

Report of Findings

Investigation # PA-043149

Summary of Investigation

1. The complainant, who represents a Canadian community-based organization, raised concerns with our Office that the RCMP refused to confirm or deny whether it uses cell site simulators (sometimes referred to as “Stingray” devices or “IMSI catchers”) as part of its surveillance activities.¹ She was particularly concerned that the RCMP may be using these types of devices to monitor large groups of people in a given location and that the devices are capable of intercepting the content of voice and text communications and extracting encryption keys that are used to protect data on cellular phones. The complainant is of the view that if these technologies are being used, the public has a right to know, since their use has the potential to subject innocent Canadians to privacy violations without their knowledge or consent.
2. Subparagraph 29(1)(h)(i) of the *Privacy Act* (the “*Act*”) states that the Privacy Commissioner shall receive and investigate complaints in respect of any matter relating to the collection, retention or disposal of personal information by a government institution. Our investigation proceeded on this premise, since the complainant’s allegation was that the surreptitious collection of personal information by the RCMP using cell site simulators may be in contravention of the *Act*.
3. On April 5, 2017, while our investigation was ongoing, the RCMP provided several media outlets with a “technical briefing,” during which it confirmed that it does in fact own and use cell site simulators during certain types of investigations.
4. In summary, the RCMP took the position in the technical briefing that its use of cell site simulators is in full compliance with Canadian laws, including the *Charter of Rights and Freedoms (Charter)*² and the *Criminal Code*,³ and that proper judicial processes as established by jurisprudence were followed. The RCMP also explained that the only personal information collected using its cell site simulators is the international mobile subscriber identity (IMSI) and the international mobile equipment identity (IMEI) number

¹ See, for example, <http://www.theglobeandmail.com/technology/digital-culture/the-covert-cellphone-tracking-tech-the-rcmp-and-csis-wont-talk-about/article20579947/>; <https://www.thestar.com/news/canada/2015/12/15/the-cellphone-spyware-the-police-dont-want-to-acknowledge.html>; <http://www.cbc.ca/news/technology/rcmp-blackberry-hack-montreal-mob-murder-pub-ban-lifted-1.3629222>; <http://www.theglobeandmail.com/news/national/case-involving-first-documented-use-of-stingray-technology-in-toronto-goes-to-trial/article30057813>.

² *The Constitution Act, 1982, Schedule B to the Canada Act 1982 (UK), 1982, c. 11.*

³ *Criminal Code, RSC 1985, c. C-46.*

associated with cellular devices – which are standardized unique numbers that identify a cellular network subscriber and a mobile device respectively – but they are not capable of collecting the content of private communications, including voice and audio communications, email messages, text messages, contact lists, images, encryption keys or basic subscriber information.⁴

5. The information provided to the media by the RCMP was consistent with the representations that it had already made to our Office with respect to our investigation. That being the case, we worked with the RCMP to independently verify the technical capabilities of its cell site simulators and sought additional information regarding the legal authority under which they are operated, and how the RCMP uses, retains, and ultimately disposes of the data collected by these devices.
6. Following a demonstration of how the RCMP uses cell site simulators and handles the personal information that is collected using these devices, we are of the view that the complaint is **not well-founded**, with the exception of six instances in which the RCMP did not obtain prior judicial authorization. In those six instances, based on the information received from the RCMP, we are of the view that the complaint is **well-founded**.

