(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 744 704**

(51) Int. CI.:

H04W 12/08 (2009.01)
H04W 8/16 (2009.01)
G06F 21/62 (2013.01)
G06F 21/60 (2013.01)
H04W 12/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **09.11.2012 PCT/FI2012/051093**

(87) Fecha y número de publicación internacional: **04.07.2013 WO13098467**

(96) Fecha de presentación y número de la solicitud europea: **09.11.2012 E 12863506 (7)**

(97) Fecha y número de publicación de la concesión europea: **03.07.2019 EP 2798871**

(54) Título: **Método y aparato que proporciona ajuste de privacidad y monitorización de interfaz de usuario**

(30) Prioridad:

30.12.2011 US 201113341290

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.02.2020

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karakaari 7
02610 Espoo, FI

(72) Inventor/es:

AAD, IMAD;
BISWAS, DEBMALYA;
PERRUCCI, GIAN PAOLO y
EBERLE, JULIEN

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Método y aparato que proporciona ajuste de privacidad y monitorización de interfaz de usuario

Campo técnico:

Las realizaciones a modo de ejemplo y no limitantes de esta invención se refieren en general a dispositivos de usuario, métodos y programas informáticos y, más específicamente, se refieren al control de datos personales de un usuario que están residentes en un dispositivo del usuario.

Antecedentes:

Los dispositivos de usuario de módem tales como teléfonos (por ejemplo, teléfonos inteligentes), tabletas, portátiles, lectores electrónicos y similares normalmente incluyen, además de capacidades de comunicación inalámbricas, uno o más sensores que pueden detectar y/o inferir el contexto del dispositivo y, por extensión, información contextual del usuario. Un ejemplo es el uso de un sensor de determinación de posición o localización tal como uno realizado como un receptor y subsistema de satélite de posicionamiento global (GPS).

Además de la gran cantidad de datos personales almacenados en estos dispositivos de usuario (registros de sms, registros de llamada, lista de contactos, etc.) pueden usarse muchos sensores para inferir la localización, contexto, hábitos personales, etc., del usuario. Toda esta información está expuesta a al menos dos amenazas de privacidad: (A) aplicaciones de terceros que el usuario instala, pero no necesariamente confía; y (B) la posibilidad de que esta información se compartirá o publicará por el mismo usuario, sin tener conocimiento de las amenazas de privacidad.

Un problema que surge se refiere al control de la información de usuario para proporcionar al usuario con un grado de privacidad deseado.

El documento “BlackBerry 101 - Application permissions | Crackberry.com”, disponible el 22-07-2015 en https://web.archive.org/web/20110106074227/http://crackberry.com/blackberry-101-application-permissions (Joseph Holder) desvela permisos de aplicación en un dispositivo Blackberry, los permisos relacionados con sensores individuales en tres categorías: conexiones, interacciones y datos de usuario.

El documento “Defending against sensor-sniffing attackes on mobile phones”, por Liang et al (PROCEEDINGS OF THE 1ST ACM WORKSHOP ON NETWORKING, SYSTEMS, AND APPLICATIONS FOR MOBILE HANDHELDS, MOBIHELD ’09), 1 de enero de 2009, desvela un marco estructural para soluciones para facilitar la aseguración de la privacidad contra intercepción en sensores de dispositivo móvil. En este marco estructural, los usuarios autorizan acceso a sensores individuales.

Sumario

Se superan los anteriores y otros problemas, y se logran otras ventajas, de acuerdo con las realizaciones a modo de ejemplo de esta invención.

En un primer aspecto de la misma las realizaciones a modo de ejemplo de esta invención proporcionan un método de acuerdo con la reivindicación 1.

En otro aspecto de la misma las realizaciones a modo de ejemplo de esta invención proporcionan un aparato de acuerdo con la reivindicación 8.

En otro aspecto más de la misma las realizaciones a modo de ejemplo de esta invención proporcionan un medio de almacenamiento de datos legible por ordenador no transitorio de acuerdo con la reivindicación 7.

Breve descripción de los dibujos

Los anteriores y otros aspectos de las realizaciones a modo de ejemplo de esta invención se hacen más evidentes en la siguiente descripción detallada, cuando se leen en conjunto con las figuras de los dibujos adjuntos, en los que:

La Figura 1 es un diagrama de bloques de un dispositivo que es adecuado para poner en práctica las realizaciones de esta invención.

La Figura 2 presenta una vista general de una arquitectura de control de privacidad de usuario que puede estar basada en el dispositivo mostrado en la Figura 1.

La Figura 3A muestra un ejemplo no limitante de una entrada de control de privacidad amigable para el usuario que se usa para construir una tabla o base de datos de ajustes de privacidad de usuario almacenados en la memoria mostrada en la Figura 1.

La Figura 3B muestra otro ejemplo no limitante de una entrada de control de privacidad amigable para el usuario.

La Figura 4 muestra un mapeo de muestra a modo de ejemplo y no limitante entre datos de sensor e información

personal.
La Figura 5 muestra un ejemplo de intercepción en tiempo real de uso de sensor por una función de monitorización de control de uso mostrada en la Figura 2.
La Figura 6 muestra un ejemplo de verificación de cumplimiento de privacidad fuera de línea (en tiempo no real).
La Figura 7 muestra un ejemplo sencillo de visualización de privacidad donde se informa a un usuario con un tipo de barra de visualización del nivel de privacidad total del usuario.
La Figura 8 muestra un ejemplo de una vista de privacidad más detallada que tiene un tipo de representación de gráfico de sectores, donde se representan diferentes categorías y subcategorías de privacidad.
Las Figuras 9A-9C, denominadas de manera colectiva como la Figura 9, muestran ejemplos de la visualización de niveles de privacidad de usuario en una base por aplicación.
La Figura 10 es un diagrama de bloques que muestra una vista diferente de la interfaz de usuario novedosa del dispositivo representado en la Figura 1.
La Figura 11 muestra ejemplos de la operación de la interfaz de usuario para establecer políticas.
La Figura 12 es un diagrama de flujo lógico que ilustra la operación de un método, y un resultado de la ejecución de instrucciones de programa informático, de acuerdo con las realizaciones a modo de ejemplo de esta invención.

Descripción detallada

Como se ha mencionado anteriormente, con teléfonos inteligentes y otros dispositivos de usuario que se están volviendo comunes, los sensores presentes en estos dispositivos pueden usarse para inferir información contextual en tiempo real muy personal acerca del usuario, por ejemplo, localización, actividades, hábitos (comportamientos habituales). Teniendo acceso a esta gran cantidad de información acerca del usuario permite que los proveedores de servicio proporcionen servicios altamente sensibles al contexto para el usuario. Sin embargo, muchos usuarios son reacios a compartir esta información con proveedores de servicio debido a las considerables implicaciones de privacidad si estos datos se ven comprendidos y se usan incorrectamente. Lo que realmente es necesario son controles/herramientas que permitan que un usuario proteja de manera eficaz su privacidad, mientras aún disfruta de los beneficios de servicios de contexto habilitado.

Puede posibilitarse que el usuario especifique ajustes de privacidad. Sin embargo, el usuario típico no tendrá conocimiento de los detalles técnicos subyacentes de su dispositivo (por ejemplo, teléfono inteligente) y por lo tanto no puede especificar los ajustes de privacidad deseados en el nivel de sensor.

En este análisis se supone que "sensores" también hacen referencia a diversos dispositivos de entrada disponibles en el teléfono (por ejemplo, un micrófono, una cámara), y un sistema de ficheros del teléfono que en general permite acceso a contenido generado por el usuario (por ejemplo, imágenes). De manera ideal, el usuario debería poder especificar un ajuste de privacidad de la forma (como un ejemplo no limitante):
"No permitir que la aplicación (aplicación) del tiempo acceda a mi GPS más de una vez por hora".

Diciéndose esto, el usuario promedio normalmente únicamente entiende de manera amplia el aspecto de localización, y no tiene conocimiento de los diferentes sensores (GPS, Wi-Fi) y algoritmos, por ejemplo, triangulación de Wi-Fi, que pueden usarse para derivar la información de localización. Esto da como resultado una necesidad de controles de privacidad amigables para el usuario que permiten que el usuario especifique ajustes de privacidad a una granularidad con la que el usuario está cómodo. Sin embargo, implementar un control de privacidad amigable para el usuario de este tipo a su vez da como resultado un número de desafíos.

Por ejemplo, los ajustes de privacidad de usuario de alto nivel (por ejemplo, localización) necesitan mapearse a los patrones de acceso de sensor o sensores de bajo nivel (por ejemplo GPS, WiFi).

Además por ejemplo, pueden usarse mapeos para monitorizar el uso de sensores relevantes en el teléfono, y para interceptar, si fuera necesario, accesos a los sensores por los programas de aplicación (denominados en lo sucesivo simplemente como 'aplicaciones').

También, por ejemplo, es deseable analizar el uso y presentar el resumen de uso al usuario. Análogo a capturar los ajustes de privacidad de una manera amigable para el usuario, el informe de resumen de uso debería presentarse al usuario en un idioma legible para el usuario. Esto implica el uso de un mapeo inverso de los detalles de uso del sensor de bajo nivel a los parámetros contextuales de nivel de usuario.

Como un ejemplo adicional y no limitante, se desea aplicar los ajustes de privacidad de usuario tomando acciones proactivas (por ejemplo, evitar que aplicaciones accedan a sensores en la violación de un ajuste de privacidad de usuario) o acciones reactivas (por ejemplo, presentar información al usuario con respecto a cualquier violación de privacidad por una aplicación).

Muchas plataformas de sistema operativo (SO) de dispositivo móvil se basan en un modelo basado en capacidades de "tiempo de instalación" para proteger privacidad de usuario, donde el acceso a un sensor se proporciona únicamente a una aplicación después de autorización explícita por el usuario durante la instalación de aplicación. En un nivel alto este modelo funciona como sigue. Las aplicaciones declaran una lista de sensores a los que necesitan

acceso (para proporcionar su funcionalidad) en un fichero de manifiesto basado en XML. Durante la instalación, se lee el fichero de manifiesto y se presenta una lista de acceso a sensor o sensores requeridos al usuario. La aplicación está permitida a instalarse únicamente si el usuario lo acuerda (introduce un "Sí"). Después de la instalación, el SO móvil proporciona el control de acceso necesario para asegurar que la aplicación únicamente tiene acceso permitido a aquellos sensores declarados en el fichero de manifiesto de la aplicación.

Aunque este tipo de procedimiento actúa como un elemento disuasorio puede mostrarse que un modelo de este tipo es inherentemente poco fiable. Por ejemplo, un modelo de certificación de aplicación es más general, donde las aplicaciones pasan a través de una comprobación de validación que se pretende para conservar la privacidad de usuario antes del despliegue, pero sin implicar el usuario. Una vez certificadas, las aplicaciones tienen acceso ilimitado a la mayoría de los sensores del teléfono.

Están disponibles diversas aplicaciones que se pretenden para informar al usuario acerca de su privacidad y para proporcionar al usuario control sobre su privacidad. Una aplicación de este tipo proporciona al usuario control detallado de los accesos a datos privados, clasificados por aplicación o por sensor. Sin embargo, y como se ha indicado anteriormente, el usuario típico es poco probable que entienda la magnitud de las amenazas cuando se presentan simplemente con la identificación de un sensor que se accede por una aplicación intrusiva.

Es claramente mucho más relevante: informar al usuario que "Esta aplicación está intentando acceder a datos que pueden usarse para identificar a su actividad actual", entonces posibilitar que el usuario diga "ocultar mi información personal cada vez que estoy en el trabajo", en lugar de tener el usuario que necesitar especificar "desactivar acceso a mi GPS, WiFi, SMS, Bluetooth, etc., cada vez que ocurra que estoy dentro de las coordenadas [x1,y1] y [x2,y2], o escuchando la WiFi 'abc', Bluetooth 'def..."

Las realizaciones a modo de ejemplo de esta invención en un aspecto de la misma proporcionan un control de privacidad amigable para el usuario para un usuario de un dispositivo, tal como un teléfono (por ejemplo, un teléfono inteligente). Las realizaciones a modo de ejemplo proporcionan ajustes de privacidad de usuario en un idioma contextual legible por el usuario, posibilita monitorizar para interceptar el uso de sensores de teléfono relevantes y también proporciona un mecanismo de realimentación para presentar información de uso de sensor al usuario, de nuevo en el idioma legible por el usuario de alto nivel. Las realizaciones a modo de ejemplo también posibilitan la aplicación de los ajustes de privacidad de usuario en tiempo real (por ejemplo, bloqueando accesos de sensor no autorizados) o en una forma retardada (por ejemplo, informando violaciones de privacidad por aplicaciones específicas al usuario).

