Una publicación de Consumer Action

¡Tenga cuidado!

El video en línea y su privacidad

La forma en que miramos videos ha cambiado. Ya no estamos limitados a mirar en casa los programas de televisión producidos profesionalmente. Usted puede mirar lo que quiera, cuando quiera y en el momento que lo pida por medio de los servicios "on demand". También los puede mirar en cualquier lugar, gracias a los dispositivos móviles. Incluso, puede mirar videos que otros comparten, o crear los suyos propios.

Mientras que los consumidores ahora tienen más opciones y mayor libertad en la forma de mirar videos, también se presentan nuevos riesgos para la privacidad personal. Usted podrá controlar los riesgos y disfrutar igual del espectáculo, si tiene presente las cuestiones de privacidad que plantean la transmisión de video por "streaming" y la tecnología para compartir videos, y si aprende sobre los pasos a tomar para protegerse.

Transmisión de video por 'streaming'

"Streaming" se refiere a ver o escuchar contenidos en "tiempo real" al mismo tiempo que se envían por Internet. Se ha convertido en una opción para muchos más consumidores gracias a Internet de alta velocidad, a dispositivos móviles y dispositivos para streaming, y a servicios y "software" para streaming.

Con respecto a los servicios pagados de televisión, muchos consumidores están "cortando el cable"; están reemplazando el servicio de cable o satélite con uno o más servicios de streaming menos costosos.

Esto significa que si usted utiliza más de un servicio de video por streaming, por ejemplo, Netflix ***y también*** Hulu ***y también*** Amazon Prime, entonces está compartiendo con varias compañías, y no con un solo proveedor de servicio de televisión pagado, su historial de reproducciones y, en muchos casos, también la información de facturación.

Además, casi siempre hay por lo menos un par de intermediarios entre usted y su video de transmisión por streaming. Estos serían su proveedor de servicios de Internet (ISP, siglas en inglés), la aplicación o "app" del servicio de streaming o el navegador de Internet, y hasta el fabricante del televisor o dispositivo.

Todo esto aumenta la posibilidad de que sus elecciones de video, historial de reproducción y ciertos datos personales sean recogidos y utilizados por otras empresas, a menudo con propósitos de publicidad o de venta a firmas de publicidad en línea y corredores de datos. (Los corredores de datos o "data brokers" son empresas que recogen y venden información sobre los consumidores, por lo general para fines de comercialización.)

La ley de protección de la privacidad sobre videos, Video Privacy Protection Act (VPPA) de 1988, prohíbe que los servicios de video compartan con terceros la información personal del cliente sin consentimiento del espectador.

Sin embargo, según una enmienda a la ley en 2012, las empresas de video por streaming deben solicitar su permiso ***una sola vez*** antes de poder compartir información sobre los videos que alquila o que compra. (Gran parte de lo que se comparte ocurre a través de las redes sociales cuando usted elige "Me gusta" o "Compartir" ("Like" o "Share") en Facebook). Si cuando le preguntan por primera vez usted no elige la opción de no compartir su información (elegir "opt out"), su consentimiento a compartir quedará vigente por dos años. Sin embargo, sí tiene derecho a retirar su consentimiento en cualquier momento.

Cada estado puede promulgar protecciones más amplias para el consumidor que las de VPPA, y muchos lo han hecho (entre otros, California, Delaware, Iowa, Luisiana, Michigan, Nueva York y Rhode Island). Para averiguar si su estado tiene sus propias leyes sobre la privacidad de video, visite el centro de información sobre privacidad electrónica, Electronic Privacy Information Center (EPIC), en línea (*http://bit.ly/21xf3U2*). O comuníquese con la oficina del procurador general ("attorney general") en su estado; busque los datos de contacto en la página web de la asociación nacional de procuradores generales, National Association of Attorneys General (*www.naag.org*).

Los clientes de Internet de banda ancha reciben algunas protecciones contra el uso indebido o la violación de sus datos personales en la ley federal de comunicaciones, Communications Act, que en un principio se creó para proteger a los clientes de servicio telefónico. Según la orden de Internet abierta, Open Internet Order de 2015, los proveedores de servicios de Internet de banda ancha sólo tienen permitido utilizar, divulgar o permitir el acceso a "información individual identificable" del cliente para prestar servicios. Sin embargo, todavía existen dudas sobre lo que se considera información privada. Las compañías de cable también están obligadas a proteger la "información personal identificable" de los suscriptores, sea cable, servicio de banda ancha o servicio telefónico el que ofrezcan.

