

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 738 505**

51 Int. Cl.:

G06F 12/00 (2006.01)

G06F 17/30 (2006.01)

H04L 29/06 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **26.05.2011 PCT/US2011/038214**

87 Fecha y número de publicación internacional: **01.12.2011 WO11150261**

96 Fecha de presentación y número de la solicitud europea: **26.05.2011 E 11787449 (5)**

97 Fecha y número de publicación de la concesión europea: **22.05.2019 EP 2577468**

54 Título: **Gestión de datos en redes informáticas y de telecomunicaciones**

30 Prioridad:

28.05.2010 US 349784 P
07.10.2010 US 900239

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
23.01.2020

73 Titular/es:

PRIVOWNY, INC. (100.0%)
Europarc Pichaury, Bat B4, 1330 avenue Jean
Rene Guillibert Gauthier de la, Lauzière
13290 Aix-en-Provence, FR

72 Inventor/es:

LE JOUAN, HERVÉ

74 Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

ES 2 738 505 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

Gestión de datos en redes informáticas y de telecomunicaciones

5 Antecedentes

10 Hay más de 1000 millones de usuarios de Internet en todo el mundo, más de 3500 millones de abonados móviles de los cuales por encima del 70 % usan sus teléfonos móviles para fines distintos de voz, y todos han comunicado al menos una vez datos personales (ya sea correo electrónico, nombre, fecha de nacimiento, dirección, número de teléfono, etc.) a compañías (proveedores de servicio, sitios de comercio electrónico, bancos, operadores móviles...) y/o han autorizado, con o sin su conocimiento, el uso de estos datos.

15 Los servicios ofrecidos en Internet/móvil que requieren autenticación cada vez son más y más numerosos y variados (correo electrónico, sitios de interconexión de red social, compras en línea, subastas, bancos, marcas comerciales, etc.). Los individuos a menudo proporcionan información personal incluso sin leer el contrato de uso asociado con su uso; reciben correo electrónico o SMS de estas compañías u otras compañías a las que nunca han comunicado sus datos personales; a menudo están en el medio, sin su consentimiento o sin estar totalmente conscientes, de múltiples bases de datos cruzadas con respecto a sus datos personales y/o comportamiento que permite una mejor focalización; y en ocasiones usan varias direcciones de correo electrónico para evitar la "contaminación/publicidad no deseada" pero también múltiples contraseñas que gradualmente conducen a confusión pero que no responden necesariamente de manera adecuada a los desafíos de visibilidad y transparencia.

25 Además, pueden instalarse otros sistemas tales como las Cookies, sin que los individuos realmente sean conscientes, que pueden recopilar información personal acerca de los individuos.

30 Uno o más de estos factores puede significar que los individuos no pueden controlar haber puesto a disposición sus datos personales; pueden olvidar su inicio de sesión y/o contraseña; ya no están más en control de sus propios datos; y, por el nivel técnico de las terminologías comúnmente usadas, tienen únicamente una vaga idea de lo que realmente está pasando, incluyendo fusión (cruzado) de ficheros de datos personales, análisis de su comportamiento de Internet, y compartición de sus datos personales entre compañías. Las autoridades nacionales y/o internacionales, entre ellas, caen en este juego con un deseo de proteger al individuo, que es loable, pero puede dar como resultado restricciones a menudo no entendidas por los individuos, no son de aplicación generalizada mientras que Internet es global, y que podrían tener un impacto negativo en un ecosistema en auge (Internet y móvil).

35 La protección de la privacidad es un problema global que preocupa tanto a individuos como a las autoridades. Por ejemplo, la cobertura de medios en el sujeto está aumentando de manera significativa, impulsada por los casos de Google y Facebook. Esta preocupación de la privacidad está ponderada a la luz de los servicios de valor añadido que está obteniendo un usuario. Internet y los teléfonos móviles ofrecen grandes cantidades de oportunidades, algunas de las cuales no se usan o no pueden usarse en el momento, para cumplir las necesidades de los individuos y que por lo tanto proporcionan el servicio o servicios que desean, con la condición de que la relación entre el proveedor y el individuo sea transparente y bien entendida. Sin embargo, si no se hace nada para asegurar que los individuos estén informados y confiados, entonces Internet, y, más ciertamente, los móviles, pueden no suministrar todas sus promesas y podrían verse en su lugar como invasores de la privacidad y por lo tanto de la libertad individual.

45 Hoy en día, en este contexto donde Internet y el teléfono móvil multiplican las oportunidades para conectar y donde la participación se vuelve un elemento clave de la relación entre los individuos y las marcas comerciales, el individuo puede desear ser el centro y especialmente el maestro, con responsabilidad total, sean cual sean los medios.

50 Hay unas pocas iniciativas que se han llevado a cabo en términos de protección de la privacidad, iniciadas por los Gobiernos y Autoridades que tienen y están aún muy activos en la implementación leyes, normativas y reglas para garantizar al consumidor y sus datos personales. También, las organizaciones tales como la Iniciativa de Publicidad en Red (www.networkadvertising.org) o Truste (www.truste.com) han implementado algunos mecanismos para informar al consumidor para ayudar a las compañías a establecer las políticas de privacidad de derechos que corresponden al interés del consumidor. Sin embargo, estas iniciativas, aunque van en la dirección correcta, no evitaban que las preocupaciones sobre la privacidad surgieran de manera significativa a lo largo de los años, ya que se centran principalmente en la compañía y no en el consumidor.

60 FTC, la Comisión Europea, ICO en el RU, la Ley Federal de Protección de Datos Alemana, CNIL en Francia, AEPD en España, IPC en Canadá, etc., están implicadas en definir reglas sobre protección de datos personales. También, los Estados Unidos y Europa han lanzado en el primer trimestre de 2010 una nueva consulta (http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0005_en.htm) que tiene como objetivo tener un enfoque internacional común. Al final de la 31ª Conferencia Internacional de Protección de Datos y Comisionado de Privacidad, que tuvo lugar en Madrid en noviembre de 2009, las autoridades de protección de datos de más de 50 países aprueban la "Resolución Madrid" sobre las normas de privacidad internacionales que constituyen la base para la elaboración de un futuro acuerdo universalmente vinculante.

La velocidad a la que el entorno digital se ha movido en los últimos 4 años, más las nuevas posibilidades que emergen con los teléfonos móviles, más la globalización que es intrínseca a Internet, más el tamaño de esta economía electrónica, hace muy difícil legislar o regular para evitar este o tal uso de datos personales. Algunas de estas autoridades y, desde luego, Ann Cavoukian, de Canadá IPC, proponen cambiar y reiniciar el sistema como se ha definido para tratar el nuevo panorama (véase, por ejemplo, <http://www.ipc.on.ca/english/Home-Page/>).

El documento US 2002/0087641 desvela un sistema y método para controlar y organizar correo electrónico basándose en alias de correo electrónico.

10 **Sumario**

La invención se define por la reivindicación 1 del sistema independiente y la correspondiente reivindicación 6 del método independiente. Se definen detalles adicionales de la invención en las reivindicaciones dependientes.

15 Un individuo puede tener derechos para participar con control:

derecho de información → consentimiento ← propietario de datos
 derecho de actualización → actualización ← auto disciplina / discernimiento
 derecho de olvido → borrado ← conformidad de identidad / privacidad

Una tercera parte confiable puede permitir que se informe el control del usuario de Internet y/o móvil, para proporcionar permisos, para proporcionar sus preferencias y para participar.

20

Breve descripción de los dibujos

La Figura 1 representa una vista conceptual de un sistema de gestión de datos controlado.

25

La Figura 2 representa un ejemplo de un sistema de suscripción de gestión de datos controlado para consumidores de información personal.

La Figura 3 representa un ejemplo de un sistema de registro de gestión de datos controlado para proveedores de información personal.

30

La Figura 4 representa un ejemplo de un sistema de generación de alias de información personal.

La Figura 5 representa un ejemplo de un sistema de servidor de correo electrónico a nivel de alias.

35

La Figura 6 representa un ejemplo de un sistema para proporcionar servicios a un usuario de un sistema de gestión de datos controlado.

Las Figuras 7A y 7B representan ejemplos de componentes adecuados para realizar las técnicas descritas en este artículo.

40

Las Figuras 8A a 8C representan ejemplos de sistemas de generación de alias con variaciones en la localidad de los componentes.

La Figura 9 representa un diagrama de flujo de un ejemplo de un método para identificar compartición de información usando un alias específico de entidad.

45

Descripción detallada

La Figura 1 representa una vista conceptual de un sistema de gestión de datos controlado 100. En el ejemplo de la Figura 1, el sistema 100 incluye una red 102, un servidor de compartición de datos controlado 104, un cliente maestro 106, y clientes de acceso limitado 108-1 a 108-N (denominados colectivamente como clientes de acceso limitado 108). La red 102 puede incluir Internet, o cualquier otra red, como se describe más adelante con referencia a las Figuras 7 y 8.

50

El servidor de compartición de datos controlado 104 puede incluir diverso hardware y/o componentes de software, como se describe más adelante con referencia a las Figuras 7 y 8. Usando las técnicas descritas en este artículo, el servidor de compartición de datos controlado 104 puede posibilitar que los usuarios estén seguros de manera razonable de que recibirán ofertas de compañías que confían, se sientan capacitados informándoles, dándoles confianza, ayudándolos a entablar relaciones transparentes y/o recompensándolos. Por lo tanto, los consumidores pueden hacerse maestros de sus propias huellas digitales.

55

60

El sistema puede ser de interés también para los gobiernos puesto que la gestión de alias puede evitar que los datos personales salgan de un país si se implementan de manera apropiada, sin limitar la capacidad de que los usuarios

dentro del país participen en comercio electrónico internacional. Los diversos datos disponibles pueden informarse para los consumidores, administradores de sistemas, entidades de terceros, etc., usando un motor de generación de información que tiene datos disponibles y/o pertinentes para la entidad particular. Por ejemplo, el servidor de compartición de datos controlado 104 tiene acceso a una gran cantidad de datos que pueden usarse para el fin de desarrollo de perfiles de comercialización de comportamiento del consumidor.

El servidor de compartición de datos controlado 104 puede posibilitar, por ejemplo, que un usuario asociado con el cliente maestro 106 vea una lista de compañías (por ejemplo, sitios de comercio electrónico, sitios de medios o editoriales, redes sociales, ISP o cualesquiera otros sitios, etc.) que mantienen un subconjunto de los datos personales del usuario (por ejemplo, nombre; dirección; dirección de correo electrónico; número de teléfono móvil, doméstico, de oficina u otro; información de tarjeta de crédito; edad; sexo; ocupación; fotos; etc.). Los datos pueden obtenerse a través de registro, proporcionarse por otra compañía o a través de otros medios. Como otro ejemplo, el servidor de compartición de datos controlado 104 puede posibilitar que el usuario vea una lista de compañías que han puesto cookies, etiquetas u otra información que recoge/rastrea dispositivos en el cliente maestro 106 u otras máquinas del usuario que permiten la monitorización de la actividad de Internet u otra del usuario para análisis de comportamiento, entrega de publicidad focalizada u otros fines. Como otro ejemplo, el servidor de compartición de datos controlado 104 puede posibilitar que el usuario vea una lista de compañías a las que el usuario ha proporcionado su dirección de correo electrónico, que se vendió posteriormente (o tal vez se predijo) o se compartió de otra manera con otras compañías (tal vez sin el permiso del usuario) a partir de lo cual el usuario o un agente del usuario ha recibido correos electrónicos. Si el usuario ha recibido un correo electrónico de una o más de las otras compañías, el usuario puede ver, en una implementación específica, una lista de cualquiera de las otras compañías en asociación con la compañía que ha compartido de manera evidente la dirección de correo electrónico. Como otro ejemplo, el servidor de compartición de datos controlado 104 puede recompensar a un usuario por uso de datos personales o aceptación de focalización de comportamiento en un mercado donde el usuario puede elegir una lista de asuntos/intereses y/o elegir que sea contactado por marcas que se han identificado en su «lista de confianza». Como otro ejemplo, el servidor de compartición de datos controlado 104 puede facilitar a un usuario que visualice ofertas de marcas comerciales/compañías, facilite que el usuario proponga a las mismas marcas comerciales/compañías, y/o posibilite que el usuario introduzca búsquedas/preferencias sobre un producto o categoría; y posibilite que el usuario firme un acuerdo para un periodo de tiempo (por ejemplo, mientras busca obtener un producto), para información específica o tipos de información, para un fin particular, y/o similares. Además, el usuario puede recibir ofertas de compañías que se recomiendan por una parte asociada con el servidor de compartición de datos controlado 104 o alguna otra parte, de manera presumible aunque no necesaria si el usuario elige recibir recomendaciones. La funcionalidad del servidor de compartición de datos controlado 104 se describe en mayor detalle más adelante.

En el ejemplo de la Figura 1, el cliente maestro 106 incluye un almacén de datos de información personal 110, un motor de transparencia de compartición de datos 112, una interfaz de red 114, y un bus 116 que conecta operacionalmente los componentes. El almacén de datos de información personal 110 puede implementarse como una estructura de datos (o múltiples estructuras de datos) almacenadas en un medio de almacenamiento legible por ordenador. A modo de ejemplo, pero sin limitación, la información personal puede almacenarse como un registro en una base de datos, como series en un fichero plano, como una tabla en memoria volátil, en una red de Internet PC/Móvil u otra nube, o de alguna otra manera conveniente. Un almacén de datos puede incluir interfaces que facilitan el acceso a datos en el almacén de datos, y/o motores que realizan otras funciones.

En una implementación específica, el almacén de datos de información personal 110 incluye un libro de direcciones. Los libros de direcciones pueden tener diversos formatos y configuraciones que incluyen a modo de ejemplo pero sin limitación, el libro de direcciones de Palm, el libro de direcciones de Outlook, el libro de direcciones de Mozilla, el libro de direcciones de Entourage, el libro de direcciones de Max OS X, o un tipo de libro de direcciones conocido aplicable o conveniente. Un libro de direcciones, o más en general un almacén de datos de información personal, puede incluir prácticamente cualquier dato, aunque implementaciones particulares pueden incluir más o menos campos o tipos de estructuras de datos que otras implementaciones.

Como se usa en este artículo, la información personal puede incluir prácticamente cualquier dato que pueda asociarse con un usuario. A modo de ejemplo, pero sin limitación, la información personal puede incluir nombre, aniversarios importantes, direcciones domésticas, direcciones de negocio, teléfono doméstico, fax doméstico, teléfono celular, teléfono de empresa, fax de empresa, correo electrónico personal, correo electrónico de empresa, organizaciones benéficas favoritas, listas de deseos, tallas de ropa, colores favoritos, vinos favoritos, comidas favoritas, sitios web favoritos, elementos de interés, enlaces a contenido, ficheros de medios, títulos de software, imágenes, vídeo, ajustes (por ejemplo, FACEBOOK®), etc.

En el ejemplo de la Figura 1, el motor de transparencia de compartición de datos 112 es opcional puesto que el motor es responsable de dar control sobre información personal a un usuario del cliente maestro 106, estableciendo un círculo virtuoso entre el usuario y otras entidades asociadas con los clientes limitados 108 basándose en transparencia minuciosa, asegurando que el usuario es el maestro de la información personal y está informado de su uso pretendido por las entidades, y/o proporcionando un espacio único en el que el usuario puede hacer uso de Internet, móviles, u otros servicios en confianza, podría implementarse en el servidor de compartición de datos controlado 104. En una implementación específica, el motor de transparencia de compartición de datos 112 puede incluir un módulo de

extensión de explorador. El módulo de extensión podría posibilitar el registro con entidades y ayudar a obtener alias para su uso con las entidades en el momento de registro, usando las técnicas descritas en este artículo. En una implementación que no incluye un motor de transparencia de compartición de datos 112, el cliente maestro 106 podría incluir un explorador u otro motor para acceder a un espacio privado en el servidor de compartición de datos controlado 104 para ver o gestionar datos, un perfil de usuario o similares.

Como se usa en este artículo, un motor incluye un procesador especializado o compartido y, hardware, firmware, o módulos de software que se ejecutan por el procesador. Dependiendo de consideraciones específicas de implementación u otras, la funcionalidad de un motor puede estar centralizada o distribuida. Un motor puede incluir hardware de fin especial, firmware, o software incorporado en un medio legible por ordenador para su ejecución por el procesador. Como se usa en este artículo, la expresión "medio de almacenamiento legible por ordenador" se pretende que incluya únicamente medios físicos, tales como memoria. Como se usa en este artículo, un medio legible por ordenador se pretende que incluya todos los medios que son legales (por ejemplo, en los Estados Unidos, bajo el 35 U.S.C. 101), y que excluya específicamente todos los medios que no son legales por su naturaleza hasta el punto que la exclusión sea necesaria para una reivindicación que incluye que el medio legible por ordenador sea válido. Medios legibles por ordenador legales conocidos incluyen hardware (por ejemplo, registros, memoria de acceso aleatorio (RAM), almacenamiento no volátil (NV), por nombrar unos pocos), aunque pueden estar limitados o no a hardware.

La interfaz de red 114 puede incluir diverso hardware y/o componentes de software, como se describe más adelante con referencia a las Figuras 7 y 8. Debería observarse que aunque únicamente se muestra una única interfaz de red para los diversos clientes en el ejemplo de la Figura 1, y en otras figuras en este artículo, es posible usar múltiples interfaces de red. Por ejemplo, el almacén de datos de información personal 110 podría distribuirse a través de múltiples localizaciones y acoplarse por medio de una red. Como otro ejemplo, el almacén de datos de información personal 110 podría estar remoto con relación al motor de transparencia de compartición de datos 112. Por lo que la interfaz de red 114 debería interpretarse de manera amplia para que incluya cualquier mecanismo conocido o conveniente aplicable para conectar los diversos componentes de un dispositivo a una red, independientemente de si los subcomponentes de un componente particular están distribuidos a través de múltiples máquinas o los diversos componentes están distribuidos a través de múltiples máquinas (como podría sugerirse por las representaciones de los componentes en un único dispositivo en los ejemplos proporcionados en las figuras en este artículo, pero que deberían observarse como una implementación específica de un concepto más amplio).

En el ejemplo de la Figura 1, los diversos componentes del cliente maestro 106 están conectados a un bus 116. Puede observarse que son posibles las realizaciones alternativas que no conectan algunos o todos los componentes al bus 116, como sería evidente para un experto en la materia en la técnica pertinente. Por lo tanto, el bus 116 podría considerarse opcional.

En el ejemplo de la Figura 1, los clientes de acceso limitado 108 incluyen las interfaces de red 118-1 a 118-N (denominadas colectivamente como interfaces de red 118) y los almacenes de datos de información de alias 120-1 a 120-N (denominados colectivamente como almacenes de datos de información de alias 120). Las interfaces de red 118 pueden incluir diverso hardware y/o componentes de software, como se describe más adelante con referencia a las Figuras 7 y 8. Los almacenes de datos de información de alias 120 pueden incluir un subconjunto de datos hallado en el almacén de datos de información personal 110, y los datos pueden incluir contenedores vacíos o valores ficticios, y al menos un alias para facilitar el control de los datos por un usuario asociado con el cliente maestro 106 de una manera que se describe más adelante.

En una implementación específica, los clientes de acceso limitado 108 pueden ser agnósticos con respecto al servidor de compartición de datos controlado 104. Lo que se pretende por agnóstico es que los clientes de acceso limitado 108 puedan asociarse con empresas que recopilan información personal de los individuos, tal como un individuo asociado con el cliente maestro 106, y recopilan información personal del cliente maestro 106 de una manera que no varía debido a la existencia del servidor de compartición de datos controlado 104. En una implementación de este tipo, un individuo asociado con el cliente maestro 106 haría uso del servidor de compartición de datos controlado 104 para introducir información personal, que incluye un alias de correo electrónico, en uno de los clientes de acceso limitado 108.

Como alternativa, uno o más de los clientes de acceso limitado 108 puede tener conocimiento de su implicación en un sistema de compartición de datos controlado. Por ejemplo, una entidad independiente puede solicitar a una entidad asociada con uno de los clientes de acceso limitado 108 que envíe un correo electrónico estructurado y/o normalizado a un alias de correo electrónico que el servidor de compartición de datos controlado 104 ha creado para un individuo que es específico a la entidad. El correo electrónico estructurado y/o normalizado puede incluir contenedores asociados con información personal que se recopila por el sitio y un enlace para una actualización, tal como, por ejemplo, nombre de la compañía, fin del uso de información personal, correo electrónico (test-test@test.com), nombre, apellidos, fecha de nacimiento, teléfono móvil, etc. Como sugiere el término, los contenedores no son valores de datos, sino que en su lugar son los campos que intentaría rellenar normalmente la entidad con información personal de un usuario. Ventajosamente, la recopilación de la información personal de un usuario podría hacerse innecesaria en algunos casos y/o implementaciones ya que sería un proceso normalizado para certificar a los usuarios. El usuario

5 puede usar o no un mecanismo, tal como un módulo de extensión de explorador, para solicitar la actualización de un perfil de usuario automáticamente, por ejemplo, añadiendo la entidad a una lista de sitios confiables, rellenando contenedores asociados con la entidad, actualizando información personal previamente proporcionada con nueva información (por ejemplo, si cambia un número de teléfono), obtener un alias para la entidad, y/u otras actividades asociadas con la entidad o los datos asociados con la entidad.

10 En una implementación específica, puede implementarse un procedimiento automatizado entre el servidor de compartición de datos controlado 104 y sitios/compañías que acuerdan enviar la información que mantienen sobre los individuos. Por ejemplo, el servidor de compartición de datos controlado 104 puede enviar a una entidad confiable una lista de individuos registrados (por ejemplo, correos electrónicos); una compañía/sitio puede enviar al servidor de compartición de datos controlado 104 una lista de individuos registrados (por ejemplo, correos electrónicos); o para cada instancia de un correo electrónico duplicado, puede solicitarse a la entidad que envíe los contenedores mantenidos para esta dirección de correo electrónico con la fecha de creación y un enlace para actualizar los datos. Ventajosamente, un usuario asociado con el cliente maestro 106 puede poder identificar entidades que recopilan su información personal y/o que han acordado por medio de cooperación con el servidor de compartición de datos controlado 104 ser transparentes. Puede ser deseable para el servidor de compartición de datos controlado 104 que proporcione una zona de "Compañías" especializada donde, por ejemplo, pueda solicitarse que las entidades intercambien datos de manera proactiva, proporcionen información acerca de ellas mismas o la información personal que recopilan, o similares.

