ROYAL CANADIAN MOUNTED POLICE

GENDARMERIE ROYALE DU CANADA

On-Device Investigative Tool (ODIT) Technical Description

Draft for Project …

Provided by: Sgt.
Date:

Contents

INTRODUCTION

1. The purpose of this document is to inform the the project investigative team about On Device Investigative Tools (ODIT) and describe how an ODIT will be used to carry out the activities for which this project intends to seek judicial authorization.

2. An ODIT is a computer program as defined in s.342.1(2) of the *Criminal Code* that is installed on a targeted computing device that enables the collection of electronic evidence from the device.

3. An ODIT collects evidentiary data and data necessary to maintain the function of the ODIT pursuant to: a Transmission Data Recorder Warrant (Section 492.2 *CC*) and a General Warrant to Intercept Computer Functions and Use ODITs (Section 487.01 *CC*). In cases where private communications are intercepted using the ODIT, an Authorization pursuant to Part VI of the *Criminal Code* is also required.

DEFINITIONS

4. **App -** A specialized computer application installed or downloaded onto a computing device. For example, iMessage and WhatsApp.

5. **CAIT** - The Covert Access and Intercept Team is a technical support section responsible for interception of data and communications from computers and mobile devices. CAIT is a section under Technical Investigation Services (TIS) which is responsible for tools and procedures to assist operational investigative sections and other law enforcement agencies.

6. **Cloud Storage** – A computing model in which data is stored on remote servers and accessed from the internet, or "cloud".

7. **Device** – A cell phone, computer, tablet, or other similar electronic device that may be used to send or receive data on a network such as the Internet, within the meaning of a computer system as defined in s. 342.1(2) of the *Criminal Code*.

8. **Encryption** - Encryption is the process of encoding data in such a way that only those who possess the decryption key can access it. Encryption can be applied to a particular network connection, file, message or other data.

9. **Hash Value -** A string of characters generated by running data, such as a file, through a mathematical function. Hashing data is generally used to ensure the integrity of that data as it is transferred from different locations.

10. **Internet Protocol ("IP") Address** - is a logical (assigned) address that identifies a device on the Internet or a local network. It allows a system to be recognized by other systems connected via the Internet protocol.

11. **Special "I"** – RCMP units located throughout Canada responsible for the deployment of covert technologies such as, tracking, covert audio equipment, undercover equipment, alarms and sensors used in covert surveillance, and the implementation of Part VI Authorizations where data is captured by CAIT.

USE OF THE ODIT

Why Use an ODIT?

12. Traditionally, the RCMP has intercepted data or communications along the network path between two computing devices, after the data departed the sending device and before it reached the recipient device. Increasingly, encryption tools that do not require input from the user have become widely available. As a result, there are an increasing number of internet transmissions that are encrypted before leaving a device. Examples of encrypted data include applications such as iMessage, WhatsApp, Telegram, Signal, Kik and Skype. Web browsing activities can also be encrypted.

13. Encrypted data that is transmitted can be intercepted, however the encryption renders it unintelligible. ODITs may be used to obtain this data in a readable format. An ODIT may be used to collect/intercept the data from within the target device while the data is in an unencrypted form. If the targeted device or network is receiving data, the ODIT may collect/intercept the data after it has been received by the device and decrypted. Further to this example, if the targeted device or network is sending data, the ODIT may collect/intercept the data before it is encrypted and sent.

14. ODITs can otherwise be used to collect evidence from or using the targeted device. For example: a) to covertly copy data stored on a device or available to that device from cloud storage or another networked device, b) to capture data that identifies the user of the device, c) to activate peripheral components of the targeted device, i.e. the camera and microphone, to conduct electronic surveillance. ODITs will also obtain device information necessary for maintenance of the ODIT.

ODIT Use and Operation

15. An ODIT requires a Transmission Data Recorder Warrant and a General Warrant to Intercept Computer Functions and Use ODITs. The General Warrant is required to authorize interception of internet based telecommunications data, other than transmission data, to and from the computer system, usually with assistance of the service provider. The contents of most internet based telecommunications are encrypted, but the metadata provides information about the device's usage patterns and system functions to facilitate the installation and maintencance of the ODIT. The General Warrant is also required to authorize the interception of functions within the device using the ODIT to obtain information about usage patterns and system functions that is necessary to maintain the ODIT, and to deploy the ODIT to collect evidence. Where the ODIT is used to intercept private communications, a Part VI Authorization is also required.

