House of Commons
ETHI Committee Meeting 92

Opening Remarks by Sharon Polsky MAPP
President
Privacy & Access Council of Canada

Use of social media platforms for data harvesting and unethical or illicit sharing of personal information with foreign entities

02 November 2023

Privacy and Access Council of Canada
Conseil du Canada de l'Accès et la vie Privée
Suite 330, Unit 440, 10816 Macleod Trail SE
Calgary AB Canada T2J 5N8
Telephone: 877.746.7222
Email: info@pacc-ccap.ca
Website: www.pacc-ccap.ca

Thank you for inviting me to share some views about whether, and how, social media can undermine privacy, safety, security, and democracy.

I am Sharon Polsky, president of the Privacy and Access Council of Canada, which is an independent, non-profit, non-partisan organization that is not funded by government or industry. It has members in the public and private sector who routinely use social media in their personal and professional lives.

Many can recall when Google mail was introduced. It was a brilliant marketing manoeuvre that preyed on human nature. Only the chosen few who were selected to have an account could have one. The invitation accorded those few people special status among their peers. This tactic and the media attention created demand. There was no talk about downsides, risk or privacy. People just wanted to have that Google account. It was simple psychology that showed how easily people can be manipulated.

Since then, we have seen countless examples of big tech manipulating us to share the most intimate details of our existence online. Social media continues to leverage human nature, and the lucrative data broker industry is the biggest beneficiary, other than those who would manipulate us for their own benefit, whether they're companies, political parties, or governments. With recent geopolitical events, it's easy to think that what people post to social media might be used to coerce, extort, or manipulate; but crediting social media alone, or social media from one country or another, is short-sighted.

Online risks reflect society and come from many sources, including familiar communication and collaboration tools that many in this room probably use most days. Every one of them is a real and constant threat. Zoom, Teams, Slack, Facebook and the rest are all foreign.

It's no secret that many companies scrape data and justify their actions by saying *they* consider the information to be public because their AI systems were able to find it on the web. Maybe the secure location where you posted personal or confidential information, or the Ontario hospital you visited recently, has been breached and now your health condition or sensitive conversations are being sold on the dark web.

If the concern is that people who use social media might disclose information that could make them politically sensitive and at greater risk of being influenced, I look to the recording we hear every time we call our cellphone provider or most other companies that says, "This call will be recorded for training", which typically means the training of artificial intelligence systems through machine learning. The human side of that training is done in countries around the world by individuals who have access to your sensitive information.

A Finnish tech firm recently started using prison labour to do data labelling. It goes on and on. We have no choice whether the labelling is done by someone in Alberta or in Albania. There is no control over it and there is nothing stopping a company or a government from purchasing information, because it is available largely through the data broker system. It is widely available internationally. I could go on and on.

Yes, certainly education is important. Computers have been on desktops for almost half a century, but the education is not there yet—as we see big tech investing tens of billions of dollars a year in objecting to and undermining efforts to regulate the industry, with the claim that it will undermine innovation. It's a red herring that's been disproven many times throughout history.

We see dating sites that people use routinely, which are wonderful for a social life, but when things like the Canadian dating site Ashley Madison are breached, I dare say that many of their customers became politically sensitive.

If children or adults go on any website, usually, before they even see the results, the fact that they have been there—whether it's for mental health, addiction or medical counselling—has already secretly been transmitted to the likes of Facebook and data brokers.

This isn't something Bill C-27 is going to fix, or any of the other legislation. In fact, most of the laws being introduced here and abroad will make the situation much worse for everybody, including children—especially children.

I am happy to take your questions. This is a massive endeavour, and I commend you all.

-End-