House of Commons
Chambre des communes
CANADA

Pat Kelly
Member of Parliament,
Calgary Rocky Ridge

Opinion-Editorial on RCMP Use of On Device Investigative Tools

2022.08.22

By Pat Kelly
Member of Parliament for Calgary Rocky Ridge and
Chair of the House of Commons Standing Committee on Access to Information, Privacy, and Ethics

It's time for a public discussion about how the Canadian Government, and its security and law enforcement agencies, balance privacy with public safety.

Earlier in 2022, the House of Commons Standing Committee on Access to Information Privacy and Ethics studied Public Health Agency of Canada's use of mobility data taken from millions of devices without the knowledge of consumers or consulting the Office of the Privacy Commissioner. We also studied the use of controversial facial recognition software and artificial intelligence by Canadian police.

Then Tako van Popta (MP Langley – Aldergrove) formally asked the government via a question on the order paper what parts of the government monitor Canadians' cellphones.

Many privacy advocates and some members of the media were surprised with the government's response. The RCMP admitted using "On-Device-Investigative-Tools" (ODITs) since 2017 to surreptitiously access devices under 10 different warrants granted under Section 6 of the criminal code. This prompted an emergency meeting of ETHI and a summer study of the use of these tools and the privacy risks to Canadians.

The most sophisticated spyware can be deployed against a target as easily as by sending a text or calling a cellular phone number. There is no need to trick the target into clicking a link, or into taking any action of their own. Once the text or call is received, the user can activate the target's camera or microphone, access contacts, calls, cloud storage, and emails. In short, the target's entire life if potentially laid bare: movements, conversations, unlimited images, banking information, health information, and any of the most intimate moments, from the bedroom, to the bathroom, to any other interaction, virtual or physical, with any other person, can be captured.

It's been called "wiretap on steroids".

Both the RCMP and Minister of Public Safety Marco Mendicino forcefully denied that the RCMP uses the notorious mercenary "Pegasus" spyware application, but they also refused to disclose the ODIT program's software supplier, in defiance of the motion passed by the committee. Both the RCMP and Minister cited concerns that public disclosure of their supplier would jeopardize police operations – a concern disputed by Munk School of Global Affairs privacy expert Ronald Deibert.

The Government claims that it values Canadians' privacy and points to the Treasury Board Secretariat's policy requiring all government departments and agencies to conduct a Privacy Impact Assessment (PIA) and provide it to the Privacy Commissioner prior to implementing any new program that could affect Canadian's privacy.

The RCMP established a program for the use of this technology in 2016, and has used such technology to hack at least 49 devices since 2017. Yet the new and former Privacy Commissioners both testified that they heard about the program for the first time in June 2022 – from media reports.

The RCMP committed to providing its privacy assessment to the Privacy Commissioner later this month.

Minister Mendicino said that it was "unfortunate" that the Privacy Impact Assessment was only coming after the public became aware of the program, but offered no apology or explanation for why the Treasury Board directive was ignored.

The RCMP and the Minister also refused to say whether or not Members of Parliament have been targeted. Yet a former CISIS employee confirmed that certain elected office holders from all levels of government "are being paid by foreign governments" and thus have been subject to surveillance. (An astonishing revelation which generated surprisingly little public reaction.)

Surveillance is an essential part of effective policing. Law enforcement technology must keep pace with communications technology. However, privacy legislation must keep pace with both as well.

Judges and legislators also need to stay up to date on telecom technology and the legal landscape. When judges authorize violation of a Canadian's privacy through a warrant, they need the technical expertise to understand the nature of privacy violation. According to Brenda McPhail, Director of the Privacy, Technology, and Surveillance Program at the Canadian Civil Liberties Association it's not good enough for judges and legislators to click "accept and continue" when dealing with invasive technology that includes policies and privacy implications they do not understand.

The RCMP testified that the programs they use are expensive to deploy, are used in rare cases as a last resort, and are removed from the device once the investigation is complete. They said that police must obtain a warrant from a judge for each use, just like conventional wiretaps. The monitor must also separate out and block off access to communication they do not have lawful access to, like phone calls and emails with a suspect's lawyer that are covered by solicitor-client privilege.

Violent criminal gangs, money launderers, human traffickers, drug dealers, terrorists, and foreign espionage agents all use technology to commit serious crimes and to threaten Canada's national security. Canadians expect law enforcement to make prudent use of appropriate tools within strict protocols that safeguard Canadians' privacy under appropriate legislative and judicial oversight.

Refusing to answer questions from Canadians' elected representatives, and ignoring the government's own privacy impact assessment requirements, harms public trust in law enforcement. It is time for the government's and law enforcement's use of technology to be part of the public debate on privacy.