16. Section 342.1(2) of the *Criminal Code* provides definitions for the interception of computer functions as follows:

    "intercept" includes listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof;

    "function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system.

17. A single ODIT may be programmed with multiple functions, including subordinate ODIT tools that collect evidence ("collectors"). The ODITs in this investigation will be used to copy data stored on the device(s) or accessible to the device(s) such as in cloud storage, to obtain data, including transmission data, as necessary to facilitate use of the ODIT. Such data includes: passwords, login credentials, encryption keys, computer usage, and the configuration of systems and programs. ODIT collectors will be installed remotely and covertly for the following evidence-gathering purpose(s):

    a. to intercept the following types of private communications:
        i. prospective communications that will be stored on the device or accessible to the device [*Stored Data Copy*];
        ii. prospective communications that will not be stored on the device (e.g., transitory or self-deleting messages) [*Screen Capture and Key/Input Loggin*g];
        iii. App-based audio communications such as WhatsApp, Skype, Signal, etc. [*Interception of App-based Audio Communications*];
        iv. communications audible to the device's microphone [*Hot Mic*].

b. to copy data other than prospective private communications, for example, historical communications, photos and documents stored on or accessible to the device [*Stored Data Copy*].

c. to monitor computer-based activity other than prospective private communications, for example, to monitor web browsing [*Stored Data Copy*, *Screen Capture*, and *Key/Input Logging*].

d. to capture photographic images of the user or the immediate surroundings of the device by means of the device camera [*Covert Activation of Camera*].

18. To gather the evidence described above, various ODIT collectors may be used requiring specific authorization. Information about these collectors follows:

a. Stored Data Copy

i. This refers to the ability to covertly copy data stored on the target device and forward it to the CAIT server. Data that may be stored and copied may include existing data stored, or accessible to the device at the time of the authorization, or prospective data, including private communications, that will be generated and stored after the authorization is granted.

ii. Unlike a computer or cell phone search, the ODIT does not create a full forensic copy of the device. Rather, the ODIT will only copy data CAIT operators select.

iii. **Required Authorization**: The General Warrant authorizes the collection of data stored both prior to and after the date the warrant is issued. If the prospective data includes private communications, a Part VI Authorization is also required.

b. Key/Input Logging

i. This refers to the ability to capture keystrokes, mouse or screen input, and other user actions on the targeted device. The logging differs depending on the collector, operating system and device.

ii. Key/Input logging can collect information such as passwords, names, phone numbers, and other user input which may include capture of the user's side of a private communication. In some cases, the collector may be configured to permit targeted collection of user input that does not constitute private communications.

iii. The context of logged input may not be possible to discern without other ODIT function(s). Analysis of logged input cannot be automated to correlate with context data gathered from other ODIT function(s).

iv. Key/Input logging may also be required to obtain information related to the installation, maintenance and removal of the ODIT.

v. **Required Authorizations:** The General Warrant authorizes the recording and

collection of computer functions including keystroke logging and user input. In the rare case where key/input logging is configured to exclude the possible capture of private communications, no further authorization is required. However, if all input is logged without restriction, a Part VI Authorization is also required.

c. Interception of App-based Audio Communications

i. Many app-based audio communications, with or without video, are encrypted or otherwise not amenable to traditional interception. ODITS may allow for the interception of the audio portion of such communications. At this time ODITs do not have the capability to capture the video portion, although screen captures may be obtained with the Screen Shot Collector described below.

ii. Depending on the ODIT, the method by which the audio is intercepted differs. For example, it may be necessary to intercept separately the not yet encrypted outgoing audio and the decrypted incoming audio. In this case, the separate parts of the conversation must be reassembled. Both the original recordings and the reassembled conversation will be retained**.**

iii. **Required Authorization**: A Part VI Authorization is required, together with the General Warrant that authorizes the collection of the intercepted communication.

d. Screen Shots

i. This refers to the ability to capture screenshots of the viewable screen of a targeted device. The screenshot capability differs depending on the collector, operating system and device. Configuration of the ODIT will determine when and how frequently screenshots are taken.

ii. Screenshots capture a static image of everything that is visually presented on the device at the moment in time. This may include a private communication and anything else displayed on the screen.