Para los fines de describir las realizaciones de esta invención un 'teléfono inteligente' puede considerarse como un dispositivo de comunicación de usuario que tiene una interfaz de usuario, al menos una modalidad de comunicación inalámbrica y suficiente capacidad de memoria y capacidad de procesamiento de datos para almacenar y ejecutar programas de aplicación en cooperación con un sistema operativo.

Un aspecto de estas realizaciones es un mapa que convierte ajustes de privacidad de usuario de alto nivel a patrones de acceso de sensor de bajo nivel, y viceversa. El mapeo depende al menos en parte en algoritmos contextuales que toman datos de sensor como información contextual de entrada y salida acerca del usuario. Los algoritmos contextuales tienen la capacidad para evolucionar con el tiempo. Las realizaciones a modo de ejemplo posibilitan también por lo tanto la actualización de los algoritmos contextuales relevantes con el tiempo protegiendo de esta manera al usuario contra amenazas de privacidad en evolución reciente.

Antes de describir las realizaciones a modo de ejemplo de esta invención en detalle adicional se hace referencia a la Figura 1 para ilustrar un diagrama de bloques simplificado de una realización a modo de ejemplo de un dispositivo electrónico 10 que es adecuado para su uso al poner en práctica las realizaciones a modo de ejemplo de esta invención. En la Figura 1 el dispositivo 10 incluye un procesador de datos 12 que está acoplado a través de un bus 12A con una memoria 14 que almacena un programa (PROG) 14A de instrucciones que son ejecutables por el procesador de datos 12. El programa 14A puede incluir un sistema operativo (SO) y otros programas necesarios para operar el dispositivo 10. El dispositivo 10 puede incluir adicionalmente una pluralidad de dispositivos y subsistemas de entrada y salida, denominados en el presente documento también como modalidades de entrada 36 y modalidades de salida 38. Como dispositivos de salida a modo de ejemplo puede haber uno o más de una pantalla de visualización visual 16, tal como un LCD o una pantalla de visualización de plasma, un transductor de salida acústico tal como un altavoz 18, un subsistema de síntesis de voz 20 que tiene una salida que puede reproducirse a través del altavoz 18 (o a través de otro transductor de salida acústico), y un dispositivo o transductor de dispositivo de salida táctil 22, tal como un dispositivo vibratorio (por ejemplo, un transductor piezoeléctrico). Estos dispositivos de salida están acoplados a correspondientes rutas de salida 12B, 12C, 12D y 12E del procesador de datos 12. Como dispositivos de entrada a modo de ejemplo puede haber uno o más de un transductor de entrada acústica tal como un micrófono 24, una función de reconocimiento del habla o voz asociada (VR) 24A, un teclado numérico o teclado 26 y un sensor de gesto 28, tal como un dispositivo que es sensible a una rotación alrededor de al menos un eje y/o a una fuerza aplicada por un dedo o lápiz óptico del usuario, tal como cuando se hace un gesto de toque. Estos dispositivos de entrada están acoplados a correspondientes rutas de entrada 12F, 12G y 12H al procesador de datos 12. Si la pantalla 16 es una pantalla táctil entonces puede haber también una entrada 16A de la pantalla 16 al procesador de datos 12. En este

caso la entrada al procesador de datos 12 puede representar la activación de una tecla o botón virtual por el usuario, a diferencia del uso del teclado numérico/teclado 26 donde la señal de entrada puede representar la activación de una tecla o botón físico (tal como una tecla alfanumérica o una tecla o botón 'programable' físico). El micrófono 24 puede estar acoplado con la funcionalidad de reconocimiento de voz del dispositivo 10 (el VR 24A) mediante la cual una palabra o palabras habladas por el usuario pueden interpretarse por el procesador de datos 12 representando un comando.

Debería apreciarse que el bloque de procesador de datos 12 puede comprender realmente un número de tipos de circuito, además de un procesador de datos de por sí, tal como convertidores de analógico a digital y convertidores de digital a analógico que soportan la operación de las diversas modalidades de entrada 36 y modalidades de salida 38.

Puede proporcionarse algún tipo de subsistema de determinación de localización, tal como un receptor de GPS 37.

Debería apreciarse que al menos alguna de las modalidades de entrada 36 puede considerarse como que son sensores del dispositivo 10 tal como, como ejemplos no limitantes, el micrófono 24, el sensor de gesto 28 y el subsistema de GPS 37. Otros ejemplos de sensores que pueden proporcionarse se describen a continuación. Es decir, la representación del dispositivo 10 mostrada en la Figura 1 es a modo de ejemplo, ya que los sensores y las funciones relacionadas con el sensor (por ejemplo, información relacionada con el dispositivo que podría accederse o interrogarse por un programa de aplicación (aplicación) 14B), puede incluir, como ejemplos no limitantes, cualquiera o todos aquellos mostrados en la Figura 4 (por ejemplo, GPS, WiFi, BT, ID de Célula, registros de llamada, SMS (servicio de mensajes cortos), audio, acelerómetro, libreta de direcciones (información de contacto), calendario, imagen, música, IMEI (Identidad de Equipo Móvil Internacional), IMSI (Identidad de Abonado Móvil Internacional), perfil de dispositivo, tipo de tono, nivel de batería (carga) e indicador de carga). Cualquiera de estas diversas unidades funcionales e información relacionada con el usuario o dispositivo puede denominarse a continuación como simplemente un "sensor".

En las realizaciones a modo de ejemplo el dispositivo 10 tiene capacidades de comunicación de usuario e incluye un transceptor 30 adecuado, tal como un transceptor de frecuencia de radio acoplado con al menos una antena 32 para llevar a cabo comunicaciones inalámbricas a través de un enlace de frecuencia de radio de largo alcance bidireccional 34 (por ejemplo, un enlace a una red de comunicación celular). La red de comunicación celular puede ser compatible con cualquier tipo de red de comunicación celular que incluye, por ejemplo, GSM, LTE, LTE-A, y así sucesivamente. Es decir, el uso de esta invención no depende del uso de cualquier tipo particular de red celular. El dispositivo 10 puede incluir también un segundo transceptor 31 acoplado con al menos una antena 33 a un enlace de frecuencia de corto alcance 35, tal como un enlace de frecuencia de radio de baja potencia que puede ser un enlace de Bluetooth™ (BT) o un enlace WiFi. En otras realizaciones el transceptor 31 puede estar basado de manera óptica y puede entonces incluir componentes de fuente y detector ópticos adecuados, tales como un emisor de infrarrojos y un detector de infrarrojos.

Debería observarse que las diversas modalidades de entrada 36 y modalidades de salida 38 son a modo de ejemplo y no todas pueden estar presentes en una implementación dada. Por ejemplo, las realizaciones a modo de ejemplo de esta invención pueden usarse con solamente la pantalla de visualización 16 y el teclado numérico/teclado 26, o con solamente la pantalla de visualización 16 si la pantalla es táctil para permitir que el usuario introduzca información y comandos. En algunas realizaciones de esta invención la interfaz de usuario podría estar basada solamente en el uso de reconocimiento de voz y síntesis de voz, y puede no ser necesaria en absoluto pantalla táctil alguna.

El programa 14A se supone que incluye instrucciones de programa que, cuando se ejecutan por el procesador de datos 12, posibilitan que el dispositivo electrónico 10 opere de acuerdo con las realizaciones a modo de ejemplo de esta invención como se analizará a continuación en mayor detalle. El programa 14A puede incluir el SO y cualesquiera utilidades de sistema de ficheros asociadas dependiendo de la implementación de la arquitectura de software del dispositivo 10.

En general, las diversas realizaciones del dispositivo 10 pueden incluir, pero sin limitación, teléfonos, teléfonos inteligentes, asistentes digitales personales (PDA) posiblemente teniendo capacidades de comunicación inalámbricas, ordenadores portátiles posiblemente teniendo capacidades de comunicación inalámbricas, dispositivos de GPS posiblemente teniendo capacidades de comunicación inalámbricas, dispositivos de captura de imagen tal como cámaras digitales posiblemente teniendo capacidades de comunicación inalámbricas, dispositivos de juegos posiblemente teniendo capacidades de comunicación inalámbricas, aparatos de almacenamiento y reproducción de música posiblemente teniendo capacidades de comunicación inalámbricas, aparatos de Internet que permiten acceso a Internet alámbrico o inalámbrico y exploración, así como unidades o terminales portátiles que incorporan combinaciones de tales funciones.

Las realizaciones a modo de ejemplo de esta invención pueden implementarse por software informático ejecutable por el procesador de datos 12, o por hardware, o por una combinación de software y hardware (y firmware).

La memoria 14 puede ser de cualquier tipo adecuado al entorno técnico local y puede implementarse usando cualquier tecnología de almacenamiento de datos adecuada, tal como dispositivos de memoria basada en semiconductores,

memoria flash, dispositivos y sistemas de memoria magnética, dispositivos y sistemas de memoria óptica, memoria fija y memoria extraíble. El procesador de datos 12 puede ser de cualquier tipo adecuado al entorno técnico local, y puede incluir uno o más de ordenadores de fin general, ordenadores de fin especial, microprocesadores, procesadores de señales digitales (DSP) y procesadores basados en arquitecturas de procesador de múltiples núcleos, como ejemplos no limitantes.

La memoria 14 se muestra como que incluye código de programa informático que implementa las diversas aplicaciones (programas de aplicación) 14B que pueden preinstalarse en el dispositivo 10 o instalarse posteriormente por el usuario, tal como descargándose mediante uno de los enlaces de frecuencia de radio 34 o 35. El mapa anteriormente mencionado que convierte ajustes de privacidad de usuario de alto nivel a patrones de acceso de sensor de bajo nivel pueden almacenarse como parte del MAPA 14C en la memoria 14. El MAPA 14C puede incluir también una estructura de datos a lo largo de las líneas representadas en la Figura 4 y descrita a continuación, además de diversos módulos de software que operan para rellenar la estructura de datos basándose en entrada de usuario (por ejemplo, véanse las Figuras 3A, 3B) e interpretar la estructura de datos a la luz de uso de sensor o el uso intentado de sensor por las aplicaciones 14B. Asociado con el MAPA 14C pueden almacenarse ajustes de privacidad de usuario 14C', o estos ajustes de privacidad puede suponerse que son implícitos en la estructura de datos mostrada en la Figura 4. La memoria 14 puede almacenar también los algoritmos contextuales de mención anteriores como los algoritmos contextuales 14D. La memoria 14 también almacena software informático que implementa una interfaz de usuario (UI) 14E de privacidad que opera en conjunto con las modalidades de entrada 36 y las modalidades de salida 38. Los aspectos de la UI de privacidad 14E se describen en detalle a continuación.

Los algoritmos contextuales 14D puede considerarse que abarcan aquellos algoritmos que se usan para determinar contexto de usuario basándose en (posiblemente de bajo nivel) lecturas de sensor del dispositivo del usuario 10. Por ejemplo, y en un caso sencillo, un algoritmo contextual 14D puede ser uno que determina actividad de usuario (por ejemplo, si el usuario está andando, corriendo, sentándose en un vehículo en movimiento, haciendo gestos con sus manos, etc.) basándose en lecturas de acelerómetro. Las realizaciones a modo de ejemplo de esta invención interceptan tales lecturas de sensor de bajo nivel y a continuación usan los algoritmos contextuales 14D para determinar la información de contexto que puede inferirse acerca del usuario. Obsérvese en este sentido que cuanta más información personal pueda inferirse, mayor es el riesgo de privacidad del usuario.

La Figura 2 presenta una vista general de una arquitectura de control de privacidad de usuario 40 que puede estar basada en el dispositivo 10 mostrada en la Figura 1. La arquitectura de control de privacidad de usuario 40 es una característica de las realizaciones a modo de ejemplo de esta invención y se describe en detalle a continuación.

La arquitectura de control de privacidad de usuario 40 incluye un número de unidades o módulos funcionales interactivos. Una de estas unidades funcionales o módulos es una interfaz de privacidad de usuario 42 que captura entrada de usuario y proporciona realimentación de usuario. La interfaz de privacidad de usuario 42 puede considerarse como un aspecto de la UI de privacidad 14E. También se muestra el MAPA 14C que puede subdividirse en un MAPA 44 que convierte uso de sensor a un informe de privacidad, un MAPA 46 que convierte los ajustes de privacidad de usuario 14C' a uso de sensor y un MAPA 48 responsable de información personal y patrones de acceso de sensor. Una actualización de este módulo puede realizarse en el transcurso de la comunicación (OTA). Otra unidad o módulo funcional de la arquitectura 40 es un módulo de control de uso 50 responsable de interceptar accesos y aplicar los ajustes de privacidad de usuario 14C'. El módulo 52 representa los diversos sensores, los dispositivos de entrada (modalidades de entrada 36), y un sistema de ficheros asociados con el SO.

