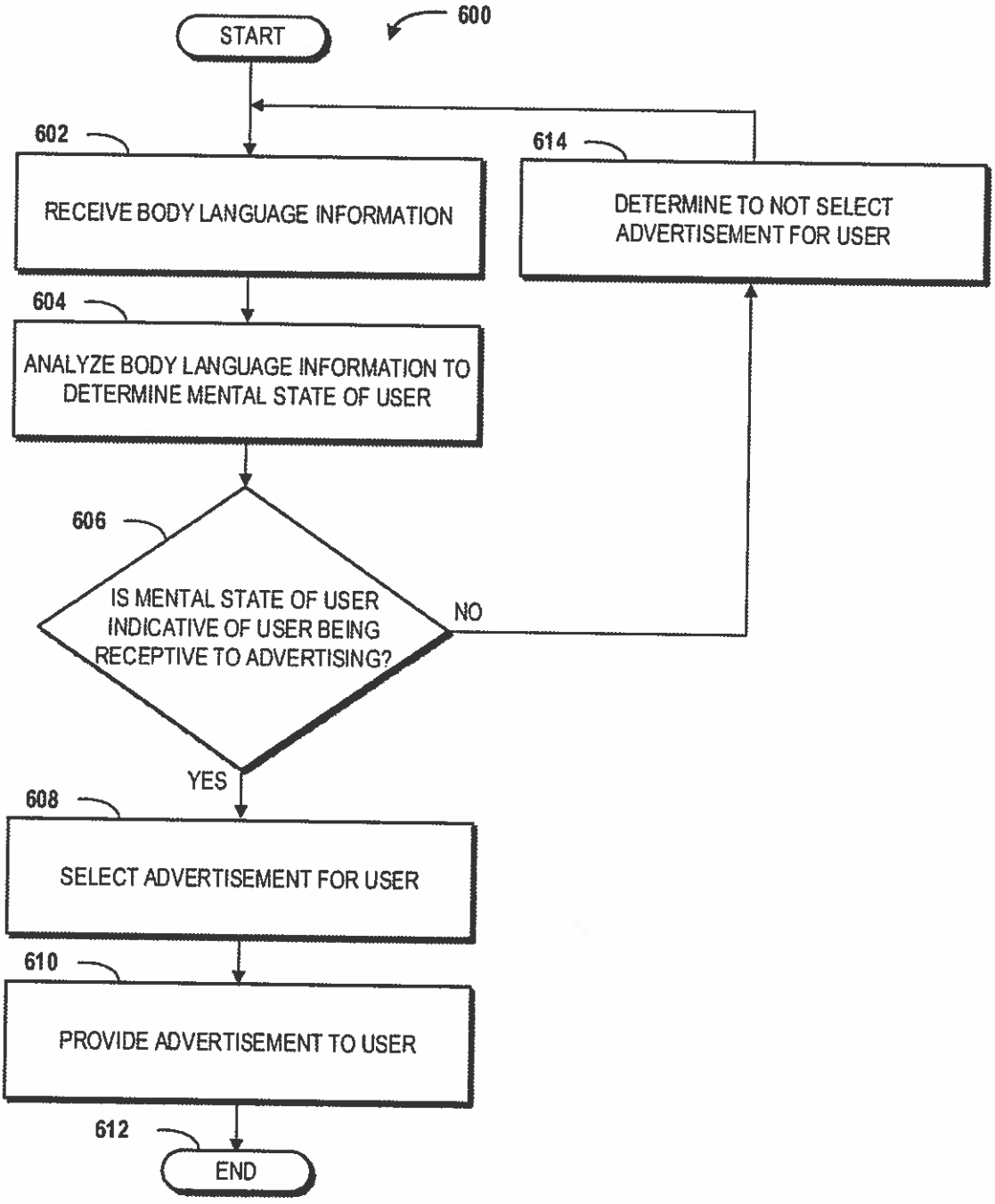

600
START
602
RECEIVE BODY LANGUAGE INFORMATION
604
ANALYZE BODY LANGUAGE INFORMATION TO DETERMINE MENTAL STATE OF USER
606
IS MENTAL STATE OF USER INDICATIVE OF USER BEING RECEPTIVE TO ADVERTISING?
NO
YES
608
SELECT ADVERTISEMENT FOR USER
610
PROVIDE ADVERTISEMENT TO USER
612
END
614
DETERMINE TO NOT SELECT ADVERTISEMENT FOR USER

FIG. 6

116TH CONGRESS
1ST SESSION

H. R. 4008

To prohibit the use of biometric recognition technology in certain federally assisted dwelling units, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JULY 25, 2019

Ms. CLARKE of New York (for herself, Ms. PRESSLEY, and Ms. TLAIB) introduced the following bill; which was referred to the Committee on Financial Services

---

A BILL

To prohibit the use of biometric recognition technology in certain federally assisted dwelling units, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "No Biometric Barriers to Housing Act of 2019".

