Los peligros del abuso de datos después de Roe:

Por qué Washington necesita protecciones significativas y aplicables.

Los EE.UU. no tienen una ley integral de privacidad de datos que exija transparencia y responsabilidad sobre cómo las empresas pueden utilizar los datos de una persona. Por lo tanto, las personas tienen poco conocimiento y aún menos control sobre cómo recopilan, utilizan, comparten y venden su información. El abuso de datos causa daños graves que se acentúan en un mundo post-Roe. Muchos estados se están moviendo rápidamente para criminalizar la atención del aborto y poner en peligro el acceso a los servicios de salud necesarios. En este nuevo panorama, los datos compartidos entre empresas, partes privadas y el gobierno podrían utilizarse para perseguir y acosar a las personas que buscan o acceden a servicios de salud reproductiva.

Estos son sólo algunos ejemplos de los tipos de datos que las empresas están explotando y de las muchas personas y comunidades que pueden verse perjudicadas por ello en los EE.UU. post-Roe.

Pacientes que abortan: Según un artículo de Rewire de 2016, se utilizaron datos de geolocalización para orientar a los visitantes de 140 clínicas abortistas con anuncios de servicios de consejería antiaborto para embazadas . En mayo de 2022, Motherboard reveló que SafeGraph, un intermediario de datos de localización, vendió los datos de localización agregados de personas que visitaron clínicas abortistas, incluyendo más de 600 Planned Parenthoods durante un período de una semana por solo $160. Los datos mostraban desde dónde viajaban los pacientes, cuánto tiempo pasaban en los centros de salud y adónde iban después. Los datos recopilados por la empresa incluye un análisis de dónde parece vivir la gente, basado en dónde suelen estar sus teléfonos móviles durante la noche. Las personas que abortan no deben ser objeto de publicidad selectiva sobre sus decisiones médicas privadas. No se debe rastrear ni compartir la ubicación de las personas que solicitan atención médica.

Usuarios de teléfonos móviles: Según una investigación de Vice Motherboard de 2019, AT&T, T-Mobile y Sprint han vendido las ubicaciones de los clientes y la información de identificación personal a empresas de terceros, con la información eventualmente cayendo en manos de empresas de fianzas y cazarrecompensas. No se debe permitir que los proveedores de servicios de telefonía móvil, que son una utilidad esencial en la sociedad moderna, compartan la identidad y la ubicación en tiempo real de sus clientes con compañías sospechosas. La información del teléfono móvil también fue decisiva en la acusación de una mujer que perdió un embarazo tras buscar en Internet información sobre el aborto farmacológico. En nuestra nueva realidad, en la que el aborto está penalizado, los datos de los teléfonos móviles pueden utilizarse para perseguir, amenazar y enjuiciar a quienes buscan atención médica.

Usuarios de redes sociales y apps de mensajería: Una adolescente y su madre fueron acusadas en el verano de 2022 en Nebraska. Se acusó a la madre de violar la ley estatal que prohíbe el aborto. Al investigar el caso, las fuerzas del orden obtuvieron información de la aplicación de mensajería de las redes sociales de la hija. Según Forbes, Meta, la empresa matriz de Facebook, Instagram, y Messenger, compartió la información con las autoridades en respuesta a una orden judicial que no mencionaba el aborto. Las personas que utilizan redes sociales y aplicaciones de mensajería pueden encontrarse en peligro cuando a las empresas se les permite retener y acceder a conversaciones privadas entre individuos.

Pacientes de la sala de emergencias: Los pacientes que esperaban atención médica en la sala de emergencias en Filadelfia fueron objeto de anuncios de abogados de lesiones personales, según un artículo de NPR de 2018. Dado que quienes buscan atención médica de emergencia a menudo se sienten asustados y adoloridos, no se les debe presionar para que tomen decisiones importantes mientras esperan atención para sus lesiones. En un entorno en el que un error puede dar lugar a una investigación penal, los datos de geolocalización podrían conllevar riesgos que van mucho más allá de la publicidad no deseada.

Usuarias de la app de seguimiento del ciclo menstrual: Aunque la ubicación de los usuarios no es necesaria para utilizar la aplicación, las personas que utilizan MyDays, son continuamente localizadas, según un informe de enero de

M. Lorena González, *Legislative Director* | mlgozalez@aclu-wa.org | www.aclu-wa.org

ACLU Washington

2021 del Consejo Noruego de Consumidores. La ubicación e información personal de los usuarios se comparte con una empresa que comercializa con compañías de seguros y otros datos personales como "el usuario ha llegado a una clínica" o "el usuario podría no estar en condiciones de conducir por falta de sueño." En 2021, Flo Health, una de las aplicaciones de seguimiento del ciclo menstrual más populares, llegó a un acuerdo con la FTC por las acusaciones de que compartía información de salud de sus 100 millones de usuarios con empresas de análisis de datos de terceros.

Las personas que intentan conseguir o evitar un embarazo no deberían temer que las compañías de seguros utilicen su información para discriminarlas.

La sentencia del Tribunal Supremo también abre la puerta a posibles restricciones futuras de otros derechos y libertades, como el matrimonio entre personas del mismo sexo, el matrimonio interracial, las relaciones íntimas entre personas del mismo sexo y la contracepción.

Usuarios de aplicaciones de citas: A los usuarios de aplicaciones de citas se les anima a revelar detalles íntimos sobre su vida para poder emparejarlos con el prospecto romántico más compatible. Las aplicaciones se aprovechan de esta información sensible compartiéndola con otras compañías. Un informe del Consejo Noruego del Consumidor de enero de 2021 descubrió que OKCupid compartía con terceros la ubicación de los usuarios e información sobre sus deseos sexuales, consumo de alcohol, opiniones políticas y origen étnico, mientras que Tinder compartía la ubicación, edad, sexo y preferencias de pareja de los usuarios.

Usuarios de la aplicación de citas LGBTQIA2S+: En 2018, Buzzfeed descubrió que la app de citas Grindr LGBTQIA2S+ estaba compartiendo el estado de VIH de sus usuarios e información de identificación personal con terceros. Aunque los usuarios tienen un verdadero interés en conocer el estado de VIH de sus potenciales parejas, un usuario señaló que dejó de compartir su estado de VIH en la app, explicando que compartir esa información indiscriminadamente "puede poner a las personas en peligro, y se siente como una invasión de la privacidad."

M. Lorena González, *Legislative Director* | mlgozalez@aclu-wa.org | www.aclu-wa.org

ACLU Washington