20 Las entidades pueden beneficiarse cooperando con el servidor de compartición de datos controlado 104. Por ejemplo, el servidor de compartición de datos controlado 104 puede hacer a los usuarios confiables de la transparencia de un sitio asociado con una entidad y por lo tanto fortalecer la relación entre usuarios y la entidad. El servidor de compartición de datos controlado 104 puede recibir información personal del usuario de entidades cooperativas que han recopilado las entidades. El servidor de compartición de datos controlado 104 puede agregar la información personal en un espacio personal asociado con el usuario.

30 La información personal puede etiquetarse o hacerse identificable de otra manera según se asocia con una entidad o grupo de entidades y transporta información acerca de la entidad. Por ejemplo, el servidor de compartición de datos controlado 104 podría identificar información personal proporcionada a una entidad con un logo específico, que podría ser visible de una aplicación/módulo de extensión cuando el usuario se encuentra en el servidor de compartición de datos controlado 104. En una implementación específica, el logo no necesita certificar contratos para el usuario de datos personales, que ya se ha hecho por compañías tales como eTrust, sino que puede demostrar que el sitio/compañía está cooperando para asegurar que la información personal se usa de manera transparente para el usuario. El logo podría tomar varias formas y/o podría transportar información de la compañía/sitio que, por ejemplo, el sitio ha acordado enviar información personal mantenida sobre un individuo al servidor de compartición de datos controlado 104, el sitio envía la información y no compartirá con otras compañías, el sitio envía la información y no venderá/compartirá con otras compañías sin entrar en contacto con el individuo, el sitio ofrece una oportunidad para salir si el usuario lo solicita, el sitio actualmente está en análisis para intercambiar los datos personales con el servidor de compartición de datos controlado 104, el sitio no desea participar, el sitio no ha respondido a una solicitud para cooperar o similares.

45 Un usuario asociado con el cliente maestro 106 puede gestionar/rastrear su información personal en un espacio proporcionado por el servidor de compartición de datos controlado 104. El espacio puede posibilitar a los anunciantes, compañías de investigación, editores, agencias, etc., promocionar/poner su búsqueda de perfiles (para investigación, para monitorizar comportamiento, para establecer paneles, para realizar ensayos, etc.) con, por ejemplo, una descripción del objeto, el objeto, duración, recompensas asociadas o similares. El espacio puede posibilitar que los individuos observen la búsqueda de perfiles, para responder, hacer preguntas, para proporcionar información personal (que incluye, por ejemplo, datos del comportamiento que podrían generarse por el servidor de compartición de datos controlado 104 en lugar de proporcionarse explícitamente por el usuario) de manera transparente a una entidad, para gestionar la concesión de información personal (toda o parte), para rastrear la compensación para compartir información personal, o similares.

55 En una implementación específica, un individuo puede proporcionársele acceso a un sistema de subastas en el que el individuo podría ofrecer su "perfil" (personal o de comportamiento) durante un periodo definido a un precio, las entidades podrían hacer ofertas para perfiles, o ambos. Esta característica puede posibilitar, por ejemplo, pujas en tiempo real para información personal. Para proteger la privacidad, es probable que el espacio fuera únicamente accesible para abonados al sistema, si el abonado es un usuario con información personal o el abonado es una entidad que busca información personal. La accesibilidad podría controlarse con una técnica conocida o conveniente aplicable para controlar el acceso, tal como requiriendo el uso de un nombre de usuario y contraseña por los abonados al servicio.

65 En una implementación específica, para aumentar de manera ostensible la calidad de información personal, podría proporcionársele la oportunidad a las entidades para calificar al individuo (por ejemplo, en la escala de 1 a 10) con respecto al "compromiso" para participar. Esta calificación puede estar basada o no en el hecho de que el individuo ha comprado un producto, ha hecho clic en carteles, o similares, y podría estar limitada a datos derivados de términos

de participación de un acuerdo con la entidad e información personal asociada. También, para el individuo, durante la subasta de información personal o cuando está respondiendo a una oferta de información personal, esta calificación puede aparecer por lo que las marcas comerciales podrán evaluar el perfil con el que están tratando.

5 En una implementación específica, un usuario puede calificar entidades en el espacio privado. Si una entidad tiene una calificación suficientemente baja (o se desconecta explícitamente) la compañía puede perder la capacidad de solicitar al usuario con correo electrónico, ofertas o similares.

10 Las entidades pueden trabajar con agencias, servidores de publicidad, firmas de comercialización o similares para asegurar que sus promociones, anuncios, focalización, etc., son efectivas para sus marcas comerciales. El servidor de compartición de datos controlado 104 puede funcionar también con tales agencias para proporcionar una lista de marcas comerciales para focalización a individuos.

15 Un individuo puede definir lo que desea y desde quién desea recibir promociones. En una implementación específica, un motor de búsqueda puede incluir varias dimensiones además de dimensiones más evidentes tales como categoría de producto, producto, marca comercial o similares. Una dimensión de tiempo podría posibilitar que un usuario indique una fecha de inicio y de un fin. Por ejemplo, si un usuario está buscando una promoción para un viaje en las próximas 3 semanas el servidor de compartición de datos controlado 104 podría proporcionar promociones durante 3 semanas y a continuación dejar de proporcionar promociones. También, el motor de búsqueda podría recordar los términos de búsqueda usados en la búsqueda inicial para eliminar la necesidad de que el usuario reitere la búsqueda múltiples veces sobre el periodo de tiempo indicado, y envíe coincidencias de criterios al usuario.

25 Otra dimensión puede ser "mi marca comercial favorita". Un usuario puede desear restringir promociones a marcas comerciales/sitios que están en el espacio privado del usuario, seleccionar marcas comerciales acerca de las que él desea recibir información, permitir que las marcas respondan a una búsqueda recomendada por otros individuos, limite los resultados de búsqueda al mismo tipo de productos o productos relacionados de otra manera o similares. Una ventaja de esta característica es que los resultados no incluirán todas estas compañías/sitios intermedios que no proporcionan ningún valor a la búsqueda y solo contaminan los resultados puesto que han obtenido palabras clave.

30 Los resultados de una búsqueda pueden ser promociones/anuncios, tal como promociones que el individuo ha recibido por correo electrónico que ha analizado el servidor de compartición de datos controlado 104, promociones que corresponden a la búsqueda (o al menos alguna parte de la búsqueda), promociones en tiempo real de marcas comerciales/compañías directamente relacionadas con la búsqueda o similares. Puede ser deseable restringir enlaces que pueden hacerse clic a promociones reales que coinciden con la búsqueda y no enlaces a sitios que son simplemente intermediarios o una página de inicio. Puede proporcionarse a los usuarios la capacidad para informar resultados de enlace en su espacio privado, bloquear que se visualice de nuevo el resultado de búsqueda asociado, o similares, y puede marcarse el enlace como potencialmente no relevante, no relevante con respecto a un tipo de productos, o no relevante en otros contextos. Podría hacerse accesible una lista para todos los usuarios de modo que puedan obtener el mejor valor. También, si los resultados aparecen en un espacio de promociones específico, podría solicitarse al individuo que enumere los sitios que él desea que aparezca algún anuncio/promociones con respecto a su búsqueda, y podría realizarse una respuesta apropiada (tal como asociarse con estos sitios). Este enfoque es diferente de la focalización de comportamiento puesto que el consumidor participa con marcas comerciales y productos de una manera diferente, sabiendo plenamente lo que obtendrá y cómo. Ya que hay una multitud de preguntas hoy en día sobre el valor de anuncios y la eficacia de los carteles, este enfoque probablemente ayudará a aumentar el valor.

50 Puede ser deseable ofrecer servicios como: totalizar todos los contactos del individuo (Interconexión de Red Social, Mensajería Instantánea, Outlook, Teléfono Móvil, etc.); enlazar con redes sociales para desarrollar la información de contexto en tiempo real; integrar una red social; y proporcionar espacios de voto, expresión, evaluación y compartición de opinión.

55 Usando las técnicas descritas en este artículo, el sistema 100 puede usarse para que los usuarios, de, por ejemplo, una sencilla/única interfaz de usuario, se vuelvan, día tras día, maestros de sus perfiles. Esto puede conseguirse manteniendo información personal mantenida por las compañías (por ejemplo nombre, correo electrónico, número de teléfono móvil, edad, sexo, ocupación, etc.); almacenar/ver las id de usuarios/contraseñas asociadas con cada sitio/marca comercial de una manera segura; rastrear suscripciones a boletines de noticias; conocer si un usuario ha comprado alguna cosa de una compañía, incluyendo tal vez fechas de transacción; conocer si un sitio usa o ha usado una cookie y cuál es el uso de datos recopilados o rastreados en asociación con la cookie; facilitar acceso directo a un perfil de usuario en estos sitios mediante un enlace directo; pedir la anulación de suscripción a información/boletines de noticias de sitios/compañías en nombre del usuario; finalizar una relación con uno o más sitios (excluyendo sitios donde se requiere esta relación, tal como bancos, proveedores de Internet, operadores móviles, etc.); proporcionar una puntuación de la apreciación de un sitio web/compañía con respecto a gestión/transparencia de privacidad de datos y confianza; posibilitar la visualización de una puntuación agregada (por ejemplo, de abonados a un servicio asociado con el servidor de compartición de datos controlado 104) para cada compañía; actualizar cierta información personal tal como dirección, correo electrónico, etc., y autorizar al servidor de compartición de datos controlado 104 o a un servicio asociado a enviar una actualización a todos o una lista definida de usuarios de compañías titulares.

5 En una implementación específica, el sistema 100 puede recopilar información usando un proceso que el usuario ha acordado instalar/activar en un ordenador de sobremesa/portátil/móvil, usando botones (miniaplicaciones) que los sitios ponen en su página de suscripción/perfil, y/o pide a las marcas comerciales que envíen automáticamente la información que mantienen sobre el usuario al servidor de compartición de datos controlado 104 o un servicio asociado. De manera presumible, los usuarios desearán que su información personal se proteja. Por lo que, por ejemplo, el sistema 100 puede implementarse de manera que se hará una interacción con compañías externas, ya sea para información de entrada o de salida, a través de API aseguradas y procesos. Algunos de tales procesos se describen más adelante.

10 En la operación, el servidor de compartición de datos controlado 104 y/o el motor de transparencia de compartición de datos 112 posibilitan que un usuario controle a través de la información personal. Por ejemplo, cuando un usuario introduce o actualiza información personal en, por ejemplo, un sitio de terceros, el sistema de gestión de datos controlado puede recopilar automáticamente alguna información dependiendo de reglas que son específicas de la implementación, configuración y/o de preferencias de usuario. Alguna información de este tipo puede incluir un contenedor únicamente (por ejemplo, Nombre: Sí, Apellido: Sí, Dirección: No, etc...), el contenedor y el contenido (por ejemplo, Nombre: Sí, Valor = «Test», Apellido: Sí, Valor= «Test1», etc...), o una combinación.

20 Los siguientes ejemplos hacen referencia a Facebook, pero podrían ser aplicables a otros sitios. La información puede derivarse de un usuario que hace clic en un botón «Me gusta» en Facebook. A continuación el sistema de gestión de datos controlado puede añadir el sitio y la información que se hace disponible para él, de manera presumible de acuerdo con preferencias de usuario. Cuando el usuario está usando una aplicación en Facebook que está recopilando información personal la aplicación puede registrarse en el sistema de gestión de datos controlado por lo que el usuario puede conocer, recordar y actuar en algún punto en el futuro. Como Facebook ofrece maneras para acceder a qué información tienen ellos que está asociada con usuarios y sus perfiles (amigos, nivel de apertura, etc...) y están usando Oauth, el sistema de gestión de datos controlado podría recopilar automáticamente esta información y hacerla evidente en el sistema de gestión de datos controlado.

30 El sistema de gestión de datos controlado puede recopilar también y rastrear qué cookies están activas en un sitio específico cuando el usuario está navegando y enlaces a compañías (a menudo terceras partes tales como servidores de publicidad, compañías de rastreo, etc...).

35 De acuerdo con las preferencias de usuario, el sistema de gestión de datos controlado puede almacenar también información de inicio de sesión para diversos sitios. La información de inicio de sesión incluye de manera frecuente un id de usuario y una contraseña. La información de inicio de sesión debería almacenarse de manera segura de una manera aplicable conocida o conveniente.

40 Si un usuario proporciona información personal directamente al sistema de gestión de datos controlado, que puede ser o no posible dependiendo de la implementación, la información puede almacenarse en uno o más perfiles. El sistema de gestión de datos controlado puede a continuación proponer que el usuario reutilice alguno o todos los datos de un perfil particular cuando se registra en un sitio de terceros.

45 Una entidad de gestión de datos controlados puede asociarse con entidades de terceros (abonados) y recopilar contenedores o titulares de datos para individuos en general, o individuos particulares. El sistema de gestión de datos controlado puede informar al usuario cuándo se suscriben nuevas entidades de terceros. El usuario puede hacer clic a continuación, por ejemplo, en una opción para ver qué compañías son abonados y qué información personal del usuario tienen las compañías (incluyendo los valores si se desea, suponiendo que el sistema de gestión de datos controlado realmente tiene los valores).

50 La Figura 2 representa un ejemplo de un sistema de suscripción de gestión de datos controlado 200 para consumidores de información personal. En el ejemplo de la Figura 2, el sistema 200 incluye una interfaz de red 202, un motor de suscripción de entidad 204, un almacén de datos de perfil de entidad 206, y un motor de etiquetado de entidad 208. La interfaz de red 202 puede incluir diverso hardware y/o componentes de software, como se describe más adelante con referencia a las Figuras 7 y 8.

55 En el ejemplo de la Figura 2, el motor de suscripción de entidad 204 está acoplado a la interfaz de red 202. El motor de suscripción de entidad 204 es operativo para posibilitar que una entidad se una a un servicio de suscripción de gestión de datos como un proveedor de contenido, bienes, o servicios y/o como un consumidor de información personal. La entidad puede contactar con el motor de suscripción de entidad 204 para formar una asociación o el motor de suscripción de entidad 204 puede contactar con la entidad para formar la asociación. La razón para hacer el contacto puede incluir, por ejemplo, un usuario que indica un interés en un sitio web, que activa el motor de suscripción de entidad 204 para enviar una invitación al sitio web; el motor de suscripción de entidad 204 puede recibir una instrucción de, por ejemplo, un administrador para enviar una invitación; el motor de suscripción de entidad 204 podría buscar automáticamente la red para socios potenciales y enviar una invitación cuando se halle uno; o por alguna otra razón.

Para fines de ilustración, se supone que la entidad recopilará alguna información personal acerca de los usuarios, pero es posible que la información sea un alias y únicamente se pase información personal anónima a la entidad. Algunas entidades pueden requerir cierta información personal, pero para fines de ilustración, se supone que al menos una sub-parte de la información personal es un alias. En una implementación específica, la información de alias incluye un alias de correo electrónico. En implementaciones alternativas, la información de alias podría incluir un número de teléfono de alias, un nombre de alias (por ejemplo, un nombre de hacer negocios como "DBA"), una dirección de alias (por ejemplo, un apartado de correos), o similares.

Es posible que una entidad recopile información personal de un usuario que no se comparte con una red de gestión de datos controlada. Sin embargo, pueden compartirse aún metadatos. Por ejemplo, en una implementación específica, el motor de suscripción de entidad 204 puede obtener mediante la interfaz de red 202 contenedores de datos que están vacíos, tienen valores ficticios, o tienen alias, y almacenar los contenedores en el perfil de la entidad 206. Los contenedores de datos representan uno o más campos de datos que pueden rellenarse con información recopilada de usuarios. Obteniendo los contenedores de terceros, el sistema 200 puede conocer qué información ha compartido un usuario con los terceros sin recopilar la información en la red de gestión de datos controlados. En una implementación específica, esta opción podría ser "por defecto" en el sentido que no habrá información identificable alguna recopilada por el sistema 200 excepto, por ejemplo, correo electrónico, que se proporcionó en el registro.

En una implementación específica, un sistema de gestión de datos controlado puede facilitar la gestión de usuarios de los campos de datos permitiendo que el usuario enlace contenedores de diferentes perfiles de entidad (o tal vez enlazando contenedores automáticamente). Por ejemplo, si dos entidades tienen contenedores que se denominan como "Nombre", es posible que el nombre proporcionado por el usuario sea el mismo para cada entidad. Enlazando los dos, el usuario puede hacer uso de otros procedimientos, suponiendo que tales procedimientos están implementados, para actualizar "Nombre" para cada entidad de terceros de manera simultánea. En una implementación específica, la voluntad de una entidad para cooperar en ciertos procedimientos puede almacenarse en el almacén de datos de perfil de entidad 206. Por ejemplo, las entidades que cooperan pueden posibilitar que el sistema de gestión de datos controlado vaya a un sitio de entidad de terceros y actualice información de usuario en nombre del usuario. Como alternativa, un usuario podría proporcionar información de inicio de sesión al sistema de gestión de datos controlado para posibilitar que el sistema actualice información que cambia en nombre del usuario. Puesto que probablemente sería deseable automatizar el procedimiento de actualización, dependiendo de la implementación, las entidades de terceros pueden necesitar posibilitar actualizaciones automatizadas, y si las entidades de terceros posibilitan actualizaciones automatizadas puede indicarse en el almacén de datos de perfil de entidad 206.

En el ejemplo de la Figura 2, el almacén de datos de perfil de entidad 206 está acoplado al motor de suscripción de entidad 204. En la operación, el motor de suscripción de entidad 204 obtiene información acerca de una entidad para asociar con el sistema de gestión de datos, que se almacena en el almacén de datos de perfil de entidad 206. Es posible formar una asociación sin recibir información alguna de la entidad. Por ejemplo, un usuario podría proporcionar información acerca de la entidad o la información podría obtenerse de alguna otra manera. Un registro de entidad en el almacén de datos de perfil de entidad 206 puede incluir el nombre de compañía, URL, número de teléfono, y/u otros campos conocidos o convenientes aplicables. En una implementación específica, un campo de estado indica la relación de una entidad con una entidad de compartición de datos controlada. Por ejemplo, el campo de estado podría indicar que se ha solicitado que la entidad se una a una red de compartición de datos controlada, pero que no se ha recibido respuesta; que la solicitud se ha denegado; que la solicitud se ha aceptado; que la entidad se ha unido a la red de compartición de datos controlada, pero comparte información personal con afiliados; que la entidad se ha unido a la red de compartición de datos controlada, pero no comparte información personal con nadie; que la entidad tiene voluntad de aceptar que un usuario está certificado a través de la red de compartición de datos controlada sin requerir ninguna información distinta de alias; que la red de compartición de datos controlada ha concedido la capacidad para actualizar información personal con la entidad si un usuario cambia su información personal; u otras indicaciones de estado dentro de la red de compartición de datos controlada que se deciden grabar.

En el ejemplo de la Figura 2, el motor de etiquetado de entidad 208 se acopla a la interfaz de red 202, el motor de suscripción de entidad 204, y el almacén de datos de perfil de entidad 206. El estado u otra información acerca de una entidad pueden almacenarse en el almacén de datos de perfil de entidad 206 por el motor de suscripción de entidad 204. El motor de etiquetado de entidad 208 puede proporcionar a través de la interfaz de red 202 información de estado u otra acerca de una entidad a través de un mensaje o alerta, un símbolo o elemento de cambio de color, u otra miniaplicación que consiga el objetivo de proporcionar información acerca de una entidad que está asociada con un sitio web u otra presencia electrónica. En una implementación alternativa, la miniaplicación podría ser indicativa de estado de entidad basándose en una localización física (por ejemplo, a través de un sistema de navegación de GPS), una localización de teléfono (por ejemplo, como una pantalla en un teléfono inteligente), o a través de algún otro mecanismo conveniente en asociación con la identificación de información acerca de la entidad. Cuando sea deseable distinguir entre las diversas tecnologías de etiquetado, un motor que proporciona una miniaplicación en asociación con una presencia electrónica puede denominarse como un motor de etiquetado electrónico de entidad, un motor que proporciona una miniaplicación en asociación con una localización física puede denominarse como un motor de etiquetado de localización de entidad, un motor que proporciona una miniaplicación en asociación con un número de teléfono puede denominarse como un motor de etiquetado de entidad número de teléfono, etc. En cada caso, la

etiqueta es indicativa de una relación y/o estado que tiene la entidad con una red de gestión de datos controlada.

La Figura 3 representa un ejemplo de un sistema de registro de gestión de datos controlado 300 para proveedores de información personal. En el ejemplo de la Figura 3, el sistema 300 incluye una interfaz de red 302, un motor de identificación de usuario 310, un motor de registro de usuario 312, un motor de recopilación de información personal 314, y un almacén de datos de perfil de usuario 314. La interfaz de red 302 puede incluir diverso hardware y/o componentes de software, como se describe más adelante con referencia a las Figuras 7 y 8.

En el ejemplo de la Figura 3, el motor de identificación de usuario 310 está acoplado a la interfaz de red 302. El motor de identificación de usuario 310 puede usarse para hallar usuarios en localizaciones particulares. Por ejemplo, podría identificarse un usuario descargando un elemento a una máquina, haciendo clic en un enlace, navegando a una localización particular en la web, identificándose a sí mismos en una red social, sitio de correo electrónico, o similares, etc. En una implementación que incluye acceso telefónico, el usuario podría identificarse haciendo una llamada de teléfono. En una implementación específica, puede identificarse un usuario usando datos previamente recopilados en un procedimiento de registro. El usuario podría registrarse, por ejemplo, en un sistema de gestión de control.