Ya que estas leyes siguen dando lugar a la preocupación sobre la privacidad de usuarios de video por streaming, usted debe ser proactivo en la protección de su información. Los siguientes son algunos pasos que puede tomar:

- Lea la política de privacidad de cualquier app o servicio de streaming que considere usar. Entérese acerca de la configuración de privacidad y acerca de las opciones "opt out" que le permitan elegir que no se comparta su información. Si la manera en que la empresa podría utilizar su información personal no le parece, busque un servicio diferente que ofrezca más derechos de privacidad. (En How to Read a Privacy Policy (Cómo leer una política de privacidad) (*http://bit.ly/1LvfaYN*) la agencia California Department of Justice ofrece valiosos consejos que aplican en cualquier estado.)
- Cuando utilice un navegador web para streaming, experimente con herramientas contra el rastreo, tal como Do Not Track Plus y Ghostery, ambos programas "plug-in" que amplían la funcionalidad del navegador. Para mayor privacidad, también ajuste la configuración de privacidad integrada en el navegador. Es posible que ciertos programas plug-in interfieran con la visualización en el navegador. Si fuera así, desinstale el plug-in desde la ventana de preferencias y pruébelo en otro navegador. (En general, las apps para dispositivos móviles, pueden rastrearlo y enviar información a terceros para comercialización y otros propósitos y no ofrecen herramientas contra el rastreo.)
- Pruebe los servicios de video por streaming que más le gusten utilizando la opción de "navegación privada" o "private browsing" de su navegador. Como en otras herramientas contra el rastreo, esto podría impedir el funcionamiento del servicio de streaming. Además probablemente no pueda evitar que el servicio de streaming reciba información suya una vez que haya abierto la sesíon. Pero si funciona la opción de navegación privada, entonces podría evitar que piratas cibernéticos o "hackers" vean sus actividades. Y como sus actividades no se agregarán al historial de su navegador o al almacenamiento en la nube, no podrán verlas otras personas que compartan un dispositivo o cuentas con usted.
- Verifique si el sitio web o la app ofrecen la opción de borrar el historial de lo que ha visto y de sus búsquedas. YouTube y Netflix son sólo dos de los servicios de video que lo ofrecen. También podría ser posible borrar el historial de streaming en su consola de juegos o en su dispositivo de streaming. Sin embargo, esto sólo impide que otros que podrían compartir un equipo, dispositivo, televisor o cuenta de streaming con usted vean su historial. En general no elimina el historial que figure en los registros del proveedor de servicios.
- Si no desea que su público en los medios sociales sepa qué videos mira, no haga clic en "Me gusta" o en cualquiera de los otros botones de "Compartir" de los medios sociales que aparecen en sitios de streaming como Netflix.com. (Recomiende películas a amigos a través de correo electrónico o mensajes privados).
- Si usted quiere gozar de las protecciones que otorga la VPPA, deberá registrar una cuenta, pagar para ver un video, descargar una app o dar algún otro paso para que lo consideren como "cliente" o "consumidor" del proveedor de servicio. Aunque sigue habiendo cierta incertidumbre, en 2015 un tribunal falló que las empresas que comparten con terceros el historial de visualización de personas "no abonadas" no infringen la ley VPPA.
- Si usted no optó por que no se divulgara su historial de visualización cuando tuvo la oportunidad, y si, al seleccionar videos, no le dan oportunidades adicionales para optar contra la divulgación de su información, puede retirar su consentimiento en cualquier momento siguiendo

las instrucciones en el sitio web de la compañía. (La ley requiere que los proveedores de servicio notifiquen a los consumidores "en forma clara y visible" sobre la capacidad de optar por no compartir más información.)

Para presentar una queja contra su proveedor de servicio de Internet, visite la página de la FCC para este tipo de denuncias (*http://bit.ly/1KZvzVz*) o llame al 888-CALL-FCC (888-225-5322)/TTY: 888-TELL-FCC (888-835-5322).