Un aspecto de esta invención es una entrada de control de privacidad amigable para el usuario 60 mostrada en la Figura 3A como una implementación no limitante y a modo de ejemplo. La entrada de control de privacidad amigable para el usuario 60 es un elemento de la UI de privacidad 14E y por lo tanto del módulo de interfaz de privacidad del usuario 42 de la Figura 2. La entrada de control 60 puede presentarse al usuario visualizándose en la pantalla 16 y representa una operación preliminar de captura de los ajustes de privacidad de usuario para almacenamiento en los ajustes de privacidad 14C'. La entrada de control 60 presenta un lenguaje amigable para el usuario tal como el ilustrado. Por ejemplo, puede presentarse al usuario con la entrada de control 60 que permite al usuario 'ocultar' (o 'exponer') su información 'personal', 'social', 'profesional' (etc., seleccionable por el usuario) cada vez que el usuario está en 'casa', 'en el trabajo', de compras' (etc., seleccionable por el usuario). Activando un botón de establecimiento 62 el ajuste de privacidad construido se almacena en los ajustes de privacidad 14C' para su uso por el MAPA 14C. Múltiples presentaciones y usos de la entrada de control 60 pueden rellenar los ajustes de privacidad 14C' con un número de diferentes ajustes de privacidad para diferentes clases de información de usuario en diferentes contextos de usuario.

La realización de la Figura 3B proporciona al usuario con una interfaz de usuario que permite al usuario establecer perfiles de usuario predefinidos (por ejemplo, 'profesional', 'contextual', 'médico') para controlar acceso a los sensores del dispositivo 10. En este caso activar el botón de establecimiento 62 indicaría que, por ejemplo, el perfil 'médico' es siempre sensible y, por lo tanto, podría usarse para restringir todos los accesos de sensor para este perfil.

Se describen en detalle a continuación aspectos adicionales de la interfaz de usuario 14E.

La Figura 4 muestra un mapeo de muestra a modo de ejemplo y no limitante entre datos de sensor e información personal. Más específicamente, la Figura 4 muestra un ejemplo de una matriz que mapea qué información personal de usuario (por ejemplo, personal, profesional, contexto, conexiones sociales, localización, médica, financiera, etc.) puede inferirse basándose en qué sensores, fuentes de información y dispositivos de entrada (por ejemplo, modalidades de entrada 36) del dispositivo 10. Obsérvese que cada categoría de privacidad de información personal puede incluir varias subcategorías. Por ejemplo, la categoría de información personal de contexto podría incluir como subcategorías: medios de transporte, actividad y modo. Una lista a modo de ejemplo de sensores, fuentes de datos y modalidades de entrada incluyen, pero sin limitación: GPS, WiFi, BT, ID de célula, registros de llamada, SMS, audio, acelerómetro, libreta de direcciones, calendario, imagen, música, IMEI, IMSI, perfil de dispositivo, tipo de tono, nivel de batería (carga) e indicador de carga. Para los fines de describir esta invención todos estos pueden denominarse de manera genérica como 'sensores'.

Los datos de diversos sensores pueden combinarse para inferir información personal, usando algoritmos que pueden ser sencillos (por ejemplo, localización instantánea) a más complicados. Como tal, la 'X' en la tabla de la Figura 4 puede hacer referencia a una única dependencia en un sensor específico S, o a patrones de acceso más complejos, por ejemplo, "los sensores S1 y S2 necesitan accederse con las frecuencias f1 y f2 dentro de periodos de tiempo t1 y t2 para inferir información de contexto C".

El MAPA 46 que convierte los ajustes de privacidad de usuario 14C' a uso de sensor de la Figura 2 es el componente que es responsable de mapear ajustes de privacidad de usuario de alto nivel, por ejemplo:
'Proteger mi información profesional cada vez que estoy en el trabajo'
a la política de nivel de sensor:
'contexto(localización, oficina) - DENEGAR(S1, frec(n1), periodo_tiempo(t1) Y DENEGAR (S2, frec(n2), periodo_tiempo(t2)) Y...'

Este ejemplo supone que infiriendo información profesional de usuario requiere acceder a los sensores S1, S2, ... con frecuencia n1, n2,... en periodos de tiempo t1, t2, ..., basándose en el mapeo representado en la Figura 4.

Puede observarse que monitorizar el uso de sensor normalmente tendrá alguna sobrecarga de rendimiento y, de manera ideal, únicamente se monitorizan sensores "relevantes", es decir, únicamente aquellos sensores que se requieren para detectar violaciones con respecto a las políticas de privacidad establecidas. Como un ejemplo, y con respecto a la política de privacidad (ajuste de privacidad) anteriormente, es suficiente interceptar acceso al sensor S1 únicamente durante el periodo de tiempo t1.

Se analiza ahora el control de uso con respecto a la monitorización, verificación y aplicación.

Una vez que los ajustes de privacidad de usuario 14C' se han mapeado a las políticas de nivel de sensor, el módulo de control de uso 50 es responsable de monitorizar uso de sensor en cumplimiento con las políticas de nivel de sensor. Hay diferentes posibilidades con respecto a 'cuándo' y 'dónde' monitorizar el uso de sensores, y también con respecto a 'qué' hacer cuando se detecta una violación.

Los datos de uso de sensor podrían interceptarse, por ejemplo, en el nivel de SO. En el nivel de SO esto implica interceptar acceso de sensor mediante sus correspondientes controladores de dispositivo.

Los datos de uso de sensor podrían interceptarse, por ejemplo, en el nivel de la plataforma. La intercepción de nivel de plataforma hace referencia, por ejemplo, a integrar la intercepción con estructuras de sensor de soporte intermedio tal como uno conocido como movilidad de Qt (QT es una marca comercial registrada de Nokia Corporation) (disponible de Nokia Corporation). En este caso el uso de un sensor se monitoriza cuando se accede al sensor mediante una correspondiente API (interfaz de programa de aplicación).

La Figura 5 describe un escenario donde el acceso a los sensores 52 soportados por Qt-Mobility 1.1.3 (acelerómetro, luz ambiental, brújula, magnetómetro, orientación, proximidad, rotación) se intercepta por el monitor de control de uso 50 y se registran como, por ejemplo:
'aplicación 1 accede la lectura de sensor R1 del sensor S1 en el punto de tiempo p1' @p1(App1,R1,S1,p1).

Los datos de uso de sensor podrían interceptarse también, por ejemplo, en el nivel de aplicación. Esto implica que la monitorización de sensor o código de registro de uso puedan estar integrados dentro del propio código de aplicación.

Los datos de uso de sensor podrían interceptarse también, por ejemplo, en el nivel de red. En este caso la intercepción tiene lugar cuando los datos de sensor se están actualizando a través de la red.

Estos diferentes escenarios de intercepción tienen diversas compensaciones con respecto a la integración requerida con la plataforma subyacente, el alcance de intercepción (por ejemplo, intercepción de nivel de red generalmente no sería aplicable si los datos están encriptados por la aplicación antes de transmitir los datos a través de la red, y también si la aplicación realiza algún procedimiento en el dispositivo en los datos antes de compartirlos a través de la red).

A lo largo de la misma línea, el uso de sensor puede procesarse tanto en tiempo real y/o como en una manera retardada (fuera de línea). El procesamiento en tiempo real implica comprobar el cumplimiento para cada acceso de sensor (antes de permitir realmente acceder a los datos de sensor). El procesamiento fuera de línea corresponde a registrar el uso de sensor en tiempo real y analizar los registros de uso para la ocurrencia de violaciones en un punto posterior en el tiempo (fuera de línea).

La Figura 6 ilustra un ejemplo de un mecanismo de verificación fuera de línea (determinación de cumplimiento). En este caso los registros (por ejemplo, un acceso de registro al acelerómetro por la APP1 y otro acceso de registro al magnetómetro por APP2) se procesan en conjunto con una política de privacidad por un submódulo de verificación de control de uso 50A del módulo de control de uso 50. Más específicamente, los registros:

@p1(App1, acelerómetro, [x, ...])
@p2(App2, magnetómetro, [x, ...])

se procesan en conjunto con una política tal como:
NOT(WeatherApp, GPS, frec(l), periodo (1 h)).

Basándose en el análisis realizado el submódulo de verificación de control de uso 50A informa uno de cumplimiento o una violación por APP1 y APP2 con respecto a sus accesos de sensor.

Pueden tomarse diferentes tipos de acciones cuando se detecta una violación por el monitor de control de uso 50 o el módulo de verificación de control de uso 50A.

Por ejemplo, un enfoque preventivo restringe el acceso en tiempo real si se detecta una violación. Este enfoque se basa en el uso de intercepción en tiempo real de accesos de sensor y la capacidad para actuar antes de que se lean realmente datos de sensor por la aplicación 14B.

Además por ejemplo, un enfoque reactivo puede funcionar de una manera análoga a una herramienta de información que proporciona información de uso de sensor detallada al usuario junto con posibles implicaciones de privacidad. Se analiza a continuación un procedimiento para mapear uso de sensor de vuelta a las implicaciones de privacidad para el usuario (que puede a continuación visualizarse al usuario).

Se describe ahora la operación del uso de sensor de mapa para el módulo de informe de privacidad 44 mostrado en la Figura 2.

Como se ha indicado anteriormente, un caso de uso posible para los datos de sensor interceptados es para presentarlos al usuario de una manera resumida. La información presentada puede incluir también detalles de cualesquiera violaciones de privacidad por las aplicaciones 14B. Para proporcionar esta realimentación relacionada con la privacidad al usuario la herramienta puede asumir el papel de un atacante poderoso que, analizando los datos de uso de sensor real, usa el mapeo (actualizado) en la Figura 4 para calcular la información personal/profesional/contextual, etc., del usuario que podría inferirse de los datos de uso de sensor real. Los detalles de uso de sensor, que incluyen posiblemente una percepción de amenaza de privacidad, se presentan a continuación al usuario tal como visualizándolos en la pantalla 16. El usuario puede aplicar esta información, por ejemplo, como una entrada para adaptar los ajustes de privacidad del usuario en respuesta al comportamiento informado de las aplicaciones 14B, por ejemplo, relajando o restringiendo ciertas políticas de uso con respecto a ciertas de las aplicaciones 14B.

Otro caso de uso es visualizar información de uso de sensor en tiempo real al usuario de una manera análoga a una utilidad de monitorización de sistema hallada en muchos sistemas informáticos. Este tipo de visualización podría ofrecerse como una alternativa seleccionable por el usuario a la manera resumida de los datos de sensor interceptados como se ha descrito anteriormente.

Una ventaja evidente y distinta y efecto técnico del uso de estas realizaciones de esta invención es que proporcionan realimentación de control de privacidad mejorada al usuario, de una manera legible y entendible para el usuario.

Se describen ahora en detalle adicional diversos aspectos de la interfaz de usuario (UI) 14E (y la interfaz de privacidad de usuario 42 mostrada en la Figura 2) que posibilita que se introduzcan y visualicen los ajustes de privacidad al usuario.

Un aspecto adicional de esta invención es proporcionar una capacidad para visualizar al usuario los ajustes de privacidad del usuario basándose en ajustes actuales de sensor y control de acceso de información por diversas aplicaciones 14B. Basándose en los ajustes actuales del sensor y control de acceso de información por diversas aplicaciones 14B, el uso de las realizaciones de esta invención visualiza los niveles de privacidad del usuario, que pueden mapearse, como en la Figura 8, a categorías de privacidad "entendibles para el usuario" específicas mientras que se abstraen las capas inferiores (por ejemplo, sensores, sistemas de ficheros) y las correspondientes amenazas de privacidad, que no son necesariamente totalmente entendibles para el usuario medio.

La Figura 7 muestra un ejemplo sencillo donde se informa al usuario con un tipo de barra de visualización del nivel de privacidad total del usuario (por ejemplo, en una escala del 0 % al 100 %, representando el 100 % la privacidad total). Es decir, ninguna aplicación puede tener acceso a cualesquiera sensores del dispositivo 10.

La Figura 8 muestra un ejemplo de una vista de privacidad más detallada, en este caso que tiene un tipo de representación de gráfico de sectores, donde se representan diferentes categorías de privacidad (por ejemplo, como se muestra en la Figura 4) y sub-categorías. Este ejemplo muestra la categoría de privacidad 'personal' y subcategorías (por ejemplo, género, edad, etc.) y una categoría 'conexiones sociales' con subcategorías (por ejemplo, tipo de conexiones, número de conexiones, etc.). En este ejemplo para la categoría personal la subcategoría ’género’ no tiene restricciones de privacidad mientras que las otras subcategorías tienen relativamente más restricciones de privacidad. Esta información se deriva de la representación matricial de la Figura 4 y se visualiza al usuario en un formato fácilmente entendible.