Relevant Facts

7. A cell site simulator is an electronic device that, when activated, mimics a cell tower in order to attract all nearby mobile phones and other cellular devices to connect to it. Unique identifiers are obtained from these devices and can subsequently be used to track the location of devices of interest or to identify the owner of the device.
8. There are several different makes and models of cell site simulators available for purchase, but very little information about their technical capabilities is publically available, including their operating range.
9. According to the RCMP, it typically refers to cell site simulators as “mobile device identifiers” (MDIs) in an operational context. The RCMP confirmed that it began evaluating MDI equipment in 2004 and procured its first MDI device in early 2005. The first operational deployment of an RCMP MDI occurred in July of 2005. The RCMP currently owns ten MDI devices.
10. The RCMP explained that MDI technology may be used to assist in high priority investigations relating to national security, serious and organized crime, and other *Criminal Code* offences that impact the safety and security of Canadians. It may also be used in exigent circumstances, such as a kidnapping, where a cellular phone needs to be located quickly. In this type of situation, police may already know the IMSI and/or IMEI information associated with that device. The MDI can be configured to use direction-finding

⁴ See <http://www.rcmp-grc.gc.ca/en/news/2017/5/rcmp-use-technology-identify-cellular-devices-law-enforcement-purposes>.

technology and lead the operator to the location of that specific device. See paragraph 42 of this report for a definition of “exigent circumstances.”

11. The RCMP is of the view that any disclosure beyond what it has made public that describes the technical capabilities of the MDI, or the techniques used to operate the MDI, has the potential to adversely impact investigations conducted by the RCMP, as well as the investigations of any other organizations that use MDI type devices. We agree with the RCMP’s view of the sensitivity of this information. While we have sought extensive representations from the RCMP during the course of our investigation, we are of the view that we are not at liberty to provide information identifying the specific MDI devices used by the RCMP, or the specific technical capabilities of such devices, beyond that which is contained in this report.
12. It can be said, however, that the RCMP owns and utilizes different makes and models of MDI equipment, but the way they are used and the type of information obtained from each MDI device is similar. According to the RCMP, its MDI devices are only operated by qualified officers who have received specialized training on the operation of the device and it obtains prior judicial authorization in the form of a warrant to use its MDI devices as investigative tools.
13. In its representations and in the technical briefing, the RCMP emphasized that its MDI equipment (which includes both the cell site simulators and the software to run them) does not, and cannot, intercept or receive any form of private communications, including the content of voice or audio communications, text messages, email messages, or encryption keys. The RCMP clarified that is not a function that can be enabled or disabled – its MDI equipment was purchased without these capabilities.
14. When attempting to identify a suspect’s phone, an MDI is operated in proximity of the suspect in several different locations. At each location, the MDI acts like a cellular tower, attracting as many cellular devices in the area as possible and quickly collects their unique identifiers, which are known as IMSI and IMEI numbers. The IMSI and IMEI numbers are 15 digit serial numbers that are unique to each cellular service subscriber and the mobile device that they are using.
15. IMSI and IMEI numbers are used by cell towers to identify a mobile device in order to determine which network it is subscribed to. An MDI device does the same thing, though it does not connect the device to a cellular network. Rather, it rejects the device’s request to connect to a network after it collects the IMSI and/or IMEI number.
16. After operating in at least three different locations, the data collected by an MDI device is filtered to determine which IMSI and/or IMEI numbers were found in all of the same locations as the suspect. Those unique identifiers can eventually be associated with the suspect of the investigation through a process of elimination.
17. The RCMP clarified that it is not possible to know any identifying information associated with IMSI and IMEI numbers without performing a “subscriber check” with the network

provider. In order to make that association with the suspect, another judicial authorization is obtained to order a telecommunications service provider to provide the name, address and phone number connected to the mobile device that was identified through the use of the MDI equipment, which would help corroborate any association between the mobile device and the suspect.

18. The RCMP acknowledges that the deployment of an MDI device will have an impact on non-targeted mobile devices, since MDIs collect the unique identifiers of as many mobile devices in the location of deployment as possible. The RCMP advised that data collected from third party cellular devices is preserved by the MDI operator(s) and access by anyone other than the MDI operator(s), including the RCMP investigators, is restricted, meaning that it is secured so that it cannot be accessed by anyone other than the MDI operator(s) or the member in charge of RCMP Technical Investigation Services. Once the investigation and all related court proceedings are completed, the data is destroyed.