En el ejemplo de la Figura 3, el motor de registro de usuario 312 está acoplado al motor de identificación de usuario 310. Cuando se identifica un usuario, el motor de registro de usuario 312 puede iniciar un procedimiento de recopilación de información personal.

En el ejemplo de la Figura 3, el motor de recopilación de información personal 314 está acoplado a la interfaz de red 302, al motor de identificación de usuario 310, y al motor de registro de usuario 312. El motor de recopilación de información personal 314 puede recopilar datos acerca de usuarios mediante la interfaz de red 302. La información recopilada por el motor de recopilación de información personal 314 puede depender de si un usuario identificado está registrado, si el usuario identificado tiene o está interactuando con una entidad abonada, preferencias de usuario previamente proporcionadas, o similares.

En el ejemplo de la Figura 3, el almacén de datos de perfil de usuario 316 está acoplado al motor de registro de usuario 312 y al motor de recopilación de información personal 314. El motor de recopilación de información personal 312 puede almacenar información acerca de un usuario en el perfil de usuario 314 cuando se recopila la información personal.

Cuando se inicia un procedimiento de registro "rápido", la información personal recopilada puede incluir únicamente una dirección de correo electrónico o número de teléfono móvil, el motor de recopilación de información personal 314 puede almacenar la dirección de correo electrónico o el número de teléfono móvil recopilados en el almacén de datos de perfil de usuario 316. El motor de registro de usuario 312 puede generar una dirección de correo electrónico de alias o número de teléfono de alias y almacenar el alias en el almacén de datos de perfil de usuario 316 en asociación con la dirección de correo electrónico o número de teléfono móvil recopilados. Por lo tanto, un usuario puede proporcionar únicamente un único campo de datos al sistema 300 y tener un alias generado en asociación con ese único campo de datos. Por supuesto, también es posible iniciar, ya sea después o en lugar de un procedimiento de registro rápido, un procedimiento de registro más comprensivo durante el cual el motor de recopilación de información personal 314 recopila más datos de un usuario durante el procedimiento de registro y ahorra los datos recopilados en el almacén de datos de perfil de usuario 316.

En una alternativa, el motor de registro de usuario 312 podría generar un id de usuario y el motor de recopilación de información personal 314 podría obtener una contraseña de usuario de un usuario (o el usuario podría proporcionar un id de usuario en lugar de tener uno generado para ello, o además de tener un identificador de usuario o número de usuario generado para ello). Por lo tanto, en esta alternativa, es posible registrar un usuario sin recopilar información sensible. Como se usa en este artículo, "información sensible" se pretende que signifique información personal que es útil para contactar o identificar el usuario fuera del sistema 300, tal como una dirección de correo electrónico, una dirección física, un número de teléfono, o similares. Tal vez la mayoría de información que un usuario almacenaría en un libro de direcciones podría considerarse información sensible, pero un id de usuario que identifica el usuario únicamente en un sistema de gestión de datos controlado no tendría que considerarse información sensible, puesto que la información no posibilitaría que una tercera parte identificara al usuario sin más. Puede observarse que incluso aunque el id de usuario puede no considerarse información sensible, puede aún desearse mantener el id de usuario en confianza.

En una implementación específica, el motor de registro de usuario 312 puede posibilitar que un usuario registre una de dos maneras. Usando la primera manera, un usuario va a un sitio asociado con un sistema de gestión de datos controlado y se registra de una manera conveniente aplicable. La primera vez que un usuario se registra con el sistema de gestión de datos controlado, dependiendo de la implementación, puede solicitarse al usuario que introduzca un valor de clave, tal como una dirección de correo electrónico. Esta puede combinarse o no con la implicación de registro con una entidad de terceros a la que el usuario puede pretender compartir o puede tener ya información personal compartida. Usando la segunda manera, el motor de registro de usuario 312 puede proporcionar un módulo al usuario, que puede embeberse en un explorador u otro sistema asociado con el usuario. El módulo podría proporcionarse también mediante la agrupación con un explorador, sistema o proveedor. El módulo puede activarse automáticamente

tras embeberse en el lado del usuario, o puede activarse por un evento, tal como cuando el usuario selecciona una opción para activar, el usuario va a un sitio particular, el motor de registro de usuario 312 activa el módulo de manera remota, o similares.

5 En una realización específica, el motor de registro de usuario 312 puede solicitar que un usuario seleccione un idioma y a continuación seleccione una opción de "Registro". La opción de registro puede visualizarse en un sitio web asociado con el sistema de gestión de datos controlado, en el explorador del usuario, en un mensaje de correo electrónico enviado al usuario, como una opción de menú, o similares. Tras la selección de la opción para registrar, puede generarse una ventana emergente, puede enviarse al usuario a un sitio asociado con el sistema de gestión de datos controlado, o similares. Después del primer registro, es poco probable que el usuario necesitara de nuevo proporcionar el valor de clave, y puede proporcionársele simplemente la opción para registrar la implicación con una entidad de terceros en registros posteriores.

15 Cuando un usuario se ha registrado o está en registro, el motor de registro de usuario 312 puede registrar registros, actualizaciones, me gusta, cookies, etc., asociados con el valor de clave (por ejemplo, dirección de correo electrónico, número de teléfono, etc.) proporcionados por el usuario ya sea directa o indirectamente mientras que, por ejemplo, se exploran en los sitios. Después de que se han registrado un cierto número de sitios, puede solicitarse al usuario que registre uno o más de los sitios. A modo de ejemplo, pero sin limitación, cuando el usuario se ha registrado en 10 sitios que mantienen información personal del usuario, el motor de registro de usuario 312 puede abrir una ventana con esta lista de sitios y proponer al usuario que se registre en uno o más de los 10 sitios.

25 El motor de registro de usuario 312 puede estar configurado para solicitar información mínima, tal como país de residencia y un valor de clave (por ejemplo, dirección de correo electrónico, número de teléfono, etc.). Sería deseable que el valor de clave sea un valor que el usuario emplea para el fin de hacer compras, suscripciones, redes sociales, u otras actividades. En otras palabras, el valor de clave probablemente no debería ser un valor ficticio. El valor de clave es importante para el sistema de gestión de datos controlado puesto que puede servir como el punto de contacto principal entre el individuo y las entidades de terceros, y el sistema de gestión de datos controlado lo usará para constituir la lista de titulares de datos personales.

30 El motor de registro de usuario 312 puede estar configurado para solicitar o asignar un id de usuario, que puede ser un apodo, la dirección de correo electrónico del usuario, o algún otro valor conveniente, y una contraseña.

35 Cuando se hace un proceso de registro inicial, el motor de registro de usuario 312 puede: 1) mostrar al usuario una lista de sitios donde hay una posibilidad alta de que él haya proporcionado un perfil (Facebook, Google, Amazon, Ebay, MSN, Yahoo!, ISP locales, etc.); 2) pedir al usuario que elija uno al que sabe que ha proporcionado sus datos personales; 3) redirigir al usuario hacia una página de perfil asociada con el sistema de gestión de datos controlado; 4) solicitar que el usuario introduzca su nombre de usuario y contraseña; 5) pedir al usuario que haga clic derecho sobre un logo en su ordenador de sobremesa/explorador y elija "Grabar este perfil"; 6) solicitar que el usuario cambie su dirección de correo electrónico yendo al campo de correo electrónico, haciendo clic derecho a continuación en el logo y elegir "Generar una dirección de correo electrónico de alias", que sustituirá su dirección de correo electrónico en el campo y el campo de confirmación también. El usuario puede a continuación grabar el formulario. Todos los correos electrónicos enviados por esta compañía a la nueva dirección de correo electrónico de alias se reenviarán a la dirección de correo electrónico anterior.

45 Después de que un usuario se ha registrado, la información de usuario puede continuar recopilándose. En una implementación específica, el motor de recopilación de información personal 314 puede iniciar un procedimiento para enviar un módulo de software a una máquina asociada con el usuario o el usuario puede iniciar un procedimiento para descargar un módulo de software a una máquina asociada con el usuario. El módulo de software puede incluir procedimientos que facilitan la implementación de un motor de transparencia de compartición de datos en la máquina del usuario (véase, por ejemplo, la Figura 1, el motor de transparencia de compartición de datos 112). Como alternativa, en lugar de poner un módulo de software en la máquina del usuario, los registros a un servicio de gestión de datos controlado pueden incluir enlaces de su sitio al sistema 300.

55 En general, el motor de recopilación de información personal 314 puede recopilar datos mediante el proceso Open Social, mediante un proceso de sistema de gestión de datos controlado, mediante un robot, mediante sitios/anuncios/medios u otras técnicas aplicables. La especificación OpenSocial v0.9, con fecha del 15 de abril de 2009, de OpenSocial and Gadgets Specification Group se incorpora por referencia. El usuario puede autorizar al sistema de gestión de datos controlado para usar información de recuperar y/u obtener datos de sitios de interconexión de red social que usan la norma Open Social.

60 El proceso de sistema de gestión de datos controlado, además de o en lugar de usar un motor de transparencia de compartición de datos en una máquina del usuario (véase, por ejemplo, la Figura 1, motor de transparencia de compartición de datos 112), que posibilita que el usuario capture datos para marcas comerciales/sitios cuando registra o actualiza información personal en los respectivos sitios o, en general, cuando proporciona información personal a una tercera parte. El proceso del sistema de gestión de datos controlado puede incluir dos procesos diferentes: 1) El usuario ya ha proporcionado información personal y desea grabar los datos a un perfil en el sistema de gestión

controlado. Cuando está en, por ejemplo, una página de perfil personal, el usuario puede hacer clic derecho, por ejemplo, en un botón visualizado en un ordenador de sobremesa del usuario, en un explorador, en un teléfono inteligente, etc., y elegir grabar la información personal a un perfil asociado con el usuario (nota: en una implementación específica, cada usuario puede tener múltiples perfiles). Puede ser deseable detectar que el usuario ha proporcionado información personal y realiza automáticamente la actualización, de manera presumible de acuerdo con preferencias de usuario, sin pedir nada del usuario. 2) El usuario está introduciendo o actualizando información personal. El proceso de gestión de datos controlado que reside en el ordenador de sobremesa del, explorador, o similares puede interceptar datos que se introducen y puede ahorrar automáticamente los datos a un perfil relevante del usuario. En cualquiera de los casos 1) y 2), cuando el usuario sale de una página o alcanza de otra manera un punto que puede caracterizarse como que completa la entrada de datos, el proceso de gestión de datos controlado puede recapitular que va a enviarse al sistema de gestión de datos controlado, y el usuario tiene que validar la información personal y/o confirmar que los datos deberían enviarse al sistema de gestión de datos controlado.

Con un robot, el proceso de gestión de datos controlado puede usar información de inicio de sesión de un usuario (presumiblemente de acuerdo con preferencias de usuario) para acceder a sitios y obtener información personal en los sitios. Los sitios pueden presentarse como una lista para el usuario, que puede elegir a qué sitios debería acceder el sistema de gestión de datos controlado. Esto puede conseguirse, por ejemplo, ejecutando un robot en la página de perfil en cada sitio aplicable, que puede rastrear la página de contenido y capturar automáticamente la información personal mantenida por el sitio. Normalmente esto requeriría un acuerdo de cada sitio para permitir que el robot rastree su sitio. A través de un proceso similar, el robot puede usarse también para actualizar información personal en el sitio que ha cambiado desde que el usuario proporcionó por último los datos.

Un usuario puede permitir que el sistema de gestión de datos controlado solicite entidades de terceros, tal como anunciantes, proveedores de medios, compañías, sitios web, etc., tal vez cuando las entidades mantienen al menos una de la dirección de correo electrónico individual/número de teléfono móvil del usuario (que coincide con un proceso de base de datos para hacerse con una tercera parte) para enviar alguna o toda la información personal relacionada que tienen sobre el usuario. El sistema de gestión de datos controlado puede solicitar también datos con respecto al uso de cookies en el sitio (pueden usarse cookies para hacer focalización de comportamiento). El usuario puede obtener, con el tiempo, una lista cada vez más comprensiva de marcas comerciales/compañías. Esto puede posibilitar que el usuario clasifique por direcciones de correo electrónico/números de teléfonos móviles. Puede ser deseable hacer que una tercera parte (tal como Axiom) realice la extracción de correos electrónicos/números de teléfonos móviles comunes entre usuarios del sistema de gestión de datos controlado y abonados de la entidad de terceros al sistema de gestión de datos controlado. Cuando se extrae la lista de correos electrónicos/números de teléfonos móviles comunes, a continuación un abonado de entidad puede extraer los datos personales que mantiene cada miembro de la lista. El abonado de entidad puede a continuación enviar los datos al sistema de gestión de datos controlado a través de un proceso asegurado y almacenado en el sistema de gestión de datos controlado. Como alternativa, podría solicitarse que los sitios envíen a únicamente contenedores de datos pero no el contenido.

El sistema de gestión de datos controlado puede etiquetar entidades que acuerdan participar por, por ejemplo, entrega un logo que puede ponerse en su sitio web para indicar a los visitantes que están certificados. Puede haber múltiples logos que reflejan el nivel de transparencia (compartición de datos personales, focalización de comportamiento, revender/proporcionar direcciones de correo electrónico a terceros que son publicidad no deseada o no, etc...), una calificación emitida de otros usuarios, o similares. Como otro ejemplo, el sistema de gestión de datos controlado puede certificar entidades cambiando color u otras características de un logo que está en exploradores de los usuarios, ordenadores de sobremesa, etc., de manera que cuando los usuarios entran en el sitio, conocerán muy rápidamente si el sitio está participando en el programa de gestión de datos controlados. Como otro ejemplo, a las entidades podría proporcionárseles la opción de enviar automáticamente un correo electrónico a usuarios pertinentes que están registrados con el sistema de gestión de datos controlado.

Las entidades de terceros pueden estar también motivadas para participar para tener su información en una lista de compañías de transparencia de compartición de datos del usuario con las que el usuario tiene información personal compartida. Esto podría evitar y/o complementar, por ejemplo, el proceso Axiom.

Para entidades de terceros que no aceptan enviar información al sistema de gestión de datos controlado (y/o aquellas que no han aceptado, pero aún no han rechazado), el sistema de gestión de datos controlado puede tener un color específico del logo que los usuarios puedan haber instalado en su máquina. A continuación, los usuarios conocerán tan pronto como estén entrando en un sitio que no están enviando información al sistema de gestión de datos controlado. Sin embargo, si el usuario desea registrar o actualizar información personal, el usuario puede usar un motor de transparencia de compartición de datos para grabar la información en el sistema de gestión de datos controlado.

Ejemplos de datos que podrían recopilarse y grabarse:

Ejemplo 1 (contenedor):

Correo electrónico: joe.smith@ejemplo.com

¿Nombre?: Sí/No
 ¿Apellidos?: Sí/No
 ¿Fecha de nacimiento?: Sí/No
 ¿Dirección?: Sí/No
 ¿Código postal?: Sí/No
 ¿Ciudad?: Sí/No

5

Ejemplo 2 (contenedor y contenido):

Correo electrónico: joe.smith@ejemplo.com
 Nombre: Joe
 Apellidos: Smith
 Fecha de nacimiento: 01/01/1970
 Dirección: 234 Calle de ejemplo
 Código postal: 99999
 Ciudad: Ciudad de ejemplo
 País: País de ejemplo

10

15

Ejemplo 3 (contenedor)

Correo electrónico: joe.smith@ejemplo.com
 ¿Nombre?: Sí/No
 ¿Nombre?: Sí/No
 ¿Fecha de nacimiento?: Sí/No
 ¿Compañía?: Sí/No
 ¿Título en compañía?: Sí/No
 ¿Foto?: Sí/No
 ¿Dirección de correo electrónico compartida con otras compañías?: Sí/No
 ¿Cookie en máquinas de usuario?: Sí/No

20

25

30

Ejemplo 4 (contenedor):

Número de teléfono móvil: 999 99 99 99 99
 ¿Nombre?: Sí/No
 ¿Nombre?: Sí/No
 ¿Género?: Sí/No
 ¿Intervalo de edad?: Sí/No

35

40

Además de correo electrónico y número de teléfono móvil, que se tratan como claves en estos ejemplos, los otros campos no se rellenan necesariamente con su valor, sino únicamente: Sí / No, que significa de propiedad o no.

45

En una implementación específica, un usuario puede crear/actualizar un perfil para posibilitar pre-llenar campos automáticamente durante el registro en sitios y actualizar una vez en el sistema de gestión de datos controlado algunos datos (por ejemplo, dirección doméstica después de un movimiento) y pedir al sistema de gestión de datos controlado que envíe la actualización a las entidades relevantes.

50

El sistema de gestión de datos controlado puede usar un sistema de gestión de datos convencional y distribuido para almacenar datos de una manera segura, una solución tal como Cassandra para gestionar los datos y bases de datos no relacionales, o alguna otra solución que cumpla las necesidades de escalabilidad, seguridad y otros asuntos aplicables.

55

60

65

Ventajosamente, a medida que los usuarios y abonados de terceros se vuelven más integrados en el sistema de gestión de datos controlado, los datos personales de un individuo pueden asumir las propiedades de objetos en el mundo físico que existen únicamente en un lugar a la vez. Es decir, el usuario sabrá dónde reside su información personal. Con esta clase de control, un usuario puede proporcionar a las compañías permiso para acceder a cierta información personal para un periodo de tiempo (y a continuación detener el acceso). Esto podría significar finalmente que las compañías obtendrían, en lugar de alguna información personal: un identificador único no reversible «U_Id» generado por el sistema de gestión de datos controlado que representa al individuo (encriptación de correo electrónico/número de teléfono móvil) tal vez con una caducidad de validez (fin del periodo de tiempo que el usuario ha autorizado a la compañía para usar sus datos); todos los datos personales que hubiera declarado/proporcionado el individuo a esta compañía se accederían a continuación por la compañía para un periodo de tiempo a través de una gestión de datos controlados API; al final del periodo, la API desconectaría el «U_Id» de los datos que por lo tanto la compañía no podría acceder a los datos personales del individuo. Otra ventaja es que para asegurar que la siguiente vez que el usuario vuelva a entrar en una relación con una entidad de terceros, el usuario no tendría que volver a introducir toda la información, que puede mantenerse en el sistema de gestión de datos controlado o en la máquina del usuario. Lo que las compañías podrían mantener es tal vez algún dato agregado (edad/rango de ingresos, ciudad,

...) para realizar estadísticas.

La Figura 4 representa un ejemplo de un sistema de generación de alias de información personal 400. Cuando un usuario precede a la declaración de información personal durante una compra o registro en un sitio de internet/móvil (por ejemplo, interconexión de red social, sitio web del editor, marca comercial, estudios de compañía, etc.), el sistema de generación de alias de información personal 400 puede generar, por ejemplo, una dirección de correo electrónico única (un alias de correo electrónico) para este sitio/marca comercial que será el buzón de correo usado para el usuario. En una implementación específica, el usuario asocia un correo electrónico personal con el alias de correo electrónico. Puede observarse que la generación de alias de información puede conseguirse durante un periodo de registro (véase, por ejemplo, la Figura 3) para un primer alias, y puede usarse un procedimiento idéntico o similar para registrar segundos alias o posteriores. Por lo tanto, "registro" puede hacer referencia a un registro de usuario cualquiera (una primera vez) o registro de entidad (cada vez o después de la primera vez).

En el ejemplo de la Figura 4, el sistema 400 incluye una interfaz de red 402, un motor de anonimización de información personal 404, un almacén de datos de información personal anónima 406, un almacén de datos de perfil de usuario 408, un almacén de datos de alias específico de empresa 410, y un motor de aprovisionamiento de información específico de empresa de alias 412. El sistema 400 puede implementarse en un servidor de compartición de datos controlado (véase, por ejemplo, la Figura 1, el servidor de compartición de datos controlado 104). Sin embargo, el servidor puede mantener o no información personal en el almacén de datos de información personal anónima 406, y puede mantener o no alguna o toda la información personal proporcionada de un usuario a una tercera parte.

La interfaz de red 402 puede incluir diverso hardware y/o componentes de software, como se describe más adelante con referencia a las Figuras 7 y 8. La interfaz de red 402 está acoplada al motor de anonimización de información personal 404 y al motor de aprovisionamiento de información personal específica de empresa de alias 412.

En el ejemplo de la Figura 4, en la operación, el sistema 400 recibe datos en la interfaz de red 402. Hasta el punto que los datos incluyen información personal, el motor de anonimización de información personal 404 almacena la información personal en el almacén de datos de información personal anónima 406 al que está acoplado. En lugar de información personal, los datos podrían incluir campos o contenedores de datos que están asociados con información personal. El almacén de datos de perfil de usuario 408, también acoplado al motor de anonimización de información personal 404, puede incluir un registro asociado con un usuario particular que posibilita que el contenedor se rellene con datos del almacén de datos de perfil de usuario 408.

Como alternativa, el sistema 400 podría posibilitar generar alias sin almacenar información personal alguna, pero en una implementación de este tipo, puede no poder enviar mensajes al usuario; el usuario tal vez tendría que iniciar sesión en el sitio de gestión de datos controlados. Sin embargo, es razonablemente probable que el usuario tenga que proporcionar información personal a terceros si ninguna se almacena en el sistema de gestión de datos controlado. Si, por otra parte, al menos alguna información personal se almacena en el sistema de gestión de datos controlado, las entidades de terceros pueden confiar que un usuario es real mediante el hecho de que el usuario está registrado con un sistema de gestión de datos controlado y tal vez posibilite que un usuario proporcione únicamente valores ficticios o alias en lugar de información personal.

