

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 882 537**

51 Int. Cl.:

G06F 21/62 (2013.01)

G06Q 30/02 (2012.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **02.10.2015** **PCT/IB2015/002132**

87 Fecha y número de publicación internacional: **07.04.2016** **WO16051279**

96 Fecha de presentación y número de la solicitud europea: **02.10.2015** **E 15813902 (2)**

97 Fecha y número de publicación de la concesión europea: **09.06.2021** **EP 3201823**

54 Título: **Sistemas y métodos para concesión basada en contexto de permisos de información de identificación personal**

30 Prioridad:

02.10.2014 US 201462059087 P

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

02.12.2021

73 Titular/es:

TRUNOMI LTD. (100.0%)
New Venture House 3rd Floor, 3 Mill Creek Road
Pembroke HM05, BM

72 Inventor/es:

LACEY, STUART H.;
SINGHAL, NARESH y
CHELINE, DOUGLAS

74 Agente/Representante:

ROEB DÍAZ-ÁLVAREZ, María

ES 2 882 537 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Sistemas y métodos para concesión basada en contexto de permisos de información de identificación personal

5 Campo técnico

Las implementaciones divulgadas se refieren generalmente a sistemas y métodos de concesión basada en contexto de permisos de información de identificación personal.

10 Antecedentes

La información de identificación personal, o "PII" (personal identifiable information), es información que se puede utilizar, ya sea sola o en combinación con otra información, para identificar de forma única a una persona en particular. En la era de la informática moderna, los usuarios generan cantidades significativas de PII en su vida cotidiana, a menudo sin ser conscientes de que lo están haciendo o sin apreciar hasta qué punto la información les permite ser identificados de forma única. A medida que los dispositivos pueden recopilar cada vez más datos sobre los usuarios (y datos más confidenciales, como información de salud, información de ubicación, etc.), las preocupaciones de privacidad sobre la PII son cada vez más relevantes.

Actualmente, cada recopilador de PII es responsable de informar a los usuarios de qué datos se recopilan, cómo se utilizan y con qué propósito. Sin embargo, con tantas entidades diferentes que recopilan, almacenan y usan la PII de una persona, es difícil para las personas entender exactamente qué entidades han permitido recopilar su PII y qué pueden hacer esas entidades con su PII. Muchos de estos acuerdos permiten al recopilador de PII una gran cantidad de libertad de uso para hacer lo que elijan con la PII y en cualquier momento. Por lo tanto, los usuarios generalmente no controlan quién tiene su PII, cómo se usa y cuándo. Los reguladores y los gobiernos son cada vez más conscientes de este problema y están buscando promulgar leyes que establezcan cómo y qué controles deben implementarse.

Además, la mayoría de los acuerdos que rigen los derechos y responsabilidades de una entidad con respecto a la PII son acuerdos no negociables del tipo "tómalo o déjalo": el usuario debe aceptar los términos o renunciar a utilizar un servicio en particular. Por ejemplo, los términos de uso que rigen una aplicación y / o dispositivo de control de la presión arterial pueden autorizar al proveedor a registrar y almacenar información sobre la presión arterial y, posiblemente, compartir la información con terceros. Dichos acuerdos no permiten que el usuario establezca restricciones, por ejemplo, sobre cuándo el proveedor puede registrar datos, cuándo se pueden compartir los datos, para qué se pueden usar los datos o con quién se pueden compartir. Los usuarios pueden simplemente negarse a aceptar los términos establecidos, pero luego no podrán utilizar el servicio o el dispositivo. En otros casos, los acuerdos son tan complejos y largos que la mayoría de los usuarios no están calificados o no pueden comprender el derecho que brindan. Estos acuerdos de usuario "generales" también crean un impedimento para que los usuarios comprendan o incluso aprecien el alcance de sus permisos. En consecuencia, los usuarios tienen la posibilidad de elegir entre autorizar el acceso generalizado a información personal confidencial o no poder utilizar tecnologías modernas beneficiosas y valiosas. Por diversas razones, los usuarios a menudo aceptan los términos, renunciando así a un control sustancial de la PII sensible.

El documento US 2010/077484 B1 describe un motor de privacidad de seguimiento de ubicación que está configurado para permitir a los usuarios definir políticas de privacidad que gobiernen cómo se proporciona la información de ubicación de cada usuario a aplicaciones y servicios sensibles al contexto. Las políticas de privacidad se pueden definir de una manera altamente flexible y específica al contexto, de modo que la ejecución de una política de privacidad dada por el motor de privacidad de seguimiento de ubicación depende de la existencia de una o más condiciones sociales, temáticas, temporales o espaciales. Las políticas de privacidad son luego ejecutadas automáticamente por el motor de privacidad de seguimiento de ubicación cuando se determina que se cumplen las condiciones asociadas con las políticas.

El documento US 2013/103759 B1 describe un enfoque para proporcionar esquemas de intercambio de datos para proporcionar servicios de dispositivo. Un usuario determina un esquema de intercambio de datos para la activación en uno o más dispositivos. Como resultado, el concentrador de contexto contenido dentro del dispositivo procesa y / o facilita un procesamiento del esquema de intercambio de datos para determinar aplicaciones, servicios o una combinación, que son al menos sustancialmente compatibles con el esquema de intercambio de datos seleccionado. El centro de contexto provoca entonces, al menos en parte, una presentación al usuario de las aplicaciones, los servicios o una combinación. A partir de entonces, el centro de contexto determina uno o más contextos asociados con el uno o más dispositivos y procesos y / o facilita un procesamiento de los contextos para provocar, al menos en parte, una recomendación de al menos otro esquema de intercambio de datos, así como cualquier aplicación, servicio, o una combinación, que sean relevantes y que cumplan con la norma, para activar en uno o más dispositivos.

Resumen

En consecuencia, sería ventajoso proporcionar sistemas y métodos que permitan a los usuarios controlar qué información de PII se comparte, con quién se comparte y cuándo se comparte. Además, sería ventajoso proporcionar sistemas, métodos e interfaces de usuario mediante los cuales los usuarios puedan controlar múltiples tipos de PII y múltiples consumidores de PII en un entorno único, fácil de entender y fácil de usar.

De acuerdo con algunas implementaciones, se describe un método para proporcionar acceso a la información personal de un usuario. El método se realiza en un sistema servidor, conectado a través de una red a uno o más dispositivos electrónicos y uno o más dispositivos solicitantes, que tiene uno o más procesadores y una memoria que almacena uno o más programas para su ejecución por el uno o más procesadores. El método incluye establecer una pluralidad de perfiles de contexto para un usuario; detectar un evento asociado con una solicitud recibida de un tercero para obtener información personal del usuario especificada por el tercero; generar una solicitud de consentimiento para compartir la información personal del usuario con un tercero; enviar, al usuario, la solicitud de consentimiento para compartir la información personal del usuario con el tercero; recibir, del usuario, consentimiento para compartir al menos un subconjunto de la información personal solicitada con el tercero cuando al menos un primer perfil de contexto, de la pluralidad de perfiles de contexto, está activo; determinar un perfil de contexto activo para el usuario en base a una o más señales indicativas del contexto del usuario; determinar si el perfil de contexto activo coincide con el primer perfil de contexto; de acuerdo con una determinación de que el perfil de contexto activo coincide con el primer perfil de contexto, facilitar el intercambio de la información personal del usuario con el tercero; y de acuerdo con una determinación de que el perfil de contexto activo no coincide con el primer perfil de contexto, no facilitar el intercambio de la información personal del usuario con el tercero.

De acuerdo con algunas realizaciones, detectar el evento asociado con la solicitud de información personal del usuario comprende recibir una solicitud de la información personal del usuario.

De acuerdo con algunas realizaciones, el perfil de contexto activo para el usuario se determina automáticamente sin intervención del usuario.

De acuerdo con algunas realizaciones, el método incluye, además, de acuerdo con una determinación de que el perfil de contexto activo coincide con el primer perfil de contexto, permitir que el tercero se ponga en contacto con el usuario; y de acuerdo con una determinación de que el perfil de contexto activo no coincide con el primer perfil de contexto, no permitir que el tercero se ponga en contacto con el usuario.

De acuerdo con algunas realizaciones, el método incluye, además, recibir una comunicación del tercero; de acuerdo con una determinación de que el perfil de contexto activo coincide con el primer perfil de contexto, reenviar la comunicación al usuario; y de acuerdo con una determinación de que el perfil de contexto activo no coincide con el primer perfil de contexto, no reenviar la comunicación al usuario.

De acuerdo con algunas realizaciones, el método incluye, además, de acuerdo con una determinación de que el perfil de contexto activo coincide con el primer perfil de contexto, permitir que el tercero se comunique directamente con el usuario; y de acuerdo con una determinación de que el perfil de contexto activo no coincide con el primer perfil de contexto, no permitir que el tercero se comunique directamente con el usuario.

De acuerdo con algunas implementaciones, la pluralidad de perfiles de contexto se almacena en un primer dispositivo electrónico de los uno o más dispositivos electrónicos, donde la información personal del usuario se almacena en un segundo dispositivo electrónico de los uno o más dispositivos electrónicos, el segundo dispositivo electrónico es distinto del primer dispositivo electrónico.

De acuerdo con algunas implementaciones, un sistema informático (por ejemplo, un sistema cliente o un sistema servidor) incluye uno o más procesadores, memoria y uno o más programas; el uno o más programas se almacenan en la memoria y se configuran para ser ejecutados por el uno o más procesadores y el uno o más programas incluyen instrucciones para realizar las operaciones del método descrito anteriormente. De acuerdo con algunas implementaciones, un medio de almacenamiento legible por computadora, no transitorio, tiene almacenadas instrucciones que cuando son ejecutadas por uno o más procesadores, hacen que un sistema informático (por ejemplo, un sistema cliente o sistema servidor) realice las operaciones de los métodos descritos anteriormente.

Los sistemas y métodos divulgados ponen al individuo en control de su información de identificación personal y permiten un control detallado sobre cómo, cuándo y con quién se comparte. De hecho, los sistemas y métodos descritos permiten un cambio en el paradigma actual de PII donde las personas deben aceptar los términos y condiciones que otorgan a un solicitante amplios permisos, lo que permite a las corporaciones y otras entidades decidir qué datos recopilan y almacenan, y cómo y cuándo pueden usarlos. Más bien, el control sobre la PII se devuelve al individuo donde pertenece. Además, al determinar automáticamente los perfiles de contexto activos, el usuario puede

preestablecer sus permisos deseados, y luego estar seguro de que esos permisos serán observados incluso sin que el usuario cambie afirmativamente los permisos o seleccione un perfil activo.

Breve descripción de los dibujos

5 Las implementaciones aquí descritas se ilustran a modo de ejemplo, y no a modo de limitación, en las figuras de los dibujos adjuntos. Los mismos números de referencia se refieren a partes correspondientes en todos los dibujos.

Las figuras 1A-1B son diagramas de bloques que ilustran un entorno cliente-servidor, de acuerdo con algunas implementaciones.

10 La figura 2 es un diagrama de bloques que ilustra un dispositivo informático cliente, de acuerdo con algunas implementaciones.

15 La figura 3 es un diagrama de bloques que ilustra un dispositivo informático solicitante, de acuerdo con algunas implementaciones.

La figura 4 es un diagrama de bloques que ilustra un dispositivo informático servidor, de acuerdo con algunas implementaciones.

20 Las figuras 5A-5C son diagramas de flujo que ilustran un método para proporcionar acceso a información personal (PII) de un usuario, de acuerdo con algunas implementaciones.

Descripción detallada

25 Se dirige ahora la atención a las figuras, y en particular a la Figura 1A, que es un diagrama de bloques de un entorno cliente-servidor 100, según algunas implementaciones, en el que los permisos de uso compartido específicos del contexto son facilitados por un servidor central. El entorno cliente-servidor 100 incluye dispositivos cliente 102-1 ... 102-n, un servidor central 104 y los dispositivos solicitantes 108-1 ... 108-n, todos conectados a través de una red 110. La red 110 incluye cualquiera de una variedad de redes, incluidas las redes de área amplia (WAN), redes de área local (LAN), redes de área personal, redes de área metropolitana, VPN, conexiones locales peer-to-peer, conexiones ad-hoc, redes inalámbricas, redes cableadas, Internet o una combinación de dichas redes.

30 En algunas implementaciones, el dispositivo cliente 102-1 está asociado con un individuo. En algunas implementaciones, el dispositivo cliente 102-1 incluye una aplicación cliente 112 que facilita la transmisión de PII a otros dispositivos, tales como el servidor central 104 y / o los dispositivos solicitantes 108-n. En algunas implementaciones, la aplicación cliente 112 también facilita la recepción de información (por ejemplo, anuncios dirigidos y / u otro contenido) de otros dispositivos, tales como el servidor central 104 y / o los dispositivos solicitantes 108-n. En algunas implementaciones, la PII transmitida desde el dispositivo cliente 102-1 a otros dispositivos incluye información resultante de interacciones directas con el dispositivo cliente 102-1 (por ejemplo, historial de navegación de Internet, perfiles de usuario, información de ubicación, información de uso de la aplicación, información operativa del dispositivo / registros, etc.). En algunas implementaciones, la PII transmitida desde el dispositivo cliente 102-1 a otro dispositivo incluye información recibida por el dispositivo cliente 102-1 desde otros dispositivos y / o periféricos, tales como dispositivos portátiles, monitores de frecuencia cardíaca, sensores de ocupación, dispositivos médicos / de salud. / sensores biométricos, dispositivos domésticos conectados, drones, vehículos autónomos, otros dispositivos informáticos, etc.

35 En algunas implementaciones, el dispositivo cliente 102-1 también facilita solicitar y recibir el consentimiento del usuario para compartir PII, incluido el intercambio de PII desde el dispositivo cliente 102-1 a otros dispositivos y / o entidades, y / o compartir PII entre otros terceros. Por ejemplo, a un usuario se le puede pedir, a través del dispositivo cliente 102-1, que apruebe o rechace una solicitud para que un tercero comparta la PII de ese usuario con otro tercero.