Prior Judicial Authorization

19. The RCMP's operational use of MDI technology is guided by the National Wiretap Experts Committee (NVEC). The NVEC provides guidance, including legal advice, to law enforcement and prosecutors on the application of legal tools (procedural powers) in the *Criminal Code*. The RCMP is further guided by its interim national policy (the "policy") on the use of MDI devices (and fact sheet), which was issued in 2011. Despite its interim nature, the policy is still in effect today. All references in this section of the report are to the current version of the policy.
20. The policy states that the use of the MDI in criminal investigations must be authorized by way of a General Warrant (section 487.01 of the *Criminal Code*) but may occur without a warrant in other serious policing matters where there is no criminal investigation in order to prevent loss of life or grievous bodily harm ("exigent circumstances"). As outlined below, the policy has been supplemented by further directives for RCMP Criminal Operations Officers to follow when using MDI technology.
21. In March 2015, following legal advice from the NVEC, the RCMP issued a directive to Criminal Operations Officers stating that it was not necessary to obtain judicial authorization prior to deploying an MDI.
22. Following a subsequent NVEC recommendation, the RCMP issued an additional directive in June 2015, recommending consultation with Crown prosecutors before making a decision to obtain or not obtain a General Warrant prior to deploying an MDI.
23. *Bill C-13: Protecting Canadians from Online Crime Act (PCOCA)* came into force in March 2015, including amendments to the *Criminal Code* to allow for the collection of transmission data associated with Internet-based communications. This new warrant is now referred to as a "Warrant for transmission data recorder" in section 492.2 of the *Criminal Code*. *PCOCA* also included a definition for "transmission data." Following subsequent advice from NVEC, the RCMP issued a further directive in October 2015 for Criminal

Operations Officers to seek a Transmission Data Recorder (TDR) Warrant prior to deploying an MDI.

24. We asked the RCMP to provide us with information regarding the number of times it has used an MDI device over the past five years (2011–2016) and under which legal authority the MDI devices were used. The RCMP advised that it deployed MDI devices during the course of 125 criminal investigations over the past five years: 91 of those deployments were authorized by a General Warrant; 22 were authorized by a TDR Warrant; in 13 deployments, no prior judicial authorization was obtained.
25. The RCMP explained that this adds up to 126, due to one investigation where a warrant was initially obtained but, during the course of the investigation, the advice from the NWECC changed, indicating that a warrant was no longer required.
26. The RCMP clarified that of those 13 cases where no warrant was obtained, 7 cases presented exigent circumstances and 6 cases were during the time period where it believed that no warrant was required (i.e., March to June 2015).
27. The RCMP also advised that it has deployed its MDI equipment in support of other Canadian law enforcement agencies in 29 criminal investigations during the past five years. These deployments are reflected in the total number of 125 criminal investigations cited in paragraph 24 of this report.
28. The RCMP clarified that in cases where prior judicial authorization was obtained for the deployment of an MDI device during an RCMP investigation, warrants were obtained by the RCMP. Where MDI devices were used by the RCMP in support of other law enforcement agencies, the warrants were obtained by those respective agencies.
29. The RCMP provided us with a sample warrant relating to the use of an MDI device, as well as the “Information to Obtain” (ITO) that was sworn for the warrant. That particular warrant was ultimately authorized by a Justice of the Peace in Ontario in September 2016. The RCMP also provided us with copies of the standard templates used for TDR Warrants and for affidavits sworn as part of the ITO relating to MDI use, as well new draft versions for our review.
30. Copies of the sample warrant and ITO referred to in the preceding paragraph are provided at Appendix A and B to this report, respectively.
31. During the course of our investigation, members of the RCMP Technical Investigation Services provided the privacy investigator and a member of our Technology Analysis Branch with access to their MDI equipment and also provided a detailed demonstration of how it is used, what types of data it collects, how that data is used, how it is retained, and how it is ultimately disposed of. As already mentioned, for reasons relating to the sensitivity of the information provided, we are unable to disclose certain details of that demonstration within this report.

