Consideraciones para jueces y proveedores de visitas supervisadas: Aplicaciones para coparentalidad y visitas

¿Por qué este tema?

En los últimos años, las aplicaciones para coparentalidad y organización de visitas se han vuelto cada vez más populares como herramientas para que los padres divorciados o separados puedan comunicarse sobre asuntos relacionados con sus hijos. Los padres pueden elegir usar estas aplicaciones de manera voluntaria. En algunos casos, los tribunales pueden exigir su uso para que los padres se comuniquen sobre temas de custodia. Esto es especialmente común en situaciones donde ha habido abuso o violencia en la relación. Algunas de estas aplicaciones tienen funciones que permiten a los tribunales supervisar todas las comunicaciones, lo cual ayuda a documentar el cumplimiento de las órdenes judiciales. Es importante considerar las implicaciones de seguridad, privacidad y confidencialidad al utilizar estas aplicaciones de comunicación.

Este documento se divide en dos secciones: una para quienes usan las aplicaciones y otra para quienes las asignan o interactúan con ellas a nivel profesional. Aunque estas aplicaciones pueden proporcionar una plataforma para que las personas (las partes del caso) se comuniquen y para que el personal del tribunal, como los jueces, los profesionales jurídicos que trabajan con las personas sobrevivientes y los proveedores de visitas supervisadas las controlen, es crucial que todos los usuarios comprendan cómo funcionan estas aplicaciones y los riesgos potenciales que pueden representar para las personas usuarias y sobrevivientes.

Consideraciones sobre la privacidad y la seguridad de las personas sobrevivientes

¿Cuándo son apropiadas las aplicaciones de comunicación?

La privacidad es crucial y está estrechamente ligada a la seguridad, especialmente en situaciones de abuso o acoso. Un progenitor que no pueda utilizar una aplicación de coparentalidad de manera segura puede tener dificultades para cumplir con los requisitos del tribunal. El propósito de las órdenes judiciales es promover el bienestar del menor, lo cual no se puede lograr si se pone inadvertidamente en peligro a uno de los progenitores. Por ejemplo, considere un escenario en el que la información personal compartida a través de la aplicación, como horarios, información de contacto o detalles sobre las actividades del menor, puede ser utilizada indebidamente para acechar, acosar, manipular y ejercer poder y control sobre la persona sobreviviente. Esto, a su vez, puede causar estrés al progenitor y afectar negativamente en el bienestar del menor.

Evaluar los problemas de privacidad que podrían ser relacionados con el uso de las aplicaciones de comunicación es un paso importante antes de utilizarlos. A continuación se presentan algunas de las preguntas que pueden ayudar en esta evaluación.

¿El aviso de privacidad es claro y útil?

El aviso de privacidad de una aplicación es el documento público que informa a los usuarios sobre cómo se recopilan y manejan sus datos. Permite a los usuarios decidir de manera informada si desean añadir sus datos delicados a la aplicación o alguna cuenta. Lamentablemente, estos avisos pueden ser difíciles de leer y entender para muchas personas. Idealmente, el aviso de privacidad debe estar escrito en un lenguaje claro y describir claramente lo siguiente:

- Qué permisos requiere del dispositivo (servicios de localización, acceso a la cámara, etc.).
- Qué datos recopila.

- Qué datos se pueden compartir y con quién.
- Cómo tratará la empresa los datos.
- Qué políticas tiene la empresa con respecto a la retención y eliminación de datos.

¿Son transparentes las solicitudes de consentimiento y permisos de los usuarios?

A veces, cuando una aplicación o un sitio web solicita consentimiento para ciertos permisos o acceso a información, no es del todo clara sobre lo que está pidiendo y puede usar tácticas engañosas para conseguir que los usuarios acepten. Un ejemplo de esto sería una solicitud que pide permiso para recopilar datos de ubicación, donde la casilla "Sí" está marcada por defecto y no aclara si compartirá esos datos.

También pueden surgir otros problemas en el diseño de las aplicaciones, que a menudo recopilan más información de identificación sobre los usuarios de lo que estos pueden darse cuenta. Comprender exactamente qué datos están recopilando la aplicación y la empresa que la respalda es crucial para garantizar un uso adecuado, especialmente cuando la privacidad está relacionada con la seguridad.

¿La aplicación requiere que se activen las funciones de localización?

Los expertos en seguridad suelen recomendar a las personas sobrevivientes que desactiven el GPS y otras funciones de localización de un dispositivo cuando no están en uso. Esto ayuda a evitar que los agresores utilicen la información del GPS para localizar a la persona sobreviviente. Las aplicaciones que requieren mantener activadas las funciones de localización en todo momento están en conflicto con esta práctica recomendada.