SEC. 2. PROHIBITION ON BIOMETRIC IDENTIFICATION TECHNOLOGY.

(a) IN GENERAL.—At any time after the expiration of the 1-year period beginning on the date of the enact-

ment of this Act, an owner of a covered federally assisted rental dwelling unit, may not use, or authorize the use of, facial recognition technology, physical biometric recognition technology, or remote biometric recognition technology in such dwelling unit or in any building or grounds containing such dwelling unit.

(b) DEFINITIONS.—For the purposes of this Act:

(1) ASSISTANCE.—The term "assistance" means any grant, loan, subsidy, contract, cooperative agreement, or other form of financial assistance, but such term does not include the insurance or guarantee of a loan, mortgage, or pool of loans or mortgages.

(2) COVERED FEDERALLY ASSISTED RENTAL DWELLING UNIT.—The term "covered federally assisted rental dwelling unit" means a residential dwelling unit that is made available for rental and for which assistance is provided, or that is part of a housing project for which assistance is provided, under—

(A) the public housing program under the United States Housing Act of 1937 (42 U.S.C. 1437 et seq.);

(B) the program for supportive housing for persons with disabilities under section 811 of

the Cranston-Gonzalez National Affordable Housing Act (42 U.S.C. 8013);

(C) the program for supportive housing for the elderly under section 202 of the Housing Act of 1959 (12 U.S.C. 1701q); or

(D) the program for project-based rental assistance under section 8 of the United States Housing Act of 1937 (42 U.S.C. 1437f).

(3) FACIAL RECOGNITION TECHNOLOGY.—The term "facial recognition technology" means technology which facilitates or otherwise enables an automated or semi-automated process that assists in identifying an individual based on the physical characteristics of an individual's face, or that logs characteristics of an individual's face, head, or body to infer emotion, associations, activities, or the location of an individual.

(4) OWNER.—The term "owner" means any private person or entity, including a cooperative, an agency of the Federal Government, or a public housing agency, having the legal right to lease or sublease dwelling units.

(5) PHYSICAL BIOMETRIC RECOGNITION TECHNOLOGY.—The term "physical biometric recognition technology" means technology which facilitates or

otherwise enables an automated or semi-automated process that assists in identifying an individual or capturing information about an individual based on the characteristics of an individual's DNA, fingerprints, palmprints, iris, or retina.

(6) REMOTE BIOMETRIC RECOGNITION TECHNOLOGY.—The term "remote biometric recognition technology" means technology which facilitates or otherwise enables an automated or semi-automated process that assists in identifying an individual or capturing information about an individual based on the characteristics of an individual's gait, voice, or other immutable characteristic ascertained from a distance, or that logs such characteristics to infer emotion, associations, activities, or the location of an individual.

SEC. 3. REPORT TO CONGRESS.

Not later than 1 year after the date of enactment of this Act, the Secretary of Housing and Urban Development shall submit to the Committee on Financial Services of the House of Representative and the Committee on Banking, Housing, and Urban Affairs of the Senate and make available to the public on the website of the Department, a report that describes—

(1) any known usage of facial recognition technology, physical biometric recognition technology, or remote biometric recognition technology in any covered federally assisted dwelling unit during the 5 years preceding the date of enactment of this Act;

(2) the impact of such technology on the residents of such covered federally assisted rental dwelling units;

(3) the purpose of installing such technologies in such covered federally assisted rental dwelling units;

(4) demographic information about the residents of each covered federally assisted rental dwelling unit where such usage occurred; and

(5) the potential impacts on vulnerable communities of additional usage of facial recognition technology, physical biometric recognition technology, or remote biometric recognition technology in covered federally assisted rental dwelling units, including impacts on resident privacy, civil rights, and fair housing.

○