OVATION AMERICAS

Boletín Mayo 2022

Privacidad, ¿Ya es demasiado tarde? (Parte 1)

¿Estamos empezando a pagar el precio de muchos años de abuso por parte de las grandes compañías tecnológicas, el gobierno y muchas empresas privadas que recopilan nuestra información personal?

¿Alguna vez se ha preguntado si realmente no seríamos víctimas de muchos años de recopilación abusiva de datos por parte de prácticamente todas las personas con las que hemos interactuado en línea, nuestro gobierno, el sector financiero, las empresas de tecnología y, además, muchos programas de vigilancia nebulosos en todo el mundo?

Nunca ha habido tanto robo de identidad, piratería, actividades fraudulentas como ransomware, phishing, etc. como lo hay hoy en día. ¿Tenemos razón al pedir una mejor privacidad? ¿Está seguro de que nuestra información está bien gestionada y protegida? En este boletín mensual, decidimos compartir con usted la totalidad de un artículo y parte de otro de Canadá que ilustran el estado de la situación.

El Toronto Globe and Mail opinión
Publicado el 7 de mayo de 2022

¿Quién quiere vivir en un estado de vigilancia? No los canadienses

Sin duda, sería extremadamente molesto para los canadienses descubrir que las empresas privadas y los servicios policiales han recopilado indiscriminadamente sus huellas dactilares y ADN y los han colocado en una base de datos.

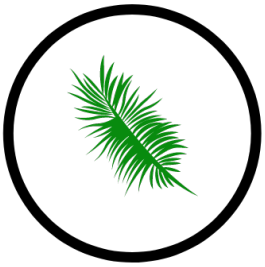
Y, sin embargo, las empresas y la policía han podido hacerlo con las llamadas huellas dactilares faciales, datos faciales biométricos tan personales e inmutables como verticilos en un dedo índice o secuenciación de ADN, generalmente sin el consentimiento de nadie.

Peor aún, en Canadá, la recopilación y el uso de la tecnología de reconocimiento facial prácticamente no están regulados. Esta es una de las principales preocupaciones planteadas esta semana por los órganos de supervisión de la privacidad de las provincias, territorios y gobiernos federales de Canadá, en una declaración conjunta al Comité Permanente del Parlamento sobre Acceso a la Información, Privacidad y Ética.

"A diferencia de otras formas de datos biométricos recopilados por los servicios policiales, como fotografías, huellas dactilares o perfiles de ADN, el uso del reconocimiento facial no está sujeto a ninguna regla legislativa específica", dijo el comisionado federal de privacidad Daniel Therrien al comité. "En cambio, su uso está regulado por un mosaico de leyes y jurisprudencia que, en su mayor parte, no abordan específicamente los riesgos que plantea el reconocimiento facial".

Esto es más que preocupante, porque los riesgos son enormes. A diferencia de la recolección de huellas dactilares o ADN, procesos que consumen mucho tiempo y que requieren intervención humana, la recopilación y el análisis de datos de reconocimiento facial pueden automatizarse por completo, gracias a la inteligencia artificial.

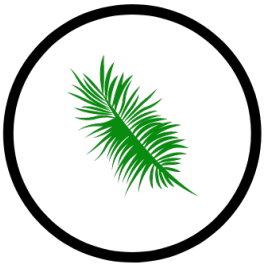
Esto también se puede hacer sin el consentimiento o incluso sin el conocimiento del interesado. Este fue el caso de Clearview AI, una compañía estadounidense que ha recuperado sitios web de redes sociales y otras fuentes públicas en línea para fotografías personales, y creó una base de datos de datos faciales biométricos adjuntos a las credenciales de más de tres mil millones de personas.



Después de que se reveló que algunos servicios policiales canadienses, incluida la RCMP, estaban utilizando los servicios de Clearview, el Comisionado Federal de Privacidad y tres contrapartes provinciales ordenaron a clearview que cesara sus operaciones en Canadá y eliminara las imágenes de canadienses de su base de datos. El caso Clearview es una demostración sorprendente de los peligros de la tecnología de reconocimiento facial. Los comisionados de privacidad dejaron en claro en su declaración al comité que el reconocimiento facial puede ser una herramienta valiosa para la aplicación de la ley, la seguridad nacional y la búsqueda de personas desaparecidas. Pero también puede ser "extremadamente intrusivo, permitir una vigilancia generalizada, proporcionar resultados sesgados y erosionar los derechos humanos, incluido el derecho a participar libremente, sin supervisión, en la vida democrática".

Es fácil imaginar cómo esto podría ser cierto. No todas las personas que participan en una protesta pública legal son tomadas por la policía, y sus huellas dactilares no se pasan a una base de datos, simplemente porque aparecieron. Claro que no. Eso nunca se permitiría en Canadá.