Como alternativa, puede ser deseable implementar un sistema en el que no se proporciona información personal o relativamente poca a entidades de terceros. En una implementación de este tipo, el hecho de que el usuario tenga un perfil de usuario puede servir como evidencia adecuada de que el usuario es real. De esta manera, los sitios que se basan en información personal para certificar que un usuario podría basarse en su lugar en el servidor independiente para confirmar que el usuario debería estar permitido a acceder a un servicio particular sin requerir que se envíe realmente información personal alguna. Dependiendo de la implementación, el contenedor podría rellenarse con valores ficticios, alias, o dejarse vacío.

Un campo de información personal que es de significado particular para correspondencia electrónica es la dirección de correo electrónico del usuario (para implementaciones de comunicaciones móviles, el número de teléfono móvil de un usuario es de significado particular). La dirección de correo electrónico personal del usuario no se proporciona a terceros, y puede o no almacenarse en el almacén de datos de perfil de usuario 408. En su lugar, el motor de anonimización de información personal 404 genera un alias para el usuario, que se almacena en el almacén de datos de alias específico de empresa 410 al que está acoplado. Para que el sistema 400 pueda generar el alias para cada entidad de terceros, el usuario debe de alguna manera (la técnica puede depender de la implementación) informar al sistema que la información personal ha de proporcionarse a una empresa. Esto podría proporcionarse a un URL asociado con la empresa al sistema 400. Para simplicidad ilustrativa, se supone que el URL u otros datos de identificación están incluidos en los datos proporcionados del usuario al motor de anonimización de información personal 404 o pueden hallarse en el almacén de datos de perfil de usuario 408 e identificarse usando datos proporcionados por el usuario. El URL podría obtenerse también a través de suscripción de entidad de terceros al sistema de gestión de datos controlado, e implicarse identificando al usuario en el sitio de entidad de terceros a través del uso de un módulo de extensión de explorador, notificación por la entidad de terceros, o similares. Para evitar que se pida al usuario generar un alias de correo electrónico en cualquier momento que lo introduzca (por ejemplo, en inicio de sesión), los URL pasados al sistema 400 podrían clasificarse e identificarse con el tiempo. Si se pide al usuario

por error que genere alias de un correo electrónico, podría ofrecerse al usuario una opción para informarlo al sistema, que puede entonces mejorar con el tiempo.

Ventajosamente, se genera un alias para cada entidad de terceros (o grupo de entidades). Por lo que si una entidad de terceros comparte datos con otras partes que intentan entrar en contacto con el usuario, el sistema de gestión de datos controlado podrá detectar que el alias específico de la entidad se está usando por una parte para la que no se generó el alias. El sistema de gestión de datos controlado y/o el usuario pueden a continuación decidir cómo tratar el tercero esa información personal compartida y/o la otra parte que presumiblemente obtuvo la información personal del tercero.

Puede observarse que en una implementación que incluye proporcionar información personal real, tal como nombre, número de teléfono, o similares, la información personal aún se hace referencia como "anónima" en este artículo cuando se proporciona el alias de correo electrónico en lugar de una dirección de correo electrónico personal real. Aunque puede ser posible rastrear a un usuario para el que una empresa tiene un nombre u otra información personal, la dirección de correo electrónico puede mantenerse en secreto. Por lo tanto, el término "anónimo", como se usa en este artículo, puede hacer referencia a anonimidad completa cuando no se proporciona información personal, alguna anonimidad cuando únicamente se proporciona un subconjunto de datos solicitados, y al menos anonimidad de correo electrónico cuando se proporciona toda la información personal solicitada (cuando una dirección de correo electrónico solicitada se sustituye por una dirección de correo electrónico de alias). Cuando se desea una distinción entre los niveles de anonimidad, "anonimidad completa" puede hacer referencia a cuando no se proporciona información personal a una empresa y "anonimidad de correo electrónico" puede hacer referencia a cuando se sustituye al menos la dirección de correo electrónico del usuario por una dirección de correo electrónico de alias. También es posible tener "anonimidad de teléfono", o más específicamente "anonimidad de teléfono móvil", o alguna otra forma de anonimidad asociada con un campo de información personal particular que se sustituye por un valor de alias o se retiene de otra manera.

En el ejemplo de la Figura 4, el motor de aprovisionamiento de información personal específica de empresa de alias 412, que está acoplado al motor de anonimización de información personal 404, combina información personal del almacén de datos de información personal anónima 406 con el alias de correo electrónico pertinente del almacén de datos de alias específico de empresa 410. El motor de aprovisionamiento de información personal específica de empresa de alias 412 envía los datos a la empresa pertinente mediante la interfaz de red 402. Como se ha mencionado anteriormente, la información personal puede incluir contenedores vacíos, valores ficticios, o alias; y el usuario puede proporcionar la información personal sin pasar la información a través del sistema de gestión de datos controlado. También, en una implementación específica, el motor de aprovisionamiento de alias de información personal específica de empresa 412 puede proporcionar el alias al usuario de modo que el usuario puede proporcionar el alias en asociación con cualquier otra información personal a una entidad de terceros sin el sistema 400 que está implicado en el procedimiento de registro. El alias aún dará como resultado correspondencia de la entidad de terceros que proviene del sistema de gestión de datos controlado para análisis y reenvío al usuario, y el usuario puede desear corresponder con la entidad de terceros enviando un mensaje al sistema de gestión de datos controlado, que puede sustituir la información de contacto del usuario con el alias pertinente. Esto puede incluir o no filtrar firmas de correo electrónico para información de contacto que no está con alias, ya sea eliminando o sustituyendo los elementos de acuerdo con preferencias de usuario, o alertando al usuario que un mensaje puede incluir información sensible.

La Figura 5 representa un ejemplo de un sistema de servidor de correo electrónico a nivel de alias 500. Cuando se usa una dirección de correo electrónico de alias en lugar de una dirección de correo electrónico personal para registrar o actualizar un perfil en un sitio, y si el sitio vende o proporciona tal información a otra compañía que usa el alias de correo electrónico para contactar con el usuario (tal vez sin haber recibido autorización), el usuario puede aprender de este evento usando el sistema de servidor de correo electrónico a nivel de alias 500. Esto puede posibilitar que el usuario identifique la compañía que envió el correo electrónico y la compañía que compartió la información. A continuación, el usuario puede actuar como el usuario considere apropiado, tal como bloqueando correos electrónicos de la nueva compañía y/o entrando en contacto con la entidad que compartió la información a reclamar. Por supuesto, este servicio opera en cascada (la Compañía A vende al correo electrónico de la Compañía B - envía un mensaje - que a su vez se vende a la Compañía C - que envía un mensaje - etc ...). Puede observarse que la mayoría del tiempo las compañías que comparten información personal están dentro de su derecho puesto que la práctica se menciona en sus términos de uso, pero el usuario no es consciente necesariamente.

En el ejemplo de la Figura 5, el sistema de servidor de correo electrónico a nivel de alias 500 incluye una interfaz de red 502, un servidor de correo electrónico 504, un motor de monitorización de correo electrónico 506, un almacén de datos de alias de correo electrónico específico de empresa 508, un almacén de datos de preferencias de usuario 510, un almacén de datos de reglas de manejo de correo electrónico 512, y un motor de personalización de correo electrónico 514. La interfaz de red 502 puede incluir diverso hardware y/o componentes de software, como se describe más adelante con referencia a las Figuras 7 y 8. La interfaz de red 502 está acoplada al servidor de correo electrónico 504.

En el ejemplo de la Figura 5, el servidor de correo electrónico 504 está acoplado al motor de monitorización de correo electrónico 506 y al motor de personalización de correo electrónico 514. El servidor de correo electrónico 504 puede

operarse para recibir correo electrónico de una empresa mediante la interfaz de red 502 y para enviar correo electrónico personalizado a un usuario mediante la interfaz de red 502. En una implementación específica en la que el usuario asocia un correo electrónico personal con un alias de correo electrónico, un motor de análisis de correo electrónico independiente puede funcionar sin sustituir un servidor de correo para ofrecer a los usuarios una "lectura" personalizada y útil de mensajes comerciales. Por lo que el servidor de correo electrónico podría implementarse en una máquina de terceros, y el servidor de correo electrónico 504 podría denominarse como un "servidor de monitorización de correo electrónico".

En el ejemplo de la Figura 5, el motor de monitorización de correo electrónico 506 está acoplado al almacén de datos de alias de correo electrónico específico de empresa 508, al almacén de datos de preferencias de usuario 510, y al almacén de datos de reglas de manejo de correo electrónico 512. Se supone para fines de ilustración que se usó un sistema de generación de alias de información personal (véase, por ejemplo, la Figura 2, el sistema 200) para crear un alias de correo electrónico para un usuario. Puesto que el alias de correo electrónico es específico a una entidad particular, el motor de monitorización de correo electrónico 506 puede mapear el destino de correo electrónico de un correo electrónico recibido de una empresa a un usuario particular que usa el almacén de datos de alias de correo electrónico específico de empresa 508. El motor de monitorización de correo electrónico 506 puede hacer una determinación basándose en el origen del correo electrónico recibido en cuanto a si el correo electrónico es de la entidad con la que está asociado el alias de correo electrónico. Por lo tanto, el motor de monitorización de correo electrónico 506 puede actuar como un sistema de advertencia que un alias ha sido comprometido.

El motor de monitorización de correo electrónico 506 puede comprobar el almacén de datos de preferencias de usuario 510 y el almacén de datos de reglas de manejo de correo electrónico 512 para determinar cómo tratar el mensaje de correo electrónico recibido. Por ejemplo, si las preferencias de usuario indican que el alias de correo electrónico ya no está más activo debido a un límite de tiempo en la vida del alias de correo electrónico, el motor de monitorización de correo electrónico 506 puede filtrar el correo electrónico.

Como otro ejemplo, si el alias de correo electrónico es evidente a partir de una entidad distinta de la entidad con la que está asociado el alias, el motor de monitorización de correo electrónico 506 puede manejar el correo electrónico de acuerdo con preferencias de usuario y tomar otras acciones de acuerdo con reglas de manejo de correo electrónico, tal como notificar a la (primera) entidad asociada con el alias para averiguar por qué una segunda entidad usó el alias de correo electrónico. El uso del alias de correo electrónico por la segunda entidad puede ser indicativo de compartición de información personal. Las preferencias de usuario pueden incluir una preferencia para que se notifique cuándo se usa un alias de correo electrónico por una entidad con que no está asociada. Puesto que, en una implementación específica, el usuario tiene acceso a una lista de entidades que han enviado un correo electrónico sin recibir el consentimiento específico del usuario (a priori), el usuario puede establecer una preferencia para provocar que el motor de monitorización de correo electrónico 506 actúe como un filtro de publicidad no deseada en una o más de estas compañías. Más en general, un usuario puede establecer preferencias para filtrar cualquier correo electrónico que provenga de una compañía específica.

Como otro ejemplo, el motor de monitorización de correo electrónico 506 puede almacenar datos asociados con el correo electrónico en un almacén de datos histórico (no mostrado). Para sitios de comercio electrónico en los que un usuario ha proporcionado un alias de correo electrónico y realizado una compra, el motor de monitorización de correo electrónico 506 puede analizar el contenido de correos electrónicos de confirmación enviados cada vez que se realiza una compra, y facilita el acceso por los usuarios a una vista sintética de todas las compras de Internet para la semana, mes, trimestre, año. Esto puede proporcionar una vista evidente de gasto por tipo de producto, proporcionar una vista evidente de gasto familiar, y permitir la identificación de fraude, que está empezando a ser un gran problema para fines de detección cuando los gastos son por pequeñas cantidades, tal como canciones de iTunes.

Los datos históricos pueden usarse también para promociones. Por ejemplo, a través de una interfaz de motor de búsqueda, puede presentarse a un usuario promociones con respecto a un tipo particular de producto/marca comercial. Esto podría ser una síntesis de promociones para un producto/marca comercial por interés de usuario según se predice por los datos históricos.

En el ejemplo de la Figura 5, el motor de personalización de correo electrónico 514 está acoplado al servidor de correo electrónico 504, al motor de monitorización de correo electrónico 506, al almacén de datos de correo electrónico específico de empresa 508, y al almacén de datos de preferencias de usuario 510. Cuando un usuario envía un correo electrónico a una entidad de terceros, el motor de personalización de correo electrónico 514 puede eliminar información sensible, sustituir la información sensible con valores ficticios o alias, o similares. Aunque el motor de personalización de correo electrónico 514 puede configurarse para identificar automáticamente ciertas cadenas de caracteres que es probable que incluyan información sensible, tal como direcciones de correo electrónico, URL, números de teléfono, números de tarjeta de crédito, u otras cadenas de caracteres que tienen formatos distintivos, cuanto más información proporcione un usuario al sistema de gestión de datos controlado, más efectivo será el motor de personalización de correo electrónico 514 al anonimizar información. Por ejemplo, si el motor de personalización de correo electrónico conoce el número de teléfono del usuario y también conoce que la entidad de terceros a la que se está enviando un correo electrónico tiene un valor ficticio para el número de teléfono, el motor de personalización de correo electrónico 514 puede sustituir un número de teléfono en el bloque de firma del correo electrónico con el valor ficticio (de manera

presumible de acuerdo con preferencias de usuario).

5 Cuando un usuario recibe correo electrónico de una entidad de terceros, el motor de personalización de correo electrónico 514 puede actualizar el correo electrónico con información útil. Por ejemplo, el alias de correo electrónico del usuario puede sustituirse por la dirección de correo electrónico real del usuario de modo que el mensaje puede enviarse al usuario, puede consultarse el almacén de datos de alias de correo electrónico específico de empresa 508 para confirmar que el correo electrónico proviene de la entidad con la que está asociado el alias y tomar acciones correctivas si el alias no está asociado con el emisor, puede incluirse un indicador de confianza en el correo electrónico para indicar el nivel de confianza que ha considerado el sistema de gestión de datos controlado a la entidad de terceros (por ejemplo, si otros usuarios están recibiendo publicidad no deseada de una primera identidad a un alias que se proporcionó a una segunda entidad, la confianza en la segunda entidad puede reducirse incluso antes de que el usuario actual reciba la publicidad no deseada; y/o el indicador podría mostrar que la entidad de terceros no es un abonado al sistema de gestión de datos controlado, ha rechazado hacerse un abonado, o es un abonado), puede incluirse información histórica pertinente o de análisis (por ejemplo, última transacción o transacciones con la compañía, los últimos 4 números de la tarjeta de crédito usada en la transacción, la cantidad total de transacciones con la compañía, la cantidad reciente de transacciones con la compañía, etc.), hiperenlaces personalizados a palabras que son de relevancia para el sistema de gestión de datos controlado (por ejemplo, alias de usuario o valores ficticios que pueden hacerse hipervínculos para posibilitar que el usuario acceda a los valores reales, valores que no parecen haberse proporcionado por el usuario a la entidad de terceros podrían hacerse hipervínculos para posibilitar que el usuario actualice contenedores o valores en el sistema de gestión de datos controlado o para tomar otras acciones si la entidad de terceros no debiera tener la información), los alias o valores ficticios podrían sustituirse o los valores reales podrían añadirse entre paréntesis cerca de los alias o valores ficticios, o similares.

25 En una implementación específica, podría usarse un sistema similar al sistema 500, pero para aplicaciones de teléfono que generan el alias del número de teléfono del usuario en lugar de la dirección de correo electrónico del usuario. Podrían implementarse también otros sistemas similares, tal como un sistema de dirección geográfica. Y los diversos sistemas podrían combinarse para posibilitar múltiples alias para diverso contacto u otra información de identificación.

30 La Figura 6 representa un ejemplo de un sistema 600 para proporcionar servicios a un usuario de un sistema de gestión de datos controlado. En el ejemplo de la Figura 6, el sistema 600 incluye una interfaz de red 602, un motor de registro 604, un motor de suministro de contenido 606, un motor testimonial 608, un módulo de mis datos personales 610, un módulo de lista de titulares de datos 612, un módulo de análisis y filtración de publicidad no deseada 614, un módulo de análisis de comercio electrónico 616, un módulo mercado 618, un módulo de búsqueda de producto 620, y un módulo de preferencias de introducción 622. Ventajosamente, puesto que los usuarios pueden proteger sus identidades de manera eficaz usando alias, puede construirse un mercado en la parte superior de un sistema que hace uso de las técnicas descritas en este artículo. Los datos personales no necesitan almacenarse realmente en un servidor centralizado (por ejemplo, podrían almacenarse en un ordenador personal y proporcionarse según fueran necesarios usando un módulo de extensión, o de alguna otra manera, tal como se describe en cualquier otra parte en este artículo).

40 En el ejemplo de la Figura 6, la interfaz de red 602 está acoplada al motor de registro 604. Un ejemplo de un motor de registro se ha descrito anteriormente (véase, por ejemplo, la Figura 3, el motor de registro de usuario 312).

45 En el ejemplo de la Figura 6, la interfaz de red 602 está acoplada al motor de suministro de contenido 606. El motor de suministro de contenido 606 puede proporcionar a los usuarios con, potencialmente entre otras cosas, opciones para gestionar su información personal. Por ejemplo el motor de suministro de contenido 606 puede posibilitar que un usuario seleccione una "lista de titulares de datos" para ver datos personales mantenidos por un sitio, ya sea en general o específicamente con respecto al usuario, y un enlace para accederlos. Como otro ejemplo que es de relevancia particular a sitios de comercio electrónico, cuando un usuario compra algo, un motor de monitorización de correo electrónico puede analizar un correo electrónico enviado por un sitio de comercio electrónico de manera que el usuario puede ver una síntesis de una última compra, o una combinación de compras, usando "análisis de comercio electrónico". Como otro ejemplo, el motor de suministro de contenido 606 puede posibilitar "análisis de publicidad no deseada" que puede ser una opción de menú destacada cuando hay algo nuevo en la carpeta de análisis de publicidad no deseada. Si un primer sitio al que el usuario ha proporcionado información personal comparte la información con un segundo sitio que a continuación usa un alias que está asociado con el primer sitio, un motor de monitorización de correo electrónico puede detectar el uso del alias por el segundo sitio. El usuario puede seleccionar una acción apropiada o preferencia en asociación con publicidad no deseada.

60 En el ejemplo de la Figura 6, la interfaz de red 602 está acoplada al motor testimonial 608. El motor testimonial 608 puede posibilitar que un usuario recomiende el sistema de gestión de datos controlado a un amigo a través de facebook, twitter, o algún otro canal de recomendación. El motor testimonial 608 puede facilitar también la entrada de recomendaciones o comentarios en abonados de entidad de terceros, productos, etc., al sistema.

65 En el ejemplo de la Figura 6, el módulo de mis datos personales 610 está acoplado al motor de suministro de contenido 606. El motor de suministro de contenido 606 puede usar el módulo para proporcionar acceso a los datos personales que ha introducido el individuo (por ejemplo, correo electrónico, país, número de teléfono móvil, etc.). Como con cada

uno de los módulos, y en general cualquier módulo descrito en este artículo, el módulo puede tratarse como parte de un motor, tal como el motor de suministro de contenido 606. Los módulos pueden ser también representativos de botones u opciones de menú en un sitio web u otra pantalla.

5 En el ejemplo de la Figura 6, el módulo de lista de titulares de datos 612 está acoplado al motor de suministro de contenido 606. El motor de suministro de contenido 606 puede usar el módulo para posibilitar que un usuario vea una lista de compañías que están manteniendo su información personal y qué campos se están manteniendo para una compañía particular (ya se visualicen en la lista o cuando se seleccione la compañía de la lista para visualizar más detalles). El usuario también puede ver qué campos se requieren en la compañía, que son opcionales, que se rellenan con valores ficticios (suponiendo que el sistema de gestión de datos controlado conoce qué valores son valores ficticios), cuáles son alias, cuáles son nulos (por ejemplo, si el titular de datos de terceros se sabe que recopila un campo de datos particular, pero no tiene datos en ese campo para el usuario), o similares. Dependiendo de las capacidades del sistema 600, un usuario puede poder tomar algunas acciones en asociación con los titulares de datos, tal como anular el registro a un boletín de noticias/promociones; optar por salir de su base de datos; optar por salir del rastreo de comportamiento (cookies, ...); calificar la compañía; acordar enviar un perfil actualizado a la compañía (cuando se cambia una dirección, número de teléfono, etc...); o similares.

20 En el ejemplo de la Figura 6, el módulo de análisis y filtrado de publicidad no deseada 614 está acoplado al motor de suministro de contenido 606. El motor de suministro de contenido 606 puede usar el módulo para posibilitar que un usuario vea una lista de compañías que están usando un alias de manera incorrecta (por ejemplo, enviando un correo electrónico a una dirección de correo electrónico de alias que no está asociada con la compañía), parece que están compartiendo información personal con otras compañías (por ejemplo, debido a que una segunda compañía ha usado un alias de correo electrónico asociado con la primera compañía), etc. El usuario también puede establecer preferencias de filtrado para las compañías en particular, o más en general para cualquier compañía que use incorrectamente un alias o parezca que está compartiendo información personal. Por lo tanto, el motor de suministro de contenido 606 puede actuar como un sistema de advertencia de identidad comprometida. En una implementación específica, el sistema 600 puede tener un motor de suministro de contenido centralizado asociado con múltiples usuarios que, sin compartir información entre usuarios, puede identificar tendencias que comprometen la identidad y alertar a otros usuarios de modo que puedan ser proactivos con respecto a un riesgo de comprometer la identidad.

30 En el ejemplo de la Figura 6, el módulo de análisis de comercio electrónico 616 está acoplado al motor de suministro de contenido 606. El motor de suministro de contenido 606 puede usar el módulo para analizar correos electrónicos de un sitio de comercio electrónico asociado con compras de usuario, proporcionar hábitos de compra históricos y cantidades en un formato conveniente, o similares.

35 En el ejemplo de la Figura 6, el módulo de mercado 618 está acoplado al motor de suministro de contenido 606. El motor de suministro de contenido 606 puede usar el módulo para permitir que un usuario trate la información personal del usuario como un recurso. Por ejemplo, el módulo puede facilitar la venta de datos personales o datos estadísticos en el perfil de usuario, ver ofertas para datos personales o estadísticos, gestionar participaciones con entidades de terceros a los que el usuario ha proporcionado información personal, o similares.