Las Figuras 9A-9C, denominadas de manera colectiva como la Figura 9, muestran ejemplos de la visualización de niveles de privacidad de usuario por categoría de privacidad en una base por aplicación (en este caso no limitante una aplicación del tiempo (aplicación)). Por ejemplo, la Figura 9A indica al usuario que para su categoría de privacidad de localización la aplicación del tiempo tiene acceso de sensor ilimitado, mientras que la categoría de privacidad financiera y la aplicación del tiempo ya casi no tienen acceso de sensor.

La interfaz de visualización puede usarse también para introducir preferencias de privacidad por el usuario y para indicar límites que no deberían superarse como se muestra en la Figura 9B, y/o para diferenciar entre la importancia de diversos componentes como en la Figura 9C (donde las diferentes categorías de privacidad se les proporciona áreas respectivas en el gráfico indicativo de su importancia relativa).

Debería señalarse que mientras que la información visual visualizada al usuario como en los ejemplos de las Figuras 7, 8 y 9, así como las Figuras 3A y 3B, se representa en el presente documento en una manera en escala de grises, en la práctica esta información puede visualizarse usando diversos colores seleccionados de una paleta de color definida por el sistema y/o definida por el usuario.

Los aspectos a modo de ejemplo de esta invención posibilitan adicionalmente actualizar los ajustes de privacidad en el dispositivo para proteger contra nuevas intrusiones de privacidad. Las realizaciones a modo de ejemplo proporcionan al usuario con una interfaz amigable/entendible (realizada como la UI 14E) que ayuda al usuario a visualizar y establecer ajustes de privacidad, sin que el usuario entienda necesariamente cómo pueden usarse los datos de sensor para inferir información personal.

Haciendo referencia a la vista del dispositivo 10 mostrado en la Figura 10, la entrada de control de privacidad amigable para el usuario de bloque 70 y la entrada de mapa de bloque a componentes de privacidad 72 se refieren a ajustes de privacidad, mientras que las métricas de privacidad de evaluación de bloque para cada componente 74 y el bloque muestra parámetros de privacidad 76 se usan para visualizar las métricas de privacidad. Como se ha mencionado anteriormente, la interfaz de visualización puede usarse también para establecer los parámetros de privacidad. Estos bloques operan con el mapeo de componente de sensor y funciones de control de uso 14C y 50 descritas anteriormente.

Analizada en primer lugar se encuentra la entrada de control de privacidad amigable para el usuario 70. El perfil de usuario puede o introducirse explícitamente o como resultado de un cuestionario que ayuda al usuario a definir el perfil de mejor ajuste del usuario. En otra realización las preferencias de usuario pueden inferirse automáticamente por el dispositivo 10 (por ejemplo, basándose en las elecciones de ajustes de privacidad que el usuario ha realizado para otras aplicaciones). El perfil del usuario podría descargarse también de un servidor de descarga de perfil 78.

Las categorías de privacidad (en este punto ejemplificadas como: personal, financiera, profesional, contextual, médica, conexiones sociales, localización) pueden ser el resultado de estudios de usuario pretendidos para hallar categorías de privacidad generales intuitivas/amigables.

También es posible combinar el ajuste de perfil de privacidad "general" con ajustes de perfil de privacidad "ocasional" tal como "ocultar mi información personal y social cada vez que estoy en el trabajo", donde "personal" y "social" son categorías de privacidad, y "estoy en el trabajo" es un contexto de usuario específico detectado por el dispositivo 10 (por ejemplo, tal como basándose en datos del subsistema de GPS 37, o basándose en la detección de una WLAN relacionada con el "trabajo" mediante el transceptor de corto alcance 31 como dos ejemplos no limitantes).

Obsérvese que tales políticas pueden establecerse usando varios métodos, por ejemplo, vocalmente (por ejemplo, usando el micrófono 24 y unidad de reconocimiento de voz 24A), gráficamente (por ejemplo usando la pantalla táctil 16), etc. En una realización el usuario podría arrastrar y soltar iconos en un "contenedor prohibido" y el texto para la política se genera automáticamente, como se muestra en la Figura 11.

Se analiza ahora la entrada de mapa al bloque de componentes de privacidad 72 de la Figura 10. Para facilitar el

mapeo entre categorías de privacidad y sensores, cada categoría de privacidad se divide en los diferentes componentes o subcategorías (por ejemplo, personal = género + edad + religión, etc.). Esta descomposición de categoría de privacidad ayuda en el mapeo de las categorías de privacidad "amigables para el usuario" al nivel de los sensores (bloques 70 y 72 de la Figura 10) así como al cuantificar el nivel de privacidad que proporciona el acceso a un ajuste dado de sensores (bloques 74 y 76 de la Figura 10).

En general estos componentes son más fáciles de cuantificar que las categorías de nivel superiores. Por ejemplo, si se proporciona una aplicación con información de sensor que ayuda a la aplicación a identificar que el usuario es cristiano o musulmán, entonces el nivel de confusión es 2/15 (suponiendo que hay un total de 15 religiones). La correspondiente información de sensor comprende coordenadas de GPS y tiempo que indica que el usuario visita regularmente un área donde puede hallarse una iglesia y una mezquita cerca entre sí. Combinar datos de GPS con otros datos de sensor puede ayudar a ajustar con perfección la suposición.

En el ejemplo anterior de 'suponer' la religión del usuario puede observarse que la información de GPS 37 puede combinarse con otros datos de sensor para reducir el nivel de ambigüedad. Por ejemplo, si la WLAN indica un punto de acceso WiFi que está más cerca de la mezquita que la iglesia, entonces el usuario móvil es más probable que sea un musulmán.

Se analiza ahora las métricas de privacidad de cada bloque de componente 74. Para evaluar el nivel de privacidad de modo que pueda visualizarse al usuario, el dispositivo 10 puede realizar el papel de un atacante analizando los datos relevados hasta ahora, usando algoritmos del estado de la técnica (que se mantienen actualizados) y resúmenes de los detalles de qué métrica de privacidad usarse (por ejemplo, entropía, k-anonimato, etc.). La métrica (o "nivel de confusión", o "nivel de ambigüedad") se calcula para cada componente de privacidad (por ejemplo, religión, género, etc.) teniendo en cuenta el espacio entero de cada componente (por ejemplo, cristiano, musulmán, budista, hindú, etc.). El nivel de privacidad (por ejemplo, "nivel de confusión") se establece a continuación para visualizarse al usuario.

Se analiza ahora el bloque de parámetros de privacidad 76. El resultado del cálculo de la métrica anterior puede visualizarse al usuario. Pueden realizarse diversas agrupaciones (por categoría, por aplicación, etc.) y promedio por conveniencias de usabilidad (puede hacerse de nuevo referencia a las Figuras 8 y 9).

El usuario puede usar esta interfaz para introducir sus preferencias, tal como los límites para visibilidad de componente específico (métrica), o cómo de importantes son los componentes para el usuario (por ejemplo ampliando el correspondiente sector, aumentando por lo tanto la visibilidad como se representa en la Figura 9C).
Además de los mensajes/gráficos relacionados con la privacidad, el panel de privacidad puede incluir una ventana para mensajes de un desarrollador de aplicación, por ejemplo:
"Para obtener el pronóstico del tiempo con la precisión más alta,
por favor establecer su visibilidad de localización al 100 %.
Su ajuste actual es del 35 %, reducir la utilidad/precisión del pronóstico".

Por lo tanto, se hace posible la comunicación entre desarrolladores de las aplicaciones 14B y el usuario basándose en los perfiles de privacidad del usuario.

Debería observarse de nuevo que las referencias a accesos a "sensores" pueden interpretarse que significan acceso a todas las fuentes de información en el dispositivo 10 tal como el sistema de ficheros (por ejemplo, lista de contactos, registros, etc.), integrados en dispositivos (por ejemplo, cámara, micrófono, etc.) además de los diversos otros sensores.

Como debería apreciarse, el uso de estas realizaciones a modo de ejemplo sirve para resumir los detalles técnicos de qué sensores / datos son sensibles a la privacidad, y resumir qué métodos de intrusión de privacidad pueden desplegarse, mapeándolos todos a un lenguaje amigable para el usuario humano, para introducir ajustes de privacidad o para visualizar el estado de privacidad al usuario.

Obsérvese que se encuentra dentro del alcance de las realizaciones a modo de ejemplo de esta invención emplear la interfaz de usuario 14E para posibilitar que el usuario defina una categoría o subcategoría de privacidad relacionada con el usuario, y a continuación mapee los sensores para la categoría o subcategoría definida por el usuario. Como un ejemplo no limitante, si un usuario es un coleccionista de libros raros el usuario puede desear definir una categoría de privacidad separada, por ejemplo, 'intereses de coleccionismo', o una subcategoría separada bajo (por ejemplo) la categoría 'personal', para controlar específicamente aquellos sensores de dispositivo que están permitidos (si los hubiera) a accederse por programas de aplicación 14B cuando el usuario está implicado en esta actividad.

La capacidad para posibilitar al usuario a que especifique ciertas categorías de privacidad está relacionada al menos en parte a hacer la herramienta de privacidad más personalizable para el usuario. Además en este sentido, y por ejemplo, cuando un usuario añade una nueva categoría o subcategoría de privacidad pueden descargarse cualesquiera algoritmos contextuales 14D relevantes automáticamente desde un servidor; los sensores relevantes (fuentes de entrada) determinados y el código de intercepción instalado automáticamente para monitorizar estos sensores; haciendo posible tanto detectar violaciones como visualizar niveles de privacidad que corresponden a la

categoría o subcategoría de privacidad nuevamente añadida.

Basándose en lo anterior debería ser evidente que las realizaciones a modo de ejemplo de esta invención proporcionan un método, aparato y programa o programas informáticos para mejorar un control del usuario sobre la privacidad del usuario. Un aspecto importante de las realizaciones a modo de ejemplo de esta invención es la interfaz de usuario que puede representar niveles de privacidad de cada programa de aplicación al usuario en un formato "amigable para el usuario". Otro aspecto importante de las realizaciones a modo de ejemplo es proporcionar al dispositivo de usuario con una capacidad para detectar y actuar o al menos informar violaciones de privacidad por los programas de aplicación.

La Figura 12 es un diagrama de flujo lógico que ilustra la operación de un método, y un resultado de la ejecución de instrucciones de programa informático, de acuerdo con las realizaciones a modo de ejemplo de esta invención. De acuerdo con estas realizaciones a modo de ejemplo un método realiza, en el bloque 12A, una etapa de operación de una interfaz de usuario de un dispositivo para recibir de un usuario, para categorías individuales de una pluralidad de categorías de privacidad de usuario, un ajuste de privacidad de usuario. En el bloque 12B hay una etapa de mapeo de cada ajuste de privacidad de usuario a uno o más sensores de dispositivo para formar una política de sensor para la categoría de privacidad del usuario. En el bloque 12C hay una etapa de monitorización de accesos de programa de aplicación a sensores de dispositivo para detectar una violación de una política de sensor.

Los diversos bloques mostrados en la Figura 12 se pueden ver como etapas de método, y/o como operaciones que resultan de la operación de código de programa informático, y/o como una pluralidad de elementos de circuito lógico acoplados construidos para llevar a cabo la función o funciones asociadas.

En general, las diversas realizaciones a modo de ejemplo pueden implementarse en hardware o circuitos de fin especial, software, lógica o cualquier combinación de los mismos. Por ejemplo, algunos aspectos pueden implementarse en hardware, mientras que otros aspectos pueden implementarse en firmware o software que puede ejecutarse por un controlador, microprocesador u otro dispositivo informático, aunque la invención no está limitada a lo mismo. Aunque pueden ilustrarse y describirse diversos aspectos de las realizaciones ilustrativas de la presente invención como diagramas de bloques, diagramas de flujo o usando alguna otra representación gráfica, se entiende bien que estos bloques, aparatos, sistemas, técnicas o métodos descritos en el presente documento pueden implementarse en, como ejemplos no limitantes, hardware, software, firmware, circuitos o lógica de fin especial, hardware o controlador de fin general u otros dispositivos informáticos, o alguna combinación de los mismos.

Debería apreciarse por lo tanto que al menos algunos aspectos de las realizaciones a modo de ejemplo de las invenciones pueden ponerse en práctica en diversos componentes tales como chips y módulos de circuito integrado, y que las realizaciones a modo de ejemplo de esta invención pueden realizarse en un aparato que se realiza como un circuito integrado. El circuito integrado, o los circuitos, puede comprender circuitería (así como posiblemente firmware) para realizar al menos uno o más de un procesador de datos o procesadores de datos, un procesador o procesadores de señales digitales, circuitería de banda base y circuitería de frecuencia de radio que son configurables para operar de acuerdo con las realizaciones a modo de ejemplo de esta invención.

