Intermediarios de datos (Data Brokers): Qué son y qué puede hacer con respecto a ellos.

Si alguna vez ha buscado su nombre en Google, es posible que haya visto en los resultados de la búsqueda, sitios que decían que le habían "encontrado" o que ofrecían información de una verificación de antecedentes. Esos sitios son intermediarios de información, de datos o Data Brokers. Básicamente son sitios que permiten al usuario buscar información sobre personas, números de teléfono o direcciones concretas. Obtienen la información de una gran variedad de registros públicos y datos de los consumidores, incluidos los registros de votación y de la propiedad, la información que usted proporcionó cuando se inscribió en una tarjeta de fidelidad en el supermercado, etc.

Los intermediarios de datos suelen proporcionar información de este tipo:

- Su nombre (y posiblemente sus alias o antiguos nombres)
- Domicilio, actual y anteriores
- Número(s) de teléfono actuales y anteriores
- Los nombres y los enlaces a las páginas de perfil de los intermediarios de datos, de sus parientes cercanos o "allegados" (esto último suele referirse, en práctica, a los compañeros de casa)
- Direcciones de correo electrónico actuales y anteriores
- Enlaces a sus cuentas de redes sociales como Facebook, Twitter y LinkedIn

Normalmente, estos sitios ofrecen una versión parcial de su perfil de forma gratuita y una versión completa para los usuarios que pagan. La versión parcial puede incluir información como el nombre completo, el número de teléfono, los parientes cercanos o incluso la dirección de su residencia. La información de la mayoría de las personas aparece gradualmente en estos sitios cuando la persona tiene entre 18 y 20 años de edad. Las personas de cualquier edad pueden descubrir que su registro se enlaza con la información de otras personas, especialmente la de los familiares con los que ha convivido.

Si alguien le localiza en una nueva dirección, usted podría suponer que le están rastreando con un programa de acoso stalkerware, o que sus dispositivos están intervenidos. Esas son posibilidades sobre las que puede leer más en nuestro Conjunto de Herramientas para las Personas Sobrevivientes. Sin embargo, su nueva dirección puede haber sido revelada a través de intermediarios de datos, ya que estos son fáciles de encontrar y utilizar; incluso por personas que nunca han oído hablar de ellos.

La buena noticia es que es posible reducir significativamente el riesgo de violación a la privacidad de parte de los intermediarios de datos, a través de medidas para mantener su información fuera del alcance de estos sitios y por medio de las solicitudes de eliminación de información *(opt-out)*. Este artículo incluye los pasos a seguir para ambas opciones.

Nota importante: Al eliminar la información que los intermediarios de datos poseen, no significa que dicha información desaparece los registros originales que se utilizaron para obtener su información en primer lugar. Alguna persona podría solicitar los registros judiciales, de la propiedad o de los votantes, pero esto significaría realizar un mayor esfuerzo en la búsqueda, al igual que conocimiento de cómo navegar por los sistemas gubernamentales o tener el dinero para poder extraer la información de esas fuentes.

Riesgos, posibilidades y medidas preventivas

Los riesgos dependen de muchos factores que pueden cambiar con el tiempo. Por ejemplo:

- ¿Es solo una persona acosadora que busca su información, o también ha solicitado que sus amistades, familiares o seguidores en línea le ayuden a obtenerla?
- ¿Qué conocimientos tiene la persona en cuanto a la búsqueda de información a través del Internet?
- ¿La amenaza es exclusivamente para usted? ¿O también para su familia o amistades?

- ¿Qué información está tratando de proteger? Por ejemplo, ¿se ha mudado lejos de la persona agresora y está tratando de proteger su nueva dirección? ¿Vive con dicha persona y trata de evitar que conozca su segundo teléfono seguro o su dirección de correo electrónico alternativa?

Eliminar información de los intermediarios de datos, es ante todo una medida preventiva para aumentar la privacidad y evitar que una persona agresora, acosadora o intimidadora acceda a su información personal. Por ejemplo, si se elimina la información a la que tienen acceso los intermediarios de datos, puede evitar que una persona acosadora desconocida o conocida, o una persona con la que usted empieza a salir y todavía no tiene la seguridad sobre la relación, llegue a conocer esta información sobre usted. Esto también puede impedir que alguien se entere de una *nueva* dirección de correo electrónico, número de teléfono o domicilio.