40 En algunas implementaciones, el dispositivo cliente 102-1 también mantiene o facilita el mantenimiento de un perfil de contexto "activo" de un usuario. Un perfil de contexto activo, discutido en este documento, se relaciona con uno o más aspectos del entorno actual del usuario, la actividad actual y / o los intereses actuales. Los perfiles de contexto incluyen, por ejemplo, contextos como "viajes", "casa", "compras", "conducir", "no molestar", "fitness", "emergencia de salud", "trabajo", "social" y similares. En algunas implementaciones, el dispositivo cliente 102-1 determina automáticamente un perfil de contexto activo. Esta determinación puede basarse en uno o más de los siguientes factores y / o criterios: hora del día, uso del dispositivo o aplicación, historial de navegación, ubicación (por ejemplo, a partir de GPS o de otro modo), luz ambiental, temperatura ambiente, información biométrica (por ejemplo, de un sensor biométrico), dispositivos / accesorios conectados (por ejemplo, dispositivos portátiles o el sistema tecnológico de un automóvil) y similares. En algunas implementaciones, otros dispositivos, además, o en lugar, del dispositivo cliente 102-1, mantienen o facilitan el mantenimiento de un perfil de contexto activo. Por ejemplo, el servidor central 104 puede comunicarse con el dispositivo cliente 102-1 para mantener el perfil de contexto activo del usuario. Como otro

ejemplo, los dispositivos periféricos pueden proporcionar señales al dispositivo cliente 102-1 y / o al servidor central 104. Estas señales son indicativas del contexto de un usuario, o pueden usarse, solas o en combinación con otras señales, datos, entradas de calendario, etc., para inferir el contexto del usuario.

5 En algunas implementaciones, la aplicación cliente 112 cifra la PII antes de enviarla al servidor central 104 y / o los dispositivos solicitantes 108-n. El dispositivo cliente 102-1 y la aplicación cliente 112, y las funciones y métodos que realizan, se describen en este documento. Cualquier descripción o descripciones del dispositivo cliente 102-1, o de las funciones o métodos realizados por el dispositivo cliente 102-1, se aplica igualmente a cualquiera o todas las instancias de los dispositivos cliente 102-n. Los dispositivos cliente ejemplares incluyen una computadora de escritorio,
10 una computadora portátil, una tableta, un dispositivo electrónico móvil (por ejemplo, un "reloj inteligente", un dispositivo electrónico portable, un rastreador de fitness / salud, etc.), un dispositivo electrónico interno (por ejemplo, un dispositivo de seguridad, de monitoreo o médico), un teléfono móvil (por ejemplo, un "teléfono inteligente"), un reproductor de medios digitales o cualquier otro dispositivo electrónico apropiado.

15 En algunas implementaciones, el dispositivo solicitante 108-1 está asociado con una entidad que recibe, almacena, usa o accede de otro modo a la PII de un individuo. Por ejemplo, un dispositivo solicitante 108-1 puede estar asociado con una entidad o entidades que usan PII por una o más de las siguientes razones: publicidad dirigida (u otro contenido) a individuos particulares; compartir PII con otras entidades; agregar y / o almacenar PII.

20 En algunas implementaciones, el dispositivo solicitante 108-1 se comunica con uno o ambos del servidor central 104 y el dispositivo cliente 102-1. El dispositivo solicitante 108-1 y las funciones y métodos que realiza se describen en este documento. Cualquier descripción o descripciones del dispositivo solicitante 108-1, o de las funciones o métodos realizados por el dispositivo solicitante 108-1, se aplica igualmente a cualquiera o todas las instancias de los dispositivos solicitantes 108-n. Los dispositivos de solicitud ejemplares incluyen una computadora de escritorio, una computadora portátil, una tableta, un dispositivo electrónico móvil, una computadora servidor (o sistema informático servidor), un teléfono móvil, un reproductor de medios digitales o cualquier otro dispositivo electrónico apropiado (o un quiosco que albergue cualquiera de los dispositivos antes mencionados). Los dispositivos ejemplares también pueden incluir vehículos que contienen tales dispositivos, incluidos automóviles, aviones, trenes y similares, o espacios de ocupación que contienen tales dispositivos, incluidos edificios, áreas comunes, espacios abiertos, entornos naturales
30 y similares.

En algunas implementaciones, el servidor central 104 está asociado con un proveedor de servicios que puede comunicarse, a través de la red 110 y / u otros medios de comunicación, con múltiples dispositivos cliente (por ejemplo, 102-n) y múltiples dispositivos solicitantes (por ejemplo, 108-n) para proporcionar y / o facilitar concesión de permisos para compartir PII entre entidades (incluyendo entre individuos y entidades de terceros, y entre dos o más entidades de terceros). En algunas implementaciones, el servidor central 104 incluye y / o se comunica con una base de datos de permisos 106. Como se describe en el presente documento, la base de datos de permisos 106 almacena información de permisos asociada con los usuarios, incluyendo, sin limitarse a, permisos concedidos previamente a entidades solicitantes para acceder, usar o compartir PII; los perfiles de contexto bajo los cuales las entidades solicitantes pueden compartir, acceder o utilizar la PII (o ciertos tipos de PII); etc. Como ejemplo específico, la base de datos de permisos 106 almacena información que indica que la información de frecuencia cardíaca de un usuario en particular puede ser compartida con un primer subconjunto de terceros cuando el perfil de contexto activo del usuario es "fitness", con un segundo conjunto de terceros cuando el perfil de contexto activo del usuario es "emergencia de salud" y a ningún tercero cuando el perfil de contexto activo del usuario es cualquier otro.

45 La figura 1B es otro diagrama de bloques del entorno cliente-servidor 100, según algunas implementaciones, que muestra comunicaciones ejemplares entre un entorno cliente 114 y un dispositivo solicitante 108-1 para aprovisionar y compartir PII.

50 La figura 1B incluye un entorno de cliente 114. El entorno de cliente 114 incluye un dispositivo cliente 102-1 en comunicación con el servidor central 104, así como cero o más dispositivos adicionales en comunicación con el servidor central 104 y / o el dispositivo cliente 102-1. Las líneas de puntos en la Figura 1B representan comunicaciones cuya transmisión o recepción puede depender de la aprobación o el permiso otorgado por la puerta de enlace de PII basada en perfiles 116. (Otras comunicaciones en la Figura 1B también pueden depender de dicha aprobación o permiso por parte de la puerta de enlace de PII basada en perfiles 116 o cualquier otro componente del entorno cliente-servidor 100, incluidos otros dispositivos / componentes no mostrados.)

En algunas implementaciones, cero o más de los dispositivos electrónicos en el entorno del cliente 114 también eluden (o son capaces de eludir) el servidor central 104 para comunicarse directamente con un dispositivo solicitante 108-1. Los dispositivos electrónicos que se comunican directamente con el servidor central 104 y / o el dispositivo solicitante 108-1 se consideran en sí mismos dispositivos cliente 102. Los dispositivos electrónicos que se comunican única o principalmente con el servidor central 104 y / o el dispositivo solicitante 108-1 a través de un dispositivo cliente separado 102-1 se consideran dispositivos periféricos. Como ejemplo, un podómetro que se comunica con un
60

dispositivo cliente 102-1 a través de BLUETOOTH u otra tecnología de comunicación de corto alcance es un ejemplo de un dispositivo periférico.

En algunas implementaciones, los dispositivos adicionales incluyen dispositivos de posicionamiento global (GPS) (por ejemplo, vehículos o dispositivos de navegación personal), drones, etiquetas RFID, iBeacons, monitores de frecuencia cardíaca, computadoras personales, sensores de salud / médicos / biométricos (por ejemplo, monitores de presión arterial, sensores de respuesta galvánica de la piel, sensores de temperatura corporal, etc.), sensores de ocupación o similares; de manera efectiva, cualquier dispositivo que puede o pueda ser capaz de recopilar información que pueda usarse individualmente o como parte de un conjunto de información que constituye PII.

La Figura 1B ilustra un proceso ejemplar mediante el cual un dispositivo solicitante solicita acceder o utilizar la PII de un individuo en particular enviando una solicitud a un servidor central. El dispositivo solicitante puede iniciar una solicitud en respuesta a una entrada del usuario, o automáticamente (por ejemplo, en respuesta a una detección automática de una condición). El servidor central facilita el proceso de solicitar y recibir permisos, restricciones y / o autorizaciones del individuo y de proporcionar la PII solicitada (o autorizar el uso de la PII) por parte del dispositivo solicitante.

Más específicamente, el dispositivo solicitante 108-1 envía una solicitud de acceso / uso de PII ("solicitud") al servidor central 104. En algunas implementaciones, la solicitud especifica uno o más de: la PII particular que se solicita (por ejemplo, el historial de navegación de Internet del usuario, la frecuencia cardíaca del usuario, etc.), para qué se puede usar la información, cuándo se puede usar la información, si (y con quién) se puede compartir la información, y similares. En algunas implementaciones, la solicitud va acompañada de un identificador de un individuo en particular. Por ejemplo, la entidad asociada con el servidor central 104 (es decir, la empresa o entidad que controla, opera o es responsable de otro modo del servidor central 104 o de los servicios proporcionados por el mismo) proporciona a los clientes individuales un identificador único. Los individuos pueden compartir este identificador con terceros, quienes luego pueden solicitar información, desde el servidor central 104, sobre el individuo asociado. Al enrutar las solicitudes de permisos de PII de múltiples terceros a través del servidor central 104, el control sobre dichas solicitudes está centralizado y estandarizado, lo que permite a los usuarios un único y simple punto de contacto para controlar quién tiene acceso a su PII, así como para qué se puede usar y cuándo se puede usar y / o recibir.

En respuesta a la recepción de una solicitud de un dispositivo solicitante 108-1, el servidor central 104 procesa la solicitud y envía una solicitud correspondiente (o reenvía la solicitud desde el dispositivo solicitante 108-1) a un dispositivo asociado con el individuo identificado en la solicitud.

El individuo recibe la solicitud del servidor central. Como se señaló anteriormente, la solicitud incluye información sobre la entidad solicitante, así como información sobre la PII en particular que se solicita y cómo, cuándo y con qué propósito se utilizará la PII. En algunas implementaciones, el usuario recibe una alerta de manera proactiva sobre la solicitud, como con un mensaje emergente en una pantalla, una alerta audible, un icono de notificación o similares. En algunas implementaciones, la solicitud se coloca en una bandeja de entrada o una cola de solicitudes que el usuario revisa en cualquier momento conveniente.

En algunas implementaciones, en lugar de enviar una solicitud al usuario, la solicitud se valida contra un conjunto de reglas establecidas por el usuario (ya sea en su dispositivo o en la puerta de enlace), y luego se valida aún más contra su contexto activo. Por tanto, las respuestas se gestionan automáticamente en función de las reglas preestablecidas y el contexto activo del usuario.

Uno o más dispositivos asociados con el entorno de cliente 114 (por ejemplo, el dispositivo de cliente 102-1) envía permisos de PII de vuelta al servidor central 104. En algunas implementaciones, los permisos devueltos incluyen la aprobación o denegación de la solicitud (en su totalidad o en parte, como se describe en este documento), así como las asignaciones de perfiles de contexto particulares para los que se otorgan los permisos. Por ejemplo, un dispositivo solicitante 108-1 puede enviar una solicitud para recibir continuamente la información de frecuencia cardíaca del usuario con el propósito de monitorear y rastrear los niveles de esfuerzo de frecuencia cardíaca y la condición física general del usuario. En respuesta, el usuario puede autorizar al solicitante a recibir y usar la información solo cuando el perfil de contexto de "fitness" del usuario está activo, y restringir el acceso y / o uso de la información de frecuencia cardíaca cuando cualquier otro perfil de contexto está activo. El servidor central 104 almacena los permisos recibidos de individuos en la base de datos de permisos 106.

En algunas implementaciones, si el individuo aprueba la solicitud de PII (y, opcionalmente, se satisfacen una o más condiciones), la PII solicitada se envía al dispositivo solicitante 108-1, ya sea directamente o a través del servidor central 104.

En algunas implementaciones, el servidor central 104 incluye una puerta de enlace de PII basada en perfiles 116 que limita el acceso a y / o el uso de datos de PII en base al perfil de contexto activo del usuario y los permisos almacenados

otorgados a las entidades solicitantes. Por ejemplo, cada vez que una entidad solicitante desea acceder y / o utilizar la PII de un usuario en particular, debe confirmar con el servidor central 104 si está autorizada para hacerlo en ese momento. En respuesta a recibir tal solicitud, la puerta de enlace de PII basada en perfiles 116 determina el perfil de contexto activo del usuario, y luego determina si el usuario ha permitido que la PII solicitada sea compartida con la entidad solicitante cuando ese perfil de contexto particular está activo. Además, en algunas implementaciones, un usuario puede optar por iniciar el proceso de compartir PII, para facilitar una transacción, por ejemplo (o para cualquier propósito). En tal caso, el usuario selecciona un contexto e inicia el intercambio de información saliente (incluida la PII seleccionada) con una entidad, sujeto a las reglas y / o restricciones impuestas por el servidor central 104, la puerta de enlace de PII basada en perfiles 116 y / o cualquier regla o restricción asociada con los perfiles de contexto del usuario.

Como ejemplo específico, si una entidad solicita información de frecuencia cardíaca de un usuario en particular, la puerta de enlace de PII basada en perfiles 116 determina que el perfil de contexto activo del usuario es "fitness" y además determina que el usuario ha autorizado que la información de frecuencia cardíaca se comparta con la entidad solicitante cuando el perfil de contexto de "fitness" está activo. Por lo tanto, la puerta de enlace de PII basada en perfiles 116 bien (i) enviará la información de frecuencia cardíaca al solicitante, (ii) informará al dispositivo cliente 102-1 para enviar la información de frecuencia cardíaca al solicitante, y / o (iii) informará el solicitante que se le permite solicitar la información de frecuencia cardíaca del dispositivo cliente 102-1.