45 El coste de obtener información personal de usuarios dependerá probablemente del nivel de aceptación. Factores pueden incluir: si un usuario acuerda introducir una relación con una entidad y proporcionar algunos datos personales; si un usuario acuerda que sea focalizado (publicidad) basándose en su comportamiento; si un usuario acuerda que sea orientado de acuerdo con su localización (móvil); si un usuario comunica más información personal (intereses, hobbies, ...); o similares.

50 Para entidades de terceros, el mercado les posibilitaría ofrecer búsqueda de contactos cualificada, tal como, por ejemplo, "Estoy buscando una mujer de 20 a 25 años de edad de Londres que esté interesada en...." En una implementación particular, las entidades de terceros pueden pagar al sistema de gestión de datos controlado por contacto cualificado dependiendo del nivel de datos personales compartido por el individuo y su compromiso y el país. Este pago únicamente está relacionado con el reclutamiento y no incluye el pago/oferta propuesto por la compañía a cambio de, por ejemplo, participación de usuario en un estudio, información personal adicional, trabajos, etc. Puede ser deseable para el sistema de gestión de datos controlado permanecer fuera del medio de una relación entre un usuario y una entidad de terceros. En el caso de una subasta del perfil de usuario (datos personales o estadísticos), la empresa que desee acceder a este lugar de subasta puede tener que pagar una suscripción mensual de y €.

60 El sistema de gestión de datos controlado puede retornar, por ejemplo, el X % de cuota de reclutamiento a usuarios que están pagando por servicios. La matemática para el X % puede depender, por ejemplo, del nivel de facturación mensual individual, tal como el 50 % si el usuario está pagando por debajo de 2 \$ por mes, el 70 % si él está pagando entre 2 \$ y 5 \$ al mes, y el 90 % si él está pagando más de 5 \$ al mes. Estos números se proporcionan a modo de ejemplo únicamente.

65 En el ejemplo de la Figura 6, el módulo de búsqueda de producto 620 está acoplado al motor de suministro de contenido 606. El motor de suministro de contenido 606 puede usar el módulo para facilitar búsquedas de producto con un motor de búsqueda, usar datos históricos para recomendar productos similares a aquellos que se han

- comprado antes, hacer comparaciones de precio o similares. Ventajosamente, el sistema 600 puede usar ciertas preferencias del usuario y datos personales para recoger datos sobre productos o solicitar ofertas usando un alias temporal que deja de usarse después de un periodo de tiempo establecido por el usuario. El motor de suministro de contenido 606 puede usar también el módulo para establecer un "Lugar de Promociones" donde el usuario puede ir para ver promociones y tener control sobre las promociones que se están visualizando. En una implementación específica, la página personal de un usuario está libre de anuncios excepto en el lugar de Mercado y el lugar de Promociones. Sin embargo, como alternativa, las promociones podrían visualizarse en una página personal del usuario.
- 5
- 10 En el área de búsqueda de producto, un motor de búsqueda permitirá que los usuarios reciban promociones actuales (carteles o enlaces patrocinados) de acuerdo con los criterios que han introducido (productos, tipos de productos específicos, etc.) incluyendo una hora (interés de ... a ...). Podrían haber algunas restricciones con respecto a cuál de los usuarios desea recibir publicidad y/o promociones (únicamente marcas comerciales favoritas, aquellas recomendadas por la comunidad del usuario, etc.). Los anunciantes/marcas comerciales pagarán por estar posicionados en la búsqueda y promocionar sus productos y el valor será mayor ya que el objetivo será confiable y estará bajo control.
- 15
- Puede compensarse a los usuarios del sistema de gestión de datos controlado por abonarse a un servicio de pago del X % (o alguna otra cantidad) de la cuál una entidad ha pagado al sistema de gestión de datos controlado para estar en los resultados de búsqueda o ha pagado por adquisición de datos de cliente. Por lo tanto, puede compensarse a un usuario por proporcionar información personal. La matemática para el X % puede depender, por ejemplo, del nivel de facturación mensual individual. Estos números se proporcionan a modo de ejemplo únicamente.
- 20
- 25 En el ejemplo de la Figura 6, el módulo de preferencias de introducción 622 está acoplado al motor de suministro de contenido 606. El motor de suministro de contenido 606 puede usar el módulo para recibir preferencias del usuario con respecto a cualesquiera acciones o elecciones no descritas previamente.
- Uno o más de los módulos pueden tener partes que son gratis para los usuarios y partes que son de pago. En una implementación específica, el usuario puede conseguir servicios adicionales para compartir información personal. Como alternativa, podría simplemente pagarse al usuario por compartir la información personal. Un ejemplo de qué podría proporcionarse gratis en una implementación particular incluye un motor de transparencia de compartición de datos en una máquina de usuario que facilite: recopilación de datos automática para dirección o direcciones de correo electrónico registradas de usuarios registrados, almacenamiento de datos, gestión de correo electrónico, generación de alias de correo electrónico específicos de empresa, encaminamiento de correo electrónico enviado al alias a la dirección personal del usuario, información (por ejemplo, uso de cookies, calificaciones promedio, codificación por color de sitios basándose en certificación de gestión de datos controlados, realimentación de comunidad, etc.).
- 30
- 35 Un ejemplo de lo que podría proporcionarse gratis en una implementación particular incluye un servidor de compartición de datos controlado que facilita: el registro de usuarios; acceso a proceso de descargas; acceso a una lista de titulares de datos; acceso a qué información personal se mantiene por cada uno de una lista de titulares de datos; acceso a suscripciones a boletines de noticias recurrentes, listas de distribución de correo o similares; acceso a si un sitio usa cookies u otros dispositivos de rastreo y por qué; acceso a un enlace para ir a una página de gestión de perfil; acceso a una página testimonial para calificar sitios en términos de confianza, reputación, apreciación, calidad del sitio, etc.; acceso a la calificación agregada de testimonios basándose en entrada de miembro de gestión de datos controlados; acceso a listas de entidades de entidades que aparentemente comparten información personal o que usan un alias que no se les asignó.
- 40
- 45 Un ejemplo de qué podría proporcionarse por una cuota en una implementación particular incluye un motor de transparencia de compartición de datos en una máquina de usuario que facilite gestión de usuario y contraseña para una familia o grupo. Esto puede posibilitar que el sistema proporcione información agregada sobre gasto, hábitos de compra, o similares para la familia o el grupo.
- 50
- Un ejemplo de qué podría proporcionarse por una cuota en una implementación particular incluye un servidor de compartición de datos controlado que facilita: detener la recepción de información de una o más entidades; pedir a una entidad que borre un perfil (posiblemente excluyendo relaciones para las que se requiere el perfil, tal como bancos, proveedores de Internet, operadores móviles, etc.), aunque el sistema necesariamente no podrá aplicar el borrado de un perfil en una entidad a menos que la entidad lo consienta; ver la calificación de agregado de reputación/apreciación basándose en entrada de la comunidad; permitir que uno o más sitios rastreen comportamiento para anuncios u otros de acuerdo con preferencias de usuario, e incluyendo posiblemente que la entidad compense al usuario por permitirle que rastree comportamiento; analizar transacciones de correo electrónico de comercio electrónico con síntesis detallada de compras por semana, mes, año, tipo de producto, marca comercial, etc.; proporcionar una vista del hogar de los gastos que incluye la consolidación de correos electrónicos bajo un apodo familiar si cada miembro usa un alias de correo electrónico para sitios de comercio electrónico; permitir que los padres obtengan información sobre dónde han dado sus hijos datos personales y qué han desvelado.
- 55
- 60
- 65 Podrían emplearse sistemas de pago conocidos o convenientes, tal vez a través de terceros, para posibilitar que los

usuarios paguen por servicios o se les de crédito por la venta de su información personal o estadística. También es posible facturar y dar crédito a usuarios en sus cuentas móviles, probablemente a través de operadores móviles.

5 Puede ser deseable asociarse con terceros tales como proveedores de servicio móviles de modo que ofrecerían estos servicios a sus abonados móviles/de internet. De hecho, este tipo de servicio sería de valor para los operadores al menos puesto que les permitiría fortalecer su imagen en el área "delicada" de la privacidad mientras les permite recopilar ingresos adicionales asociados con servicios de valor añadido.

10 Estos servicios se cobrarían a continuación directamente en las facturas de los teléfonos móviles individuales y podrían ser una compartición de ingresos entre el sistema de gestión de datos controlado y los operadores. Por otra parte, para un mecanismo de compensación que permitiera dar crédito al individuo en su cuenta móvil cuando él venda sus datos personales, la red resultante entre servicios de pago y ventas de datos personales aparecería como un "+" o "-" en su factura de teléfono móvil. Esto podría significar que el sistema de gestión de datos controlado puede no tener que almacenar o gestionar detalles bancarios de usuarios y definitivamente tendría más sentido para las personas que no tengan una cuenta bancaria pero tengan una factura de teléfono móvil.

15 La siguiente descripción de las Figuras 7A y 7B se pretende para proporcionar una vista general de hardware informático y otros componentes de operación adecuados para realizar las técnicas descritas en este artículo. El hardware informático y otros componentes de operación pueden ser adecuados como parte de los aparatos que implementan las técnicas descritas en este artículo. Las técnicas pueden ponerse en práctica con otras configuraciones de sistema informático, que incluyen dispositivos portátiles, sistemas multiprocesador, electrónica basada en microprocesador o electrónica de consumo programable, PC de red, miniordenadores, ordenadores centrales, dispositivos inalámbricos y similares. Las técnicas pueden ponerse en práctica también en entornos informáticos distribuidos donde las tareas se realizan por dispositivos de procesamiento remotos que están vinculados a través de una red de comunicaciones.

20 La Figura 7A representa un sistema en el que puede implementarse una estructura para el sistema de gestión de datos controlado. La Figura 7A representa un sistema en red 700 que incluye varios sistemas informáticos acoplados juntos a través de una red 702, tal como internet. El término "Internet" como se usa en el presente documento hace referencia a una red de redes que usa ciertos protocolos, tales como el protocolo de TCP/IP, y posiblemente otros protocolos tales como el protocolo de transferencia de hipertexto (HTTP) para documentos del Lenguaje de Marcas de Hipertexto (HTML) que componen la red informática mundial (la web). Las conexiones físicas de la Internet y los protocolos y procedimientos de comunicación de la Internet son bien conocidos para los expertos en la materia.

30 El servidor web 704 es normalmente al menos un sistema informático que opera como un sistema informático de servidor y está configurado para operar con los protocolos de la red informática mundial y está acoplado a Internet. El sistema de servidor web 704 puede ser un sistema informático de servidor convencional. Opcionalmente, el servidor web 704 puede ser parte de un ISP que proporciona acceso a Internet para sistemas de cliente. El servidor web 704 se muestra acoplado al sistema informático de servidor 706 que por sí mismo está acoplado a contenido web 708, que puede considerarse un almacén de datos de medios. Mientras que se muestran dos sistemas informáticos 704 y 706 en la Figura 7A, el sistema de servidor web 704 y el sistema informático de servidor 706 pueden ser un sistema informático que tiene diferentes componentes de software implementados en hardware y que proporciona la funcionalidad de servidor web y la funcionalidad de servidor proporcionada por el sistema informático de servidor 706, que se describirá adicionalmente a continuación.

45 El acceso a la red 702 se proporciona normalmente por proveedores de servicio de Internet (ISP), tales como los ISP 710 y 716. También es posible usar operadores móviles y de red móvil que suministran conexiones de Internet fijas. En el caso de los móviles, el acceso a Internet a menudo es una 3G, 4G, GPRS, EDGE, etc. También, Wifi es una manera para acceder a Internet que se proporciona de manera diferente. Un experto en la materia reconocerá que pueden usarse maneras conocidas y convenientes para acceder a Internet. Los usuarios en los sistemas de cliente, tales como los sistemas informáticos de cliente 712, 718, 722, y 726 obtienen acceso a Internet a través de los ISP 710 y 716. El acceso a Internet permite que los usuarios de los sistemas informáticos de cliente intercambien información, reciban y envíen correos electrónicos, y vean documentos, tales como documentos que se han preparado en el formato de HTML. Estos documentos a menudo se proporcionan por servidores web, tal como el servidor web 50 704, que se denominan como que están "activados" en Internet. A menudo estos servidores web se proporcionan por los ISP, tal como el ISP 710, aunque puede establecerse un sistema informático y conectarse a Internet sin que ese sistema sea también un ISP. En el caso de los móviles, en ocasiones se usa un servidor de aplicación en lugar de un servidor web, y este puede ser el caso para aplicaciones de PC, tal como iTunes, juegos, etc., que no están usando algún servidor web ni un explorador. Un experto en la materia reconocerá que las aplicaciones están aumentando y que pueden usar tecnologías conocidas o convenientes para obtener documentos.

60 Los sistemas informáticos de cliente 712, 718, 722, y 726 puede cada uno, con el software de exploración web apropiado, ver páginas de HTML proporcionadas por el servidor web 704. El ISP 710 proporciona conectividad de Internet al sistema informático de cliente 712 a través de la interfaz de módem 714, que puede considerarse parte del sistema informático de cliente 712. Un experto en la materia reconocerá que los mecanismos de conexión, tal como la interfaz de módem 714, pueden modificarse o sustituirse con tecnologías conocidas o convenientes para hacer uso

de diversas redes, tales como GPRS, EDGE, 3G, 4G, etc. El sistema informático de cliente puede ser un sistema informático personal, un ordenador de red, un sistema de TV web, u otro sistema informático. Mientras que la Figura 7A muestra la interfaz de módem 714 generalmente como un "módem," la interfaz puede ser un módem analógico, módem de isdn, módem de cable, interfaz de transmisión por satélite (por ejemplo "PC directo"), u otra interfaz para acoplar un sistema informático a otros sistemas informáticos.

Similar al ISP 714, el ISP 716 proporciona conectividad de Internet para sistemas de cliente 718, 722, y 726, aunque como se muestra en la Figura 7A, las conexiones no son las mismas para estos tres sistemas informáticos. El sistema informático de cliente 718 está acoplado a través de una interfaz de módem 720 mientras que los sistemas informáticos de cliente 722 y 726 son parte de una LAN 730.

Los sistemas informáticos de cliente 722 y 726 están acoplados a la LAN 730 a través de las interfaces de red 724 y 728, que pueden ser Ethernet u otras interfaces de red. La LAN 730 también está acoplada a un sistema informático de pasarela 732 que puede proporcionar cortafuegos y otros servicios relacionados con Internet para la red de área local. Este sistema informático de pasarela 732 está acoplado al ISP 716 para proporcionar conectividad de Internet a los sistemas informáticos de cliente 722 y 726. El sistema informático de pasarela 732 puede ser un sistema informático de servidor convencional.

Como alternativa, un sistema informático de servidor 734 puede estar directamente acoplado a la LAN 730 a través de una interfaz de red 736 para proporcionar ficheros 738 y otros servicios a los clientes 722 y 726, sin la necesidad de conectarse a Internet a través del sistema informático 732.

La Figura 7B representa un sistema informático 740 para su uso en el sistema 700 (Figura 7A). El sistema informático 740 puede ser un sistema informático convencional que puede usarse como un sistema informático de cliente o un sistema informático de servidor o como un sistema de servidor web. Un sistema informático de este tipo puede usarse para realizar muchas de las funciones de un proveedor de servicio de Internet, tal como el ISP 710 (Figura 7A).

En el ejemplo de la Figura 7B, el sistema informático 740 incluye un ordenador 742, dispositivos de E/S 744, y un dispositivo de visualización 746. El ordenador 742 incluye un procesador 748, una interfaz de comunicaciones 750, memoria 752, controlador de pantalla 754, almacenamiento no volátil 756, y controlador de E/S 758. El sistema informático 740 puede ser acoplarse a o incluir los dispositivos de E/S 744 y el dispositivo de visualización 746.

El ordenador 742 se interconecta a sistemas externos a través de la interfaz de comunicaciones 750, que puede incluir un módem o interfaz de red. Se apreciará que la interfaz de comunicaciones 750 puede considerarse que es parte del sistema informático 740 o una parte del ordenador 742. Un ordenador puede incluir móviles y cualquier otro dispositivo conectado que tenga un procesador. La interfaz de comunicaciones puede ser un módem analógico, módem de ISDN, módem de cable, interfaz de anillo con paso de testigo, interfaz de transmisión por satélite (por ejemplo "PC directo"), u otras interfaces para acoplar un sistema informático a otros sistemas informáticos.

El procesador 748 puede ser, por ejemplo, un microprocesador convencional tal como un microprocesador Intel Pentium o microprocesador Motorola power PC, o algún otro procesador convencional o no convencional. La memoria 752 está acoplada al procesador 748 por un bus 760. La memoria 752 puede ser memoria de acceso aleatorio dinámica (DRAM) y puede incluir también ram estática (SRAM). El bus 760 acopla el procesador 748 a la memoria 752, también al almacenamiento no volátil 756, al controlador de visualización 754, y al controlador de E/S 758.

Los dispositivos de E/S 744 pueden incluir un teclado, unidades de disco, impresoras, un escáner, y otros dispositivos de entrada y salida, incluyendo un ratón u otro dispositivo apuntador. El controlador de visualización 754 puede controlar de la manera convencional una pantalla en el dispositivo de visualización 746, que puede ser, por ejemplo, un tubo de rayos catódicos (CRT) o pantalla de cristal líquido (LCD). El controlador de visualización 754 y el controlador de E/S 758 pueden implementarse con tecnología conocida o conveniente aplicable.

El almacenamiento no volátil 756 a menudo es un disco duro magnético, un disco óptico, u otra forma de almacenamiento para cantidades de datos grandes. Algunos de estos datos a menudo están escritos, por un proceso de acceso a memoria directa, en memoria 752 durante la ejecución de software en el ordenador 742. Los objetos, métodos, cachés en línea, estados de caché y otros componentes orientados a objetos pueden almacenarse en el almacenamiento no volátil 756, o escribirse en memoria 752 durante la ejecución de, por ejemplo, un programa de software orientado a objetos. De esta manera, los componentes ilustrados en, por ejemplo, las Figuras 1-6 se pueden generar una instancia en el sistema informático 740.

El sistema informático 740 es un ejemplo de muchos posibles sistemas informáticos que tienen diferentes arquitecturas. Por ejemplo, los ordenadores personales basados en un microprocesador Intel a menudo tienen múltiples buses, uno de los cuales puede ser un bus de E/S para los periféricos y uno que directamente conecta el procesador 748 y la memoria 752 (a menudo denominado como un bus de memoria). Los buses están conectados juntos a través de componentes de puente que realizan cualquier traducción necesaria debido a protocolos de bus diferentes.

Los ordenadores en red son otro tipo de sistema informático que puede usarse para implementar las técnicas descritas en este artículo. Los ordenadores en red no incluyen habitualmente un disco duro u otro almacenamiento masivo, y los programas ejecutables se cargan de una conexión de red en la memoria 752 para su ejecución por el procesador 748. Un sistema de TV Web también se considera que es un sistema informático, pero puede carecer de alguna de las características mostradas en la Figura 7B, tal como ciertos dispositivos de entrada o salida. Un sistema informático típico incluirá normalmente al menos un procesador, memoria, y un bus que acopla la memoria al procesador.

Además, el sistema informático 740 se controla por el software de sistema operativo que incluye un sistema de gestión de ficheros, tal como un sistema operativo de disco, que es parte del software del sistema operativo. Un ejemplo de un software de sistema operativo con su software de sistema de gestión de ficheros asociado es de la familia de sistemas operativos conocidos como Windows® de Microsoft Corporation de Redmond, Washington, y sus sistemas de gestión de ficheros asociados. Otro ejemplo de software de sistema operativo con su software de sistema de gestión de ficheros asociado es el sistema operativo Linux y su sistema de gestión de ficheros asociado. El sistema de gestión de fichero se almacena normalmente en el almacenamiento no volátil 756 y provoca que el procesador 748 ejecute los diversos actos requeridos por el sistema operativo para introducir y emitir datos y para almacenar datos en memoria, incluyendo almacenar ficheros en el almacenamiento no volátil 756.

Las Figuras 8A a 8C representan ejemplos de sistemas de generación de alias 800A a 800C con variaciones en la localidad de los componentes. En el ejemplo de la Figura 8A, el sistema 800A incluye un dispositivo de cliente 802, un sistema de gestión de datos controlado 804, un dispositivo de terceros 806, y un servidor de mensaje 808. En el ejemplo de la Figura 8A, el dispositivo de cliente 802 está acoplado al sistema de gestión de datos controlado 804, al dispositivo de terceros 806, y al servidor de mensaje 808. El dispositivo de cliente 802 está en asociación con un usuario que tiene información personal asociada, y puede ser similar al cliente maestro 106 de la Figura 1.

En el ejemplo de la Figura 8A, el sistema de gestión de datos controlado 804 incluye un motor de generación de alias 810, un almacén de datos de alias 812, y un motor de agente de alias 814. En el ejemplo de la Figura 8A, el motor de generación de alias 810 está acoplado al dispositivo de cliente 802 y el motor de agente de alias 814 está acoplado al dispositivo de terceros 806 y al servidor de mensaje 808. El motor de generación de alias 810 puede generar un alias de un valor de clave. En el ejemplo de la Figura 8A, el dispositivo de cliente 802 proporciona el valor de clave, que puede incluir un valor de contacto, tal como una dirección de correo electrónico o un número de teléfono, al motor de generación de alias 810; el motor de generación de alias 810 genera un alias del valor de clave, que se almacena en el almacén de datos de alias 812 y se proporciona también al dispositivo de cliente 802. El alias es específico a una entidad que está asociada con el dispositivo de terceros 806. El motor de agente de alias 814 puede recibir un mensaje para el alias y cambiar el valor de contacto del alias al valor de clave.