Especialmente en situaciones como la de un cambio a una nueva dirección segura, estas medidas preventivas pueden ser fundamentales para mantener el control sobre su información. Hay algunas fuentes de datos, como los registros de la propiedad, en las que sus opciones son limitadas. Pero en el caso de las fuentes de datos de los consumidores, como las tarjetas de fidelidad de los supermercados o las suscripciones a revistas o listas de correo, puede utilizar una versión parcial de su nombre (por ejemplo, el nombre y el segundo nombre, o el segundo nombre y el apellido) o, si está permitido, un nombre ficticio. También puede utilizar una dirección de correo electrónico creada exclusivamente para este fin, o una herramienta como Mozilla Relay o SimpleLogin para "esconder" su dirección de correo electrónico. Si se requiere un número de teléfono, puede utilizar un número VoIP (basado en Internet, como Google Voice, MySudo o TextNow).

En los Estados Unidos, la mayoría de los estados cuenta con un programa de confidencialidad de direcciones (ACP por sus siglas en inglés) que permite a las víctimas de determinados delitos (normalmente violencia doméstica, agresión sexual o acoso) recibir correo en una dirección determinada que no es la de su domicilio y utilizar dicha dirección para diversos fines gubernamentales que normalmente requieren una

dirección real; como la licencia de manejo o registrarse para votar. De este modo, su dirección real se mantiene fuera de esos registros públicos, lo que también ayuda a que los intermediarios de datos se mantengan alejados. ACP difieren en cuanto a su alcance y requisitos de elegibilidad. Puede ser recomendable trabajar con una persona intercesora o gestora de casos mientras se solicita o se interactúa con estos programas. Algunos estados exigen que la solicitud sea completada por una persona intercesora.

Por último, aunque no pueda acogerse al programa de confidencialidad de direcciones de su estado, las empresas denominadas Agencias Receptoras de Correo Comercial (CMRA por sus siglas en inglés), le permiten arrendar una dirección virtual. Una dirección virtual es un buzón alquilado en una dirección real (no en un apartado de correos) que reenviará su correo a su dirección real o digitalizará su correo y se lo enviará por Internet. Las CMRAs incluyen UPS, US Global Mail, iPostal, Physical Address y muchas más. Algunos estados pueden permitirle usar una dirección virtual en lo que se refiere a su licencia de manejo u otras necesidades gubernamentales, pero deberá consultarlo con las agencias gubernamentales de su estado. Incluso si no puede utilizar esa dirección para fines gubernamentales, podrá usarla para registrarse en servicios para el consumidor lo que podría reducir el flujo de información sobre usted hacia los intermediarios de datos.

Manual: Hágalo por su propia cuenta, eliminación de información *opt-out*

Existen docenas de intermediarios de datos (Data Brokers). Aunque es complicado, usted puede eliminarse manualmente de ellos de uno en uno. Algunos plantean más riesgos que otros debido a su popularidad, a la cantidad de información proporcionada o a su posición en los resultados de las búsquedas. Algunos tienen un efecto de "goteo", en el que la exclusión de uno de ellos le eliminará automáticamente de otros. Dependiendo de lo que le preocupe, es posible que quiera excluirse de tantos como le sea posible o solamente de los intermediarios de datos más populares o de los que revelaran su nombre más fácilmente en los resultados de búsqueda. En los próximos párrafos hablaremos de las siguientes estrategias, que pueden utilizarse por separado o de manera conjunta:

1. Evaluar los resultados de los motores de búsqueda para identificar lo que una persona, que utiliza Google u otros motores de búsqueda, podría encontrar y dar prioridad a la eliminación de datos en dichos sitios.
2. Darle prioridad a la eliminación de datos para reducir rápidamente el riesgo de que alguien, que pueda conocer a los intermediarios de datos conocidos o de alta calidad, recurra directamente a ellos.
3. Eliminar completa o casi completamente su información de los intermediarios de datos.

Nota importante: aunque elimine su información de un determinado intermediario de datos, ésta puede continuar apareciendo ahí debido a la entrada de nuevos datos. Si se elimina manualmente, se puede conservar una lista y comprobar esos sitios cada tres o seis meses. Los servicios de privacidad de pago por suscripción lo podrían hacer por usted.

Posiblemente usted desee repetir las estrategias elegidas para todos los familiares que vivan o hayan vivido con usted. Una persona podría buscarlos a ellos con la esperanza de encontrar pistas sobre usted, y a veces una búsqueda del nombre le llevará a ellos o a usted. Se recomienda que hable de este tema con esos familiares, ya que la mayoría de los intermediarios de datos requieren que la persona testifique que está decidiendo por ella misma o por alguien que le ha dado permiso para hacerlo.