Diversas modificaciones y adaptaciones a las realizaciones a modo de ejemplo anteriores de esta invención pueden hacerse evidentes para los expertos en las materias pertinentes en vista de la descripción anterior, cuando se leen en conjunto con los dibujos adjuntos.

Debería observarse que los términos "conectado", "acoplado", o cualquier variante de los mismos, quieren decir cualquier conexión o acoplamiento, o bien directo o bien indirecto, entre dos o más elementos, y pueden abarcar la presencia de uno o más elementos intermedios entre dos elementos que están "conectados" o "acoplados" entre sí. El acoplamiento o conexión entre los elementos puede ser físico, lógico o una combinación de los mismos. Como se emplea en el presente documento dos elementos pueden considerarse que están "conectados" o "acoplados" juntos por el uso de uno o más alambres, cables y/o conexiones eléctricas impresas, así como por el uso de energía electromagnética, tal como energía electromagnética que tiene longitudes de onda en la región de frecuencia de radio, la región de microondas y la región óptica (tanto visible como invisible), como varios ejemplos no limitantes y no-exhaustivos.

Además, los diversos nombres usados para las categorías de privacidad descritas (por ejemplo, personal, profesional, contexto, conexiones sociales, etc.) y subcategorías de las mismas no se pretende que sean limitantes en ningún aspecto, ya que estas categorías y subcategorías de privacidad pueden identificarse por cualesquiera nombres adecuados. Además, los diversos nombres asignados a diferentes sensores no se pretende que sean limitantes en ningún aspecto, ya que estos sensores pueden identificarse por cualesquiera nombres adecuados.

Además, algunas de las características de las diversas realizaciones no limitantes y a modo de ejemplo de esta invención se pueden aprovechar sin el uso correspondiente de otras características. Como tal, la descripción anterior debería considerarse como simplemente ilustrativa de los principios, enseñanzas y realizaciones a modo de ejemplo de esta invención, y no como limitación de la misma.

REIVINDICACIONES

1. Un método, que comprende:

operar (12A) una interfaz de usuario de un dispositivo para recibir de un usuario, un ajuste de privacidad de usuario, y monitorizar (12C) accesos de programa de aplicación a sensores de dispositivo para detectar una violación de una política de sensor, donde al menos algunas categorías de privacidad de información personal de usuario comprenden una pluralidad de subcategorías,
caracterizado por
recibirse el ajuste de privacidad de usuario para categorías individuales de una pluralidad de categorías de privacidad de información personal de usuario, y
mapear (12B) cada ajuste de privacidad de usuario a uno o más sensores de dispositivo para formar una política de sensor para la categoría de privacidad de información personal de usuario, donde el mapeo forma una política de sensor para cada una de las subcategorías, en donde al menos uno de los sensores de dispositivo es pertinente para más de una subcategoría, en donde el ajuste de privacidad de usuario se recibe para un contexto de usuario específico, y
en donde el ajuste de privacidad de usuario se aplica en respuesta a que el dispositivo esté en el contexto de usuario específico.

2. Un método de acuerdo con la reivindicación 1, donde la monitorización (12C) comprende aplicar ajustes de privacidad de usuario en tiempo no real registrando un acceso por un programa de aplicación a un sensor que viola una política de sensor, e informar del acceso.

3. Un método de acuerdo con al menos una de las reivindicaciones 1 a 2, donde la monitorización (12C) se realiza en un nivel de sistema operativo, en un nivel de plataforma, el nivel del programa de aplicación y/o un nivel de red.

4. Un método de acuerdo con al menos una de las reivindicaciones 1 a 3, donde la monitorización (12C) comprende adicionalmente:

registrar accesos de programa de aplicación a sensores de dispositivo;
basándose al menos en el mapeo, determinar qué información personal de usuario podría inferirse basándose en los accesos de programa de aplicación registrados; e
informar la información personal inferida determinada al usuario.

5. Un método de acuerdo con al menos una de las reivindicaciones 1 a 4 , donde operar la interfaz de usuario (12A) comprende adicionalmente al menos uno de presentar al usuario una representación de un nivel de privacidad actual del usuario para subcategorías individuales de las subcategorías de una categoría de privacidad de información personal de usuario particular,
presentar al usuario una representación de un nivel de privacidad actual del usuario para categorías individuales de las categorías de privacidad de información personal de usuario para un programa de aplicación particular,
presentar al usuario una representación de una preferencia de privacidad actual del usuario para categorías individuales de las categorías de privacidad de información personal de usuario para uno o más de, indicar límites que no deberían superarse y diferenciar entre una importancia relativa de las categorías de privacidad de información personal de usuario entre sí,
presentar al usuario una comunicación de un desarrollador de un programa de aplicación con información relacionada con un ajuste de privacidad sugerido para el programa de aplicación.
y donde el mapeo a un sensor de dispositivo mapea a un único sensor de dispositivo o a una combinación de dos o más sensores de dispositivo.

6. Un método de acuerdo con al menos una de las reivindicaciones 1 a 5, donde operar la interfaz de usuario (12A) comprende adicionalmente posibilitar que el usuario defina una categoría de privacidad de información personal de usuario o una subcategoría de privacidad, y mapear al menos un sensor de dispositivo para formar una política de sensor para la categoría de privacidad o subcategoría de privacidad de información personal de usuario definida por el usuario.

7. Un medio legible por ordenador no transitorio que contiene instrucciones de programa de software, donde la ejecución de las instrucciones de programa de software por al menos un procesador de datos da como resultado la realización de operaciones que comprenden:

operar una interfaz de usuario de un dispositivo para recibir de un usuario un ajuste de privacidad de usuario, y monitorizar accesos de programa de aplicación a sensores de dispositivo para detectar una violación de una política de sensor, donde al menos algunas categorías de privacidad de información personal de usuario comprenden una pluralidad de subcategorías,
caracterizado por
ejecución de las instrucciones de programa de software por el al menos un procesador de datos que da como resultado la realización de:

recibirse el ajuste de privacidad de usuario para categorías individuales de una pluralidad de categorías de privacidad de información personal de usuario, y
mapear cada ajuste de privacidad de usuario a uno o más sensores de dispositivo para formar una política de sensor para la categoría de privacidad de información personal de usuario y donde el mapeo forma una política de sensor para cada una de las subcategorías, en donde al menos uno de los sensores de dispositivo es relevante para más de una subcategoría, en donde se recibe el ajuste de privacidad de usuario para un contexto de usuario específico, y en donde
el ajuste de privacidad de usuario se aplica en respuesta a que el dispositivo esté en el contexto de usuario específico.

8. Un aparato (10), que comprende:

medios para recibir (36) de un usuario un ajuste de privacidad de usuario;
medios para monitorizar (12) accesos de programa de aplicación a sensores para detectar una violación de una política de sensor, donde al menos algunas categorías de privacidad de información personal de usuario comprenden una pluralidad de subcategorías,
caracterizado por
los medios para recibir (36) que están configurados para recibir el ajuste de privacidad de usuario para categorías individuales de una pluralidad de categorías de privacidad de información personal de usuario;
medios para mapear (12) cada ajuste de privacidad de usuario a uno o más sensores de dispositivo para formar una política de sensor para la categoría de privacidad de información personal de usuario, y
medios para formar (12) una política de sensor para cada una de las subcategorías, en donde al menos uno de los sensores de dispositivo es relevante para más de una subcategoría, en donde el ajuste de privacidad de usuario se recibe para un contexto de usuario específico y en donde el ajuste de privacidad de usuario se aplica en respuesta a que el dispositivo esté en el contexto de usuario específico.

9. Un aparato (10) de acuerdo con la reivindicación 8, que comprende adicionalmente medios para aplicar (12) ajustes de privacidad de usuario en tiempo no real registrando un acceso por un programa de aplicación a un sensor que viola una política de sensor e informar del acceso.

10. Un aparato (10) de acuerdo con al menos una de las reivindicaciones 8 a 9, en el que los medios de monitorización (12) comprenden monitorizar acceso de programa de aplicación a uno o más de un nivel de sistema operativo, un nivel de plataforma, en un nivel de programa de aplicación y un nivel de red.

11. Un aparato (10) de acuerdo con al menos una de las reivindicaciones 8 a 10, comprendiendo adicionalmente el aparato: medios para registrar (12) accesos de programa de aplicación a sensores de dispositivo; basándose al menos en el mapeo, medios para determinar qué información personal de usuario podría inferirse basándose en los accesos de programa de aplicación registrados; y medios para informar la información personal inferida determinada al usuario.

12. Un aparato (10) de acuerdo con al menos una de las reivindicaciones 8 a 11, comprendiendo adicionalmente el aparato al menos uno de:
medios para presentar (16) al usuario una representación de un nivel de privacidad global actual del usuario, medios para presentar (16) al usuario una representación de un nivel de privacidad actual del usuario para subcategorías individuales de las subcategorías de una categoría de privacidad de información personal de usuario particular, medios para presentar (16) al usuario una representación de un nivel de privacidad actual del usuario para categorías individuales de las categorías de privacidad de información personal de usuario para un programa de aplicación particular, medios para presentar (16) al usuario una representación de una preferencia de privacidad actual del usuario para categorías individuales de las categorías de privacidad de información personal de usuario para uno o más de indicar límites que no deberían superarse y para diferenciar entre una importancia relativa de las categorías de privacidad de información personal de usuario unas de las otras, y medios para presentar (16) al usuario una comunicación de un desarrollador de un programa de aplicación con información relacionada con un ajuste de privacidad sugerido para el programa de aplicación.

13. Un aparato (10) de acuerdo con al menos una de las reivindicaciones 8 a 12, comprendiendo adicionalmente el aparato medios para posibilitar (12) que el usuario defina una categoría de privacidad o subcategoría de privacidad de información personal de usuario y mapee al menos un sensor de dispositivo para formar una política de sensor para la categoría de privacidad o subcategoría de privacidad de información personal de usuario definida por el usuario.

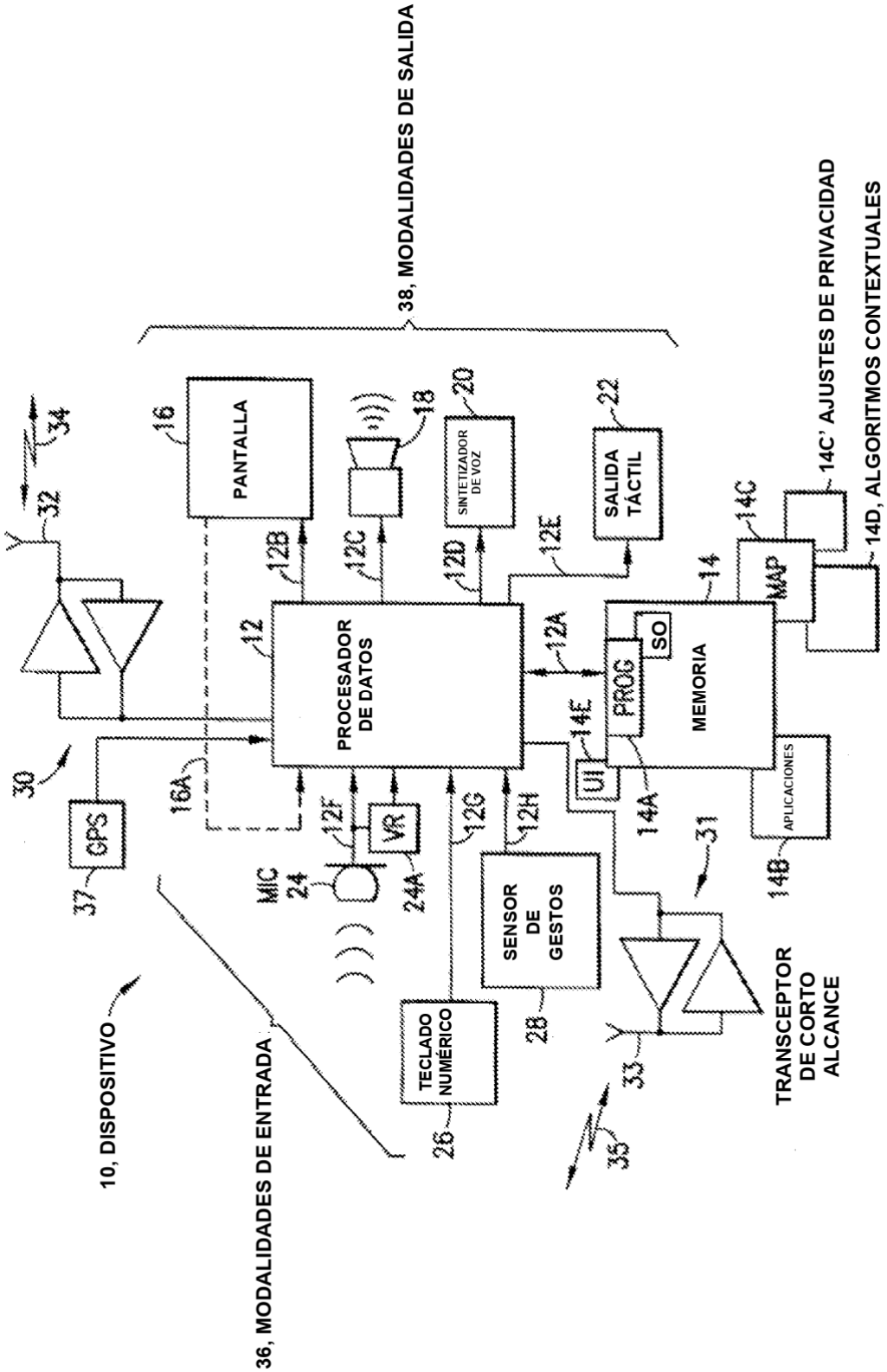

38, MODALIDADES DE SALIDA
PANTALLA
SINTETIZADOR DE VOZ
SALIDA TÁCTIL
14C' AJUSTES DE PRIVACIDAD
14D, ALGORITMOS CONTEXTUALES
PROCESADOR DE DATOS
MEMORIA
MAP
SO
PROG
UI
APLICACIONES
GPS
MIC
VR
SENSOR DE GESTOS
TECLADO NUMÉRICO
TRANSCEPTOR DE CORTO ALCANCE
10, DISPOSITIVO
36, MODALIDADES DE ENTRADA