Si bien la Figura 1B muestra la PII siendo enviada directamente desde el entorno del cliente 114 a un dispositivo solicitante 108-1, en algunas implementaciones, esta comunicación todavía está gobernada por la puerta de enlace de PII basada en perfiles 116. Por ejemplo, la PII solo se enviará al dispositivo solicitante 108-1 una vez que uno o ambos del dispositivo solicitante 108-1 y el dispositivo cliente 102-1 hayan recibido la confirmación de la puerta de enlace de PII basada en perfiles 116 de que la comunicación está autorizada.

La puerta de enlace de PII basada en perfiles 116 también controla si se permite que un dispositivo solicitante 108-1 se ponga en contacto con un individuo con anuncios, ofertas u otras comunicaciones. En algunas implementaciones, el dispositivo solicitante 108-1 envía un anuncio, oferta u otra comunicación al servidor central 104, y la puerta de enlace de PII basada en perfiles 116 determina si los permisos del individuo permiten que esa parte en particular envíe comunicaciones al individuo basándose en el perfil de contexto activo. Si es así, la comunicación se reenvía al dispositivo cliente 102-1. En caso contrario, no se reenvía al dispositivo cliente 102-1 (aunque podría almacenarse para su recuperación y revisión en una etapa posterior por parte del usuario una vez que se active un perfil de contexto apropiado). Alternativamente, en lugar de enviar la comunicación al servidor central 104, el dispositivo solicitante 108-1 puede solicitar aprobación para enviar información al dispositivo cliente, y la puerta de enlace de PII basada en perfiles 116 responde con una aprobación o una denegación, y el dispositivo solicitante 108-1 reacciona en consecuencia enviando o no enviando la comunicación según corresponda.

La puerta de enlace de PII basada en perfiles 116 permite a los usuarios establecer permisos relacionados con su PII y los terceros que pueden acceder a su PII para que compartan y reciban información de una manera que sea relevante para su contexto actual. Por ejemplo, permitir que se comparta información sobre la talla de la ropa en momentos en que el usuario se encuentra en un perfil de "compra" ayuda a garantizar que el usuario no sea abordado con ofertas, anuncios u otras comunicaciones relacionadas con la compra de ropa cuando el usuario se encuentre en un perfil de contexto diferente, como "trabajo" o "vacaciones". También ayuda a proporcionar al usuario ofertas, anuncios u otras comunicaciones que son particularmente relevantes y oportunas para su perfil de contexto activo. Así, cuando el usuario está en un perfil de "compras", será más probable que reciba contenido relacionado con la ropa que con eventos deportivos cercanos o restaurantes cercanos a su lugar de trabajo, por ejemplo.

Sin embargo, la imposición de un conjunto limitado de permisos puede afectar negativamente la exposición de un usuario a información deseable. Por ejemplo, limitar a los terceros que pueden recibir PII o contactar a un usuario con ofertas, anuncios u otras comunicaciones (o cuando se les permite hacerlo) puede evitar que el usuario conozca un producto o servicio en el que podría estar interesado. En consecuencia, en algunas implementaciones, los usuarios pueden aumentar los permisos otorgados a uno o más terceros, de modo que los terceros puedan acceder a PII adicional y / o los terceros puedan comunicarse con el usuario de formas adicionales o en contextos adicionales. Además, el servidor central 104 permite a los usuarios cambiar los permisos de múltiples terceros a la vez, permitiéndoles el beneficio de una mayor exposición a contenido deseable sin que tengan que cambiar individualmente los permisos para cada tercero. En cambio, el usuario puede ingresar en un "modo de descubrimiento" donde se otorgan permisos adicionales a terceros nuevos y / o diferentes. A partir de entonces, el usuario puede, con una sola solicitud, salir del modo de descubrimiento y devolver a cada tercero a los permisos previamente aplicables.

El modo de descubrimiento afecta a cualquiera de los múltiples permisos posibles. En algunas implementaciones, el modo de descubrimiento permite la creación de una Política de Privacidad Provisional (IPP, Interim Privacy Policy) con terceros adicionales, otorgándoles los derechos y recibir y acceder a la PII de un usuario, o permitiendo que terceros adicionales se comuniquen con un usuario. Por ejemplo, los permisos de un usuario solo pueden permitir que

algunos terceros específicos accedan a la PII o envíen anuncios u ofertas al usuario. Sin embargo, cuando el modo de descubrimiento está activo, se otorgan permisos a terceros adicionales para acceder a la PII del usuario o enviar comunicaciones al usuario. En otro ejemplo, un usuario podría estar comprando un seguro de vida y en su modo normal solo estaría compartiendo su PII relevante (por ejemplo, altura, edad, peso, historial de salud, datos de frecuencia cardíaca, datos de condición física, química sanguínea, etc.) con entidades ya aprobadas por ellos para recibir dicha información. Al ingresar al modo de descubrimiento, el usuario puede autorizar y compartir esta información con un amplio conjunto de competidores que ofrecen productos de seguros de vida, de modo que cada uno tenga la misma información de PII y, por lo tanto, el usuario pueda recibir un amplio conjunto de cotizaciones personalizadas competitivas y precisas. El permiso de estos datos de PII por parte del usuario mientras está en modo de descubrimiento crea un IPP y, por lo tanto, permite que los otros proveedores tengan legalmente los derechos para usar la PII de los usuarios para ayudarlos a ofertar por el negocio. Una vez que se cierra el modo de descubrimiento, el IPP finaliza y cesa el permiso relacionado.

En algunas implementaciones, el modo de descubrimiento permite a terceros acceder a información de PII adicional a la que de otro modo no se les permitiría acceder. Por ejemplo, en los modos de funcionamiento normales, a un minorista se le puede permitir acceder a las tallas de ropa de un usuario, mientras que, en el modo de descubrimiento, a ese mismo minorista (y / o minoristas adicionales) también se le puede permitir acceder al historial de navegación de un usuario, la ubicación y similares.

En algunas implementaciones, el modo de descubrimiento permite que terceros se comuniquen con el usuario a través de opciones de comunicación adicionales. Por ejemplo, en los modos de funcionamiento normales, a un tercero solo se le puede permitir enviar correos electrónicos al usuario, mientras que, en el modo de descubrimiento, a ese mismo tercero (y / o terceros adicionales) también se le puede permitir contactar al usuario con mensajes de texto, anuncios emergentes, anuncios en banners, pantallas en dispositivos portables, etc. Como otro ejemplo, en los modos de funcionamiento normales, a un tercero solo se le puede permitir enviar comunicaciones a la computadora de escritorio de un usuario, mientras que, en el modo de descubrimiento, a ese mismo tercero (y / o terceros adicionales) también se le puede permitir contactar al usuario en cualquier dispositivo electrónico asociado (por ejemplo, televisión, teléfono inteligente, dispositivo portátil, sistema de "información y entretenimiento" del vehículo, etc.

Por supuesto, no es necesario que el modo de descubrimiento otorgue permisos ilimitados a todos los terceros. Más bien, en algunas implementaciones, un usuario puede seleccionar cómo el modo de descubrimiento afecta los permisos otorgados a terceros. Por ejemplo, un usuario puede configurar el modo de descubrimiento de modo que se otorguen permisos a todos y cada uno de los terceros para acceder a la PII del usuario y / o enviar comunicaciones al usuario, y para cualquier área temática. Otro usuario, por el contrario, puede configurar el modo de descubrimiento de modo que solo un pequeño número de terceros adicionales puedan acceder a la PII del usuario y / o enviar comunicaciones al usuario. En consecuencia, en algunas implementaciones, el comportamiento del modo de descubrimiento es específico y configurable por el usuario.

En algunas implementaciones, modos adicionales, además del modo de descubrimiento, otorgan permisos adicionales y / o diferentes a terceros cuando están activos. Por ejemplo, en algunas implementaciones, un modo de emergencia permite que cualquier PII que pueda ser útil para rescatar a un usuario se envíe a los servicios de emergencia, profesionales de la salud, miembros de la familia y / o similares (o se otorga acceso a PII a las anteriores entidades). Dicha PII puede incluir, sin limitación, ubicación actual, medicamentos actuales, condiciones de salud preexistentes, registros médicos y cualquier información biométrica apropiada como frecuencia cardíaca, presión arterial, niveles de azúcar en sangre, respuesta galvánica de la piel, temperatura corporal, etc. Por lo tanto, al igual que el modo de descubrimiento, el modo de emergencia cambia y / o anula los permisos que de otro modo están activos como resultado de que un perfil de contexto particular esté activo. Así, por ejemplo, si el perfil de contexto activo de un usuario tiene muy pocos permisos (correspondientes a un modo de "no molestar" o "tiempo en familia"), el modo de emergencia ampliará los permisos para permitir que se brinden servicios beneficiosos al usuario.

En algunas implementaciones, se ingresa en el modo de emergencia automáticamente al detectar una determinada condición. Por ejemplo, se puede ingresar en el modo de emergencia al detectar que un usuario ha estado en un accidente automovilístico (por ejemplo, según la información del acelerómetro de un teléfono inteligente, sensores de colisión en un vehículo, etc.), o al detectar que el usuario está sufriendo una emergencia de salud (por ejemplo, basado en frecuencia cardíaca, azúcar en sangre u otra información biométrica), o similar.

En algunas implementaciones, además, o en lugar de, la selección automática, un usuario ingresa manualmente al modo de emergencia. Por ejemplo, un usuario puede seleccionar el modo de emergencia en cualquier momento apropiado, como después de sufrir una lesión.

La figura 2 es un diagrama de bloques que ilustra un dispositivo cliente 102-1, de acuerdo con algunas implementaciones. Si bien la Figura 2 ilustra una instancia de un dispositivo cliente (es decir, el dispositivo cliente 102-

1), la figura y la descripción asociada se aplican igualmente a cualquier dispositivo cliente (por ejemplo, 102-1 - 102-n).

En algunas implementaciones, el dispositivo cliente 102-1 es cualquiera de: una computadora de escritorio, una computadora portátil, una tableta, un dispositivo electrónico móvil (por ejemplo, un "reloj inteligente", un dispositivo electrónico portable, un rastreador de fitness / salud, etc.), un teléfono móvil (por ejemplo, un "teléfono inteligente"), un reproductor de medios digitales o cualquier otro dispositivo electrónico apropiado.

El dispositivo cliente 102-1 incluye típicamente una o más unidades centrales de proceso (CPU) 204, una interfaz de usuario 206, al menos una interfaz de comunicaciones de red 212 (cableada y / o inalámbrica), un dispositivo de captura de imágenes 214, un sistema de posicionamiento 216, un dispositivo de captura biométrica 217, memoria 218 y al menos un bus de comunicación 202 para interconectar estos componentes. Cada bus de comunicación 202 puede incluir circuitos (a veces denominados chipset) que interconectan y controlan las comunicaciones entre los componentes del sistema. En algunas implementaciones, la interfaz de usuario 206 incluye una pantalla 208 y dispositivo(s) de entrada 210 (por ejemplo, teclado, ratón, pantalla táctil, teclados numéricos, etc.).

El dispositivo de captura de imágenes 214 es cualquier dispositivo que sea capaz de capturar una imagen de una escena u objeto del mundo real. En algunas implementaciones, el dispositivo de captura de imágenes 214 es una cámara digital (que incluye cualquier lente o lentes, sensores y otros componentes apropiados). En algunas implementaciones, podría ser un dispositivo de captura de imágenes remoto (por ejemplo, en un dron o un dispositivo portable).

El sistema de posicionamiento 216 incluye dispositivos y / o componentes para determinar la ubicación del dispositivo cliente 102-1, incluidos, entre otros, sensores del sistema de posicionamiento global (GPS), receptores de radio (por ejemplo, para triangulación de torres de telefonía móvil, posicionamiento basado en WiFi, etc.), sensores inerciales y acelerómetros. En algunas implementaciones, el dispositivo cliente 102-1 no incluye (o no se basa en) un sistema de posicionamiento 216 separado. Por ejemplo, cuando el dispositivo cliente 102-1 está conectado a Internet (por ejemplo, a través de la interfaz de comunicaciones de red 212), la ubicación del dispositivo cliente 102-1 se puede determinar usando técnicas de geolocalización de direcciones IP. También se contemplan otras técnicas para determinar la ubicación del dispositivo cliente, incluidas las que se basan en un sistema de posicionamiento incorporado o conectado y las que no. En algunas implementaciones, la ubicación puede estar definida por la red a la que se está conectando (por ejemplo, en un avión, tren o edificio) u otra información de sensor que pueda identificar la ubicación.

El dispositivo de captura biométrica 217 incluye dispositivos y / o componentes para capturar datos biométricos de una persona. En algunas implementaciones, el dispositivo de captura biométrica 217 es un escáner de huellas dactilares. En algunas implementaciones, es un escáner de retina. En algunas implementaciones, es un escáner facial. En algunas implementaciones es un escáner de reconocimiento de voz. En algunas implementaciones, el dispositivo de captura biométrica 217 es un dispositivo de captura de múltiples propósitos que puede capturar múltiples tipos de datos biométricos de un usuario (por ejemplo, huellas de manos, huellas dactilares, imágenes faciales, etc.). En algunas implementaciones, los dispositivos de captura biométrica 217 incluyen cualquiera de un monitor de frecuencia cardíaca, un monitor de respuesta galvánica de la piel, un monitor de azúcar en sangre, un monitor de alcohol en sangre, un monitor de oxígeno en sangre o cualquier otro monitor / sensor biométrico que pueda ser externo o interno. En algunas implementaciones, el dispositivo de captura biométrica 217 es un dispositivo periférico (es decir, no está en la misma carcasa que otros componentes del dispositivo cliente 102-1) y se comunica con el dispositivo cliente 102-1 a través de uno o más enlaces de comunicación, incluyendo, por ejemplo, BLUETOOTH, WiFi o cualquier otro enlace o enlaces de comunicación por cable o inalámbricos apropiados.