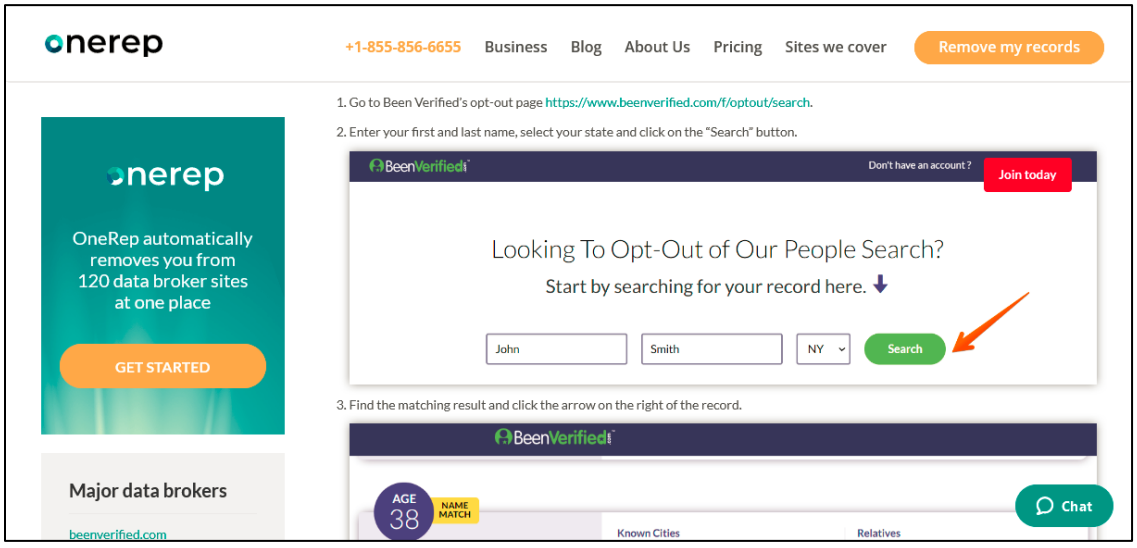
El hacer la eliminación de información (opt-out) puede ser estresante, especialmente cuando se trata de una amenaza concreta o un peligro previsible. Es posible que pueda obtener ayuda de una persona intercesora o una amistad, o procesar sus emociones a través de una línea telefónica como la Línea Nacional de Violencia Doméstica.

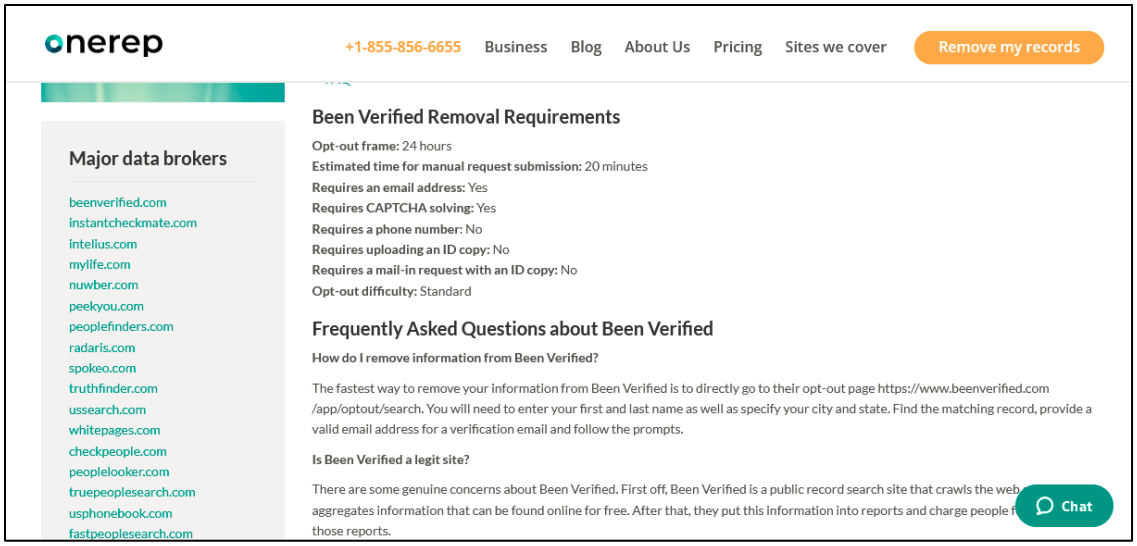
Evaluación de los resultados de los motores de búsqueda

Un método útil para aquellas personas que piensan que una persona agresora utilizará los motores de búsqueda para encontrarlas, es buscar diferentes combinaciones de su nombre y las ciudades actuales o anteriores en las que ha vivido. Por ejemplo, si Fulana de Tal, que se hace llamar fulanita, vive en Houston, Texas, después de haber vivido en

Dallas, Texas; la persona agresora podría buscar: "fulanita de tal houston texas", "fulanita de tal dallas texas", "fulanita de tal texas", "fulanita de tal houston texas", etc. Intente hacer esto y haga una lista con los sitios y enlaces que encuentre en las primeras dos páginas de los perfiles con información actual sobre usted o sus familiares cercanos. A continuación, realice el procedimiento de eliminación o exclusión de cada sitio (en la mayoría de los casos, esto requerirá proporcionar una dirección de correo electrónico o un número de teléfono - si esto le preocupa, puede crear una dirección de correo electrónico específicamente para este propósito).