Para presentar una queja contra una empresa que, por medio de Internet de banda ancha, ofrece servicios, contenidos, productos o apps, visite la página web para quejas de la Federal Trade Commission (FTC) (*www.ftccomplaintassistant.gov*) o llame al 877-FTC-HELP (877-382-4357).

Televisores inteligentes ('Smart TV')

Cualquier dispositivo que se conecta a Internet es vulnerable a la violación de datos por piratas cibernéticos o "hackers". Esto incluye televisores "inteligentes", o sea, televisores habilitados para Internet. En pruebas realizadas por investigadores de seguridad, pudieron conseguir acceso a un televisor inteligente y encenderle su cámara integrada y micrófonos. También existe la posibilidad de robar los nombres de inicio de sesión y las contraseñas y de instalar programas maliciosos.

Además existe la posibilidad que los fabricantes de televisores inteligentes recopilen y compartan el historial de lo que ha visto. Los televisores inteligentes utilizan el llamado "reconocimiento automático de contenido" (Automatic Content Recognition o ACR) para identificar lo que está mirando y luego enviar esa información en tiempo real a terceros, por lo general para fines de análisis o comercialización.

Mientras que los riesgos parecen graves, son parecidos a los que enfrenta cada vez que navega por Internet, y algunos de los pasos para proteger su privacidad son los mismos. (Para obtener más consejos sobre la seguridad en línea consulte "Póngale seguro: Proteja su privacidad en Internet" (*http://bit.ly/2d2twSv*).)

- Instale todas las actualizaciones del "software" del sistema operativo del televisor. A menudo, las actualizaciones abordan problemas de seguridad recién descubiertos.
- Descargue apps sólo en fuentes de confianza.
- No ingrese información delicada, sea personal o financiera, usando el navegador de Internet o las apps del televisor.
- De ser posible, cree una cuenta de "invitado" en su red wifi y conecte a su televisor por medio de esta cuenta. Así, si los hackers consiguen acceso, no podrán llegar a su computadora u a otros dispositivos conectados a su red. (Busque las instrucciones de su enrutador wifi en línea o póngase en contacto con el fabricante o con su proveedor de servicio de Internet para obtener ayuda.)
- Cuando programe el televisor inteligente por primera vez, es muy probable que le den la oportunidad de optar por no permitir el rastreo de contenidos ("opt out"). Si no le dan la oportunidad, o si no la vio, puede desactivar el rastreo más adelante. (*Consumer Reports* ofrece instrucciones (*http://bit.ly/1QHcK5v*). También puede verificar la configuración en el televisor, o ponerse en contacto con el fabricante para obtener ayuda.)

Los televisores inteligentes están programados para reconocer ciertas palabras, como "TV on" ("encender televisor"). Dependiendo de la marca y modelo del televisor, debe recibir una alerta cuando se activa el modo "escucha", al aparecer un micrófono en la pantalla o por medio de un sonido o alguna otra señal.

Los datos de voz por lo general se transfieren a un servidor de terceros para procesar el cumplimiento de su solicitud. Es probable que esto no sea una amenaza a su privacidad personal, al menos no mayor a la de Siri en el iPhone o la de dispositivos electrónicos similares que responden a comandos de voz. Pero si desea desactivar esta función, puede hacerlo. El proceso será diferente en diferentes modelos de televisores, pero en general requiere cambiar la configuración desde el botón de menú en el control remoto.

Cuentas de televisión de pago

Los usuarios con cuentas de televisión por cable o satélite ("televisión de pago") deben ser notificados cuando se registran para el servicio, y por lo menos una vez al año después de registrarse, sobre qué tipo de información personal recopilará el proveedor, cómo se utilizará, y por cuánto tiempo será mantenida.