En el ejemplo de la Figura 8A, el dispositivo de cliente 802 o un dispositivo asociado recibe el alias del motor de generación de alias 810 y proporciona al menos el alias, y potencialmente otra información personal, tal como un id de usuario, contraseña, u otros datos, al dispositivo de terceros 806. Independientemente de si se incluye otra información personal, los datos proporcionados al dispositivo de terceros 806 pueden denominarse como información personal de alias puesto que incluyen al menos el alias.

En el ejemplo de la Figura 8A, el dispositivo de terceros 806 recibe la información personal de alias. De manera presumible el dispositivo de terceros 806 almacenará alguna o toda la información personal de alias en un almacén de datos (no mostrado). Puesto que el alias incluye un valor de contacto, el dispositivo de terceros 806, o un dispositivo asociado, puede usar el alias para enviar un mensaje a un usuario asociado con el dispositivo de cliente 802. En el ejemplo de la Figura 8A, el dispositivo de terceros 806 envía un mensaje para el alias, que se recibe en el motor de agente de alias 814.

En el ejemplo de la Figura 8A, el motor de agente de alias 814 usa el almacén de datos de alias 812 para hallar un valor de clave asociado con el alias para el mensaje enviado del dispositivo de terceros 806 o un dispositivo asociado al alias. El motor de agente de alias 814 puede proporcionar información adicional en el mensaje, tal como el origen del mensaje al alias. Puesto que el alias es específico de entidad, si el origen del mensaje al alias es de una entidad que no está asociada con el dispositivo de terceros, a continuación el motor de agente de alias 814 puede determinar que el alias se usó por una entidad distinta de una a la que se proporcionó el alias en la información personal de alias. El motor de agente de alias 814 puede incluir en un mensaje al destino de valor de clave que el alias se usó por una entidad distinta de la entidad para la que se generó el alias. En una implementación específica, el motor de agente de alias 814 puede tomar acciones, tal como filtrado del mensaje, de acuerdo con preferencias de usuario.

En el ejemplo de la Figura 8A, el servidor de mensaje 808 está acoplado al dispositivo de cliente 802 y al motor de agente de alias 814. En el ejemplo de la Figura 8A, el servidor de mensaje 808 recibe el mensaje al destino de valor de clave que se envió por el motor de agente de alias 814. El mensaje al destino de valor de clave puede enviarse a continuación al dispositivo de cliente 802 o un dispositivo asociado. Un usuario puede comparar el origen del mensaje al alias, o la información que se añade al mensaje al destino de valor de clave con respecto al origen del mensaje al alias. De esta manera, el usuario puede determinar si la entidad que envió el mensaje al alias es la entidad que está asociada con el alias, y tomar acciones como el usuario considere apropiado.

Ventajosamente, el sistema 800A puede conseguir gestión de datos controlados con relativamente poca información personal almacenada en el sistema de gestión de datos controlado 804. Como mínimo, el sistema de gestión de datos controlado 804 puede mantener únicamente el valor de clave y cualquier alias específico de entidad que se genera para el valor de clave. Es probable que el sistema de gestión de datos controlado 804 incluirá alguna otra información, tal como un nombre de usuario y contraseña para el usuario asociado con el dispositivo de cliente 802, para posibilitar que el usuario gestione una cuenta de gestión de datos controlados, aunque esto no es absolutamente necesario para la funcionalidad descrita.

La Figura 8B representa un ejemplo de un sistema 800B que almacena en cierto modo más información personal en un sistema de gestión de datos controlado. En el ejemplo de la Figura 8B, el sistema 800B incluye un dispositivo de cliente 822, un sistema de gestión de datos controlado 824, un dispositivo de terceros 826, y un servidor de mensaje 828. En el ejemplo de la Figura 8B, el dispositivo de cliente 822 está acoplado al sistema de gestión de datos controlado 824, al dispositivo de terceros 826, y al servidor de mensaje 828. El dispositivo de cliente 822 está en asociación con un usuario que tiene información personal asociada, y puede ser similar al cliente maestro 106 de la Figura 1.

En el ejemplo de la Figura 8B, el sistema de gestión de datos controlado 824 incluye un motor de generación de alias 830, un almacén de datos de alias 832, un motor de aprovisionamiento de información de alias 834, un almacén de datos de información personal 836, y un motor de agente de alias 838. En el ejemplo de la Figura 8B, el motor de generación de alias 830 está acoplado al dispositivo de cliente 822; el almacén de datos de alias 832 está acoplado al motor de generación de alias 830, al motor de aprovisionamiento de información de alias 834, y al motor de agente de alias 838; el motor de aprovisionamiento de información de alias 834 está acoplado al dispositivo de cliente 822, al almacén de datos de información personal 836, y al dispositivo de terceros 826; y el motor de agente de alias 838 está acoplado al dispositivo de terceros 826 y al servidor de mensaje 828.

El motor de generación de alias 830 puede generar un alias de un valor de clave. En el ejemplo de la Figura 8B, el dispositivo de cliente 822 proporciona el valor de clave, que puede incluir un valor de contacto tal como una dirección de correo electrónico o un número de teléfono, al motor de generación de alias 820; el motor de generación de alias 820 genera un alias del valor de clave, que se almacena en el almacén de datos de alias 832. El alias es específico a una entidad que está asociada con el dispositivo de terceros 826. El motor de aprovisionamiento de información de alias 834 puede recibir información personal del dispositivo de cliente 822 o un dispositivo asociado y almacenar la información personal en el almacén de datos de información personal 836. El motor de aprovisionamiento de información de alias 834 puede usar también el alias en el almacén de datos de alias e información personal proporcionado por el dispositivo de cliente 822 y/o que se almacena en el almacén de datos de información personal 836 para generar información personal de alias apropiada para aprovisionamiento a una entidad que está asociada con el alias. El motor de agente de alias 838 puede recibir un mensaje para el alias y cambiar el valor de contacto del alias al valor de clave.

En el ejemplo de la Figura 8B, el motor de aprovisionamiento de información de alias 834 obtiene el alias del almacén de datos de alias 832 y potencialmente otra información personal, tal como un id de usuario, contraseña, u otros datos, del dispositivo de cliente 822 y/o el almacén de datos de información personal 836 y proporciona información personal de alias al dispositivo de terceros 826. Independientemente de si se incluye otra información personal, los datos proporcionados al dispositivo de terceros 826 pueden denominarse como información personal de alias puesto que incluyen al menos el alias.

En el ejemplo de la Figura 8B, el dispositivo de terceros 826 recibe la información personal de alias. De manera presumible el dispositivo de terceros 826 almacenará alguna o toda la información personal de alias en un almacén de datos (no mostrado). Puesto que el alias incluye un valor de contacto, el dispositivo de terceros 826, o un dispositivo asociado, puede usar el alias para enviar un mensaje a un usuario asociado con el dispositivo de cliente 822. En el ejemplo de la Figura 8B, el dispositivo de terceros 826 envía un mensaje para el alias, que se recibe en el motor de agente de alias 838.

En el ejemplo de la Figura 8B, el motor de agente de alias 838 usa el almacén de datos de alias 832 para hallar un valor de clave asociado con el alias para el mensaje enviado del dispositivo de terceros 826 o un dispositivo asociado al alias. El motor de agente de alias 838 puede proporcionar información adicional en el mensaje, tal como el origen del mensaje al alias. Puesto que el alias es específico de entidad, si el origen del mensaje al alias es de una entidad que no está asociada con el dispositivo de terceros, a continuación el motor de agente de alias 838 puede determinar que el alias se usó por una entidad distinta de una a la que se proporcionó el alias en la información personal de alias. El motor de agente de alias 838 puede incluir en un mensaje al destino de valor de clave que el alias se usó por una entidad distinta de la entidad para la que se generó el alias. En una implementación específica, el motor de agente de alias 838 puede tomar acciones, tal como filtrado del mensaje, de acuerdo con preferencias de usuario.

En el ejemplo de la Figura 8B, el servidor de mensaje 828 está acoplado al dispositivo de cliente 822 y al motor de agente de alias 838. En el ejemplo de la Figura 8B, el servidor de mensaje 828 recibe el mensaje al destino de valor de clave que se envió por el motor de agente de alias 838. El mensaje al destino de valor de clave puede enviarse a continuación al dispositivo de cliente 822 o un dispositivo asociado. Un usuario puede comparar el origen del mensaje al alias, o la información que se añade al mensaje al destino de valor de clave con respecto al origen del mensaje al

alias. De esta manera, el usuario puede determinar si la entidad que envió el mensaje al alias es la entidad que está asociada con el alias, y tomar acciones como el usuario considere apropiado.

5 La Figura 8C representa un ejemplo de un sistema 800C que incluye un motor de transparencia de compartición de datos en un dispositivo de cliente. En el ejemplo de la Figura 8C, el sistema 800C incluye un sistema de generación de perfiles de entidad 842, dispositivo de cliente 844, un sistema de terceros 846, y un sistema de gestión de datos controlado 848. Un servidor de mensaje (no mostrado) podría estar acoplado también entre el dispositivo de cliente 844 y el sistema de gestión de datos controlado 848 (véase, por ejemplo, las Figuras 8A y 8B).

10 En el ejemplo de la Figura 8C, el sistema de generación de perfiles de entidad 842 incluye un motor de generación de perfil de entidad 850 y un almacén de datos de perfil de entidad 852. El motor de generación de perfil de entidad 850 puede generar un perfil para una entidad recibiendo información de la entidad cuando la entidad se abona a un servicio, buscando información públicamente disponible acerca de la entidad, recibiendo información de usuarios de la entidad, o a través de algún otro procedimiento conveniente. El motor de generación de perfil de entidad 850 puede almacenar información relevante acerca de la entidad en el almacén de datos de perfil de entidad 852. En una implementación específica, alguno o todo del almacén de datos de perfil de entidad 852 puede localizarse en el dispositivo de cliente 844 (no mostrado).

20 En el ejemplo de la Figura 8C, el dispositivo de cliente 844 incluye un motor de etiquetado de sitio 854, un motor de navegación 856, un motor de generación de alias 858, un almacén de datos de modificación de alias 860, un motor de aprovisionamiento de información de alias 862, un almacén de datos de modificación de perfil de usuario 864, y un motor de recepción de mensaje 866. En el ejemplo de la Figura 8C, el motor de etiquetado de sitio 854 está acoplado al almacén de datos de perfil de entidad 852 y al motor de navegación 856; el motor de navegación 856 está acoplado al sistema de terceros 846; el motor de generación de alias 858 está acoplado al sistema de terceros 846 y al almacén de datos de modificación de alias 860; el motor de aprovisionamiento de información de alias 862 está acoplado al sistema de terceros 846, al almacén de datos de modificación de alias 860, al almacén de datos de modificación de perfil de usuario 864, y al sistema de gestión de datos controlado 848; y el motor de recepción de mensaje está acoplado al sistema de gestión de datos controlado 848.

30 El motor de etiquetado de sitio 854 puede usar datos acerca de una entidad del almacén de datos de perfil de entidad 852 para proporcionar a un usuario información acerca de la entidad. Cuando se proporciona la información en un dispositivo que está visualizando actualmente una localización de una entidad, tal como un sitio web asociado con la entidad, la información puede estar caracterizada como una etiqueta. Las etiquetas pueden indicar si una entidad es conocida para el sistema de gestión de datos controlado, rechaza participar en gestión de datos controlados, comparte información personal con afiliados u otras partes, es un abonado de sistema de gestión de datos controlado, u otra información que se considera apropiada. El motor de navegación 856 puede fijar (virtualmente) la etiqueta a una localización de la entidad, tal como proporcionando una opción de menú en un explorador que, cuando se elige, visualiza información acerca de la entidad, como una etiqueta que se inserta automáticamente en el explorador cuando se navega a un sitio web asociado con la entidad, o de alguna otra manera que hace a la información acerca de la entidad, si la hubiera, disponible para un usuario.

45 El motor de generación de alias 858 puede generar un alias que es específico para una entidad. En el ejemplo de la Figura 8C, el motor de generación de alias 858 almacena el alias en el almacén de datos de modificación de alias 860. El almacén de datos de modificación de alias 860 puede incluir o no únicamente un subconjunto de alias conocidos para un usuario. Una razón de que no todos los alias sean necesarios es que las modificaciones de alias pueden proporcionarse al sistema de gestión de datos controlado 848, que puede interceptar mensajes dirigidos al alias y proporcionar información relevante asociada con, por ejemplo, el origen de la información. Sin embargo, también es posible mantener todos los alias en el almacén de datos de modificación de alias 860, que significaría que en lugar de un almacén de datos de "modificación" de alias, el almacén de datos podría denominarse como un almacén de datos de alias, que, para un perfil de usuario específico, la información de alias en el dispositivo de cliente 844 y el sistema de gestión de datos controlado 848 podrían ser el mismo. En una implementación en la que se mantiene toda la información de alias en el dispositivo de cliente 844, el motor de recepción de mensaje 866 puede acoplarse al almacén de datos de alias, y generar información asociada con el alias similar a la generada en el sistema de gestión de datos controlado 848.

55 El motor de aprovisionamiento de información de alias 862 puede recibir información personal de un usuario a través de un dispositivo de entrada, del almacén de datos de modificación de perfil de usuario 864, o de algún otro origen de información personal. Cuando el motor de aprovisionamiento de información de alias 862 obtiene nueva información o actualizada, la información personal puede almacenarse en el almacén de datos de modificación de perfil de usuario 864. El almacén de datos de modificación de perfil de usuario 864 es un almacén de datos de "modificación" puesto que el motor de aprovisionamiento de información de alias 862 puede proporcionar la información al sistema de gestión de datos controlado 848. Como alternativa, la información personal puede mantenerse en el dispositivo de cliente 844 y no compartirse, o únicamente puede compartirse un subconjunto, con el sistema de gestión de datos controlado 848. El motor de aprovisionamiento de información de alias 862 puede usar el alias en el almacén de datos de modificación de alias 860 y la información personal obtenida y/o que se almacena en el almacén de datos de información personal 864 para generar información personal de alias apropiada para aprovisionamiento para una entidad que está asociada

con el alias. El motor de aprovisionamiento de información de alias 862 puede actualizar también el sistema de gestión de datos controlado 848 con alias y/o datos de perfil de usuario, dependiendo de la implementación, configuración, y/o preferencias de usuario.

5 El motor de recepción de mensaje 866 puede recibir mensajes que se dirigieron a un alias. Los mensajes pueden direccionarse o no al alias cuando se reciben en el motor de recepción de mensaje 866. Por ejemplo, el sistema de gestión de datos controlado 848 puede posibilitar sustituir el alias por una dirección de destino del usuario. En una implementación específica, el motor de recepción de mensaje 866 puede analizar el mensaje para determinar si el alias usado por el origen del mensaje es específico a la entidad que es el origen del mensaje. Cuando un alias que no es específico para una entidad se usa por esa entidad, el motor de recepción de mensaje 866 puede indicar al usuario que el alias no se usó por la entidad a la que se asignó el alias, que puede ser indicativo de compartición de datos.

15 En el ejemplo de la Figura 8C, el sistema de terceros 846 incluye un motor de registro 868, un almacén de datos de información personal 870, y un motor de mensajería de usuario 872. En el ejemplo de la Figura 8C, el motor de registro 868 está acoplado al motor de navegación 856, al motor de generación de alias 858, al motor de aprovisionamiento de información de alias 862, y al almacén de datos de información personal 870. El motor de registro 868 puede proporcionar una forma de entrada de datos a un usuario, tal como en una página web, que se visualiza por el motor de navegación 856. El motor de registro 868 puede usar también correo electrónico, mensajes de texto, o alguna otra técnica de contacto para iniciar el registro de un usuario. Como se usa en este artículo, se pretende el registro de un usuario incluya ampliamente registro explícito en un sitio asociado con una entidad, que proporciona información por cualquier razón, o extraiga información de un usuario con o sin el conocimiento del usuario. Sería deseable para hacer que el usuario tenga el máximo conocimiento posible de las restricciones tecnológicas o informativas.

25 Cuando el motor de registro 868 intenta obtener información de contacto de un usuario, el motor de generación de alias 858 puede generar un alias para su uso en lugar de la información de contacto. Por ejemplo, si el motor de registro 868 obtiene direcciones de correo electrónico como parte de un procedimiento de registro, el motor de generación de alias 858 puede generar una dirección de correo electrónico de alias. El motor de registro 868 a continuación recibe información de alias del motor de aprovisionamiento de información de alias 862. Independientemente de si se incluye otra información personal, los datos recibidos en el motor de registro 868 pueden denominarse como información personal de alias puesto que incluyen al menos el alias. El motor de registro 868 puede almacenar la información personal de alias en el almacén de datos de información personal 870. Puesto que el alias incluye un valor de contacto, el motor de mensajería de usuario 872 puede usar el alias para enviar un mensaje a un usuario asociado con el dispositivo de cliente 844. En el ejemplo de la Figura 8C, el motor de mensajería de usuario 872 envía un mensaje para el alias, que se recibe en el motor de agente de alias 880.

35 El motor de agente de alias 880 puede proporcionar información adicional en el mensaje, tal como el origen del mensaje al alias. Puesto que el alias es específico de entidad, si el origen del mensaje al alias es de una entidad que no está asociada con el dispositivo de terceros, a continuación el motor de agente de alias 880 puede determinar que el alias se usó por una entidad distinta de una a la que se proporcionó el alias en la información personal de alias. El motor de agente de alias 880 puede incluir en un mensaje al destino de valor de clave que el alias se usó por una entidad distinta de la entidad para la que se generó el alias. En una implementación específica, el motor de agente de alias 880 puede tomar acciones, tal como filtrado del mensaje, de acuerdo con preferencias de usuario. En una alternativa, el mensaje al alias podría recibirse en el motor de recepción de mensaje 866, omitiendo el motor de agente de alias 880, y el motor de recepción de mensaje 866 podría llevar a cabo funcionalidad similar a la descrita para el motor de agente de alias 880.

50 Ventajosamente, un usuario puede comparar el origen del mensaje al alias, o la información que se añade al mensaje al destino de valor de clave con respecto al origen del mensaje al alias. De esta manera, el usuario puede determinar si la entidad que envió el mensaje al alias es la entidad que está asociada con el alias, y tomar acciones como el usuario considere apropiado.

55 La Figura 9 representa un diagrama de flujo 900 de un ejemplo de un método para identificar compartición de información usando un alias específico de entidad. En el ejemplo de la Figura 9, el diagrama de flujo 900 se inicia en el módulo 902 obteniendo un valor de clave para su uso en comunicación con un usuario. El valor de clave puede incluir, por ejemplo, una dirección de correo electrónico, un número de teléfono, una dirección, u otro valor de contacto aplicable.

60 En el ejemplo de la Figura 9, el diagrama de flujo 900 continúa al módulo 904 generando a partir del valor de clave un alias para su uso en comunicación con una tercera parte. El alias puede estar en un formato similar al del valor de clave. Por ejemplo, si el valor de clave es una dirección de correo electrónico, el alias puede ser también una dirección de correo electrónico. El alias se pretende para sustituir el valor de clave en comunicaciones entre un usuario y una entidad (o entidades) para las que se crea el alias.

65 En el ejemplo de la Figura 9, el diagrama de flujo 900 continúa al módulo 906 con la recepción de un mensaje que tiene un primer destino de mensaje que incluye el alias. Esto es indicativo de un mensaje que se envía por una entidad usando el alias.

5 En el ejemplo de la Figura 9, el diagrama de flujo 900 continúa al módulo 908 sustituyendo el primer destino de mensaje con un segundo destino de mensaje que incluye el valor de clave para su uso en comunicación con el usuario. Puede ser deseable incluir el primer destino de mensaje (alias) en alguna forma. Por ejemplo, el alias podría ponerse en el campo cc., incluirse como parte de un adjunto, incluirse en el cuerpo del mensaje, o proporcionarse a través de un canal separado.

10 En el ejemplo de la Figura 9, el diagrama de flujo 900 finaliza en el módulo 910 enviando el mensaje al segundo destino de mensaje. Tras la recepción del mensaje, un usuario puede determinar si el alias se usó por una primera identidad para la que se creó el alias, o por una segunda entidad. El usuario puede desear tomar ciertas acciones después de la determinación, tal como informar una o ambas de las entidades, mensajes de filtro de la segunda entidad, intentar anular el registro de la primera entidad, o similares.

15 Algunas porciones de la descripción detallada pueden presentarse en términos de algoritmos y representaciones simbólicas de operaciones en bits de datos dentro de una memoria informática. Estas descripciones y representaciones algorítmicas son los medios usados por los expertos en la materia en las técnicas de procesamiento de datos para transportar más eficazmente la materia de su trabajo a otros expertos en la materia. Un algoritmo se concibe en este punto, y en general, una secuencia auto-consistente de operaciones que conduce a un resultado deseado. Las operaciones son aquellas que requieren manipulaciones físicas de cantidades físicas. Normalmente, aunque no necesariamente, estas cantidades toman la forma de señales eléctricas o magnéticas que pueden almacenarse, transferirse, combinarse, compararse y manipularse de otra manera. Se ha probado conveniente en 20 ocasiones, principalmente por razones de uso común, hacer referencia a estas señales como bits, valores, elementos, símbolos, caracteres, términos, números, o similares.

25 Debe tenerse en cuenta, sin embargo, que estos términos y similares han de asociarse con las cantidades físicas apropiadas y son simplemente etiquetas convenientes aplicadas a estas cantidades. A menos que se establezca específicamente de otra manera como evidente a partir del siguiente análisis, se aprecia que a través de toda la descripción, los análisis que utilizan términos tales como "procesamiento" o "cómputo" o "cálculo" o "determinación" o "visualización" o similares, hacen referencia a la acción y procesos de un sistema informático, o dispositivo informático 30 electrónico similar, que manipula y transforma datos representados como cantidades físicas (electrónica) dentro de los registros del sistema informático y memorias en otros datos representados de manera similar como cantidades físicas dentro de las memorias o registros del sistema informático u otro almacenamiento, transmisión de información de este tipo o dispositivos de visualización.