FIG. 1

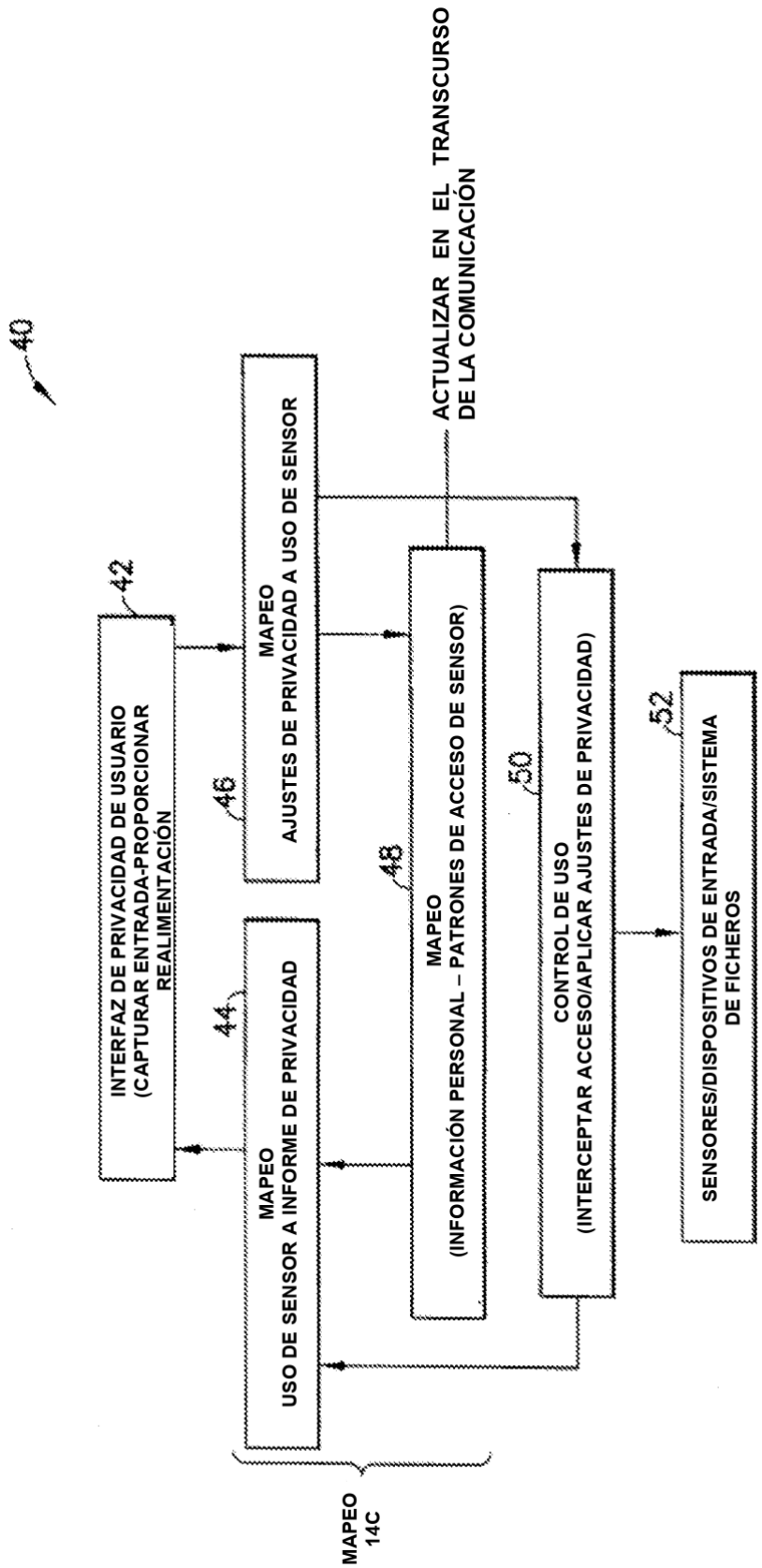

40
INTERFAZ DE PRIVACIDAD DE USUARIO (CAPTURAR ENTRADA-PROPORCIONAR REALIMENTACIÓN
42
MAPEO USO DE SENSOR A INFORME DE PRIVACIDAD
44
MAPEO AJUSTES DE PRIVACIDAD A USO DE SENSOR
46
MAPEO (INFORMACIÓN PERSONAL – PATRONES DE ACCESO DE SENSOR)
48
CONTROL DE USO (INTERCEPTAR ACCESO/APLICAR AJUSTES DE PRIVACIDAD)
50
SENSORES/DISPOSITIVOS DE ENTRADA/SISTEMA DE FICHEROS
52
ACTUALIZAR EN EL TRANSCURSO DE LA COMUNICACIÓN
MAPEO 14C

FIG.2

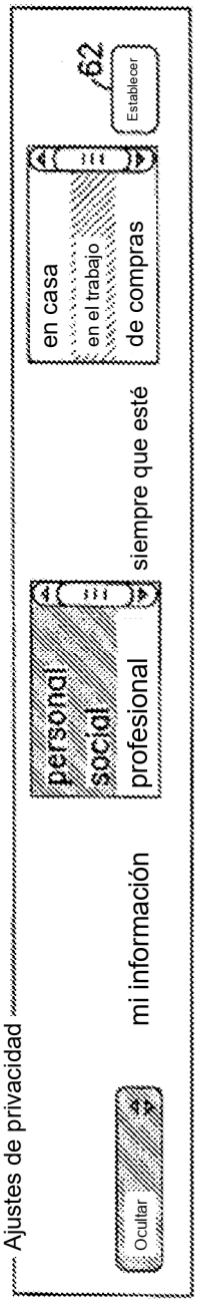

Ajustes de privacidad
Ocultar
mi información
personal
social
profesional
siempre que esté
en casa
en el trabajo
de compras
62
Establecer
60

FIG.3A

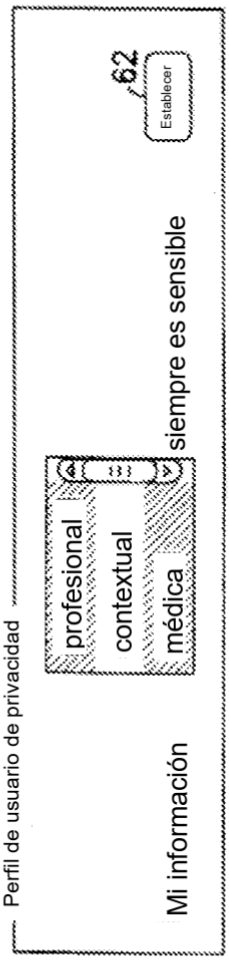
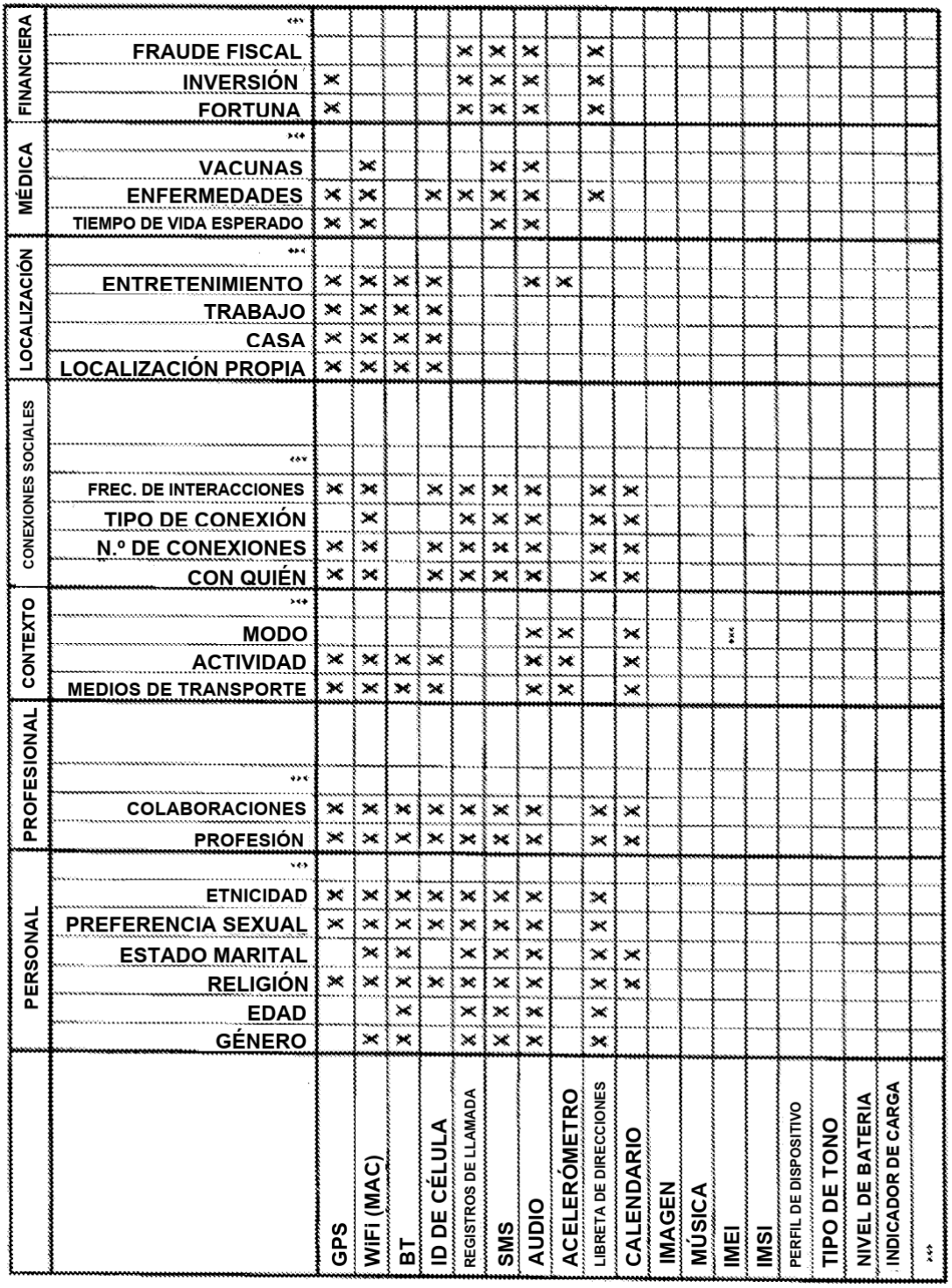

Perfil de usuario de privacidad
Mi información
profesional
contextual
médica
siempre es sensible
62
Establecer
61

