Project SIRA

INSET File# 2022-123

PPSC File #: F22-004

Canada

Province of Ontario

**SUPERIOR COURT OF JUSTICE**

**(East Region)**

**IN THE MATTER OF** Applications for:

An Authorization to Intercept Private Communications pursuant to the provisions of sections 185 and 186 of the *Criminal Code*;

General Warrants pursuant to section 487.01 of the *Criminal Code*;

A Transmission Data Recorder Warrant pursuant to section 492.2(1) of the *Criminal Code*;

A Tracking Warrant pursuant to section 492.1 (2) of the *Criminal Code*;

An Assistance Order pursuant to section 487.02 of the *Criminal Code*; and

An Order sealing all materials not otherwise covered by section 187 of the *Criminal Code*.



THE HONOURABLE

JUSTICE Bertha Wilson ) Wednesday, the 1st day of June,

) 2022.

**AUTHORIZATION TO INTERCEPTION COMMUNICATIONS AND RELATED ORDERS AND WARRANTS**

UPON THE APPLICATION in writing, made the 31st day of May, 2022, by Sandra O'Connor, an agent specially designated in writing for the purposes of sections 185,487.01 (4) and (5) of the *Criminal Code* by the Minister of Public Safety and Emergency Preparedness for an Order authorizing the interception of communications pursuant to sections 185 and 186 of the *Criminal Code*; a general warrant authorizing observations by means of a television camera or other electronic device pursuant to section 487.01 of the *Criminal Code*; and an Assistance Order pursuant to section 487.02 of the *Criminal Code*;

AND UPON THE APPLICATION in writing made this same date by Sergeant Tom Erdely a peace officer, for General Warrants pursuant to section 487.01 of the *Criminal Code*; transmission data recorder warrants pursuant to section 492.2(1) of the *Criminal Code*; tracking warrants pursuant to section 492.1 (2) of the *Criminal Code*; an assistance order pursuant to section 487.02 of the *Criminal Code*; and an order sealing all materials not otherwise covered by sections 187 of the *Criminal Code*;

UPON READING the applications, and the supporting information and affidavit of Tom Erdely, dated the 29th day of May, 2022;

UPON BEING SATISFIED that the requirements of sections 185, 186(1)(a) and (b), 492.1(2), 492.2(1), 487.01, and 487.02 of the *Criminal Code* have been met;

**IT IS ORDERED THAT:**

Any peace officer, and any person acting under the direction thereof, is authorized to intercept communications in accordance with the terms and conditions of this Authorization.

Further, any peace officer is authorized to observe by means of a television camera or other similar electronic device in accordance with the terms and conditions of this Authorization.

**OFFENCES**

1. The offences in respect of which communications may be intercepted and observations may be made are:

    a. Possession of Explosives with the intent to cause damage to property contrary to section 81(1)(a) of the *Criminal Code*;

    b. Possession of Explosives with intent to cause damage to property contrary to section 81(1)(c) of the *Criminal Code*;

c. Participation in activity of terrorist group contrary to section 83.18(1) of the Criminal Code;

d. Facilitating terrorist activity contrary to section 83.19 (1) of the *Criminal Code*;

f. Participation in activity of terrorist group contrary to section 83.18 (1) of the *Criminal Code*; and

e. Conspiracy to commit, attempt to commit, or being an accessory after the fact to the commission of, or any counselling in relation to any of the above offences contrary to section 465 (1)(c) of the *Criminal Code*.

**TYPES OF COMMUNICATIONS AND OBSERVATIONS**

2. The types of communications that may be intercepted are all private oral communications and telecommunications, and all radio-based telephone communications. The observations that may be made are of the activities in circumstances in which persons have reasonable expectations of privacy.

**PERSONS**

3. The persons whose communications may be intercepted and who may be observed are:

a. Principal Named Persons:

i. Name: Charlie BLACK

Date of Birth: October 1st, 1999

Address: 123 Main Street, Ottawa, Ontario

Occupation: Web developer

ii. Name: Sam WHITE

Date of Birth: December 1st, 1989

Address: 234 First Street, Ottawa

Occupation: Administrative assistant

iii. Name: Jordan RED

Date of Birth: September 1st , 2000

Address: 345 Second Avenue, Ottawa

Occupation: IT Specialist

c. Unknown persons:

i. Any other person intercepted or observed at any place in paragraph 4 or over any computer system or telecommunication service in paragraph 5.