La memoria 218 incluye memoria de acceso aleatorio de alta velocidad, como DRAM, SRAM, DDR RAM u otros dispositivos de memoria de estado sólido de acceso aleatorio, y puede incluir memoria no volátil, como uno o más dispositivos de almacenamiento de disco magnético, dispositivos de almacenamiento de disco óptico, dispositivos de memoria flash u otros dispositivos de almacenamiento de estado sólido no volátil. La memoria 218 puede incluir opcionalmente uno o más dispositivos de almacenamiento ubicados remotamente desde la o las CPU 204 (por ejemplo, un dispositivo o servicio de almacenamiento conectado a la red, tal como un servicio de almacenamiento basado en "nube"). La memoria 218, o alternativamente el o los dispositivos de memoria no volátil dentro de la memoria 218, incluye un medio de almacenamiento no transitorio legible por ordenador. En algunas implementaciones, la memoria 218 o el medio de almacenamiento legible por ordenador de la memoria 218 almacena los siguientes programas, módulos y estructuras de datos, o un subconjunto de los mismos:

un sistema operativo 220 que incluye procedimientos para manejar varios servicios básicos del sistema y para realizar tareas dependientes del hardware;

un módulo de comunicación 222 que se utiliza para conectar el dispositivo cliente 102-1 a otras computadoras a través de una o más interfaces de comunicación de red 212 (cableadas o inalámbricas) y una o más redes de comunicación, como Internet, otras redes de área amplia, redes de área local, redes de área personal, redes de área metropolitana, VPN, conexiones locales peer-to-peer y / o ad-hoc, etc.

un módulo de interfaz de usuario 224 que recibe comandos y / o entradas de un usuario a través de la interfaz de usuario 206 (por ejemplo, desde el o los dispositivos de entrada 210, que puede incluir teclado(s), pantalla(s) táctil(es), micrófono(s), dispositivo(s) de puntero y similares), y proporciona objetos de interfaz de usuario en una pantalla (por ejemplo, la pantalla 208);

un módulo de dispositivo de captura de imágenes 226 (que incluye, por ejemplo, aplicaciones, controladores, etc.) que funciona junto con el dispositivo de captura de imágenes 214 para capturar imágenes, tales como imágenes o escaneos de documentos físicos, rostros, escenas del mundo real, etc.;

un módulo de dispositivo de captura biométrica 227 que funciona junto con el dispositivo de captura biométrica 217 (y / o el dispositivo de captura de imágenes 214) para capturar datos biométricos de un usuario, incluyendo datos relacionados con cualquier característica física o biológica apropiada de un usuario;

un módulo de sistema de posicionamiento 228 que, junto con el sistema de posicionamiento 216, determina una ubicación actual (por ejemplo, latitud y longitud, dirección de calle, ciudad, estado, municipio, etc.) del dispositivo cliente 102-1; y

uno o más módulos de aplicación cliente 230 para permitir que el dispositivo cliente 102-1 realice los métodos y / o técnicas descritos en este documento, donde los módulos de aplicación cliente 230 incluyen, pero no están limitados a:

un módulo de gestión de permisos de PII 231 para recibir preferencias de usuario relacionadas con permisos de PII, incluido qué terceros pueden recibir / acceder a PII, qué PII pueden ser recibidas / accedidas por terceros, cuándo pueden ser recibidas / accedidas PII por terceros, cómo terceros pueden contactar al usuario, qué terceros pueden contactar al usuario, cuándo pueden terceros contactar al usuario, etc., y para asignar permisos a uno o más perfiles de contexto;

un módulo de selección de perfil de contexto 232 para recibir selecciones de usuario de un perfil de contexto activo y para detectar disparadores para seleccionar automáticamente un perfil de contexto activo.

En algunas implementaciones, el dispositivo cliente 102-1 incluye un subconjunto de los componentes y módulos que se muestran en la Figura 2. Además, en algunas implementaciones, el dispositivo cliente 102-1 incluye componentes y / o módulos adicionales que no se muestran en la Figura 2.

La figura 3 es un diagrama de bloques que ilustra un dispositivo solicitante 108-1, de acuerdo con algunas implementaciones. Si bien la Figura 3 ilustra una instancia de un dispositivo solicitante (es decir, el dispositivo solicitante 108-1), la figura y la descripción asociada se aplican igualmente a cualquier dispositivo solicitante (por ejemplo, 108-1 - 108-n).

En algunas implementaciones, el dispositivo solicitante 108-1 es cualquiera de: una computadora de escritorio, una computadora portátil, una tableta, una computadora servidor (o sistema servidor), un dispositivo electrónico móvil, un teléfono móvil, un vehículo, un reproductor de medios digitales, o cualquier otro dispositivo electrónico apropiado (o un quiosco que contenga cualquiera de los dispositivos antes mencionados).

El dispositivo solicitante 108-1 incluye típicamente una o más CPU 304, una interfaz de usuario 306, al menos una interfaz de comunicaciones de red 312 (cableada y / o inalámbrica), un dispositivo de captura de imágenes 314, memoria 318 y al menos un bus de comunicación 302 para interconectar estos componentes. Cada bus de comunicación 302 puede incluir circuitos (a veces denominados chipset) que interconectan y controlan las comunicaciones entre los componentes del sistema. En algunas implementaciones, la interfaz de usuario 306 incluye una pantalla 308 y dispositivo(s) de entrada 310 (por ejemplo, teclado, ratón, pantalla táctil, teclados numéricos, etc.).

El dispositivo de captura de imágenes 314 es cualquier dispositivo que sea capaz de capturar una imagen de una escena u objeto del mundo real. En algunas implementaciones, el dispositivo de captura de imágenes 314 es una cámara digital (que incluye lentes, sensores u otros componentes apropiados). En algunas implementaciones, el dispositivo de captura de imágenes es un escáner (por ejemplo, un escáner de superficie plana). En algunas implementaciones, el dispositivo de captura de imágenes 314 se incorpora en una carcasa común con el dispositivo solicitante 108-1, o en un dispositivo externo o conectado capaz de efectuar la captura de imágenes para el usuario (por ejemplo, un dron, etc.).

La memoria 318 incluye memoria de acceso aleatorio de alta velocidad, como DRAM, SRAM, DDR RAM u otros dispositivos de memoria de estado sólido de acceso aleatorio, y puede incluir memoria no volátil, como uno o más dispositivos de almacenamiento de disco magnético, dispositivos de almacenamiento de disco óptico, dispositivos de memoria flash u otros dispositivos de almacenamiento de estado sólido no volátil. La memoria 318 puede incluir opcionalmente uno o más dispositivos de almacenamiento ubicados remotamente desde la(s) CPU(s) 304. La memoria 318, o alternativamente el o los dispositivos de memoria no volátil dentro de la memoria 318, incluye un medio de almacenamiento no transitorio legible por ordenador. En algunas implementaciones, la memoria 318 o el medio de almacenamiento legible por ordenador de la memoria 318 almacena los siguientes programas, módulos y estructuras de datos, o un subconjunto de los mismos:

un sistema operativo 320 que incluye procedimientos para manejar varios servicios básicos del sistema y para realizar tareas dependientes del hardware;

un módulo de comunicación 322 que se utiliza para conectar el dispositivo solicitante 108-1 a otras computadoras a través de una o más interfaces de red 312 (cableadas o inalámbricas) y una o más redes de comunicación, como Internet, otras redes de área amplia, redes de área local, redes de área personal, redes de área metropolitana, VPN, conexiones locales peer-to-peer y / o ad-hoc, etc.

un módulo de interfaz de usuario 324 que recibe comandos y / o entradas de un usuario a través de la interfaz de usuario 306 (por ejemplo, desde el dispositivo de entrada 310, que puede incluir teclado(s), pantalla(s) táctil(es), micrófono(s), dispositivo(s) de puntero y similares), y proporciona objetos de interfaz de usuario en una pantalla (por ejemplo, la pantalla 308);

un módulo de dispositivo de captura de imágenes 326 (que incluye, por ejemplo, aplicaciones, controladores, etc.) que funciona junto con el dispositivo de captura de imágenes 314 para capturar imágenes, como imágenes o escaneos de documentos físicos, rostros, escenas del mundo real, etc.

uno o más módulos de aplicación 328 para permitir que el dispositivo solicitante 108-1 realice los métodos y / o técnicas descritos en este documento, donde el o los módulos de aplicación 328 incluyen, pero no se limitan a:

un módulo de solicitud de permisos de PII 330 para solicitar permisos de PII de uno o más dispositivos cliente y / o servidores centrales; y

una base de datos de permisos de PII 332 para almacenar y administrar permisos de PII previamente otorgados;

una base de datos de PII 334 para almacenar PII, si está autorizado para hacerlo, sujeto a todos y cada uno de los permisos relacionados con PII; y

una base de datos de anuncios / comunicaciones 336 para almacenar anuncios y / u otras comunicaciones (por ejemplo, contenido para correo electrónico, correo físico, mensajes de texto / SMS / MMS, mensajes emergentes, etc.) que se pueden enviar a los dispositivos del cliente.

En algunas implementaciones, el dispositivo solicitante 108-1 incluye un subconjunto de los componentes y módulos que se muestran en la Figura 3. Además, en algunas implementaciones, el dispositivo solicitante 108-1 incluye componentes y / o módulos adicionales que no se muestran en la Figura 3.

La figura 4 es un diagrama de bloques que ilustra un servidor central 104, de acuerdo con algunas implementaciones. En algunas implementaciones, el servidor central 104 es cualquiera de: una computadora de escritorio, una computadora portátil, una tableta, una computadora servidor (o sistema servidor), un dispositivo electrónico móvil, un teléfono móvil, un reproductor de medios digitales o cualquier otro dispositivo electrónico apropiado (o un quiosco que albergue cualquiera de los dispositivos antes mencionados).

El servidor central 104 incluye típicamente una o más CPU 404, una interfaz de usuario 406, al menos una interfaz de comunicaciones de red 412 (cableada y / o inalámbrica), memoria 414 y al menos un bus de comunicaciones 402 para interconectar estos componentes. Cada bus de comunicación 402 puede incluir circuitos (a veces denominados chipset) que interconectan y controlan las comunicaciones entre los componentes del sistema. En algunas implementaciones, la interfaz de usuario 406 incluye una pantalla 408 y dispositivo(s) de entrada 410 (por ejemplo, teclado, ratón, pantalla táctil, teclados numéricos, etc.).

La memoria 414 incluye memoria de acceso aleatorio de alta velocidad, como DRAM, SRAM, DDR RAM u otros dispositivos de memoria de estado sólido de acceso aleatorio, y puede incluir memoria no volátil, como uno o más

dispositivos de almacenamiento de disco magnético, dispositivos de almacenamiento de disco óptico, dispositivos de memoria flash u otros dispositivos de almacenamiento de estado sólido no volátil. La memoria 414 puede incluir opcionalmente uno o más dispositivos de almacenamiento ubicados remotamente desde la o las CPU 404. La memoria 414, o alternativamente el o los dispositivos de memoria no volátil dentro de la memoria 414, incluye un medio de almacenamiento legible por ordenador no transitorio. En algunas implementaciones, la memoria 414 o el medio de almacenamiento legible por ordenador de la memoria 414 almacena los siguientes programas, módulos y estructuras de datos, o un subconjunto de los mismos:

un sistema operativo 416 que incluye procedimientos para manejar varios servicios básicos del sistema y para realizar tareas dependientes del hardware;

un módulo de comunicación 418 que se usa para conectar el servidor central 104 a otras computadoras a través de una o más interfaces de red 412 (cableadas o inalámbricas) y una o más redes de comunicación, tales como Internet, otras redes de área amplia, redes de área local, redes de área personal, redes de área metropolitana, VPN, conexiones locales peer-to-peer y / o ad-hoc, etc.

un módulo de interfaz de usuario 420 que recibe comandos y / o entradas de un usuario a través de la interfaz de usuario 406 (por ejemplo, desde el dispositivo de entrada 410, que puede incluir teclado(s), pantalla(s) táctil(es), micrófono(s), dispositivo(s) de puntero y similares), y proporciona objetos de interfaz de usuario en una pantalla (por ejemplo, la pantalla 408);

uno o más módulos de aplicación de servidor 422 para permitir que el servidor 104 realice los métodos y / o técnicas descritos en este documento, donde el módulo o módulos de aplicación de servidor 422, incluyen, pero no se limitan a:

una puerta de enlace de PII basada en perfiles 116 para recibir solicitudes de PII y / o comunicaciones dirigidas a dispositivos cliente de terceros, para recibir respuestas de dispositivos cliente y para reenviar comunicaciones de terceros a dispositivos cliente y viceversa, según el perfil de contexto activo del usuario y permisos asociados;

un módulo de recepción 426 para recibir información (por ejemplo, PII) de dispositivos remotos (por ejemplo, dispositivos cliente 102-n, dispositivos solicitantes 108-n), que incluye, pero no se limita a: documentos, calificaciones de verificación, datos extraídos de documentos, información de cuenta (por ejemplo, nombre, dirección, número de seguro social, contraseña, preguntas / respuestas de recuperación de cuenta, datos biométricos, credenciales de inicio de sesión, etc.), etc.;

un módulo de cifrado 428 opcional para cifrar la información del usuario (incluyendo, pero no limitado a, documentos, calificaciones de verificación, datos extraídos de documentos, información de cuenta o cualquier PII) para el almacenamiento seguro, si la información del usuario no estaba cifrada antes de que la recibiera el servidor 104;

un módulo de empaquetado / cifrado de información 432 para recopilar, empaquetar y cifrar la información del usuario (incluyendo, entre otros, documentos, calificaciones de verificación, datos extraídos de documentos, información de cuenta o cualquier PII) para ser enviados a, o accedidos de otro modo por, un solicitante (por ejemplo, un dispositivo solicitante 108-n), y para enviar la información al solicitante;

y una base de datos de permisos 106 que incluye información asociada con una pluralidad de usuarios;

una base de datos de anuncios / comunicaciones 434 para almacenar anuncios y / u otras comunicaciones (por ejemplo, contenido para correo electrónico, correo físico, mensajes de texto / SMS / MMS, mensajes emergentes, etc.) que se pueden enviar a los dispositivos del cliente.

