OVATION AMERICAS

May 2022 Newsletter

Privacy Protection, is it already to late? (Part 1)

Are we beginning to pay the price of many years of abuse from the Big Tech, the Government and many Private Companies collecting our Personal Informations.

Have you ever ask yourself if we might not be actually the victims of many years of abusive data collection by virtually everyone we interacted with online, from our government, the financial sector, the tech companies and on top of this from many nebulous around the world surveillance programs.

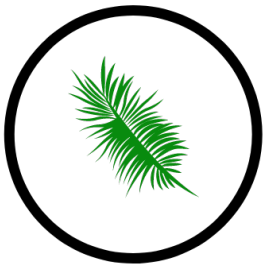
There never been so many identity theft, hacking, fraudulent activity such as

ransomware, phishing, etc. than now. Are we in right to ask for better privacy protection? Do you trust that our informations is well manage and protect? In this month newsletter, we decide to share with you the integrality of an article and a parts of another one from Canada that illustrate well the state of the situation.

The Toronto Globe and Mail opinion
Published May 7, 2022

Who wants to live in a surveillance state? Not Canadians

It would no doubt be extremely upsetting to Canadians to discover that private companies and police services had indiscriminately collected their fingerprints and their DNA, and had put them in a database.



And yet, companies and cops have been able to do just that with so-called faceprints – biometric facial data that are as personal and unchanging as the whorls on an index finger or the sequencing in DNA – usually without anyone's consent.

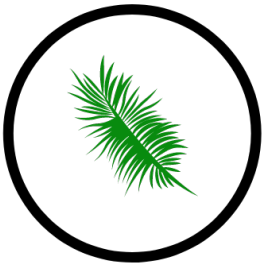
Worse, in Canada, the collection and use of facial-recognition technology is basically unregulated. This was among the chief concerns raised this week by Canada's provincial, territorial and federal privacy watchdogs, in a joint statement to Parliament's standing committee on access to information, privacy and ethics.

“Unlike other forms of biometrics collected by police agencies, such as photographs, fingerprints or DNA profiles, facial-recognition use is not subject to any focused statutory rules,” Federal Privacy Commissioner Daniel Therrien told the committee. “Instead, its use is regulated through a patchwork of statutes and case law that, for the most part, do not specifically address the risks posed by facial recognition.”

This is beyond worrisome, because the risks are huge.

Unlike the collection of fingerprints or DNA – time-consuming processes that require human intervention – the collection and analysis of facial-recognition data can be completely automated, thanks to artificial intelligence.

It can also be done without the consent or even the knowledge of the person involved. This was the case with Clearview AI, a U.S. company that scraped social-media websites and other public online sources for personal photographs, and created a database of biometric facial data attached to the identifying information of more than three billion people.



After it came to light that some Canadian polices forces, including the RCMP, were using Clearview’s services, the federal privacy commissioner and three provincial counterparts ordered it to stop operating in Canada, and to delete images of Canadians from its database.

The Clearview case is a stark demonstration of the dangers of facial-recognition technology.

The privacy commissioners made it clear in their statement to the committee that facial recognition

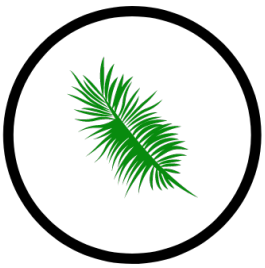
can be a valuable tool for law enforcement, for national security, and in searching for missing people. But it can also be "extremely intrusive, enable widespread surveillance, provide biased results, and erode human rights, including the right to participate freely, without surveillance, in democratic life."

It's easy to imagine how that could be true.

People who take part in a legal, public protest aren't all fingerprinted by police, and their prints aren't run through a database, just because they showed up. Obviously not. That would never be permitted in Canada.

So why would police be able to use surveillance cameras to capture the faces of protesters, or anyone in a public place, and run the images through a faceprint database? For many, that would be a deterrent to taking part in a legal and democratic activity.

Parliament needs to heed the privacy commissioners' advice and move quickly to ensure that Canadians' ancient rights aren't eviscerated by new technologies.



The law should clearly state when biometric facial data – just like fingerprints and DNA – can be collected, from whom, and under what authority. The use of facial-recognition technology should be "targeted, intelligence-led, and subject to appropriate time limitations," the privacy commissioners said. And mass face-scanning should only be permitted in the most rare of circumstances.

There should also be a ban on the indiscriminate collection of biometric facial data. There is good

reason why the state collects the fingerprints of convicted offenders; adding their faceprint to a database would make sense. But building mass databases of the faceprints of everyday Canadians simply cannot be allowed, for commercial or police purposes, in a free country.

After seven years in power, and a lot of talk, the Trudeau government has had no success passing laws to rein in Big Tech, or to tackle online harassment and disinformation. But those headline-catching issues pale in comparison to the threat to our freedoms from mass surveillance by facial recognition. It's an issue that is staring us in the face, and it needs to be addressed.

True North news published May 5, 2022

Canadians should be informed if their data is being collected by feds: committee

The House of Commons ethics committee wants the federal government to inform Canadians if they're

being spied on and to give them the option to opt out of data-collection surveillance programs.

The recommendations come as parliamentarians probe the Public Health Agency of Canada (PHAC) secretly spying on the locations of millions of Canadians.

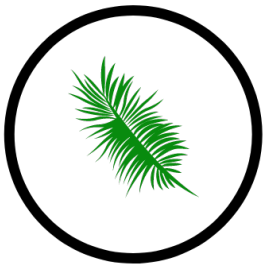
Last year it was revealed that the federal department obtained data from 33 million devices to conduct "population mobility patterns" research during lockdowns.

The project was only unveiled after PHAC put out a tender notice seeking contractors to continue the surveillance program until May 31, 2023.

Committee members have called for the government to notify people included in future sweeps "in a manner that clearly outlines the nature and purpose of the data collection."

Additionally, parliamentarians said they would like to see upgraded privacy laws to protect de-identified and aggregate information.

In February, the House of Commons narrowly voted to temporarily halt the PHAC surveillance despite opposition from Liberal MPs.



"We are simply not at the point of understanding how this data was collected, whether it was properly de-identified, what the risks of re-identification are and why the Privacy Commissioner was not involved in the process," said Conservative MP John Brassard.

The program is also currently being audited by the federal privacy commissioner.

Although PHAC officials maintain that personally identifiable information was stripped from the data, privacy experts have disputed the claim and have called the program a violation of Canadians' rights.

Ontario's former privacy commissioner and Executive Director of Global Privacy and Security by Design Ann Cavoukian told True North in December that Canadians should have "zero trust" in the federal government's assurances regarding their conduct.

"They are collecting all of this mobile data," she said. "33 million mobile devices and mobile devices are usually linked to personal identifiers, and you have to take some measures to remove them and de-identify the data in a strong way so it can't be reidentified. We have no assurances to that effect whatsoever."

Privacy & Security is very much a matter of good personal habits but even with it, there is still much that seems out of our hands for now. We all know how good are our governments at managing and securing the collected data…our unique biometrics data isn't it the last call? So maybe that why we can wonders if the actual situation is not the result of the too long and excessive abuse? Bad intent peoples, get what they need by easily scraping too many data base.

Let's keep learning and stay up to date on Privacy and Security issues to give us the best chance of avoiding costly hacks and scams.

For comments, information or to know how to minimize your data exposure, feel free to contact us at:

info@ovationamericas.com or visit our website at: www.ovationamericas.com

OVATION
AMERICAS