35 Un aparato puede construirse específicamente para implementar las técnicas descritas en este artículo, o puede comprender un ordenador de fin general activado o reconfigurado selectivamente por un programa informático almacenado en el ordenador para producir una máquina de fin especial. Un programa informático de este tipo puede almacenarse en un medio de almacenamiento legible por ordenador, tal como, pero sin limitación, cualquier tipo de disco incluyendo discos flexibles, discos ópticos, CD-ROM, y discos magneto-ópticos, memorias de solo lectura 40 (ROM), memorias de acceso aleatorio (RAM), EPROM, EEPROM, tarjetas magnéticas u ópticas, o cualquier tipo de medio adecuado para almacenar instrucciones electrónicas y cada uno acoplado a un bus de sistema informático.

45 Los algoritmos y visualizaciones presentados en el presente documento no están intrínsecamente relacionados con algún ordenador particular u otro aparato. Pueden usarse diversos sistemas de fin general con programas de acuerdo con las enseñanzas en el presente documento, o puede probar ser conveniente construir un aparato más especializado para realizar los métodos de algunas realizaciones.

REIVINDICACIONES

1. Un sistema que comprende:

5 al menos un procesador de hardware;
una memoria que almacena código de programa, siendo ejecutable el código de programa por el al menos un procesador de hardware, comprendiendo el código de programa:

un motor de generación de alias operativo para:

10 obtener una dirección de correo electrónico de clave para su uso en comunicación con un usuario particular;
de acuerdo con una solicitud para obtener información de contacto de usuario en un sitio web accedido desde un dispositivo de cliente usando un explorador, generar una dirección de correo electrónico de alias para que el sistema reciba, en nombre del usuario particular, mensajes de una entidad asociada al sitio web, estando asociada de manera inequívoca la dirección de correo electrónico de alias a la entidad;
15 almacenar la dirección de correo electrónico de clave en asociación con la dirección de correo electrónico de alias en el almacén de datos de alias; proporcionar la dirección de correo electrónico de alias a un dispositivo de cliente asociado al usuario particular, posibilitando de esta manera que el usuario particular proporcione información personal de alias que incluye la dirección de correo electrónico de alias en lugar de la dirección de correo electrónico de clave;

un motor de agente de alias operativo para:

25 recibir, de un dispositivo de terceros, un mensaje de correo electrónico que tiene un origen de mensaje de un tercero, y un primer destino de mensaje que incluye la dirección de correo electrónico de alias;
determinar si el tercero es o no la entidad, usando el origen del mensaje del mensaje de correo electrónico y la dirección de correo electrónico de alias incluida en el primer destino de mensaje;
al menos cuando se determina que el tercero es la entidad, sustituir el primer destino de mensaje por un segundo destino de mensaje que incluye la dirección de correo electrónico de clave almacenada en el
30 almacén de datos de alias en asociación con la dirección de correo electrónico de alias;
enviar el mensaje de correo electrónico al segundo destino de mensaje.

2. El sistema de la reivindicación 1, en el que el motor de generación de alias es operativo para almacenar un identificador de la entidad en asociación con la dirección de correo electrónico de alias en el almacén de datos de alias.

3. El sistema de la reivindicación 1, que comprende adicionalmente un almacén de datos de información personal, acoplado a un motor de aprovisionamiento de información de alias, en donde el motor de aprovisionamiento de información de alias es operativo para almacenar información personal en el almacén de datos de información personal y en donde la información personal de alias incluye alguna información personal.

4. El sistema de la reivindicación 1, que comprende adicionalmente un servidor de mensaje operativo para:

45 recibir el mensaje del motor de agente de alias;
proporcionar el mensaje al dispositivo de cliente.

5. El sistema de la reivindicación 3, en el que el motor de aprovisionamiento de información de alias es operativo adicionalmente para proporcionar actualizaciones del almacén de datos de alias a un servidor de gestión de datos controlados.

6. Un método que comprende:

55 obtener una dirección de correo electrónico de clave para su uso en comunicación con un usuario particular;
de acuerdo con una solicitud para obtener información de contacto de usuario en un sitio web accedido desde un dispositivo de cliente usando un explorador, generar una dirección de correo electrónico de alias para que un sistema reciba, en nombre del usuario particular, mensajes de una entidad asociada al sitio web, estando asociada de manera inequívoca la dirección de correo electrónico de alias a la entidad;
almacenar la dirección de correo electrónico de clave en asociación con la dirección de correo electrónico de alias en un almacén de datos de alias;
60 proporcionar la dirección de correo electrónico de alias a un dispositivo de cliente asociado al usuario particular, posibilitando de esta manera que el usuario particular proporcione información personal de alias que incluye la dirección de correo electrónico de alias en lugar de la dirección de correo electrónico de clave;
recibir, de un dispositivo de terceros, un mensaje de correo electrónico que tiene un origen de mensaje de un tercero, y un primer destino de mensaje que incluye la dirección de correo electrónico de alias;
65 determinar si el tercero es o no la entidad, usando el origen de mensaje del mensaje de correo electrónico y la dirección de correo electrónico de alias incluida en el primer destino de mensaje;

al menos cuando se determina que el tercero es la entidad, sustituir el primer destino de mensaje por un segundo destino de mensaje que incluye la dirección de correo electrónico de clave almacenado en el almacén de datos de alias en asociación con la dirección de correo electrónico de alias;
enviar el mensaje de correo electrónico al segundo destino de mensaje.