**PLACES**

4. The communications of the persons in paragraph 3 may be intercepted at:

a. Custodial Places

i. Any place stationary or mobile, where a person in paragraph 3a is held in lawful custody.

b. Hot Mic Places

i. Any place, stationary or mobile, within audible range of a computer system in paragraph 5a.

c. Other Places

i. Any other place, stationary or mobile, that there are reasonable grounds to believe is being, or will be resorted to, or used by a person in paragraph 3a.

And the persons in paragraph 3a may be observed at:

d. **Places of Observation**

i. Any place stationary or mobile, where a person in paragraph 3a is held in lawful custody.

**COMPUTER SYSTEMS AND TELECOMMUNICATION SERVICES**

5. The communications of the persons in paragraph 3 may be intercepted when made using the following computer systems or telecommunication services:

a. Mobile device or telecommunication service associated to:

i. Telephone number 613-555-2345, and associated International Mobile Identity number (IMEI) 34589877987798779877 used by Charles BLACK; and

ii. Telephone number 613-555-3456, and associated International Mobile Identity number IMEI 34121471147114711471 used by Charles BLACK.

**For greater certainty** interception pursuant to paragraph 5a may continue on any mobile device associated with the above telephone number, IMEI number, IMSI number or any other unique mobile device or telecommunication service identifier that were associated together by the telecommunication service provider on the date when this Authorization was granted;

b. any other computer system or telecommunication service believed on reasonable grounds to be used by any person in paragraph 3a. Interception pursuant to this subparagraph may continue on any device or telecommunication service identifier associated with the telephone number, IMEI number, IMSI number or any other unique computer system or telecommunication service identifier that were associated together by the telecommunication service provider at the time that interception began pursuant to this subparagraph; and

c. any call transfer, call forwarding or voice mail feature associated with any telephone at any place in paragraph 4, or any computer system or telecommunication service in paragraph 5.

**OTHER TERMS AND CONDITIONS**

6. It is further ordered that:

**Solicitor-client communications**

a. No communications may be intercepted at the office or residence of a solicitor, or at any other place ordinarily used by solicitors for the purpose of consultation with clients;

b: When a monitor reasonably believes that a solicitor is a party to a communication, intercepted at any place or over any device, the monitor must discontinue the interception. At reasonable intervals, the monitor may resume the interception for the purpose of determining whether the solicitor remains a party to the communication. When communications have been

intercepted while on automatic monitoring, the monitor who subsequently reviews the communication must cease reviewing the communication as soon as the monitor reasonably believes that a solicitor is a party to the communication, but may monitor the communication by reviewing at reasonable intervals for the purpose of determining whether the solicitor remains a party to the communication. No person shall access any communication to which a solicitor is a party that is recorded pursuant to this authorization except as authorized by this Court;

**Provided however**, that in the event that a communication or communications have been intercepted and to which access has been denied pursuant to this paragraph, and it is reasonably believed that a communication may be subject to solicitor-client privilege, then the communication or communications may be submitted to this Court for an *ex-parte* determination whether access will be allowed to any of the communications.

**Live monitoring**

c. Interception at the places referred to in paragraph 4a shall be accompanied by live visual surveillance, or live audio monitoring. The interception of a communication shall be discontinued once it has been determined that none of the persons in paragraph 3a is a party to it. However, interception may be resumed at reasonable intervals to determine whether such a person has become a party to the communication. If so, then the interception may continue.

**For greater certainty**, communications treated in accordance with this paragraph that are intercepted using a delayed delivery system are deemed to be live monitored.

**For greater certainty**, paragraph 6c does not apply to interception by means of an On Device Investigative Tool, (a computer program known as an ODIT), and does not apply to the interception of non-oral telecommunications.

**Interceptions with On Device Investigative Tool ("ODIT")**

d. When oral communications have been intercepted using an ODIT, the monitor who subsequently reviews the communication must cease reviewing the communication as soon as the monitor determines that no person in paragraph 3a is a party to the communication, or where the interception is made by hot mic at a place in 4b, that no person in paragraph 3a is within audible range of the computer system in 5a. The monitor may review the communication at reasonable intervals for the purpose of determining whether a person in paragraph 3a becomes a party to the communication, or is within audible range of the computer system in 5a, in which case the review may continue. No person shall access any communication to which no person in paragraph 3a is a party, or within audible range of the device in paragraph 5a, except as authorized by this Court.

**Observations**

f. In respect of observations at the places in paragraph 4d, all observations described in paragraph 2 shall only be made by a peace officer. In respect of places of observation, no observations will be made at the office or residence or a solicitor, or at any other place ordinarily used by solicitors for the purpose of consultations with clients, or in any bedroom or washroom.