Entonces, ¿por qué la policía podría usar cámaras de vigilancia para capturar los rostros de los manifestantes, o de cualquier otra persona en un lugar público, y publicar las imágenes en una base de datos de huellas dactilares faciales? Para muchos, esto disuadiría la participación en actividades legales y democráticas. El Parlamento debe prestar atención al consejo de los comisionados de privacidad y actuar rápidamente para garantizar que los viejos derechos de los canadienses no sean eviscerados por las nuevas tecnologías.



La ley debe dejar claro cuándo se pueden recopilar datos faciales biométricos, así como huellas dactilares y ADN, de quién y bajo qué autoridad. El uso de la tecnología de reconocimiento facial debe ser "dirigido, dirigido por inteligencia y sujeto a límites de tiempo apropiados", dijeron los comisionados de privacidad. Y el escaneo masivo de la cara debe permitirse solo en las circunstancias más raras.

También debe prohibirse la recopilación indiscriminada de datos faciales biométricos. Hay buenas razones por las que el estado recopila las huellas dactilares de los delincuentes condenados; agregar su huella facial a una base de datos tendría sentido. Pero la construcción de bases de datos masivas sobre las huellas dactilares faciales de los canadienses comunes simplemente no puede ser autorizada, con fines comerciales o policiales, en un país libre.

Después de siete años en el poder y mucha discusión, el gobierno de Trudeau no ha logrado aprobar leyes para frenar a las grandes tecnológicas o para combatir el acoso y la desinformación en línea. Pero estos temas que acaparan titulares palidecen en comparación con la amenaza a nuestras libertades de vigilancia masiva a través del reconocimiento facial. Este es un problema al que nos enfrentamos y que debe abordarse.

True North news publicado el May 5, 2022

Los canadienses deben ser informados si sus datos son recopilados por el gobierno federal: El Comité

El comité de ética de la Cámara de los Comunes quiere que el gobierno federal informe a los canadienses si están siendo espiados y les dé la oportunidad de optar por no participar en los programas de monitoreo de recopilación de datos. Las recomendaciones se producen cuando los parlamentarios investigan la Agencia de Salud Pública de Canadá (PHAC), que está espiando en secreto las ubicaciones de millones de canadienses.

El año pasado, se reveló que el ministerio federal había obtenido datos de 33 millones de dispositivos para realizar investigaciones sobre los "patrones de movilidad de la población" durante los confinamientos. El proyecto solo se dio a conocer después de que PHAC emitió un aviso de licitación pidiendo a los contratistas que continuaran con el programa de monitoreo hasta el 31 de mayo de 2023. Los miembros del comité pidieron al gobierno que notifique a los incluidos en futuros barridos "de una manera que describa claramente la naturaleza y el propósito de la recopilación de datos".

Además, los parlamentarios dijeron que les gustaría ver mejores leyes de privacidad para proteger la información anónima y agregada. En febrero, la Cámara de los Comunes votó por un estrecho margen para detener temporalmente la supervisión de PHAC a pesar de la oposición de los parlamentarios liberales. "Simplemente no estamos en el punto de entender cómo se recopilaron estos datos, si se anonimizaron adecuadamente, cuáles son los riesgos de la reidentificación y por qué el Comisionado de Privacidad no participó en el proceso", dijo el diputado conservador John Brassard.

El programa también está sujeto a una auditoría por parte del Comisionado de Privacidad federal. Si bien los funcionarios de PHAC argumentan que la información de identificación personal se eliminó de los datos, los expertos en privacidad refutaron la acusación y calificaron el programa como una violación de los derechos de los canadienses.

Ann Cavoukian, ex comisionada de privacidad y directora ejecutiva de Global Privacy and Security by Design, dijo a True North en diciembre que los canadienses deberían tener "cero confianza" en las garantías del gobierno federal sobre su conducta. "Recopilan todos estos datos móviles", dijo. "33 millones de dispositivos móviles y dispositivos móviles suelen estar vinculados a identificadores personales, y es necesario tomar medidas para eliminarlos y desidentificar los datos de una manera sólida para que no se puedan volver a identificar. No tenemos ningún seguro en ese sentido. »

La privacidad y la seguridad son realmente sobre buenos hábitos personales, pero incluso con ella, todavía hay muchas cosas que parecen fuera de nuestras manos por ahora. Todos sabemos lo buenos que son nuestros gobiernos en la gestión y seguridad de los datos recopilados... ¿No es nuestra biometría única la última llamada? Entonces, ¿tal vez por eso podemos preguntarnos si la situación real no es el resultado de que el abuso sea demasiado largo y excesivo? Las personas maliciosas obtienen lo que necesitan raspando fácilmente demasiadas bases de datos.

Sigamos aprendiendo y manteniéndonos al día sobre temas de privacidad y seguridad para darnos la mejor oportunidad de evitar hackeos y estafas costosas.

Para comentarios, información o para saber cómo minimizar su exposición de datos, no dude en ponerse en contacto con nosotros en la siguiente dirección:

info@ovationamericas.com o visite nuestro sitio web en: www.ovationamericas.com

OVATION
AMERICAS