La figura 4 ilustra además una parte de la base de datos de permisos de usuario 106 relacionada con una cuenta de usuario 436 para un usuario ejemplar "n". La cuenta de usuario 436 incluye, pero no se limita a:

información de la cuenta 438 asociada con el usuario (por ejemplo, nombre, dirección, número de seguro social, contraseña, preguntas / respuestas de recuperación de cuenta, datos biométricos, credenciales de inicio de sesión, etc.);

datos de permiso 440 asociados con un usuario, incluidos qué terceros pueden recibir / acceder a PII, qué PII pueden ser recibidas / accedidas por terceros, cuándo puede PII ser recibida / accedida por terceros, cómo pueden terceros contactar al usuario, qué terceros pueden contactar al usuario, cuando pueden terceros contactar al usuario, etc., y para asignar permisos a uno o más perfiles de contexto; y

perfiles de contexto 442 asociados con el usuario, que incluyen, por ejemplo, perfiles de contexto para trabajo, viajes, hogar, vacaciones, compras, conducción, fitness, navegación, no molestar y similares.

- 5 En algunas implementaciones, parte de, o toda, la información del usuario en la base de datos de permisos 106 está encriptada. Además, en algunas implementaciones, el proveedor de servicios no posee claves de descifrado para la información del usuario. Por consiguiente, el proveedor de servicios y / o el servidor central 104 no pueden descifrar, ver, leer o modificar la información del usuario.
- 10 En algunas implementaciones, el servidor central 104 incluye un subconjunto de los componentes y módulos que se muestran en la Figura 4. Además, en algunas implementaciones, el servidor central 104 incluye componentes y / o módulos adicionales que no se muestran en la Figura 4.
- 15 Las figuras 5A-5C son diagramas de flujo que ilustran un método 500 para proporcionar acceso a información personal (PII) de un usuario, de acuerdo con algunas implementaciones. Cada una de las operaciones mostradas en las Figuras 5A-5C puede corresponder a instrucciones almacenadas en una memoria de computadora o en un medio de almacenamiento legible por computadora. En algunas implementaciones, los pasos se realizan en un dispositivo electrónico con uno o más procesadores (o núcleos) y memoria que almacena uno o más programas para que los ejecuten uno o más procesadores (o núcleos). Por ejemplo, en algunas implementaciones, los pasos se realizan en cualquiera (o cualquier combinación) del dispositivo cliente 102-1, el servidor central 104 y el dispositivo solicitante 108-1. Además, los pasos individuales del método pueden distribuirse entre los múltiples dispositivos electrónicos de cualquier manera apropiada.
- 20
- 25 Cualquiera o todas las comunicaciones entre dispositivos descritas con respecto a las Figuras 5A-5C son, en algunas implementaciones, aseguradas y / o encriptadas usando cualquier técnica de seguridad y / o de encriptación apropiada, incluyendo, pero sin limitarse a, Hypertext Transport Protocol Secure (HTTPS), Secure Sockets Layer (SSL), Transport Layer Security (TLS), Secure Shell (SSH), Internet Protocol Security (IPSec), cifrado de clave pública y similares (incluido cualquier método de cifrado y / o seguridad apropiado aún por desarrollar).
- 30 El método incluye establecer una pluralidad de perfiles de contexto para un usuario. En algunas implementaciones, los perfiles de contexto se activan automáticamente (por ejemplo, una detección de que el usuario está en un automóvil activa un perfil de "viaje"). En algunas implementaciones, los perfiles de contexto se relacionan con uno o más aspectos del entorno del usuario, la actividad actual o los intereses actuales. En algunas implementaciones, el usuario selecciona manualmente un perfil de contexto activo.
- 35 El método incluye además la detección de un evento asociado con una solicitud de información personal del usuario. En algunas implementaciones, el evento corresponde a una entidad solicitante que solicita PII para un usuario en particular, una entidad solicitante que proporciona un identificador único de un usuario en particular, etc.
- 40 El método incluye además generar una solicitud de consentimiento o permiso para compartir la información personal del usuario con un tercero. En algunas implementaciones, la solicitud incluye una opción para que el usuario apruebe o niegue el permiso para elementos seleccionados de la información solicitada (es decir, menos o más de lo que se incluye en la solicitud), y una opción para que el usuario asigne los permisos (o denegación de los permisos) a perfiles particulares de la pluralidad de perfiles de contexto.
- 45 El método incluye además enviar, al usuario, la solicitud de consentimiento o permiso para compartir la información personal del usuario con un tercero.
- 50 El método incluye además recibir, del usuario, el consentimiento para compartir al menos un subconjunto de la información personal solicitada con el tercero cuando al menos un primer perfil de contexto, de la pluralidad de perfiles de contexto, está activo. En particular, el consentimiento está vinculado a perfiles específicos; es decir, el usuario puede dar su consentimiento para compartir información personal con un tercero en particular en algunos perfiles, pero no en otros perfiles. En algunas implementaciones, el método comprende además recibir, del usuario, la denegación del consentimiento para compartir al menos un subconjunto de la información personal solicitada con el
- 55 tercero cuando al menos un segundo perfil de contexto, de la pluralidad de perfiles de contexto, está activo. Así, por ejemplo, un usuario puede permitir que un tercero acceda y / o use la PII (por ejemplo, la altura, el peso, la talla de la ropa y los hábitos de compra del usuario) cuando el usuario está en un primer perfil (por ejemplo, un perfil de "compra"), pero no cuando el usuario está en otro perfil (por ejemplo, un perfil de "trabajo").
- 60 El método incluye además determinar un perfil de contexto activo para el usuario basándose en una o más señales indicativas del contexto del usuario. Las señales pueden ser de cualquiera de múltiples dispositivos, calendarios, horarios o similares. Por ejemplo, un vehículo puede enviar una señal a un dispositivo apropiado (por ejemplo, a un dispositivo cliente 102 y / o al servidor central 104) cuando el vehículo está siendo conducido para hacer que un perfil

de contexto de "conducción" se active. En algunas implementaciones, las señales indicativas del contexto del usuario corresponden a una selección manual de un perfil de contexto particular.

5 El método incluye además determinar si el perfil de contexto activo coincide con el primer perfil de contexto. De acuerdo con una determinación de que el perfil de contexto activo coincide con el primer perfil de contexto, el método incluye compartir la información personal del usuario con el tercero. De acuerdo con una determinación de que el perfil de contexto activo no coincide con el primer perfil de contexto, el método incluye no compartir la información personal del usuario con el tercero.

10 En algunas implementaciones, detectar el evento asociado con la solicitud de información personal del usuario comprende recibir una solicitud de información personal del usuario.

En algunas implementaciones, el perfil de contexto activo para el usuario se determina automáticamente sin la intervención del usuario. Por ejemplo, el perfil de contexto activo se basa en heurísticas sobre la ubicación, actividad, etc. del usuario, incluyendo si el usuario está conduciendo, haciendo ejercicio, en casa, en el trabajo, en un establecimiento comercial, etc.

20 En algunas implementaciones, el método incluye, además, de acuerdo con una determinación de que el perfil de contexto activo coincide con el primer perfil de contexto, permitir que el tercero se ponga en contacto con el usuario. Se le puede permitir al tercero contactar al usuario a través de cualquier técnica de comunicación apropiada, incluyendo un banner publicitario, mensaje directo (correo electrónico, texto, etc.), llamada de voz / alerta, y similares. De acuerdo con una determinación de que el perfil de contexto activo no coincide con el primer perfil de contexto, el método incluye además no permitir que el tercero se ponga en contacto con el usuario.

25 En algunas implementaciones, el método incluye además recibir una comunicación del tercero. La comunicación está dirigida o destinada a un usuario en particular. El método incluye, además, de acuerdo con una determinación de que el perfil de contexto activo coincide con el primer perfil de contexto, reenviar la comunicación (por ejemplo, un correo electrónico, texto, banner publicitario, llamada / alerta de voz, etc.) al usuario. De acuerdo con una determinación de que el perfil de contexto activo no coincide con el primer perfil de contexto, el método incluye no reenviar la comunicación al usuario.

30 También se describe un método para proporcionar permisos aumentados a la información personal de un usuario (por ejemplo, a través de un modo de "descubrimiento"), de acuerdo con algunas implementaciones. En algunas implementaciones, los pasos se realizan en un dispositivo electrónico con uno o más procesadores (o núcleos) y memoria que almacena uno o más programas para que los ejecuten uno o más procesadores (o núcleos). Por ejemplo, en algunas implementaciones, los pasos se realizan en cualquiera (o cualquier combinación) del dispositivo cliente 102-1, el servidor central 104 y el dispositivo solicitante 108-1. Además, los pasos individuales del método pueden distribuirse entre los múltiples dispositivos electrónicos de cualquier manera apropiada.

40 Cualquiera o todas las comunicaciones entre dispositivos descritas con respecto a las Figuras 5A-5C son, en algunas implementaciones, aseguradas y / o encriptadas usando cualquier técnica de seguridad y/o de encriptación apropiada, incluyendo, pero sin limitarse a, Hypertext Transport Protocol Secure (HTTPS), Secure Sockets Layer (SSL), Transport Layer Security (TLS), Secure Shell (SSH), Internet Protocol Security (IPSec), cifrado de clave pública y similares (incluido cualquier método de cifrado y / o seguridad apropiado aún por desarrollar).

45 El método incluye establecer una pluralidad de perfiles de contexto para un usuario, en el que al menos un perfil de contexto de la pluralidad de perfiles de contexto está asociado con uno o más de los siguientes:

50 Un conjunto de una o más áreas temáticas pertinentes al al menos un perfil de contexto. Las áreas temáticas pertinentes a un perfil de contexto incluyen categorías de bienes o servicios que son relevantes para un contexto particular. Por ejemplo, las áreas temáticas pertinentes a un perfil de viaje incluyen, por ejemplo, gasolineras, comida, reparación de automóviles, etc. Las áreas temáticas pertinentes a un perfil de hogar incluyen, por ejemplo, información de televisión / entretenimiento, entrega de comida, artículos para el hogar, etc. Las áreas temáticas pertinentes a un perfil de compra incluyen, por ejemplo, tiendas minoristas, ropa, electrónica, cualquier clase de producto asociada con un perfil de usuario, etc.

60 Un primer conjunto de cero o más permisos que identifican a los respectivos terceros con los que se puede compartir información personal cuando el al menos un perfil de contexto está activo. En particular, cada perfil de contexto identifica con quién se puede compartir la PII (y / o quién puede usar la PII del usuario) cuando ese perfil de contexto está activo.

Un segundo conjunto de cero o más permisos que identifican qué información personal se puede compartir con los respectivos terceros cuando el al menos un perfil de contexto está activo. En particular, cada perfil de contexto

identifica cero o más categorías, clases o instancias de información de identificación personal que se puede compartir o acceder / utilizar por los respectivos terceros. Por ejemplo, el segundo conjunto de permisos puede incluir un permiso que indique que la frecuencia cardíaca y la información de ubicación se pueden compartir con un servicio de monitorización de la condición física particular cuando el contexto activo es "fitness".

Un tercer conjunto de cero o más permisos que identifican a los respectivos terceros a los que se les permite contactar al usuario cuando el al menos un perfil de contexto está activo. En particular, solo algunos terceros (por ejemplo, minoristas, anunciantes, proveedores de servicios, etc.) pueden comunicarse con el usuario cuando un perfil en particular está activo. Por ejemplo, se puede permitir que un minorista de ropa se ponga en contacto con el usuario (por ejemplo, por correo electrónico, banner publicitario, etc.) cuando el perfil de "compra" del usuario está activo.

Un cuarto conjunto de cero o más permisos que identifican cómo los respectivos terceros pueden contactar al usuario cuando el al menos un perfil de contexto está activo (por ejemplo, por correo electrónico, banners publicitarios (basados en navegador / aplicación), etc. cuando el al menos un perfil de contexto está activo:

El método incluye, además, cuando se opera en un modo regular, realizar al menos una de las siguientes acciones. (En algunas implementaciones, un modo regular corresponde a un modo en el que se aplican los permisos establecidos asociados con el perfil de contexto; por ejemplo, solo los terceros aprobados pueden recibir información aprobada, y solo los terceros aprobados pueden contactar al usuario, y solo a través de una comunicación aprobada tipos.)

Compartir información personal con los respectivos terceros de acuerdo con el primer conjunto de uno o más permisos y el segundo conjunto de uno o más permisos (por ejemplo, proporcionar PII a ciertos terceros y negarse a proporcionar PII a otros terceros).

Recibir información de los respectivos terceros de acuerdo con el tercer conjunto de uno o más permisos y el cuarto conjunto de uno o más permisos (por ejemplo, recibir correos electrónicos, anuncios, mensajes de texto, banners publicitarios, etc., de ciertos terceros y rechazar recibir comunicaciones de otros terceros)

El método incluye, además, cuando se está en un modo de descubrimiento, realizar al menos uno de los siguientes. (En algunas implementaciones, un modo de descubrimiento corresponde a un modo en el que el contexto del perfil aún se aplica, pero se otorgan permisos adicionales, por ejemplo, para permitir que otros terceros aún no aprobados accedan a un usuario y / o para permitir que terceros accedan a un usuario a través de metodologías de comunicación adicionales que no estaban permitidas anteriormente (por ejemplo, se permiten banners publicitarios de un tercero en particular cuando están en modo de descubrimiento, que en cualquier otro caso no se permiten).

Compartir información personal con primeros terceros adicionales de acuerdo con una versión ampliada del primer conjunto de cero o más permisos. Por ejemplo, cuando un perfil de compras está activo, un usuario puede permitir que un determinado grupo de minoristas reciba y / o use PII. Sin embargo, en el modo de descubrimiento, los minoristas adicionales a los que de otro modo no se les permita recibir y / o usar PII podrán hacerlo. En algunas implementaciones, los primeros terceros adicionales están asociados cada uno con al menos un área temática del conjunto de una o más áreas temáticas pertinentes al al menos un perfil de contexto. Por lo tanto, si un modo de descubrimiento para un perfil de contexto de viaje solo otorgará permisos expandidos a terceros adicionales que están asociados con áreas temáticas como estaciones de servicio, alimentos, reparación de automóviles, etc.