The observations at the places in paragraph 4d shall only be commenced if there are reasonable grounds to believe that a person in paragraph 3a is, or is about to be, at that place. When it is reasonably believed that none of the persons in paragraph 3a are at that place, the observations shall be discontinued.

**MANNER OF INTERCEPTION AND OBSERVATION**

7. Electromagnetic, acoustic, mechanical, or other devices, including means of an ODIT. The manner of observations that may be made is by means of a television camera or other similar electronic device.

**TRANSMISSION DATA RECORDER WARRANT (s. 492.2(1))**

8. It is ordered that peace officers be authorized to obtain transmission data by means of transmission data recorders, including ODITs, and to covertly or otherwise install, activate, use, maintain, monitor, and remove, transmission data recorders in relation to the places in paragraph 4 when used by persons named in paragraph 3a and the computer systems and telecommunication services in paragraph 5.

**GENERAL WARRANT TO OBTAIN DIALED CHARACTERS (s. 487.01)**

9. It is ordered that peace officers be authorized to obtain and record all dialed characters not otherwise authorized by paragraph 2 of this Authorization in relation to the places in paragraph 4 when used by persons named in paragraph 3a and the computer systems and telecommunication services listed in paragraph 5.

**GENERAL WARRANT TO INTERCEPT COMPUTER FUNCTIONS AND USE ODITS (s. 487.01)**

10. It is ordered that peace officers are authorized to do the following:

a. "Intercept" all "functions" (as both are defined in section 342.1 (2) of the *Criminal Code*), including but not limited to, web browsing and data, or information that will assist in accessing, installing, maintaining, or removing an ODIT, on any computer system at a place in paragraph 4 and of any computer system or telecommunication service in paragraph 5, or acquire the substance, meaning or purport thereof, not otherwise authorized by paragraphs 2 or 8 of this authorization. The interception of the functions described in this paragraph is not subject to live monitoring.

b. Covertly and remotely or otherwise, access and modify computer systems in paragraph 5a to install, activate, maintain, or remove by any means an ODIT in or on the computer system.

c. Copy from the computer systems in paragraph 5a, using an ODIT, any data for purposes of installing, maintaining and removing the ODIT, including but not limited to:

i. Passwords, passcodes, and encryption keys; and

ii. Computer usage, computer user identity, or the configuration of the computer system's functions and programs.

d. Copy from the computer systems in paragraph 5a, using an ODIT, any data stored on or available to the computer system, wherever the data may be physically stored, that may constitute evidence of the offences in paragraph 1, including:

i. Telecommunications, including received, sent, and unsent private communications, dated after and including January 1, 2021, but before the date this Authorization is issued, including data relating to the identity of the initiator or receiver of those communications.

ii. Data including:

a. Dates and times including offsets (Time Zone), if available, for all the following types of data;
b. Global Positioning System (GPS) and Geolocation data;
c. Phone call logs including those dialed, missed or received;
d. Multimedia files, including photographs, video files, audio, or any other images and associated metadata;
e. Electronic documents and notes, including scanned copies or images of text files, word processor documents, portable document format (PDF), spreadsheets, databases, task reminders, calendar events, travel documents such as travel itineraries and travel maps, passport information and/or electronic boarding passes;

f. Metadata and EXIF data that forms part of a file and that includes dates and times created/modified, camera model, author, title, subject, Windows, Mac and Linux file attributes, address, location, encryption status, deleted data, language, format, subject, and/or file size;
g. Any of the data listed herein that may be found on networked services that is available and contained within the data extractions;
h. Any of the data listed herein that may be found on social media applications (apps) or Cloud storage on the Internet that is available and contained within the data extractions;

iii. Data related to:

a. Ownership, possession, access or use or control of the device;
b. The configuration of the device's systems and programs;
c. Passwords, passcodes and encryption keys required to access any of the preceding data; and
d. Contact lists.

e. Obtain photos of the computer system's surroundings by activating the camera function of the computer systems in paragraph 5a;

f. Covertly and remotely or otherwise, store any data obtained using an ODIT on the computer system from the computer systems in paragraph 5a on which the ODIT is installed, and forward that data to police servers;

**Terms and conditions related to use of an ODIT**

g. Only members of the RCMP's Covert Access and Intercept Team ("CAIT") or a person acting under their direction may deploy and activate an ODIT.

h. ODIT deployment is subject to the following terms and conditions:

i. An ODIT shall initially obtain only computer system identifying data;

ii. The ODIT's collectors may only be activated after it is determined that the ODIT is on a computer system in paragraph 5a. The ODIT shall be removed from any other computer system; and

iii. All identifying data obtained from a computer system not in paragraph 5a must be stored securely and not shared with investigators or used for any other purpose without further order of the Court. 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.

