NATIONAL POST

Big Brother is watching you. No, I mean, literally. And that's a problem

Marni Soupcoff

March 10, 2020

Facial-recognition technology threatens privacy. In the hands of law enforcement, it could be used to identify and target law-abiding people who are critical of the government, as easily as it can be used to identify and target criminals. Now that we know that the Mounties have been using the technology for months (an admission that was preceded by denials and came only after leading facial recognition company Clearview AI's list of clients was hacked), it's something we can no longer ignore.

We can't opt out of facial recognition. We are vulnerable to identification by facial search apps such as Clearview's if we have posted photos of ourselves on Twitter, Facebook or a million other sites. We are vulnerable even if we haven't posted a single pic of ourselves — your image could be out there because a cousin uploaded a shot of you at a family picnic, or even because a stranger posted his vacation pics and you happened to have wandered into the edge of the frame of his portrait of the CN Tower at dusk.

Does it matter? If hundreds of law-enforcement agencies have already started using the technology, is there anything we can do anyway? It truly does and there is, and that is at a minimum insisting that police be transparent, upfront and scrupulously honest about the technology they are using to monitor the public

How have we managed to threaten the existence of private spaces, forget about one of the most basic of civil liberties, and endanger the personal autonomy of every member of our free population without even having a debate about the wisdom of such a move? The entire development ought to be appreciated as a call to action — suspend the government's use of Clearview's app until boundaries have been set to protect personal privacy from being breached by the state.

Charlie Angus, an NDP MP with whom I agree about little, has called on the Liberal government to ban all use of facial-recognition software, "at least until we know for a fact that no laws in Canada have been breached." Consequently, I can still say that I'm not on the exact same page as the NDP. It's not necessary to completely prohibit all use of facial-recognition tech. For a start, it is far less dangerous if a private company is using this sort of surveillance to minimize shoplifting losses or enhance marketing than it is if government is using it for any reason, simply because government has more power. Macy's can't put you in jail. The government can.

Even then, it's possible to contemplate ways the government could use facial-recognition software for valid law-enforcement purposes without crossing the line into illegal invasions of privacy.

As the Cato Institute's Matthew Feeney suggested in an article in Business Insider on Sunday, the right balance could be struck if law enforcement stuck to using facial-image databases that contained information that was limited to people who are already wanted for serious crimes. This would restrict the civil-libertarian nightmare scenario of law enforcement using the technology for keeping tabs on argumentative protesters or pesky journalists who ask too many questions, rather than tracking down murderers and child molesters.

That's the real point, the one that should guide the boundaries set by regulations of government use of Clearview-type software: the tech should not be permitted to allow police to learn any information about a person unless there's already been enough evidence amassed to satisfy a judge or magistrate that the person in question may be arrested and detained.

It's far from clear that the RCMP has been abiding by such restrictions in its use of Clearview, a database that we know includes massive swathes of the law-abiding population — and can spit out their names, addresses and phone numbers with a scan of their faces. The Mounties' vague explanation to CBC that it has used six trial Clearview licences "to assess its potential for use in a criminal investigation, or to help advance a criminal investigation," provides no reassurance. When Charlie Angus calls for a moratorium on public sector use of facial-recognition tech until there is both clear guidance about what is permissible and clear communication about what is being done, he has a point.

In this technological age, when advances in artificial intelligence promise to do so much to improve the length and quality of lives, how can we risk missing out on the benefits by failing to establish ground rules that keep our right to privacy intact?