Compartir información personal adicional con los respectivos terceros de acuerdo con una versión ampliada del segundo conjunto de cero o más permisos. Por ejemplo, cuando un perfil de compras está activo, la talla de ropa de un usuario puede compartirse con un grupo particular de terceros. En el modo de descubrimiento, se comparte información adicional, como la edad del usuario, historial de compras, compras anteriores, ubicación y similares.

Recibir información de segundos terceros adicionales de acuerdo con una versión ampliada del tercer conjunto de cero o más permisos. Por ejemplo, en un perfil de compras, ciertos minoristas pueden enviar información, como anuncios, correos electrónicos y similares, al usuario. En el modo de descubrimiento, otros minoristas podrían hacerlo. En algunas implementaciones, los segundos terceros adicionales están asociados cada uno con al menos un área temática del conjunto de una o más áreas temáticas pertinentes al al menos un perfil de contexto. Por ejemplo, en un perfil de compra, los terceros adicionales pueden estar restringidos a otros minoristas. Por lo tanto, aunque terceros adicionales, de otro modo no autorizados, pueden enviar información al usuario, la información aún sería pertinente para el perfil de contexto activo del usuario.

Recibir información de terceros correspondientes de acuerdo con una versión ampliada del cuarto conjunto de cero o más permisos. Como se señaló anteriormente, el cuarto conjunto de permisos se relaciona con cómo un tercero puede contactar a un usuario. En consecuencia, una versión ampliada del cuarto conjunto de permisos permite a terceros utilizar modos de comunicación adicionales que de otro modo no están permitidos. Por ejemplo, un minorista

al que solo se le permite contactar al usuario por correo electrónico cuando el modo normal está activo podría usar modos adicionales de comunicación (por ejemplo, mensajes de texto, anuncios emergentes, etc.) cuando el modo de descubrimiento está activo.

5 Como se señaló anteriormente, no es necesario que el modo de descubrimiento otorgue permisos completos a todos los posibles terceros. Más bien, los permisos adicionales otorgados en el modo de descubrimiento pueden ser establecidos por cada usuario individual y pueden ser solo un pequeño aumento en los permisos.

10 En algunas implementaciones, el cuarto conjunto de uno o más permisos que identifican cómo terceros pueden contactar al usuario incluye un primer subconjunto de permisos que identifican los momentos en los que se permite que terceros contacten al usuario; y un segundo subconjunto de permisos que identifican los tipos de comunicación que los terceros pueden usar para contactar al usuario.

15 En algunas implementaciones, el cuarto conjunto de uno o más permisos que identifican cómo terceros pueden contactar al usuario incluye un tercer subconjunto de permisos que identifican momentos en los que no se permite que terceros contacten al usuario; y un cuarto subconjunto de permisos que identifican los tipos de comunicación que los terceros no están autorizados a utilizar para contactar al usuario.

20 Los métodos ilustrados en las Figuras 5A-5C y descritos anteriormente pueden regirse por instrucciones que se almacenan en un medio de almacenamiento legible por ordenador y que son ejecutadas por al menos un procesador de al menos un dispositivo electrónico (por ejemplo, uno o más dispositivos cliente 102- n, uno o más dispositivos solicitantes 108-n, o un servidor central 104). Cada una de las operaciones mostradas en las Figuras 5A-5C puede corresponder a instrucciones almacenadas en una memoria de computadora no transitoria o en un medio de almacenamiento legible por ordenador. En varias implementaciones, el medio de almacenamiento no transitorio legible por ordenador incluye un dispositivo de almacenamiento de disco magnético u óptico, dispositivos de almacenamiento de estado sólido, tales como memoria Flash, u otro dispositivo o dispositivos de memoria no volátil. Las instrucciones legibles por ordenador almacenadas en el medio de almacenamiento no transitorio legible por ordenador pueden estar en código fuente, código en lenguaje ensamblador, código objeto u otro formato de instrucción que sea interpretado y / o ejecutable por uno o más procesadores (o núcleos).

30 Se pueden proporcionar varias instancias de componentes, operaciones o estructuras descritos en el presente documento como una sola instancia. Finalmente, los límites entre varios componentes, operaciones y almacenes de datos son algo arbitrarios, y las operaciones particulares se ilustran en el contexto de configuraciones ilustrativas específicas. Se prevén otras asignaciones de funcionalidad y pueden caer dentro del alcance de la o las implementaciones. En general, las estructuras y la funcionalidad presentadas como componentes separados en las configuraciones de ejemplo pueden implementarse como una estructura o componente combinado. De manera similar, las estructuras y funcionalidades presentadas como un solo componente pueden implementarse como componentes separados. Estas y otras variaciones, modificaciones, adiciones y mejoras caen dentro del alcance de la implementación.

40 También se entenderá que, aunque los términos "primero", "segundo", etc. pueden usarse en este documento para describir varios elementos, estos elementos no deberían estar limitados por estos términos. Estos términos solo se utilizan para distinguir un elemento de otro. Por ejemplo, un primer contacto podría denominarse segundo contacto y, de manera similar, un segundo contacto podría denominarse primer contacto, lo que cambiaría el significado de la descripción, siempre que todas las apariciones del "primer contacto" se renombren de forma coherente y todas las apariciones del segundo contacto se renombren de forma coherente. El primer contacto y el segundo contacto son ambos contactos, pero no son el mismo contacto.

50 La terminología utilizada en este documento tiene el propósito de describir implementaciones particulares únicamente y no pretende ser una limitación de las reivindicaciones. Como se usa en la descripción de las implementaciones y las reivindicaciones adjuntas, las formas singulares "un", "una" y "el/la" están destinadas a incluir las formas plurales también, a menos que el contexto indique claramente lo contrario. También se entenderá que el término "y / o" como se usa en este documento se refiere y abarca todas y cada una de las combinaciones posibles de uno o más de los elementos enumerados asociados. Se entenderá además que los términos "comprende" y / o "que comprende", cuando se usan en esta especificación, especifican la presencia de características, números enteros, pasos, operaciones, elementos y / o componentes declarados, pero no excluyen la presencia o adición de una o más características, números enteros, etapas, operaciones, elementos, componentes y / o grupos de los mismos.

60 Como se usa en el presente documento, el término "si" puede interpretarse que significa "cuando" o "sobre" o "en respuesta a la determinación" o "de acuerdo con una determinación" o "en respuesta a la detección" de que una condición precedente declarada es cierta, dependiendo del contexto. De manera similar, la frase "si se determina (que una condición precedente declarada es verdadera)" o "si (una condición precedente declarada es verdadera)" o "cuando (una condición precedente declarada es verdadera)" puede interpretarse en el sentido de "al determinar" o

"en respuesta a determinar" o "de acuerdo con una determinación" o "al detectar" o "en respuesta a detectar" que la condición precedente declarada es verdadera, dependiendo del contexto.

5 La descripción anterior incluyó ejemplos de sistemas, métodos, técnicas, secuencias de instrucciones y productos de programas de máquinas informáticas que incorporan implementaciones ilustrativas. A efectos de explicación, se establecieron numerosos detalles específicos con el fin de proporcionar una comprensión de varias implementaciones del tema inventivo. Sin embargo, será evidente para los expertos en la técnica, que las implementaciones de la materia objeto de la invención se pueden practicar sin estos detalles específicos. En general, no se han mostrado en detalle instancias, protocolos, estructuras y técnicas de instrucción bien conocidas.

10 La descripción anterior, con fines explicativos, se ha descrito con referencia a implementaciones específicas. Sin embargo, las discusiones ilustrativas anteriores no pretenden ser exhaustivas o limitar las implementaciones a las formas precisas descritas. Son posibles muchas modificaciones y variaciones en vista de las enseñanzas anteriores. Las implementaciones se eligieron y describieron con el fin de explicar mejor los principios y sus aplicaciones prácticas, para permitir así a otros expertos en la técnica utilizar mejor las implementaciones y diversas implementaciones con diversas modificaciones según se adapten al uso particular contemplado.

15

REIVINDICACIONES

1. Un método para proporcionar acceso a información personal de un usuario, que comprende:
5 en un sistema de servidor (104), conectado a través de una red (110) a uno o más dispositivos electrónicos (102 - 1, ... 102-n) y uno o más dispositivos solicitantes (108-1, ... 108-n), donde el uno o más dispositivos electrónicos (102-1, ... 102-n) tiene uno o más procesadores y memoria que almacena uno o más programas para su ejecución por el uno o más procesadores:
establecer una pluralidad de perfiles de contexto para un usuario;
10 detectar un evento asociado con una solicitud recibida de un tercero para obtener información personal del usuario especificada por el tercero;
generar una solicitud de consentimiento para compartir la información personal especificada del usuario con el tercero;
15 enviar, al usuario, la solicitud de consentimiento para compartir la información personal especificada del usuario con el tercero;
recibir, del usuario, consentimiento para compartir al menos un subconjunto de la información personal solicitada especificada con el tercero cuando al menos un primer perfil de contexto, de la pluralidad de perfiles de contexto, está activo;
20 determinar un perfil de contexto activo para el usuario en base a una o más señales indicativas del contexto de usuario;
determinar si el perfil de contexto activo coincide con el primer perfil de contexto;
de acuerdo con una determinación de que el perfil de contexto activo coincide con el primer perfil de contexto, facilitar el intercambio de la información personal del usuario con el tercero; y
de acuerdo con una determinación de que el perfil de contexto activo no coincide con el primer perfil de
25 contexto, no facilitar el intercambio de la información personal del usuario con el tercero.
2. El método de la reivindicación 1, en el que el perfil de contexto activo para el usuario se determina automáticamente sin intervención del usuario.
- 30 3. El método de una de las reivindicaciones anteriores, que además comprende:
de acuerdo con una determinación de que el perfil de contexto activo coincide con el primer perfil de contexto, permitir que el tercero se ponga en contacto con el usuario; y
de acuerdo con una determinación de que el perfil de contexto activo no coincide con el primer perfil de
35 contexto, no permitir que el tercero se ponga en contacto con el usuario.
4. El método de una de las reivindicaciones anteriores, que además comprende:
recibir una comunicación del tercero;
de acuerdo con una determinación de que el perfil de contexto activo coincide con el primer perfil de contexto, reenviar la comunicación al usuario; y
40 de acuerdo con una determinación de que el perfil de contexto activo no coincide con el primer perfil de contexto, no reenviar la comunicación al usuario.
5. El método de una de las reivindicaciones anteriores, que además comprende:
de acuerdo con una determinación de que el perfil de contexto activo coincide con el primer perfil de contexto,
45 permitir que el tercero se comunique directamente con el usuario; y
de acuerdo con una determinación de que el perfil de contexto activo no coincide con el primer perfil de contexto, no permitir que el tercero se comunique directamente con el usuario.
6. El método de una de las reivindicaciones anteriores, en el que la pluralidad de perfiles de contexto se
50 almacena en un primer dispositivo electrónico (102-1, ... 102-n) de los uno o más dispositivos electrónicos (102-1, ... 102 -n), donde la información personal del usuario se almacena en un segundo dispositivo electrónico (102-1, ... 102-n) de los uno o más dispositivos electrónicos (102-1, ... 102-n), el segundo dispositivo electrónico (102-1, ... 102-n) es distinto del primer dispositivo electrónico (102-1, ... 102-n).
- 55 7. Un dispositivo electrónico (102-1, ... 102-n), que comprende:
una pantalla (308, 408); y
medios para realizar el método de cualquiera de las reivindicaciones 1 a 6.