5

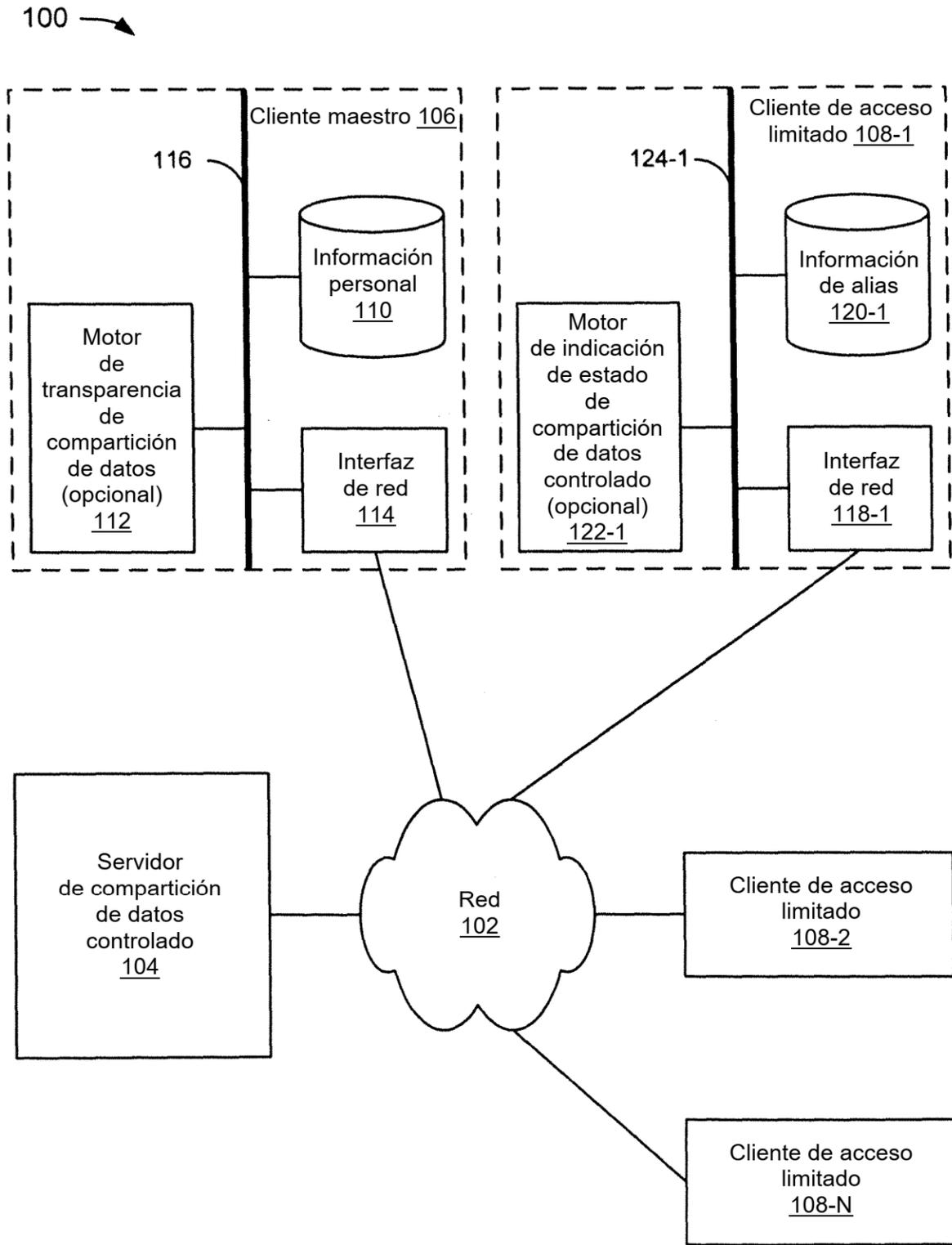


FIG. 1

200 →

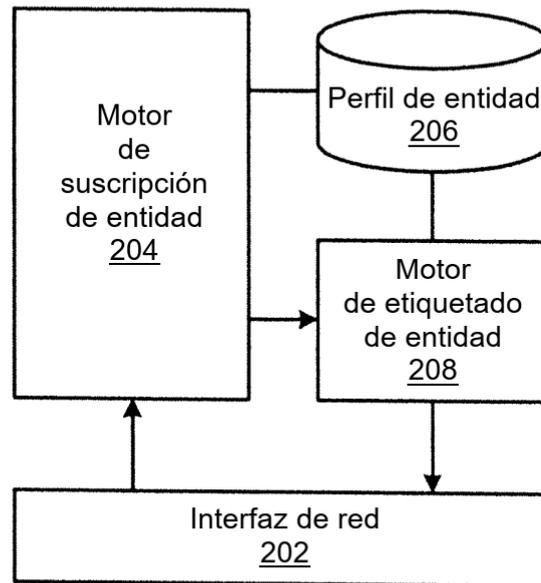


FIG. 2

300 →

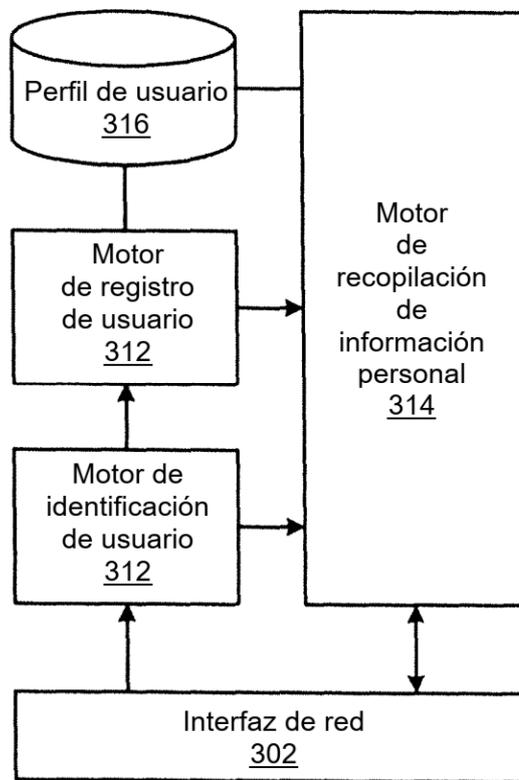


FIG. 3

400 →

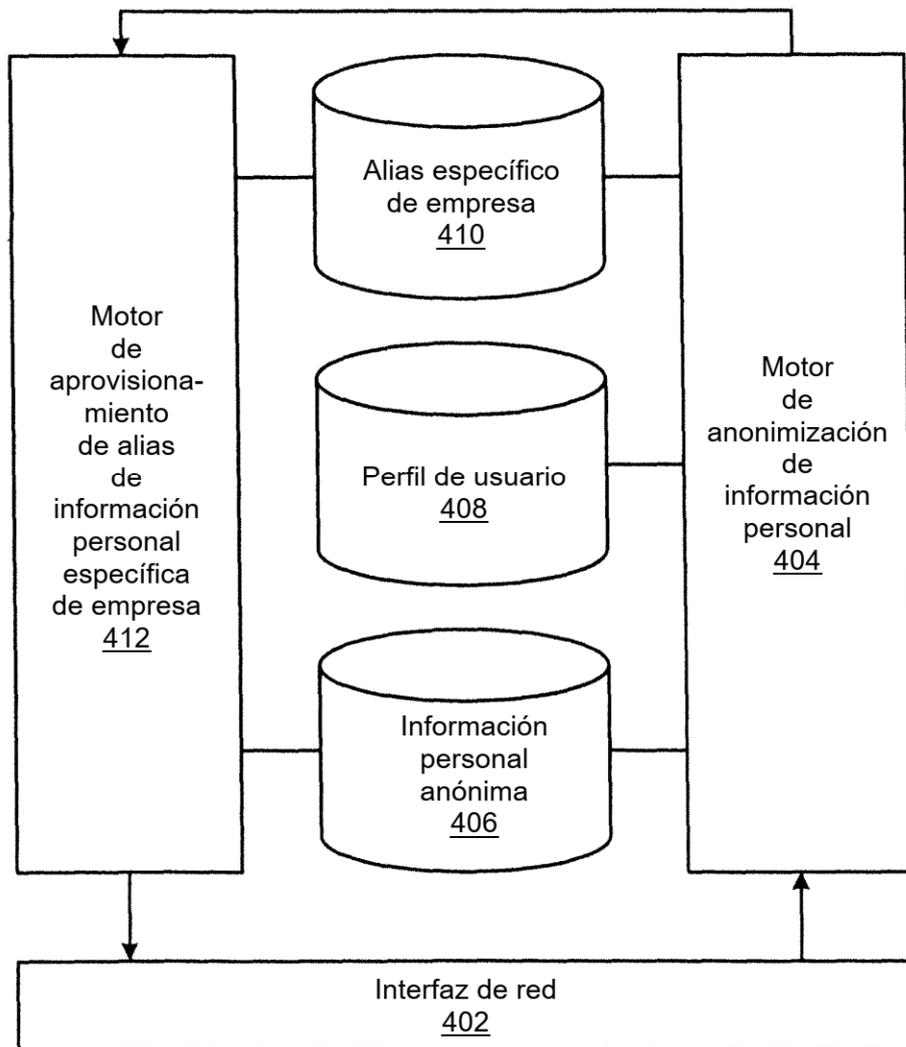


FIG. 4

500 →

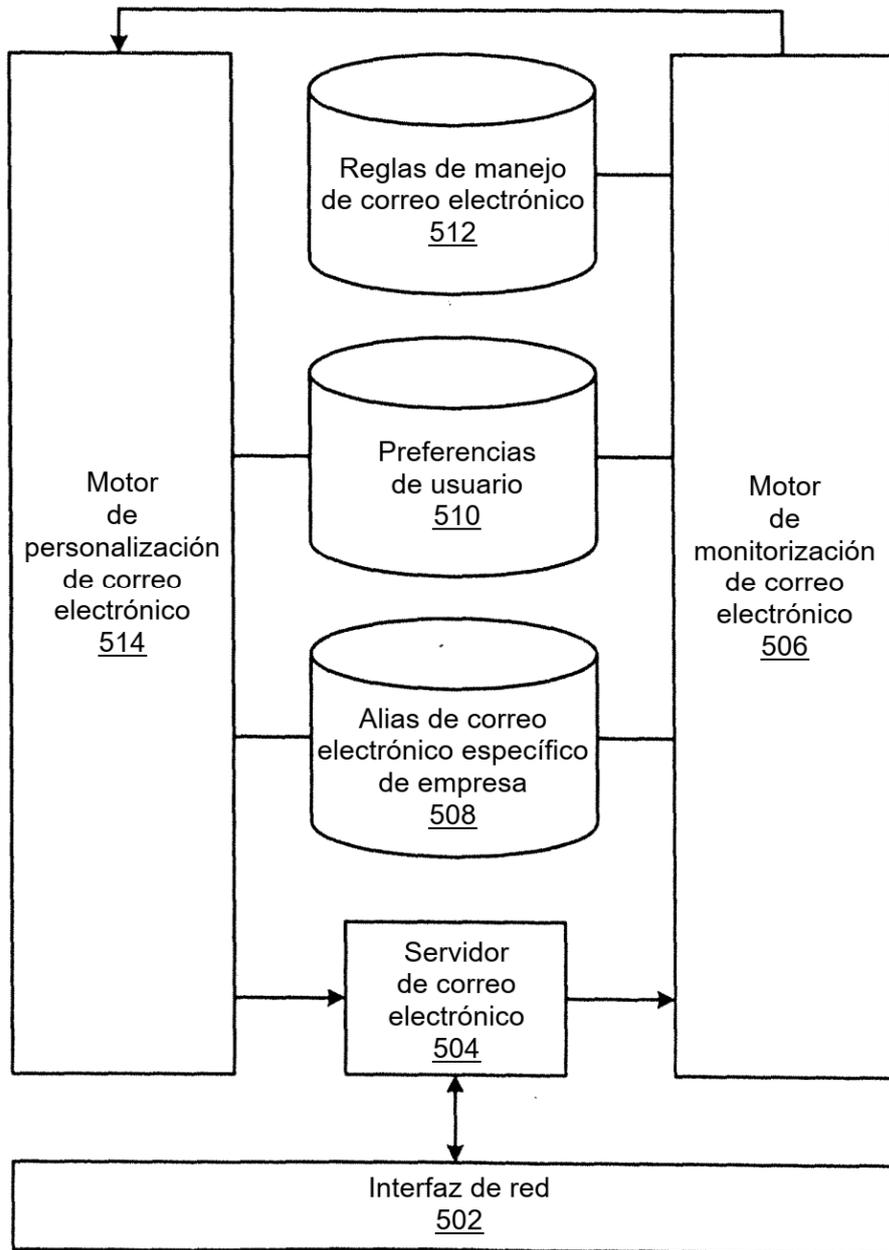


FIG. 5

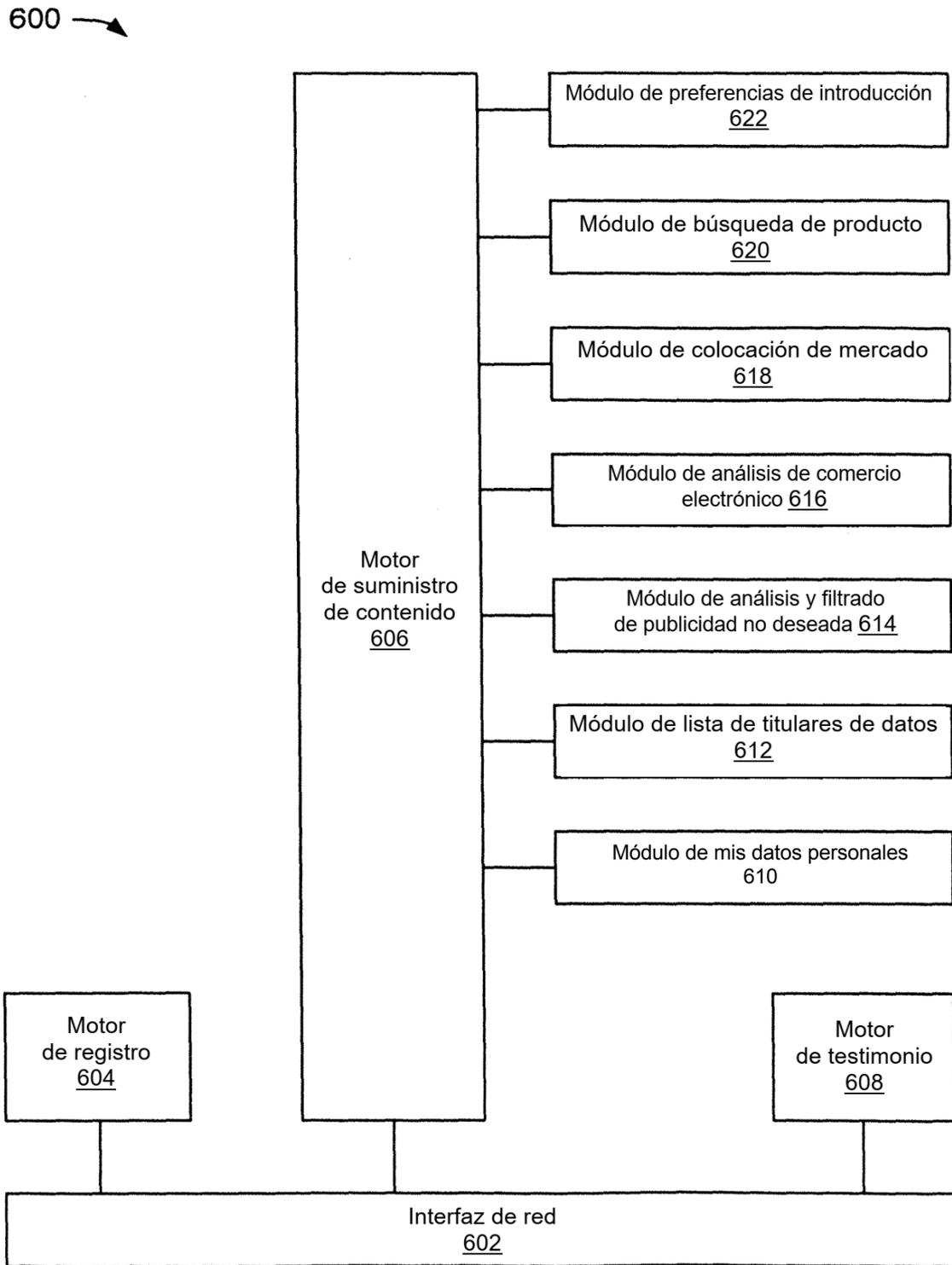


FIG. 6

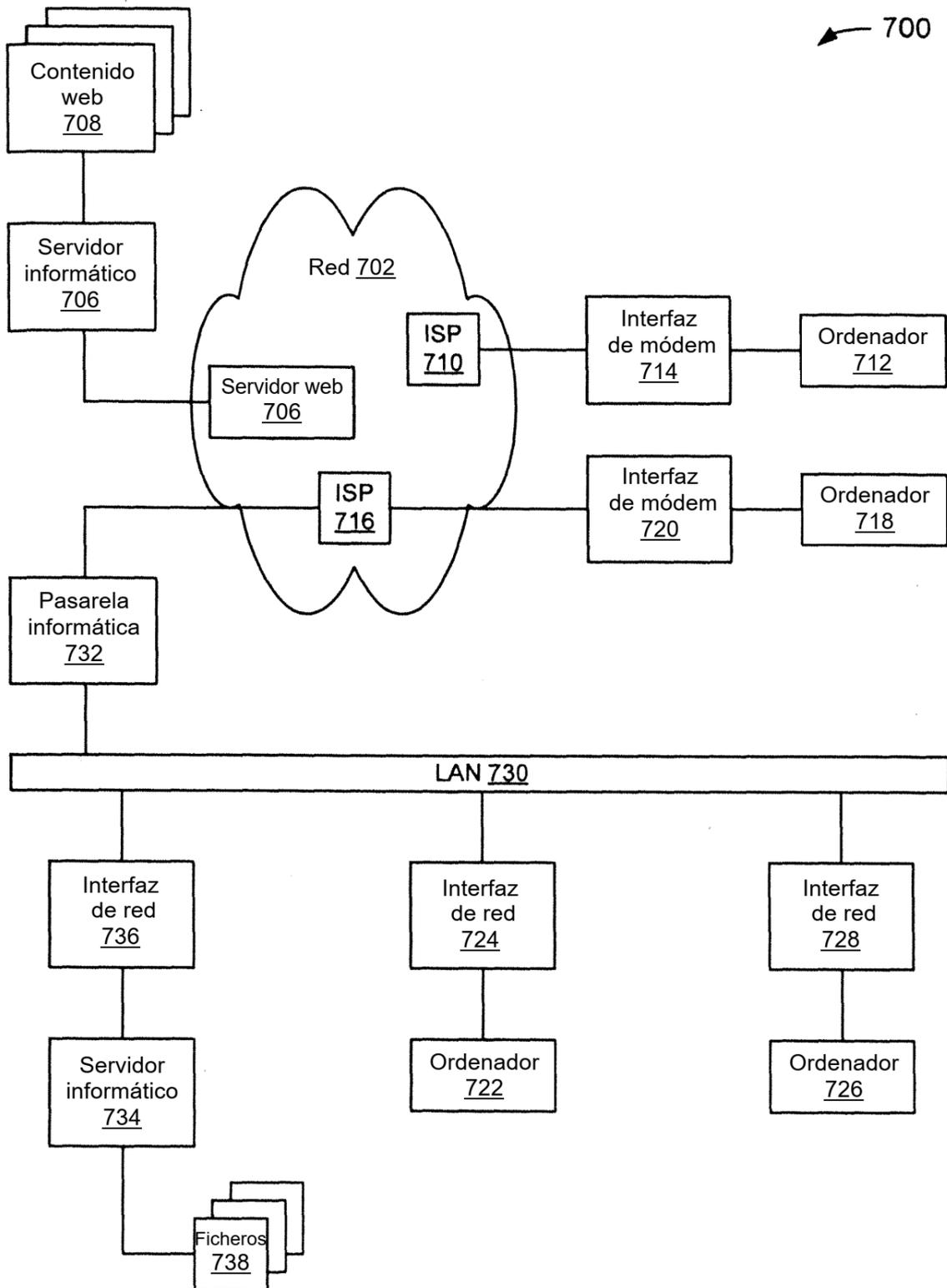


FIG. 7A

740 →

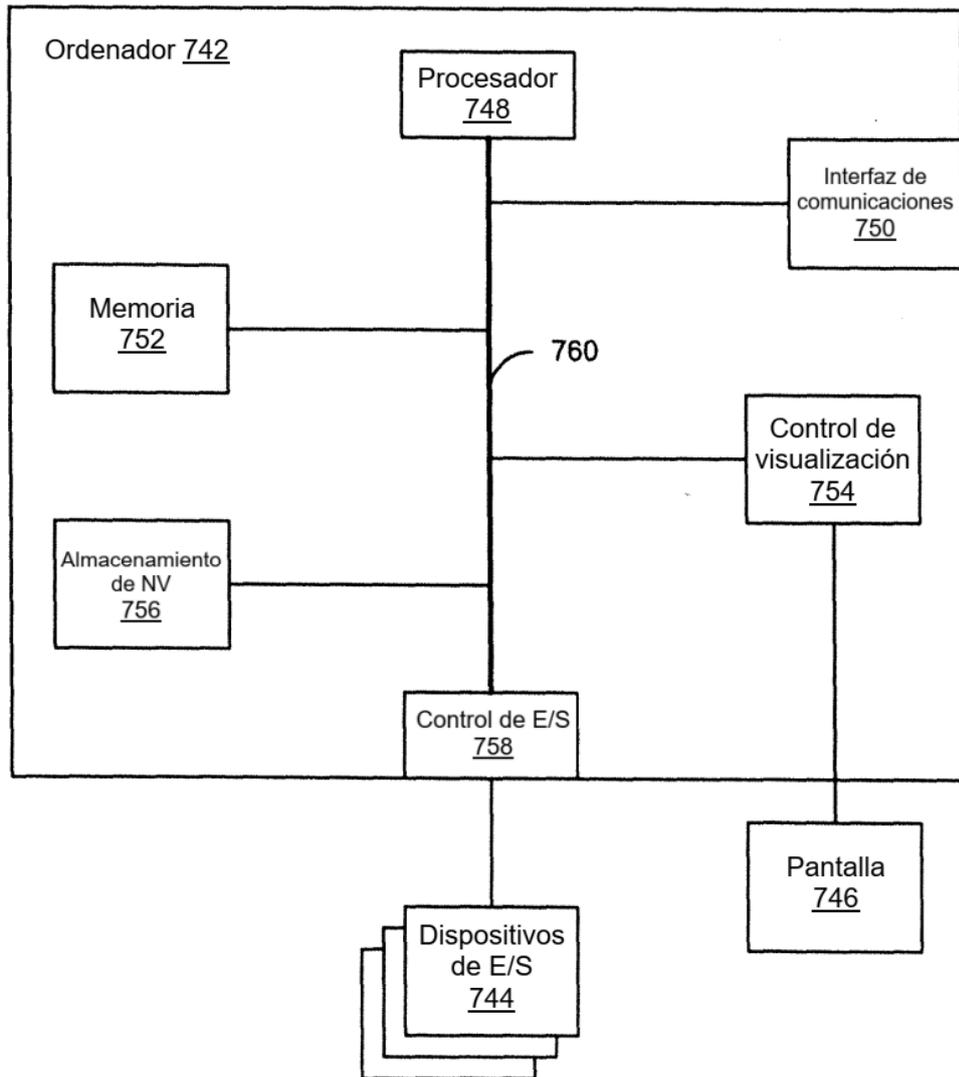


FIG. 7B

800A →

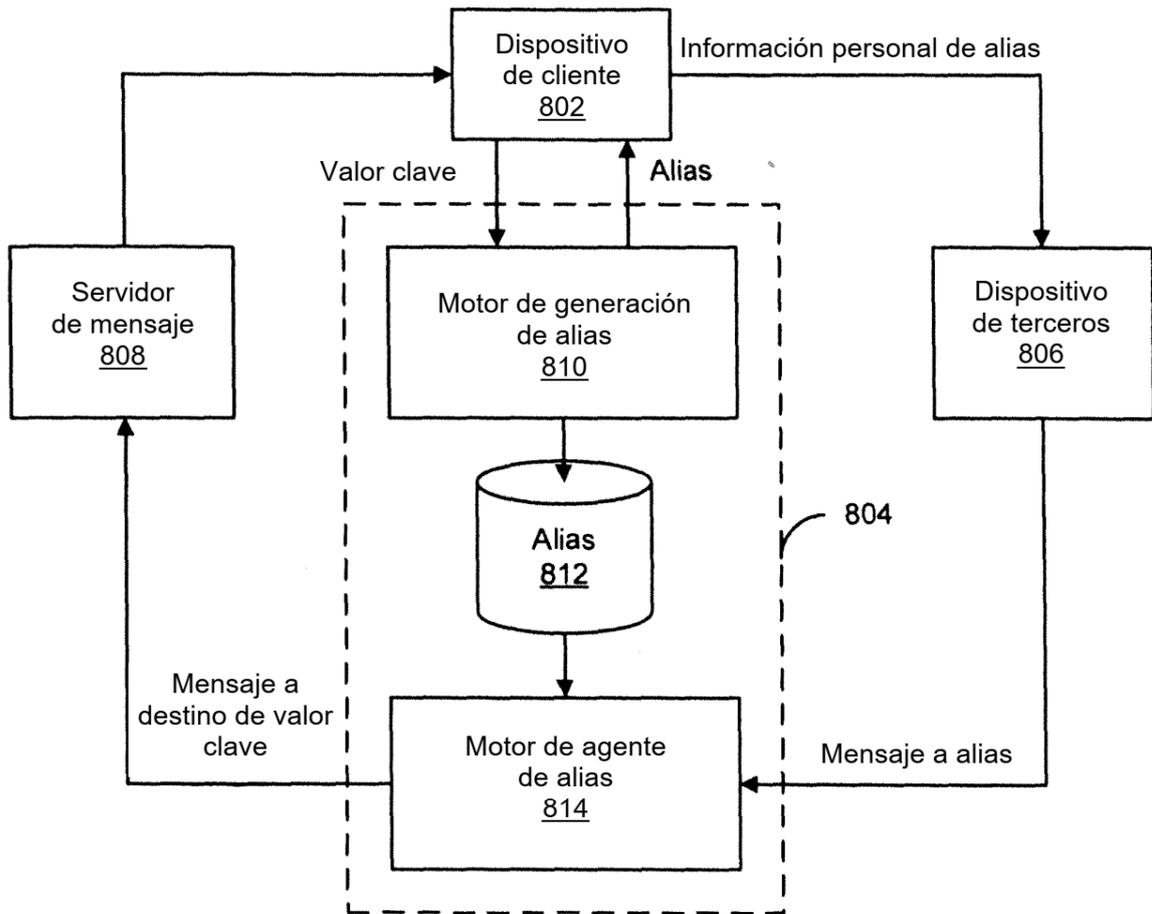


FIG. 8A

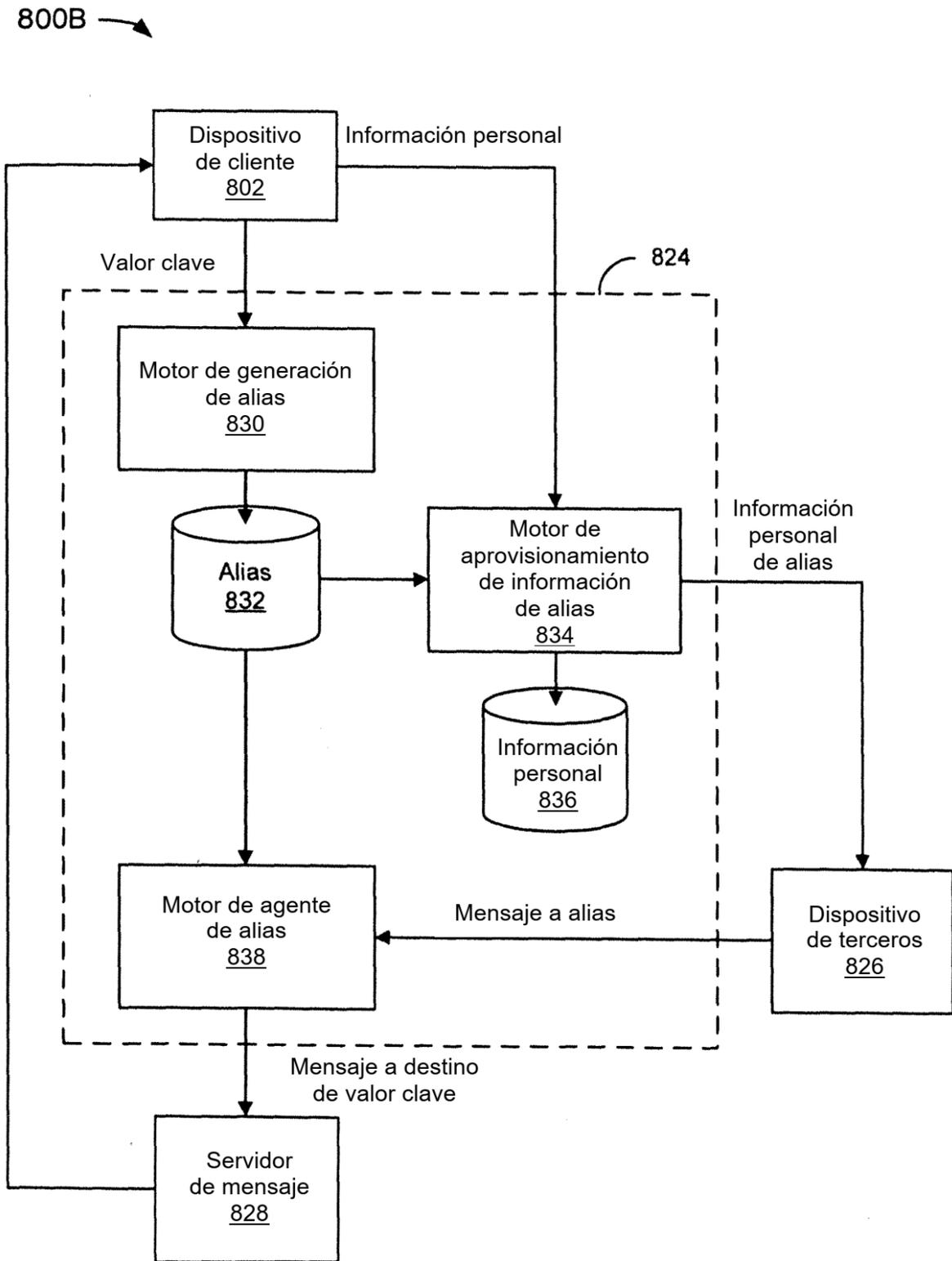


FIG. 8B

800C

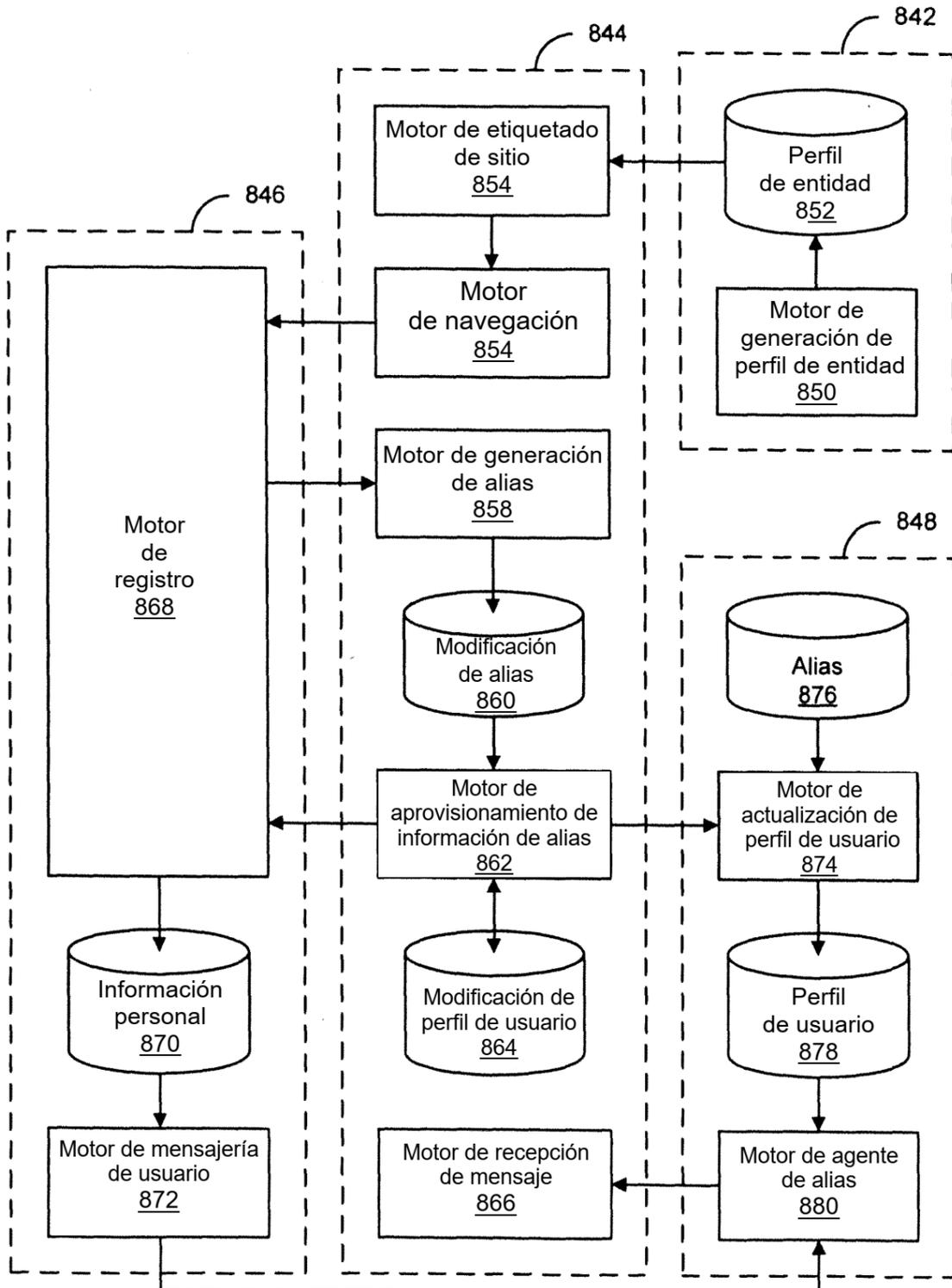


FIG. 8C

900 →

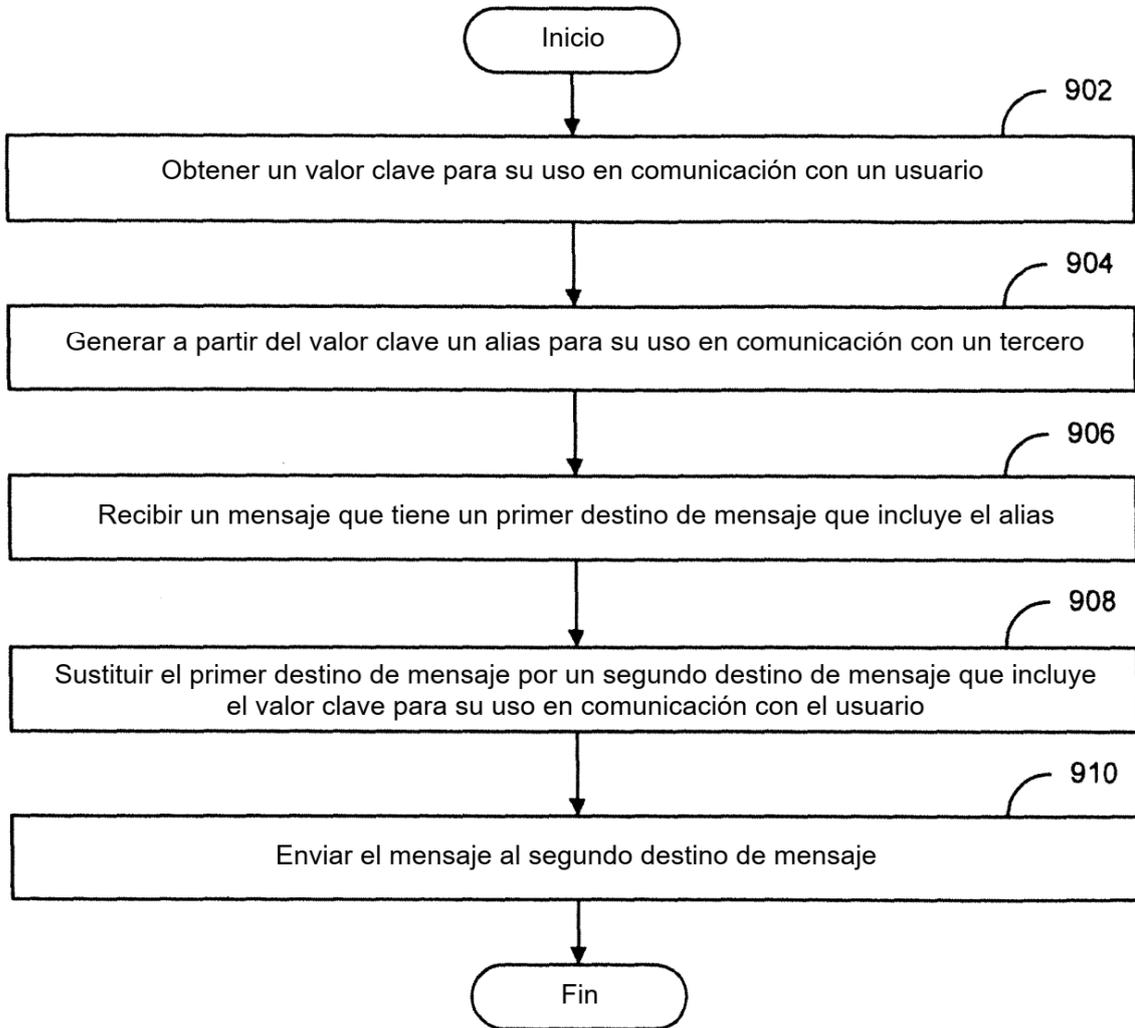


FIG. 9