FIG.3B



	PERSONAL							PROFESIONAL			CONTEXTO				CONEXIONES SOCIALES						LOCALIZACIÓN					MÉDICA				FINANCIERA			
	GÉNERO	EDAD	RELIGIÓN	ESTADO MARITAL	PREFERENCIA SEXUAL	ETNICIDAD	...	PROFESIÓN	COLABORACIONES	...	MEDIOS DE TRANSPORTE	ACTIVIDAD	MODO	...	CON QUIÉN	N.º DE CONEXIONES	TIPO DE CONEXIÓN	FREC. DE INTERACCIONES	...	...	LOCALIZACIÓN PROPIA	CASA	TRABAJO	ENTRETENIMIENTO	...	TIEMPO DE VIDA ESPERADO	ENFERMEDADES	VACUNAS	...	FORTUNA	INVERSIÓN	FRAUDE FISCAL	...
GPS			X		X	X		X	X		X	X			X	X		X			X	X	X	X		X	X			X	X	
WiFi (MAC)	X		X	X	X	X		X	X		X	X			X	X	X	X			X	X	X	X		X	X	X		X	X	
BT	X	X	X	X	X	X		X	X		X	X			X	X					X	X	X	X								
ID DE CÉLULA			X		X	X		X	X		X	X			X	X		X			X		X	X		X	X			X	X	
REGISTROS DE LLAMADA	X	X	X	X	X	X		X	X						X	X	X	X			X									X	X	
SMS	X	X	X	X	X	X		X	X						X	X	X	X			X									X	X	
AUDIO	X	X	X	X	X	X		X	X		X	X	X		X	X	X	X			X									X	X	
ACELERÓMETRO											X	X	X								X									X	X	
LIBRETA DE DIRECCIONES	X	X	X	X	X	X		X	X						X	X	X	X			X									X	X	
CALENDARIO			X	X				X	X		X	X	X		X	X	X	X			X									X	X	
IMAGEN																					X									X	X	
MÚSICA																					X									X	X	
IMEI														...							X									X	X	
IMSI																					X									X	X	
PERFIL DE DISPOSITIVO																					X									X	X	
TIPO DE TONO																					X									X	X	
NIVEL DE BATERIA																					X									X	X	
INDICADOR DE CARGA																					X									X	X	
...																					X									X	X	

FIG.4

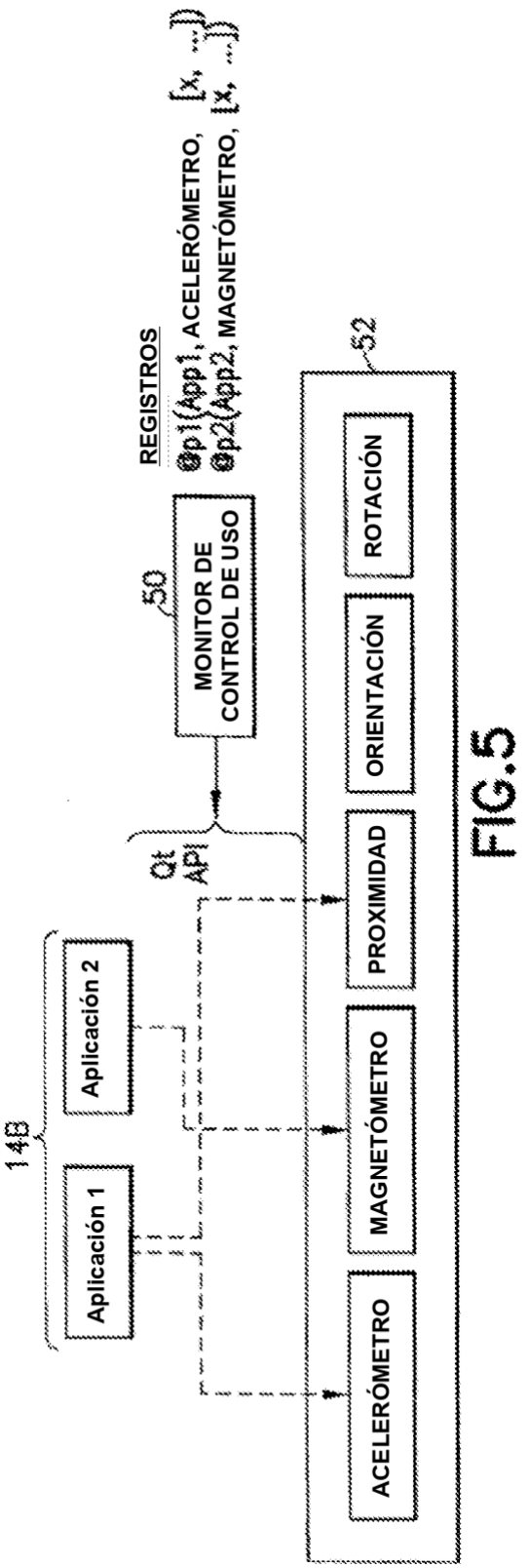

148
Aplicación 1
Aplicación 2
Qt API
50
MONITOR DE CONTROL DE USO
REGISTROS
@p1(App1, ACELERÓMETRO, [x, ...])
@p2(App2, MAGNETÓMETRO, [x, ...])
52
ACELERÓMETRO
MAGNETÓMETRO
PROXIMIDAD
ORIENTACIÓN
ROTACIÓN

FIG.5

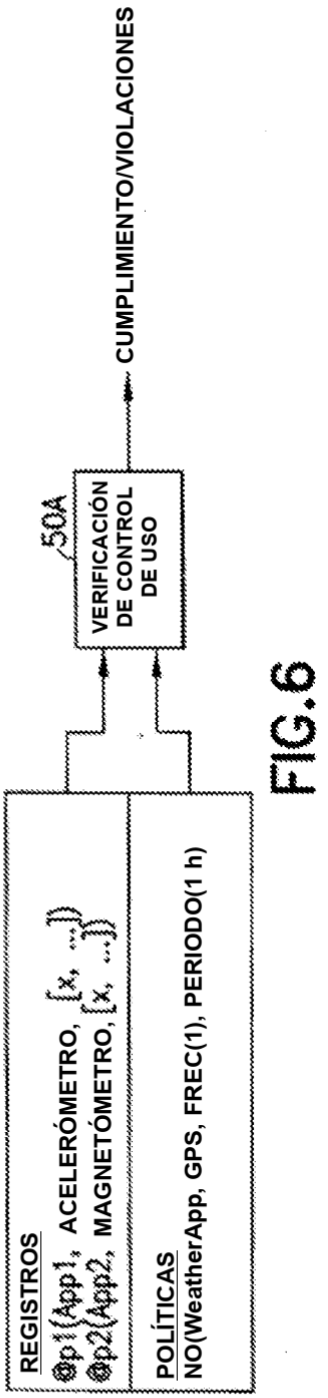

50A
VERIFICACIÓN DE CONTROL DE USO
CUMPLIMIENTO/VIOLACIONES
REGISTROS
@p1(App1, ACELERÓMETRO, [x, ...])
@p2(App2, MAGNETÓMETRO, [x, ...])
POLÍTICAS
NO(WeatherApp, GPS, FREC(1), PERIODO(1 h)

FIG.6

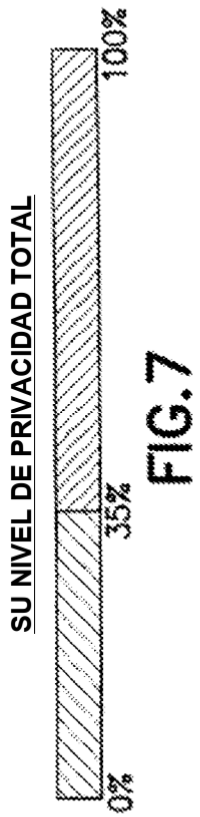

SU NIVEL DE PRIVACIDAD TOTAL
100%
35%
0%

FIG.7

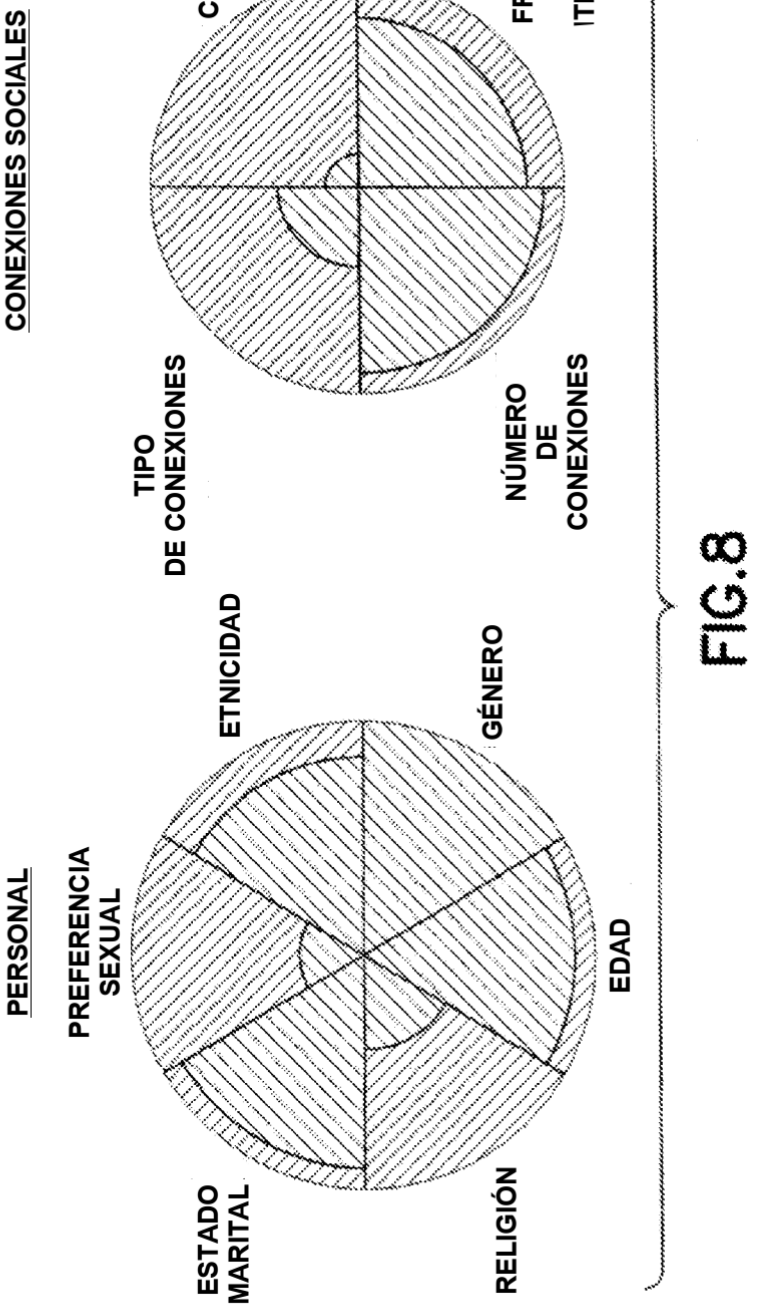

CONEXIONES SOCIALES
CON QUIÉN
FRECUENCIA DE ITERACIONES
TIPO DE CONEXIONES
NÚMERO DE CONEXIONES
PERSONAL
PREFERENCIA SEXUAL
ETNICIDAD
GÉNERO
EDAD
ESTADO MARITAL
RELIGIÓN