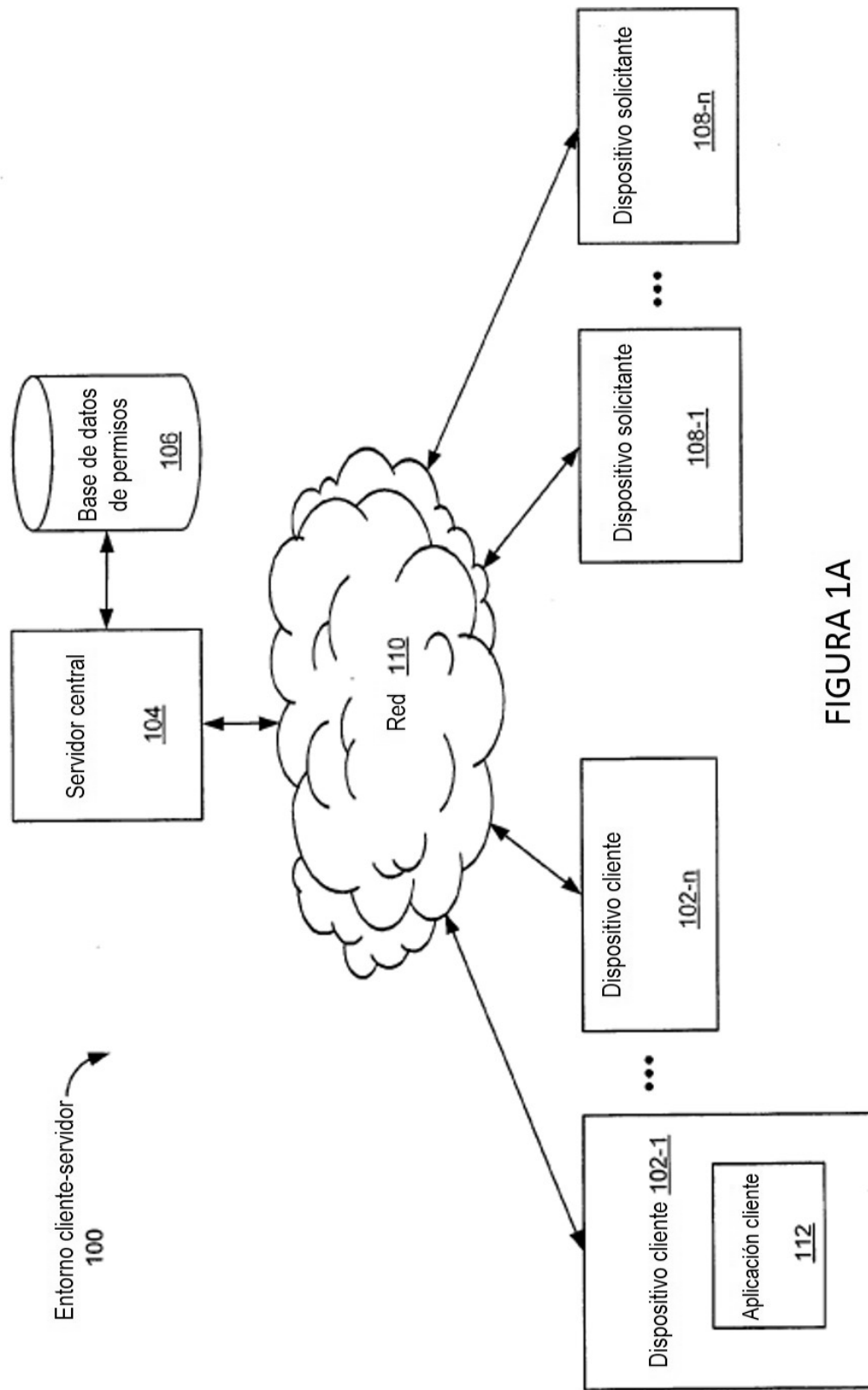


FIGURA 1A

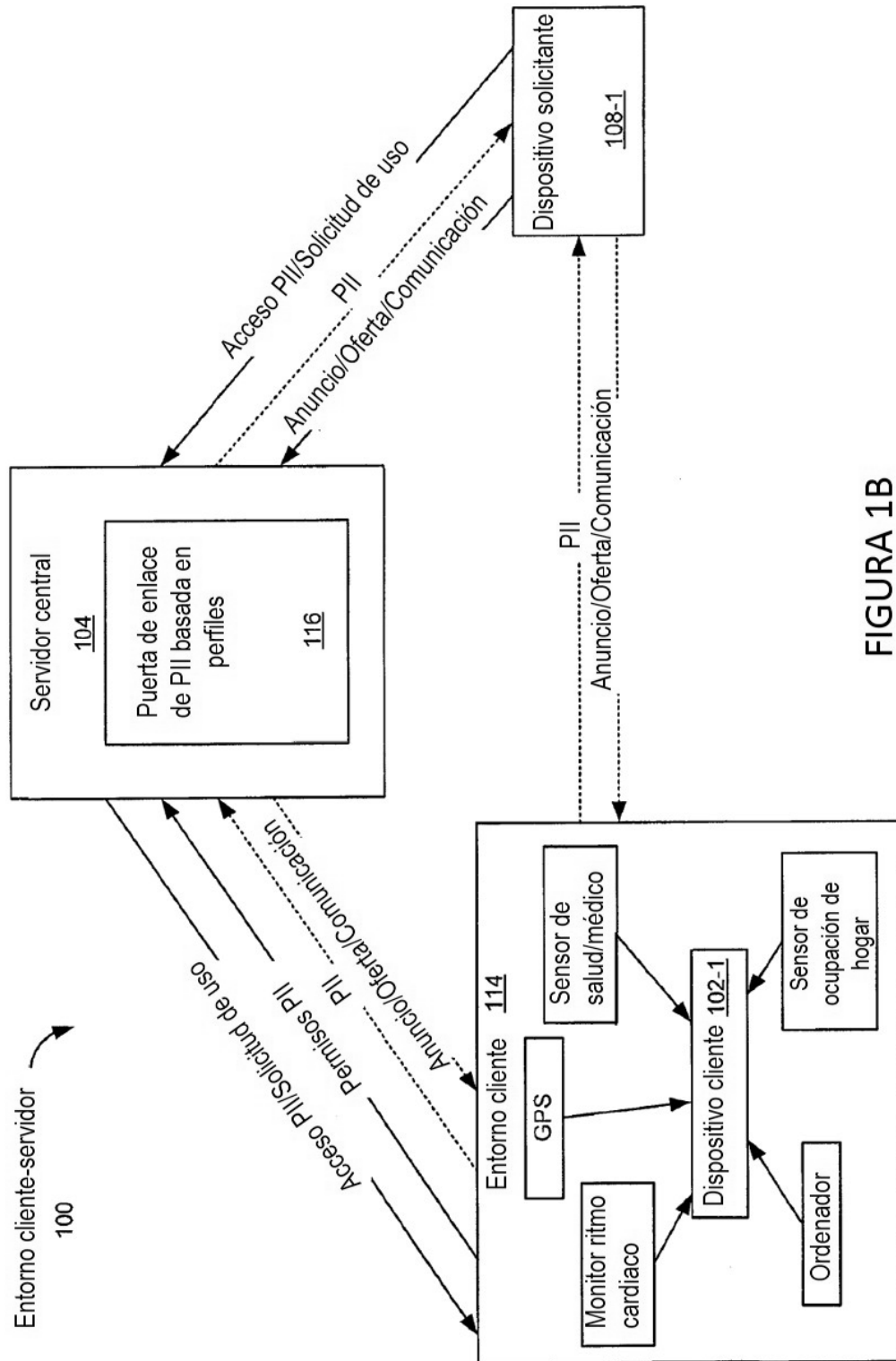
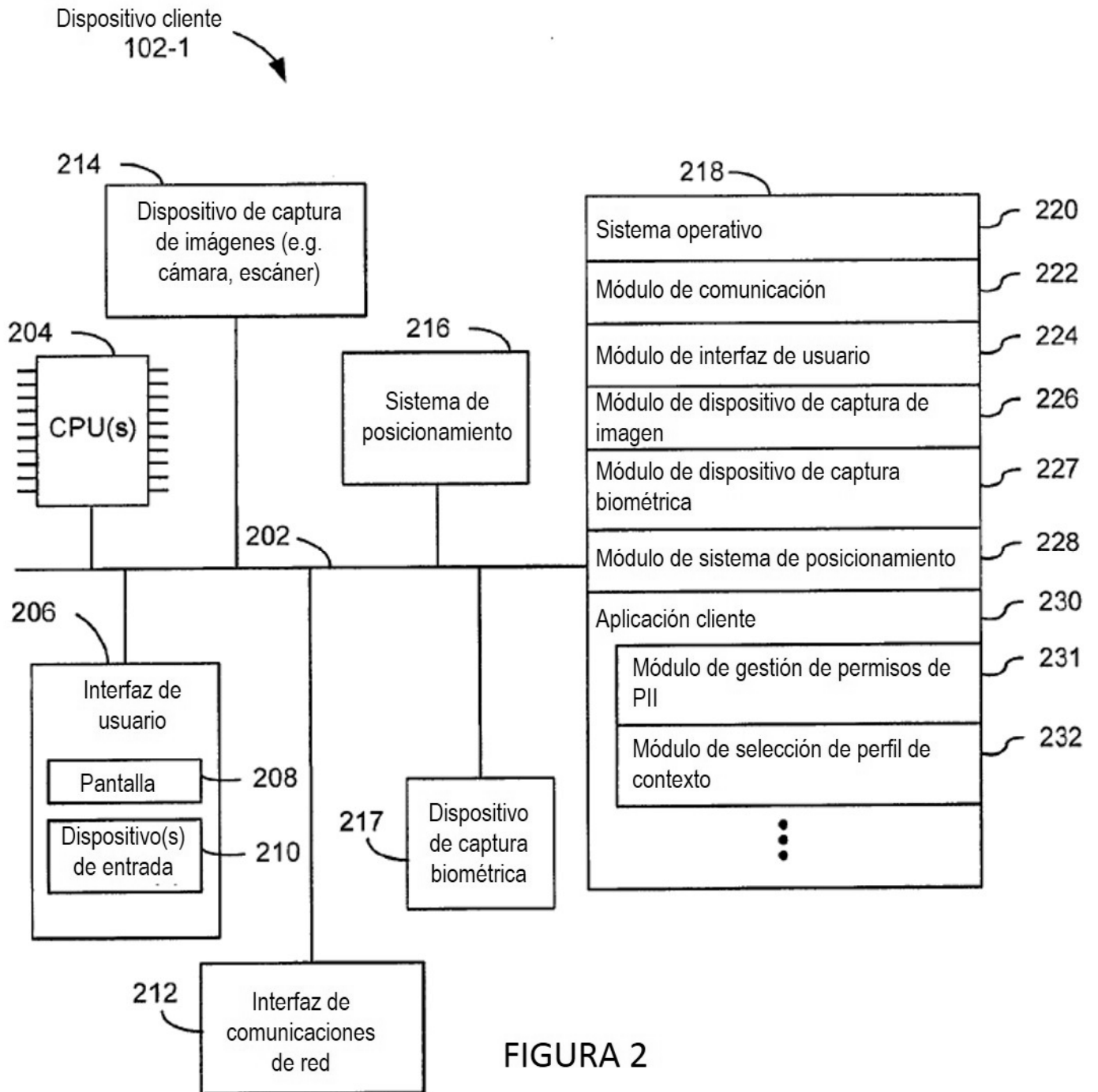
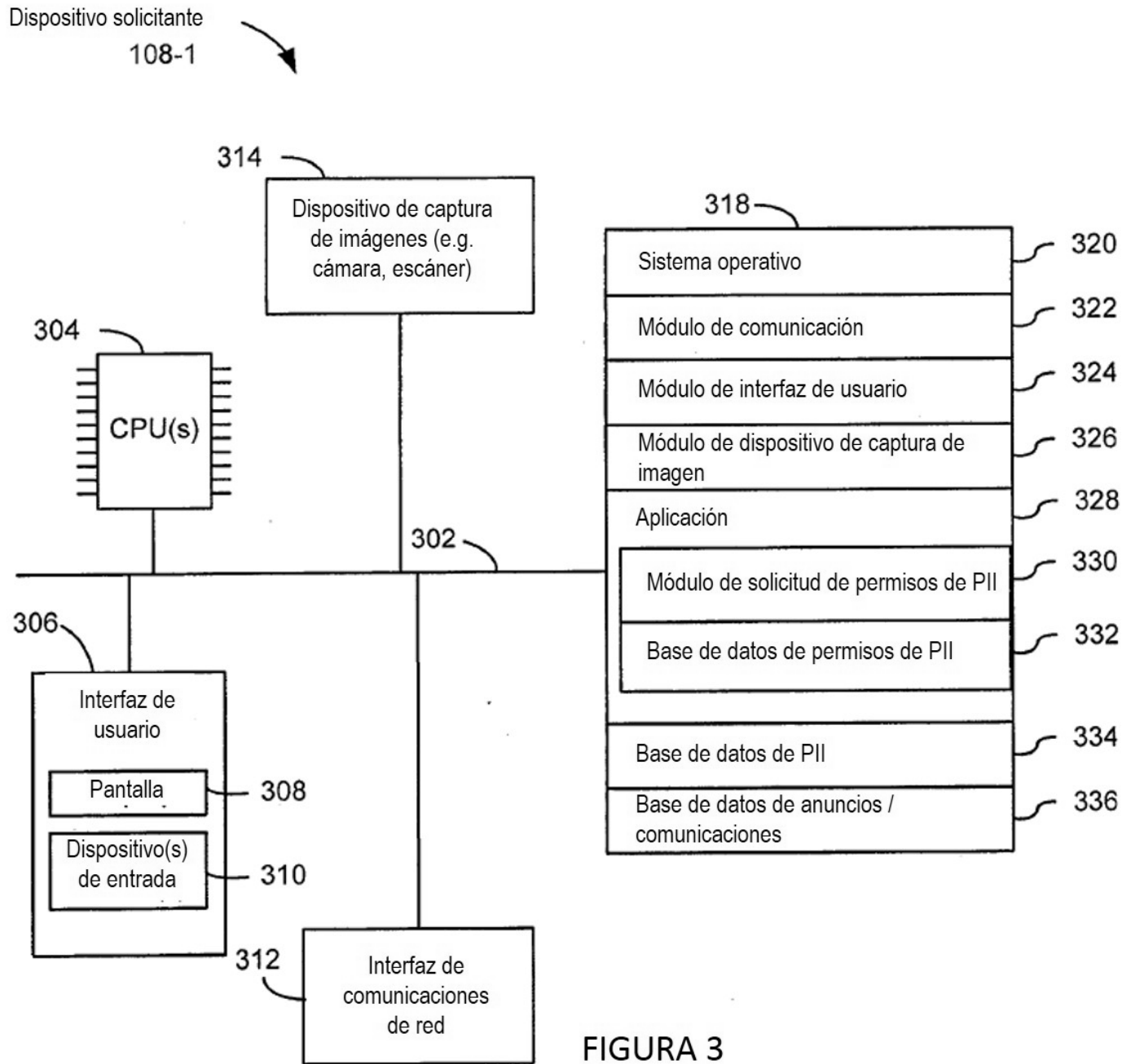


