Latest stories

Q&A with an expert in electronic surveillance on the challenges and opportunities of collecting evidence

Sgt. Dave Cobey specializes in how police can access and use electronic surveillance tools. *Credit: RCMP*

July 27, 2022

Related links

Police help victim of crypto-fraud get money back (/en/gazette/police-help-victim-crypto-fraud-get-money-back?gz)

RCMP helps stop malware that stole millions from Canadians (/en/gazette/rcmp-helps-stop-malware-stole-millions-canadians?gz)

Today's communications landscape is dotted with electronic devices that Canadians use for almost everything. Criminals do the same, and their electronic correspondence can be used as evidence in investigations. Gazette writer Paul Northcott spoke to RCMP Sgt. Dave Cobey, who specializes in the complex process of how police can request, access and use electronic surveillance tools to investigate serious crimes.

What's your role at the RCMP?

I'm an advisor with the RCMP's national Technical Case Management Program and I work with investigators and the Crown to make sure surveillance is done responsibly and is compliant with the *Canadian Charter of Rights and Freedoms*. Our program staff also ensure that technology used in investigations is described accurately in warrants, while also protecting sensitive investigative techniques. Currently, I'm assigned to the National Technology Onboarding Program, which was created in 2021 to improve how the RCMP manages the use of new technologies and investigative tools that involve the collection and use of personal information.

When and how does the RCMP collect digital evidence?

Investigators have to identify what they want and then obtain the proper judicial authority to get it. They must prepare a detailed affidavit that spells out the offence and the reasons why other investigative options won't work. If they get the OK from a judge to proceed, investigators will ultimately work with technical specialists, and other staff, to try and collect or intercept the information.

However, we often ask investigators: "Are there other places where the information may be found?" A lot of people use very simple passwords for their devices and some write down those passwords. Information can also be stored on other hardware or virtually. So maybe a search warrant could be used to get that information instead.

What are some of the challenges you face?

Before mobile devices there were landlines, or phones, attached to your wall. They were usually provided to people or businesses by one big company and they were tied to one geographic location. At that time, if an officer had a judicial order to conduct surveillance under those circumstances, they went to one of the big telecommunications companies with their judicial order.

Today, there are a variety of devices, produced by different companies, that are tied to people not places. Many organizations that provide those services are not located in Canada. And those devices use different software and applications. All of that makes data collection a challenge.

Encryption is also an issue. It's an important feature in today's world because it protects sensitive information and people's privacy. However, encryption helps criminals carry out illegal activities and avoid detection by police. The extensive use of end-to-end encryption poses a significant challenge for police because even if they are able to collect the encrypted data, it may be unintelligible.

What is an ODIT and how does it help police?

On-Device Investigative Tools (ODITs) can be used on encrypted devices to get information. An ODIT is a computer program that can be installed on a device without the owner's knowledge. It allows police to covertly collect electronic evidence. Specially trained officers use ODITs to collect data either before it's encrypted or after it's decrypted. ODITs can be installed physically or remotely and can be programmed to perform several tasks. The RCMP has used them sparingly. They are only used for serious criminal and national security investigations and only after judicial authorization has been obtained.

What does the future look like for tracking digital evidence?

The challenges associated with the collection of digital evidence will only continue to get more and more complicated as technology changes and new technology develops. However, the RCMP will have to continue to collaborate and build partnerships with prosecutors, legal advisors and private- and public-sector partners that have surveillance specialities.

But, no matter how things unfold, conducting effective electronic surveillance that respects the *Canadian Charter of Rights and Freedoms* will always require extensive and on-going communication between investigators. For example, it will always be important for officers to consult with their Special I Section — these are provincial teams that provide expert support in the area of covert electronic surveillance — and other units, before deciding what action is appropriate. And if officers ever consider new techniques to collect or use personal information, they must consult with the National Technology Onboarding Program.

Date modified:

2022-07-27