FIG.8

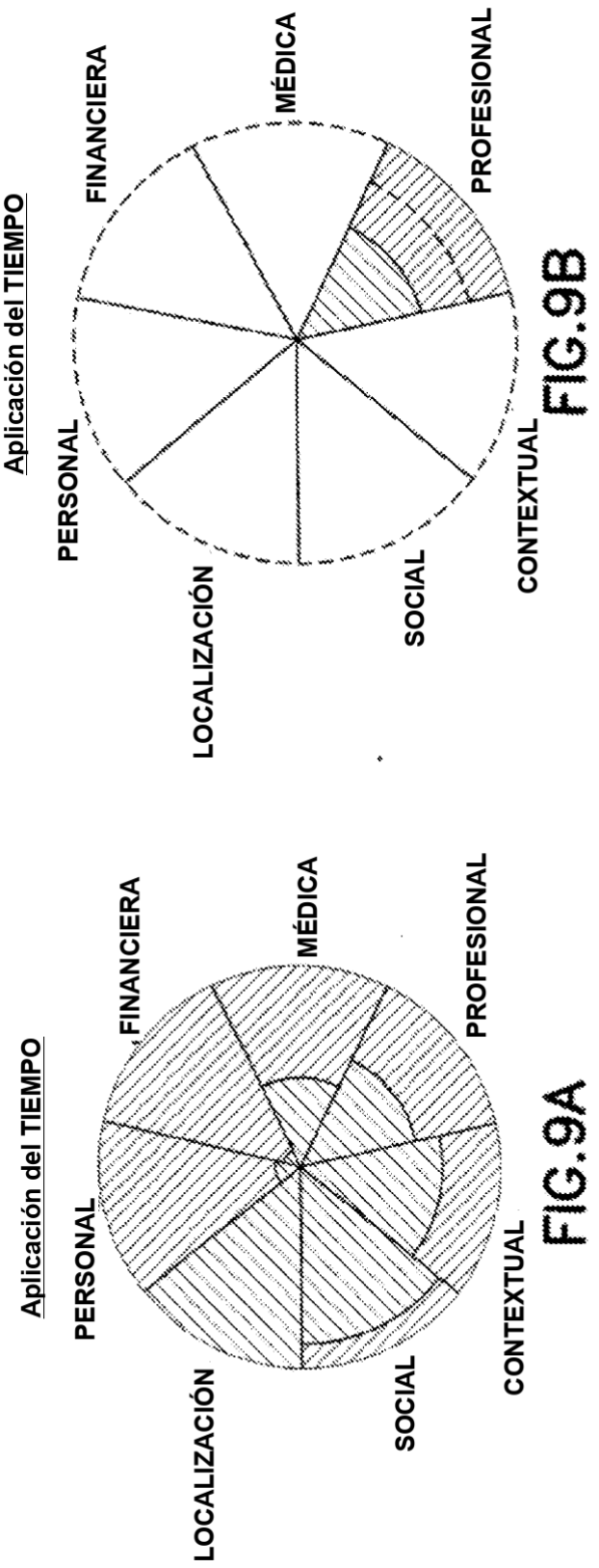


FIG.9A

FIG.9B

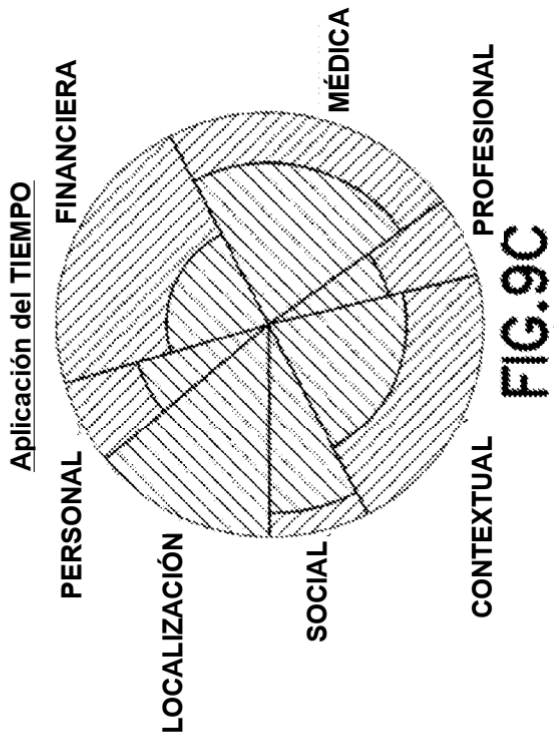


FIG.9C

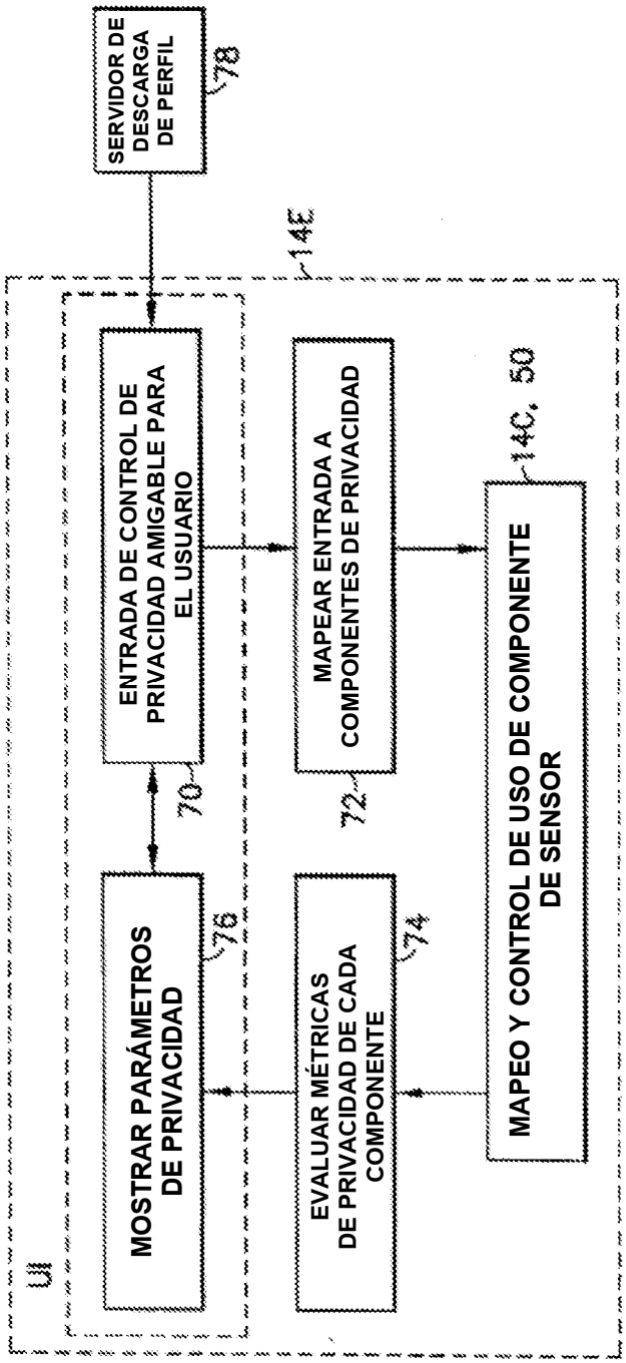

SERVIDOR DE DESCARGA DE PERFIL
78
14E
ENTRADA DE CONTROL DE PRIVACIDAD AMIGABLE PARA EL USUARIO
70
MAPEAR ENTRADA A COMPONENTES DE PRIVACIDAD
72
14C, 50
MAPEO Y CONTROL DE USO DE COMPONENTE DE SENSOR
MOSTRAR PARÁMETROS DE PRIVACIDAD
76
EVALUAR MÉTRICAS DE PRIVACIDAD DE CADA COMPONENTE
74
UI
DISPOSITIVO MÓVIL, 10

FIG. 10

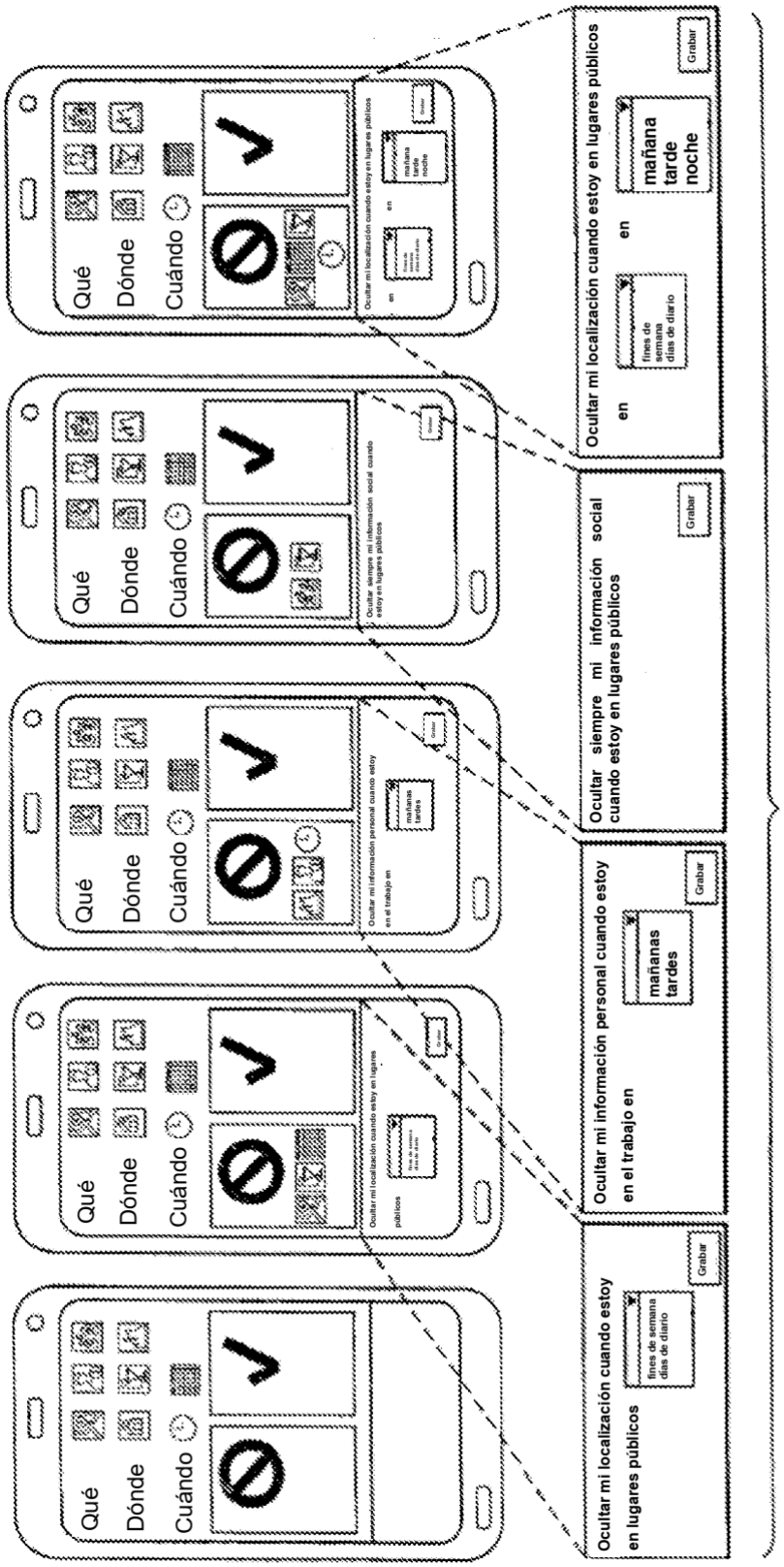

Qué
Dónde
Cuándo
Ocultar mi localización cuando estoy en lugares públicos
en
fines de semana
días de diario
Grabar
Ocultar mi información personal cuando estoy en el trabajo en
mañanas
tardes
Grabar
Ocultar siempre mi información social cuando estoy en lugares públicos
Grabar
Ocultar mi localización cuando estoy en lugares públicos
en
fines de semana
días de diario
en
mañana
tarde
noche
Grabar

FIG.11

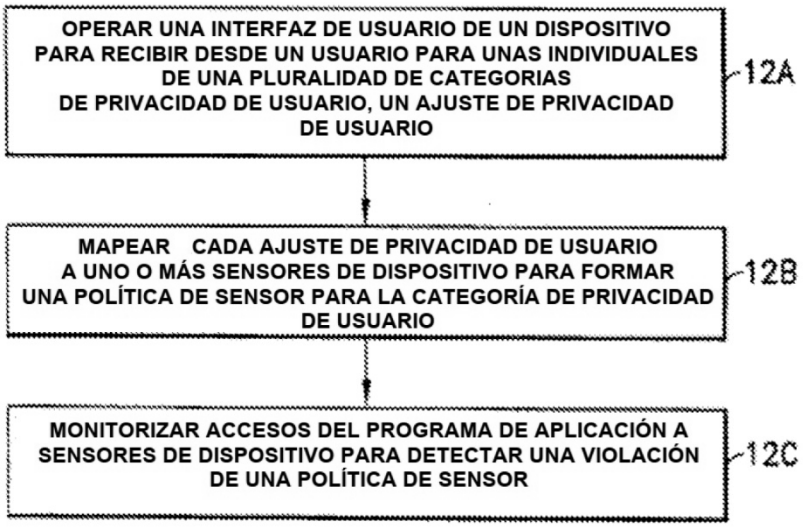

OPERAR UNA INTERFAZ DE USUARIO DE UN DISPOSITIVO PARA RECIBIR DESDE UN USUARIO PARA UNAS INDIVIDUALES DE UNA PLURALIDAD DE CATEGORIAS DE PRIVACIDAD DE USUARIO, UN AJUSTE DE PRIVACIDAD DE USUARIO
12A
MAPEAR CADA AJUSTE DE PRIVACIDAD DE USUARIO A UNO O MÁS SENSORES DE DISPOSITIVO PARA FORMAR UNA POLÍTICA DE SENSOR PARA LA CATEGORÍA DE PRIVACIDAD DE USUARIO
12B
MONITORIZAR ACCESOS DEL PROGRAMA DE APLICACIÓN A SENSORES DE DISPOSITIVO PARA DETECTAR UNA VIOLACIÓN DE UNA POLÍTICA DE SENSOR
12C

FIG.12