Algunas funciones de una aplicación de coparentalidad pueden requerir que los servicios de localización estén activados para fines de documentación. Por ejemplo, la aplicación puede documentar si un progenitor estuvo en un lugar específico a una hora determinada para que el otro progenitor pudiera recoger al menor. Sin embargo, estas situaciones solo representan una pequeña parte de la vida de un progenitor y de su crianza. Una función de la aplicación que permita al usuario cargar una ubicación a una hora programada ofrece más opciones de seguridad que una aplicación que exija tener la ubicación activada constantemente.

¿Es una aplicación móvil, un portal web o ambos?

Algunas aplicaciones solo pueden utilizarse a través de un teléfono o una tableta, mientras que otras también (o únicamente) ofrecen un portal web que permite a los usuarios iniciar sesión desde cualquier dispositivo con un navegador. Dado que no todo el mundo tiene un teléfono inteligente o una tableta, es importante conocer estos requisitos antes de emitir una orden judicial o hacer una recomendación. Más allá de la accesibilidad, también hay consideraciones de seguridad para las personas sobrevivientes.

Además, no siempre es seguro que las personas sobrevivientes utilicen sus propios teléfonos o tabletas. Los agresores o acosadores pueden haber instalado en ellos programas de acoso (stalkerware) que les permiten ver toda la actividad de las aplicaciones, incluidas contraseñas o información financiera de la persona sobreviviente. Si un agresor y una persona sobreviviente no viven separadamente o viven cerca, el agresor también puede tener acceso físico a los dispositivos móviles de la persona sobreviviente. Si una aplicación tiene un portal web, una persona sobreviviente sin un dispositivo móvil seguro puede utilizar un dispositivo alternativo, como la computadora de una amistad, familiar o biblioteca, para interactuar con la aplicación. Por razones de seguridad, es importante

que una aplicación con un portal web ofrezca la protección mediante contraseña.

El reverso de esta moneda es que si el dispositivo móvil de una persona sobreviviente es seguro para su uso, pero el agresor conoce o puede adivinar las contraseñas de su cuenta, el portal web puede introducir una vulnerabilidad (ya que el agresor podría acceder a su cuenta desde cualquier lugar). Por ello, es preferible que cualquier aplicación de coparentalidad o de visitas supervisadas admita *alguna forma de autenticación multifactor*. La autenticación multifactor significa que, además de una contraseña, alguien que acceda a una cuenta debe proporcionar al menos otro «factor». Esto puede ser un código enviado por SMS o correo electrónico a la persona que inicia sesión, la verificación a través de una aplicación de autenticación, un escáner de reconocimiento facial o cualquier otra medida. Esta práctica recomendada en materia de seguridad también protege la información destinada al control del cumplimiento por parte del tribunal contra posibles hackers o piratas informáticos.

Como se mencionó anteriormente, contar con versiones tanto móviles como web de una aplicación suele ser una ventaja para las personas sobrevivientes, ya que les permite elegir la opción más segura para ellas. No obstante, es igualmente importante asegurarse de que todas estas opciones tengan la seguridad adecuada.

¿Qué metadatos contienen las imágenes y los vídeos?
Los metadatos son «datos sobre datos» y también pueden denominarse «propiedades» o «información» del archivo, dependiendo del sistema operativo. Por ejemplo, uno de los padre toma una foto de su hijo con un dispositivo digital. Los datos son la imagen de la foto almacenada como

información del archivo (como un archivo .JPG). Los tipos de metadatos de esa foto dependerán de las capacidades del dispositivo digital que se haya utilizado. Los metadatos pueden incluir la fecha y la hora en que se tomó la foto, la ubicación en la que se tomó (si el dispositivo era un smartphone), el nombre o identificador de usuario de la persona propietaria del dispositivo o de una cuenta relacionada, información sobre el dispositivo, etc. Existen numerosas herramientas en línea que eliminan los metadatos. Si un tribunal está considerando ordenar una aplicación y no tiene clara su política de metadatos, también podría considerar sugerir una de estas herramientas de terceros.

¿Qué permisos requiere la aplicación?

Las aplicaciones requieren ciertos «permisos» para funcionar, que pueden ser para una funcionalidad básica o una característica opcional. Algunos ejemplos que podrían encontrarse en aplicaciones de coparentalidad y visitas supervisadas son:

- La aplicación podría solicitar permiso para acceder al micrófono del dispositivo, permitiendo a un progenitor grabar un mensaje de voz para su hijo.
- La aplicación podría solicitar permiso para acceder a la ubicación del dispositivo con el fin de documentar que un progenitor llegó a un lugar específico a una hora determinada.
- La aplicación podría solicitar permiso para acceder a la cámara del dispositivo para una sesión de visita virtual. Si el usuario deniega este permiso, no podrá aparecer en video durante la reunión.

También puede haber distintos niveles de permisos. Por ejemplo, un usuario puede conceder a una aplicación acceso a la ubicación del

dispositivo todo el tiempo, solo mientras la está usando, o denegarle el permiso por completo.