FIGURA 1B





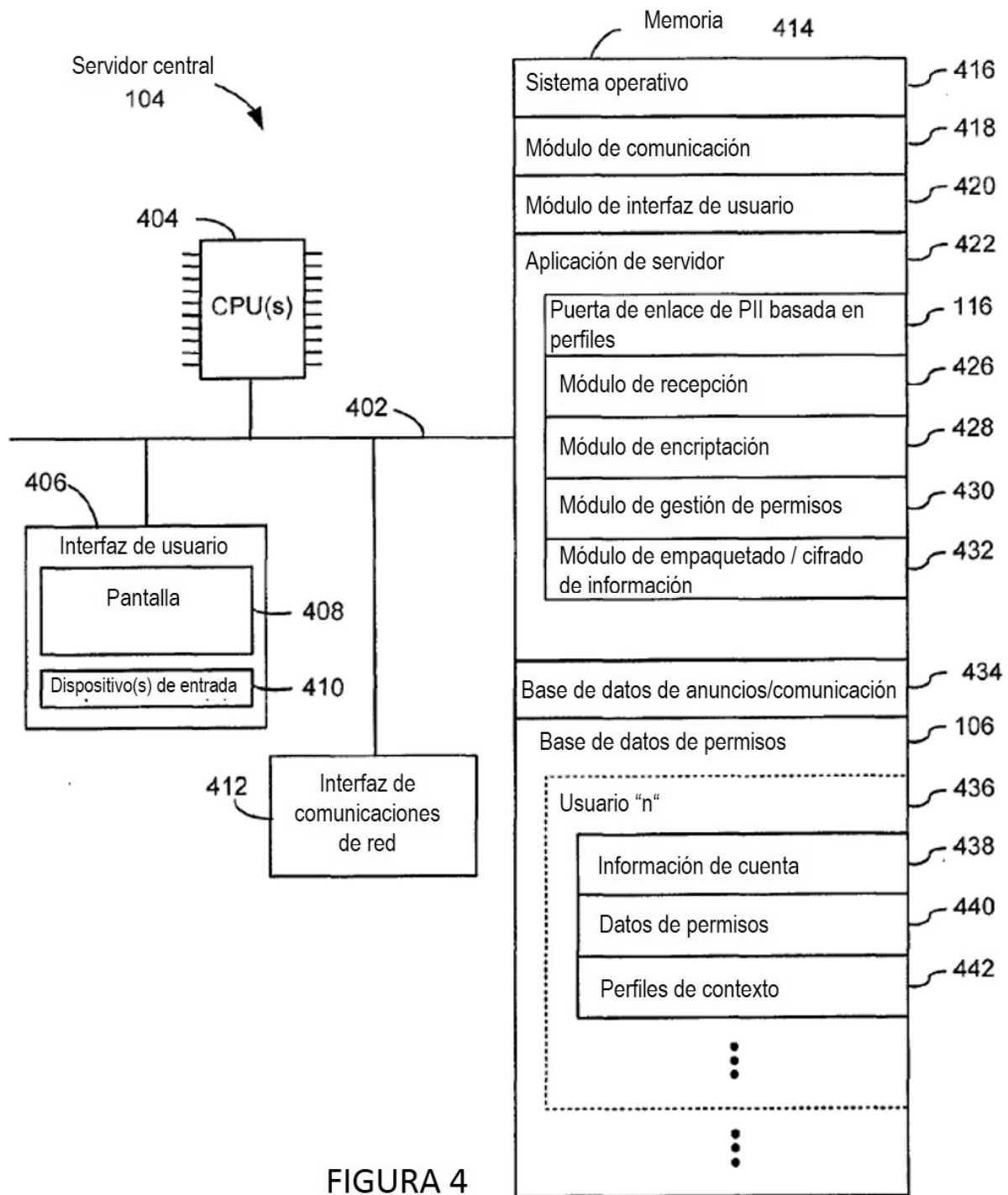


FIGURA 4

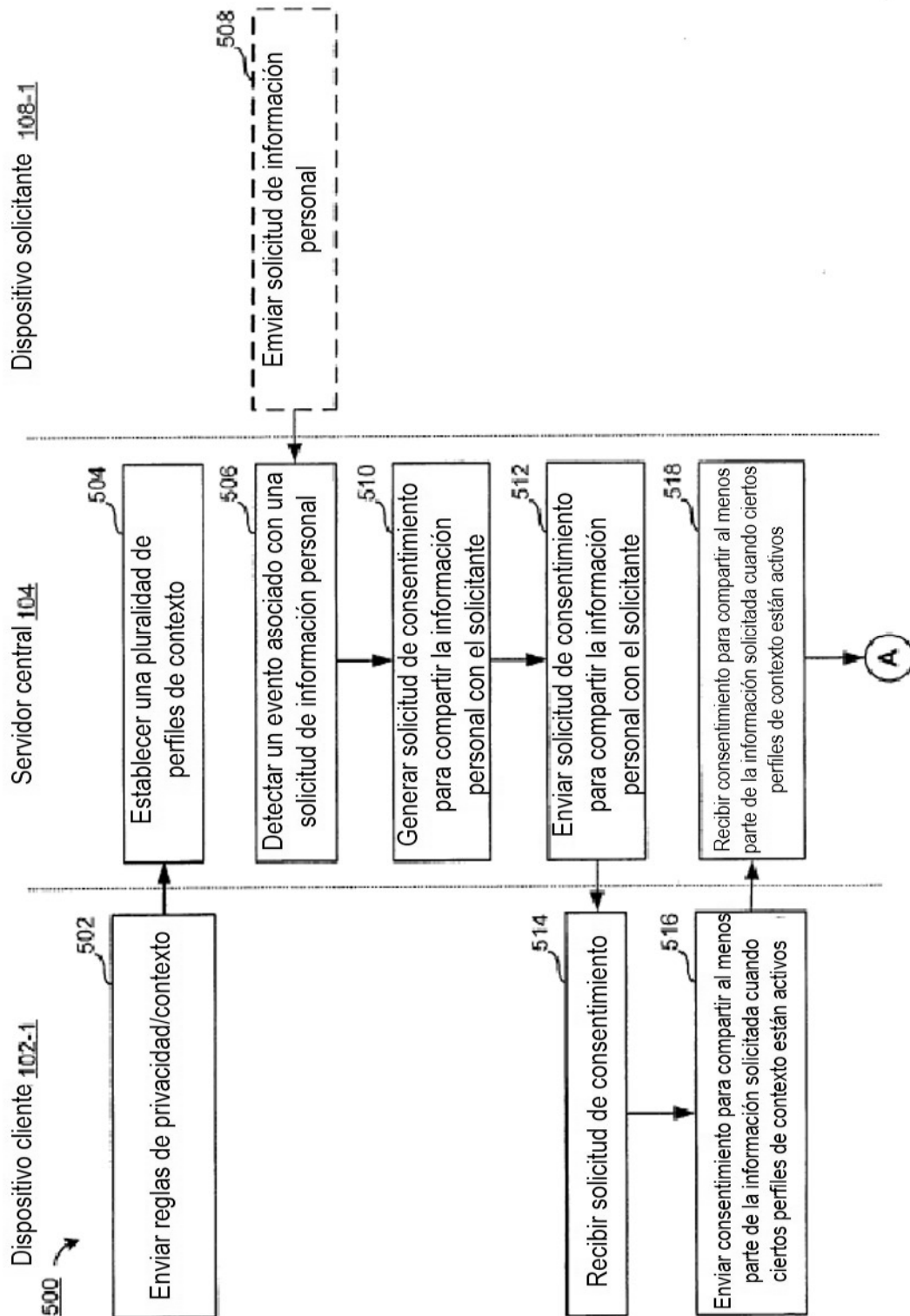


FIGURA 5A

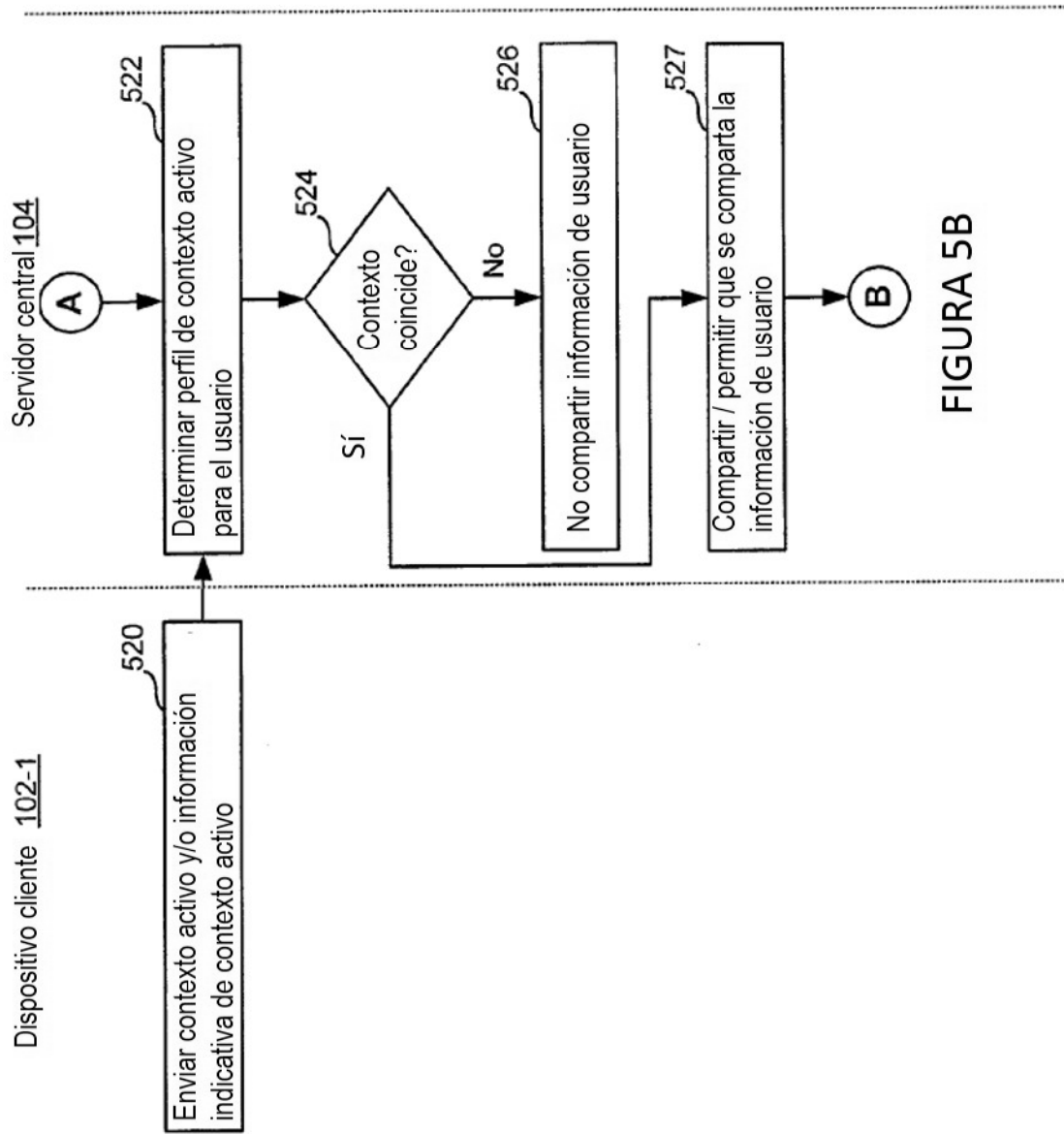


FIGURA 5B

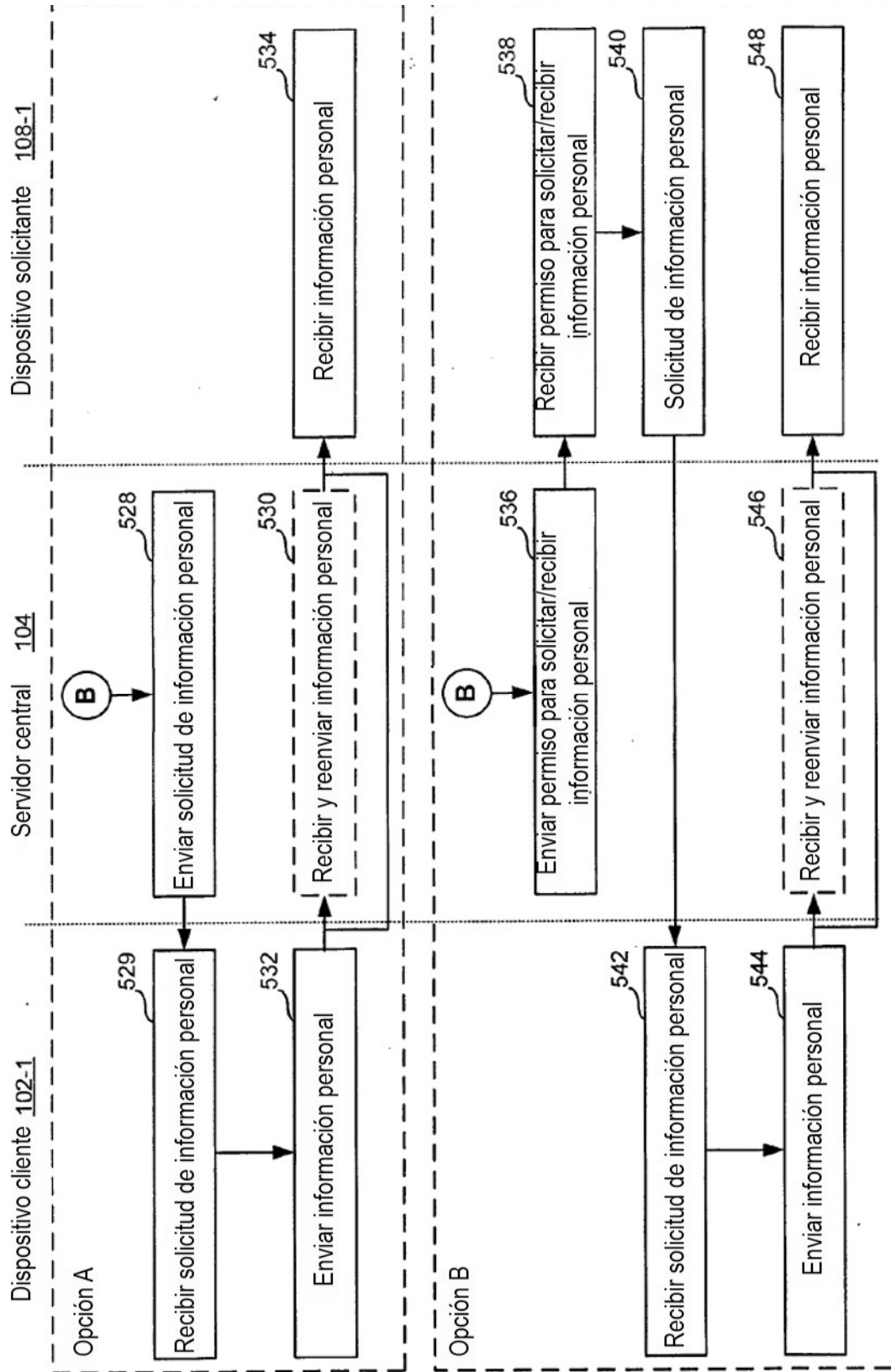


FIGURA 5C