GlobalResearch
Center for Research on Globalization

Canada's National Police Force Admits Use of Spyware to Hack Phones

The RCMP says it needs to use malware because encryption has made surveillance "exponentially more difficult."

By Maura Forrest
Global Research, July 04, 2022
POLITICO 29 June 2022

Region: Canada
Theme: Intelligence, Police State & Civil Rights

***

In a "remarkable" disclosure, Canada's national police force has described for the first time how it uses spyware to infiltrate mobile devices and collect data, including by remotely turning on the camera and microphone of a suspect's phone or laptop.

The Royal Canadian Mounted Police says it only uses such tools in the most serious cases, when less intrusive techniques are unsuccessful. But until now, the force has not been open about its ability to employ malware to hack phones and other devices, despite using the tools for several years. Between 2018 and 2020, the RCMP said it deployed this technology in 10 investigations.

> "This is a kind of capability that they have done everything possible to keep incredibly quiet," said Christopher Parsons, senior research associate at the University of Toronto's Citizen Lab.
>
> "This is a remarkable finding and, for the first time, publicly reveals that the RCMP is using spyware to infiltrate mobile devices, as well as the broad capabilities of their spyware," he said.

The RCMP says the increasing use of encrypted communication means police need new tools to keep up. But critics say the advent of the digital era means police have access to vastly more information than ever before. They say there needs to be a public discussion about what limits to place on the use of malware and other intrusive tools.

…

The RCMP can use spyware to collect a broad range of data, including text messages, email,

photos, videos, audio files, calendar entries and financial records.

The police can also gather “audio recordings of private communications and other sounds within range of the targeted device” and “photographic images of persons, places and activities viewable by the camera(s) built into the targeted device,” the document says.

Click here to read the full article.

*

Note to readers: Please click the share buttons above or below. Follow us on Instagram, Twitter and Facebook. Feel free to repost and share widely Global Research articles.

Articles by: Maura Forrest