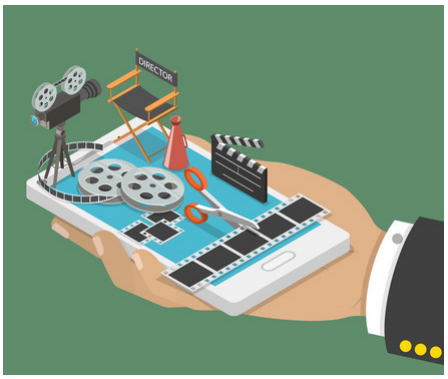
Las empresas de televisión de pago no pueden recopilar su "información personal identificable", o sea, la que podría usarse para identificar a un individuo particular, sin su consentimiento escrito o electrónico, excepto según sea necesario para la prestación de servicios o para detectar el uso no autorizado (robo) de servicio de cable. Y no pueden divulgar su información personal identificable sin su consentimiento escrito o electrónico (o en algunos casos, sin darle la oportunidad de prohibir o limitar la divulgación), salvo cuando sea necesario para proporcionar servicios o en respuesta a una orden judicial.

Si el proveedor de servicios de cable infringe sus derechos de privacidad, usted puede demandar a la empresa y se le podría otorgar indemnización de hasta $1,000, daños punitivos y honorarios de abogado.

Streaming en vivo ('livestreaming') y videos compartidos

Las apps de transmisión en vivo de streaming ("livestreaming") como Meerkat y Periscope les permiten a los usuarios compartir video en tiempo real con su dispositivo móvil. Esto plantea nuevas preguntas acerca de la privacidad de los transeúntes.

Las leyes de privacidad normalmente no protegen a las personas cuando están en la vía pública. Por lo tanto, en términos generales, es legal que alguien tome y comparta un video de usted cuando está en un lugar público, como en la calle, en un parque o en un mitin. Sin embargo, no es legal utilizar tal video con fines comerciales a menos que usted haya firmado una renuncia.



En un lugar privado donde se tiene la expectativa razonable de privacidad, tal como en su casa o una habitación de hotel, tomar fotografías o grabar video o audio sin su permiso por lo general es ilegal.

YouTube, por medio del cual se comparten millones de videos, permite solicitar la eliminación de cualquier video publicado sin el consentimiento del individuo si contiene su imagen o voz, nombre completo, información financiera, datos de contacto u otra información de identificación personal (*http://bit.ly/1XW4bcM*). Otros servicios podrían ofrecer algo similar; verifíquelo en el sitio web de cada servicio.

Acerca de Consumer Action

www.consumer-action.org

A través de materiales de educación del consumidor en varios idiomas, extensión a la comunidad y defensa en base a temas importantes, Consumer Action faculta al consumidor infrarrepresentado a nivel nacional para hacer valer sus derechos y prosperar económicamente.

Asistencia y asesoramiento al consumidor: Presente quejas del consumidor en: *https://complaints.consumer-action.org/forms/spanish-form* o 415-777-9635. Se hablan chino, inglés y español.

Estos son algunos consejos para proteger su privacidad en la transmisión en vivo de streaming y en videos compartidos:

- Si no quiere correr el riesgo de ser incluido en un video, considere evitar lugares o eventos donde es probable que se hagan grabaciones.
- Si le dan la opción para acceder a servicios de video compartido con su contraseña de cuenta de Facebook o Google pero no quiere que su historial de reproducciones sea ligado a esas cuentas, cree una cuenta de inicio de sesión independiente. (Si ha usado Facebook o Google+ para acceder a aplicaciones o servicios de terceros, ambos le permiten revisar y desconectarse de los inicios de sesión con terceros.)
- Solicite a quien esté compartiendo su imagen que la elimine si no desea que se utilice públicamente. (Si fue tomada en un lugar público y no se utiliza para fines comerciales, es posible que no estén de acuerdo en retirarla, pero incluso así lo puede pedir). Si alguien está usando su imagen para fines comerciales o promocionales, aunque haya sido tomada en un lugar público, usted tiene el derecho a presentar una demanda si no ha dado su consentimiento.
- Si comparte video que ha creado usted mismo, ajuste la configuración de privacidad del sitio o de la app de videos compartidos según sus preferencias. Busque herramientas de privacidad bajo las pestañas "Settings" o "Privacy". Sus opciones podrían incluir permitir que cualquiera vea su video o que nadie pueda verlo; permitir que sólo amigos o seguidores puedan verlo; permitir que sólo los que tengan una contraseña lo puedan ver y otras opciones. También puede controlar quién puede compartir o publicar su video y dónde pueden hacerlo. Las opciones de privacidad varían según el proveedor de servicios.

Acerca de esta guía

Consumer Action creó a esta guía con una subvención de Rose Foundation.