iii. In some cases, the collector may be configured to permit targeted collection of screenshots, for example when a particular app is being used. However, the screenshot will still capture anything else on the screen such as when a split screen or multiple applications are visible.

iv. Depending on the configuration of the ODIT it may not be possible to differentiate between communications and non-communications data. For example, screenshots of a browser window may intercept web browsing activity or private communications from a web-based email client.

v. Screenshots may not provide a complete record of activity on the device due to lapses in time between screenshots. The more frequently the ODIT is configured to take screenshots, the less likely it is that context will be lost. However, it is not practical or technically feasible to covertly capture screen shots on a continuous high frequency basis.

vi. The context of screenshots may not be possible to discern without other ODIT

function(s). Analysis of screenshots cannot be automated to correlate with context data gathered from other ODIT function(s).

vii. When the screen capture collector is deployed to capture screenshots of applications not limited to private communications such as a browser, it will capture both private communications and other types of data.

viii. **Required Authorizations**: a Part VI Authorization is required, together with the General Warrant that authorizes the recording and collection of computer functions including screen display.

e. Hot Mic

i. This refers to the ability to activate the microphone on a targeted device and record sounds within the audible range of that microphone, including private communications.

ii. Control of the hot mic collector differs depending on the ODIT, operating system, device and telecommunication service. It is not possible to activate and deactivate the recording in live time, as such commands can only be implemented when the ODIT communicates with the CAIT server. This may be delayed where circumstances interfere with such communication.

iii. Where the hot mic is activated by an ODIT, a condition for post-review of the communication should be included in order to permit minimization in the event that external circumstances known to the investigator such as physical surveillance, or review by a monitor of the communication itself, leads to a determination that no principal known person is a party to the communication.

iv. **Required Authorization:** a Part VI Authorization with the restriction described in paragraph iii, together with the General Warrant that authorizes the collection of the intercepted communications.

f. Covert Activation of Camera

i. This refers to the ability to covertly activate the selfie mode camera function of a device to photograph and identify the person using the device at the time the camera is activated. The camera activation capability differs depending on the collector, operating system and device. Configuration of the ODIT will determine when and how frequently photographs can be taken.

ii. The collector may also activate the camera function to photograph what is in view of the user.

iii. Covert camera activation captures a static image of everything that is viewable when the camera is activated. This may capture images of an intimate nature and of third parties.

iv. The collector may be configured to permit targeted camera activation, for example when the device is being accessed or when a particular app is being used. However, it is not practicable to limit camera activation based on the device

location, and it is not possible to limit camera activation based on activities within view when the camera is activated.

v. **Required Authorization**: At present, this technique is contemplated to involve still photography. The General Warrant is required to obtain and collect photos of the computer system's surroundings. In the event that video capture is possible and contemplated, a general video warrant would be required.

ODIT INSTALLATION & DEPLOYMENT

19. Only members of CAIT, or a person acting under their direction will install and deploy an ODIT, pursuant to the terms and conditions of a valid warrant and/or Part VI Authorization.

20. The capability of the ODIT depends on the hardware and operating system of the targeted device. To provide the requested assistance, CAIT must first acquire information about the targeted device, such as make and model, unique identifiers, operating system and version, software version, apps installed on the device, network and configurations. This information may be used or required to determine which ODIT will function on the device and how it will be installed. The information may be obtained from investigative file information, but will typically be obtained under a General Warrant to passively intercept computer functions.

21. An ODIT can be installed on a targeted device physically or remotely. Both physical and remote installation may leverage hardware or software vulnerabilities that allow CAIT to install the ODIT. Physical installation occurs in circumstances where the RCMP has physical access to the device. When installing an ODIT remotely, the CAIT operator uses network or wireless capabilities to remotely interact with the targeted device or the network.

22. When deploying an ODIT by interacting with a network the ODIT may be installed on any device on the network having the same make, model and operating system as the targeted device. Therefore, the ODIT will initially only obtain device identifying information. The ODIT will be removed from any devices with identifiers that do not match those of the targeted device. Once it has been verified that the ODIT has been installed on the correct device, data authorized can be collected by CAIT operator via the ODIT. Identification information obtained from non-target devices will be stored securely by CAIT or Special I and not shared or used for any other purpose without further order of the Court. This identification information shall be destroyed at the conclusion of the investigation if no charges are laid, or when all charges arising from the investigation are finally disposed of, including all appeals.