En OneRep Wiki puede encontrar instrucciones detalladas y generalmente actualizadas para optar por la eliminación de la mayoría de los intermediarios de datos. OneRep también cuenta con un servicio con costo para eliminación, y lo primero que le sugerirá el sitio es que se suscriba. En vez de ello, vaya a las instrucciones "manuales" de cada intermediario de datos, donde encontrará un vídeo y un texto. Las siguientes dos capturas de pantalla de las instrucciones parciales para excluirse del popular intermediario de datos BeenVerified, ilustran de qué modo se presentan las instrucciones.





Orden de prioridad de los intermediarios de datos conocidos, para la exclusión voluntaria.

Otra manera de proteger la privacidad, especialmente si la posible persona acosadora u hostigadora está familiarizada con los intermediarios de datos o que pudiera estar trabajando con una amistad o investigador(a) que lo hace, es centrarse en las desactivaciones voluntarias de los intermediarios de datos más populares y de aquellos cuyos datos se filtran a otros intermediarios. El proceso de exclusión o eliminación voluntaria es el mismo; la diferencia estriba en cuáles se priorizan. El libro de trabajo sobre la privacidad digital de Michael Bazzell enumera los “mejores” intermediarios de datos para este propósito.

Eliminación total

Cualquiera de las dos estrategias mencionadas anteriormente reduce el riesgo. Puede dar el paso adicional de excluirse de otros intermediarios de datos para eliminar parcialmente o totalmente su información. Algunos recursos que puede utilizar son:

- El OneRep Wiki
- La guía de exclusión de DeleteMe DIY
- Libro de trabajo gratuito sobre privacidad digital de Michael Bazzell, que incluye una lista completa de intermediarios de datos e instrucciones de exclusión. La lista incluye más de un centenar de intermediarios, por lo que, si se eliminan unos cuantos al día, se tardará uno o dos meses en completarla.

Servicios de suscripción de pago.

Otra opción son las empresas, donde usted paga para que le eliminen y le excluyan de los sitios. Le eliminarán de un gran número de intermediarios y le mantendrán fuera mientras dure su suscripción. No aconsejamos ningún servicio de suscripción específico.

DeleteMe

DeleteMe es un servicio de la empresa Abine. Ofrecen los servicios de eliminar información a través de una suscripción para una, dos o cuatro personas, lo que le permite cubrir también a los miembros de su familia u otras personas. Eliminan su información de muchas bases de datos y le permiten solicitar una eliminación personalizada si descubre que su información se encuentra en un sitio que no incluyen. DeleteMe utiliza agentes que son personas reales para realizar la eliminación y la supervisión.

OneRep

OneRep ofrece planes mensuales para una o varias personas. Ofrece un costo muy bajo para este tipo de servicio y utiliza un proceso automatizado. Al momento de escribir este artículo, cubre 120 intermediarios de datos.

Safe Shepherd

Safe Shepherd, al igual que OneRep, utiliza un proceso automatizado, junto con la posibilidad de consultar con un "perito en privacidad" según sea necesario. Envía alertas cuando encuentra o elimina su información de un sitio. Además, proporciona información para la eliminación o exclusión de los sitios donde el proceso automatizado de Safe Shepherd no funciona. Tiene un período de prueba gratuito y varios planes y precios con diversos niveles de protección de la privacidad.

Después de hacer la eliminación de información (Opt-out)

Recurso para eliminar el contenido obsoleto de las cachés y las vistas previas de los motores de búsqueda.

Una vez que los intermediarios de datos han eliminado su información, podría transcurrir un período de tiempo durante el cual los resultados del motor de búsqueda todavía muestran vistas previas de la información anterior a la eliminación. Puede obtener información sobre el por qué ocurre esto y qué hacer al respecto con nuestro recurso Eliminar contenido delicado del Internet.

 Apoyado por Subvención# 15JOVW-21-GK-02216-MUMU de DOJ-OVC de los Estados Unidos. Las opiniones y conclusiones o recomendaciones expresadas son de las personas autoras y no reflejan necesariamente las opiniones del Departamento de Justicia de los Estados Unidos.

Actualizamos nuestros materiales con frecuencia. Visite TechSafety.org para obtener la última versión de este y otros materiales.