Algunos de estos permisos podrían revelar información delicada sobre una persona sobreviviente. Si está considerando ordenar a los coprogenitores que utilicen una aplicación determinada, es fundamental asegurarse de que tiene prácticas responsables respecto a los permisos. Esto también puede implicar replantearse las propias necesidades del tribunal, con el fin de limitar la recopilación de datos que podrían comprometer la seguridad de una persona sobreviviente. El propósito del tribunal al ordenar el uso de estas aplicaciones es supervisar el cumplimiento de las órdenes judiciales: ¿qué necesita realmente el tribunal para este propósito? Si se obliga a una persona sobreviviente a usar una aplicación que no le permite tomar las medidas de seguridad discutidas con un defensor de violencia doméstica u otro profesional del área, la persona puede sentirse confundida.

¿Qué datos recopila la aplicación o el portal web? ¿Con quién se comparten?

En general, las aplicaciones y los sistemas de software solo deben recopilar los datos que necesitan para funcionar. Si no recolectan los datos, no pueden ser vulnerados ni compartidos. Para una aplicación destinada a documentar las comunicaciones entre los padres, los datos necesarios serán más que para otros tipos de aplicaciones. Sin embargo, los tribunales deben seguir considerando si las aplicaciones recopilan datos innecesarios. Por ejemplo, si la aplicación es un mecanismo de comunicación entre las partes, no tiene por qué recopilar y almacenar los números de teléfono o direcciones de los usuarios. Tampoco debería necesitar recopilar información sobre el uso del dispositivo que no esté relacionada con la aplicación.

Además, está la cuestión de quién más puede ver los datos. La mayoría de los sistemas de software utilizan una pila tecnológica, lo que significa que integran otros productos tecnológicos como componentes del suyo propio. Esto es análogo a que un carpintero use ladrillos, tablas y tuberías fabricados por otros, en lugar de tener que fabricar todos sus propios materiales desde cero. ¿Pueden otras empresas tecnológicas cuyos productos forman parte de la pila tecnológica de una aplicación o sitio web acceder a los datos de los usuarios de manera legible? Junto con la pila tecnológica, muchas aplicaciones y sitios web comparten datos con socios publicitarios o se los venden. Si un desarrollador de una aplicación de coparentalidad o visitas supervisadas hace esto, podría significar que personas mucho más allá del tribunal tengan acceso a los datos de los usuarios de la aplicación. A menudo es posible ver qué datos comparte una aplicación con otras organizaciones al acceder a su página en la tienda Google Play y hacer clic en «Seguridad de los datos». Cuantos más datos se recopilen y más empresas tengan acceso a ellos, mayor será el potencial de exposición y el riesgo para la seguridad de las personas sobrevivientes.

¿Cuáles son las políticas de conservación y eliminación de datos del desarrollador de la aplicación?

Los aspectos prácticos de una aplicación de coparentalidad o visitas, especialmente una ordenada por los tribunales, pueden requerir que los datos se conserven durante cierto tiempo. Sin embargo, esto no implica que todos los datos deban conservarse indefinidamente. ¿Permite la aplicación a los usuarios borrar sus datos si el caso se resuelve y la aplicación ya no es necesaria para sus fines o los del tribunal? ¿Qué datos almacena y cómo están protegidos? ¿Durante cuánto tiempo? Conservar datos innecesarios o utilizar prácticas de ciberseguridad deficientes al almacenarlos, crea un riesgo si el desarrollador de la aplicación es hackeado o pirateado.

Cuando los tribunales o los centros de visitas supervisadas exigen a las víctimas que utilicen aplicaciones específicas, es crucial considerar los riesgos potenciales para la seguridad y apoyar a las personas sobrevivientes incorporando una planificación de seguridad. La colaboración con programas locales contra la violencia doméstica o coaliciones estatales puede ofrecer valiosos conocimientos y recursos. Trabajando juntos, podemos crear un enfoque integral para abordar la seguridad tecnológica, garantizando que las personas sobrevivientes estén informadas y apoyadas en su uso de la tecnología necesaria. Dado que la mayoría de los jueces, funcionarios del tribunal y proveedores de visitas no son expertos en ciberseguridad, también podría ser útil trabajar con un consultor externo. Un profesional de tecnología e informática con experiencia en ciberseguridad o privacidad de datos puede evaluar si una aplicación ofrece la seguridad adecuada. También, si tiene preguntas específicas, puede comunicarse con Safety Net en safetynet@nnedv.org o visitar nuestro sitio web, techsafety.org.

 Apoyado por US DOJ-OVW Subvención #15JOVW-23-GK-05170-MUMU. Las opiniones, resultados y conclusiones o recomendaciones expresadas son de los autores y no representan necesariamente los puntos de vista del Departamento de Justicia de los Estados Unidos.

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