23. CAIT will profile usage patterns and the status of intercepted system functions of the targeted device on an on-going basis to facilitate evidence collection and maintenance of the ODIT.

24. The interaction between an ODIT and CAIT servers varies by the type of target device, network connectivity, and the design of a particular ODIT. In all cases the ODIT will attempt to communicate with CAIT servers at defined intervals to send the collected evidence as authorized by the Warrant or Authorization. These periodic transmissions notify the CAIT operator that the ODIT is functioning properly, and is able to accept commands to collect data authorized by the respective Warrant or Authorization. The periodic transmissions include data such as the IP address of the target device.

25. The functionality of an ODIT depends on the specific ODIT deployed. There are many different ways that the operator may interact and control the ODIT. Some ODITs allow full interactive remote control of the targeted device which would be similar to interacting with any computer file system. Other types of ODITs call back to a CAIT server and await for commands that are queued for execution. For example, an ODIT could be set to contact the CAIT server every 5 hours and if there are commands queued it will execute them, however if there are no commands queued, it will do nothing and call back again five hours later. ODITs could also be pre-programmed with certain functionality prior to installation so that they will execute a command automatically once installed on the targeted device. If an ODIT is capable of a more than one of the functions described in this paragraph, the choice of such a functionality is left with the CAIT operator to ensure that the ODIT remains covert and is used in accordance with the conditions of the authorization.

26. A common feature of ODITs is that they record and store data on the targeted device, which data is subsequently forwarded to CAIT servers. As such live monitoring to minimize the interception of privileged or third party private communications is not possible.

27. The process of storing targeted data on the target device and subsequently forwarding it to the CAIT servers operates in different ways:

    a. ODIT collectors that create data not otherwise stored on the target device (i.e., key/input logging, screen captures, hot mic audio recordings and covert camera activation) store data in a file on the target device. When conditions are appropriate for downloading that data to CAIT servers, a digital copy of that data is forwarded. Upon confirming receipt of a true digital copy, the CAIT servers command the ODIT to remove (delete) the file that had been temporarily storing the original data on the target device.

    b. When an ODIT collector is used to copy files ordinarily retained and stored on the target device, a copy is sent to the CAIT server either by directly copying the data to the CAIT server or by a process of temporary storage, transfer and removal as described in the above subparagraph.

28. Integrity and authenticity of the data captured from the target device is confirmed by the following process: when the ODIT is commanded to transfer data to the CAIT server, it

generates a hash value for the data and sends the hash value to the server. Once the data is copied to the CAIT server, it is hashed again and the two hashes are compared. If the hashes do not match, the copied data is deleted.

29. Data obtained using ODIT collectors may require post-processing and analysis to re-assemble communications and ascertain the context of other collected data.

30. In some cases, targeting and downloading specific data is not feasible. For example, if the investigators were looking for messages in a database file which were sent or received between certain dates, the entire database associated to the particular software application would need to be extracted. It will generally not be possible to determine what is contained in the database until it is extracted and processed. Ordinarily, data that is not relevant evidence, including communications outside a specified date range must also be extracted. When this occurs, the entire data set must be made available to members of CAIT or Special I for the purpose of making the information intelligible and to apply automated filtering to segregate data that plainly falls outside of limiting terms of the General Warrant or authorization. However, only members of CAIT or Special I will see the segregated information, which may be used by CAIT for the purpose of installing, maintain and removing the ODIT. Only the filtered data set will be shared with investigators. Any data that was extracted, but not sent to the investigators, will be stored securely by CAIT or Special I. This data shall be destroyed at the conclusion of the investigation if no charges are laid, or when all charges arising from the investigation are finally disposed of, including all appeals. Original files containing private communications and related information will be left unmodified on the targeted device(s).

NETWORK, SYSTEM and USER IMPACT

31. The ODIT uses a small portion of storage space on the targeted device to remain undetected and to temporarily store data to be sent to CAIT servers. As a result, the amount of storage space available to the user is reduced. The end user should not experience any noticeable decrease in performance or usability of the device. Also, employing an ODIT requires use of the network connection(s) / data plan associated to the target device.

32. When an ODIT is installed on a targeted device, the CAIT operator may modify settings in the operating system to facilitate installation, maintenance and removal of the ODIT and to protect the ODIT from being discovered. The changes can be reversed if required.