i. CAIT or Special "I" shall make reasonable efforts to segregate any data copied pursuant to paragraph 10d that is not within the defined time period. The segregated data may only be used by CAIT or Special "I" for the purposes described in 10c, and shall not be shared with investigators or used for any other purpose without further order of the court. The segregated 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.

j. If on review it is reasonably believed that any of the data copied and forwarded to police servers pursuant to this General Warrant constitutes a private communication to which a solicitor is a party, that communication is subject to the terms and conditions in paragraph 6b.

k. There is no limit to the number of times peace officers may do the things described in this General Warrant.

l. The interception of computer functions using an ODIT is not subject to live monitoring.

m. Pursuant to section 487.01 (5.1) of the *Criminal Code*, notice of access to a computer system in paragraph 5a pursuant to this General Warrant shall be given to the person who was the object of the ODIT's deployment and activation. The time within which notice shall be given pursuant to section 487.01(5.1) of the *Criminal Code* is no later than ninety days after the expiration of this General Warrant, subject to any extension granted under section 487.01 (5.2) of the Cri*minal Code*, and any computer system that is accessed more than once requires only one notice to the person who was the object of the technique.

**GENERAL WARRANT TO OBTAIN SUBSCRIBER INFORMATION (s. 487.01)**

11. It is ordered that peace officers are authorized to obtain from telecommunication service providers the basic subscriber information (customer name and address) for any Internet Protocol addresses that will be identified through the transmission data recorder warrant or general warrant to intercept computer functions.

**TRACKING WARRANT (s. 492.1 (2))**

12. It is ordered that peace officers are authorized to obtain tracking data by means of a tracking device, including an ODIT, and to, covertly or otherwise, install, activate, use, maintain, monitor and remove tracking devices in or on the computer systems or telecommunication services in paragraph 5.

**ENTRY**

13. To carry out the terms of this Authorization and related orders and warrants, peace officers are authorized to enter, covertly or otherwise, the places in paragraph 4 and their immediate surroundings, other than any residence, to install, maintain or remove any electro-magnetic, acoustic, mechanical, or other device, any television camera or other similar electronic device, and any tracking device.

**ASSISTANCE ORDER (s. 487 .02)**

14. Pursuant to section 487.02 of the *Criminal Code*, it is ordered that Synergy Communications, Bell Canada, Bell Mobility Inc., Rogers Communications Canada Inc., Telus Communications Inc., Freedom Mobile Inc., and any other persons in Canada who provide telephone or telecommunication services shall provide such assistance as is reasonably required to give effect to this Authorization and related orders and warrants. Without restricting the generality of the foregoing, such assistance shall include:

a. Provide information and facilities needed for installation, maintenance, monitoring, and removal of any electromagnetic, acoustic, mechanical, or other devices, or television camera or similar electronic device to intercept communications, or to make observations.

b. Make all reasonable efforts to allow access to voice mail in a manner that cannot be detected by the subscriber.

c. Provide information and facilities needed for installation, maintenance, activation, use, monitoring, and removal of a transmission data recorder, and provide transmission data.

d. Provide the published and unpublished basic subscriber information (customer name and address) and all Service Provider Identification Information (SPID), including all telecommunication service providers and their resellers, associated to the telephone numbers, IMEI and IMSI numbers identified through the transmission data recorder warrant. Notwithstanding paragraph 15, the requirement to produce information remains in effect until the information has been produced.

e. Provide all basic subscriber information (customer name and address) described in paragraph 11.

f. Provide information and facilities needed for installation, activation, use, maintenance, monitoring, and removal of tracking devices, and provide tracking data.

g. Covertly activate any function of a computer system or telecommunication service in paragraph 12 and take any steps required to allow for the current geographical position information to be obtained from the computer system or telecommunication service.

h. No person providing assistance, including their employees, servants and agents, may directly or indirectly disclose or permit disclosure of any assistance provided, or the content,

existence or operation of this Authorization, and related orders and warrants, to any person except as may be necessary for the purposes of compliance with the assistance order, or obtaining the advice or assistance of legal counsel, unless otherwise ordered by a Court of competent jurisdiction.

**DURATION**

15. This Authorization and related orders and warrants shall be valid for a period not exceeding 60 days, from and including the date of issuance.

**SEALING ORDER**

16. All materials related to this Authorization and related orders and warrants, shall be sealed from public view in the same packet and treated in accordance with s. 187 and s.487.3 of the *Criminal Code.*

**DATED** at Ottawa, Ontario, the 1st day of June, 2022

The Honourable Justice

_____

Bertha Wilson

Of The Superior Court of Justice