Application

32. In our analysis of the RCMP's representations in this matter, we considered sections 3, 4, and 5 of the *Act*.
33. Section 3 of the *Act* defines personal information as information about an identifiable individual that is recorded in any form including information relating to race, national or ethnic origin, colour, religion, age, marital status, education, medical, criminal or employment history, financial transactions, identifying numbers, fingerprints, blood type, personal opinions, etc.
34. The types of information at issue in the investigation are identifying numbers on cellular devices. This type of information may be revealing in terms of the identity and location of the mobile device user. The collection of this type of personal information using an MDI device includes information about all third party cellular devices in the range of the MDI device, not just the targeted suspects. As such, this clearly qualifies as the personal information of identifiable individuals.
35. Section 4 of the *Act* provides that personal information collected by a government institution must relate directly to an operating program or activity of the institution.
36. The RCMP is of the view that the information in question is directly relevant to its duties as set out in section 18 of the *Royal Canadian Police Act*,⁵ which include the preservation of the peace, the prevention of crime and of offences against the laws of Canada, the apprehension of criminals and offenders and others who may be lawfully taken into custody, and the execution of all warrants, and the performance of all duties and services in relation thereto, that may be lawfully executed and performed by peace officers.
37. Section 5 of the *Act* states that, whenever possible, personal information shall be collected directly from the individual to whom it relates and that the individual shall be informed of the purpose for the collection, except in certain circumstances:
- 5 (1) A government institution shall, wherever possible, collect personal information that is intended to be used for an administrative purpose directly from the individual to whom it relates except where the individual authorizes otherwise or where personal information may be disclosed to the institution under subsection 8(2).
- (2) A government institution shall inform any individual from whom the institution collects personal information about the individual of the purpose for which the information is being collected.
- (3) Subsections (1) and (2) do not apply where compliance therewith might

⁵ *Royal Canadian Mounted Police Act*, RSC 1985, c. R-10.

- (a) result in the collection of inaccurate information; or
- (b) defeat the purpose or prejudice the use for which information is collected.

38. The RCMP is of the view that its collection of personal information using MDI equipment is consistent with section 5 of the *Act*, since it would not be possible to collect the personal information directly from a suspect without compromising an investigation.

Analysis

39. A warrant is an order by a Judge or Justice of the Peace under statute authorizing the collection or seizure of evidence that is relevant to an offence. Warrants have the effect of permitting intrusion of a person's reasonable expectation of privacy that is otherwise protected under section 8 of the *Charter*. The RCMP takes the position that, since October 2015, it generally obtains prior judicial authorization in the form of a TDR Warrant before deploying its MDI devices for investigative purposes.⁶ As noted at paragraph 23 of this report, the provision allowing for a TDR Warrant is section 492.2 of the *Criminal Code*.

Warrant for transmission data recorder

492.2 (1) A justice or judge who is satisfied by information on oath that there are reasonable grounds to suspect that an offence has been or will be committed against this or any other Act of Parliament and that transmission data will assist in the investigation of the offence may issue a warrant authorizing a peace officer or a public officer to obtain the transmission data by means of a transmission data recorder.

Scope of warrant

(2) The warrant authorizes the peace officer or public officer, or a person acting under their direction, to install, activate, use, maintain, monitor and remove the transmission data recorder, including covertly.

Limitation

(3) No warrant shall be issued under this section for the purpose of obtaining tracking data.

40. Subsection 492.2(6) of the *Criminal Code* provides the following relevant definitions:

transmission data means data that

- (a) relates to the telecommunication functions of dialling, routing, addressing or signalling;

⁶ According to the RCMP, although it most often obtains prior judicial authorization in the form of a TDR Warrant, some jurisdictions instead obtain a General Warrant for the deployment of MDI devices. In some instances, it may also obtain a Tracking Device Warrant pursuant to section 492.1 of the *Criminal Code* in addition to a TDR Warrant.

(b) is transmitted to identify, activate or configure a device, including a computer program as defined in subsection 342.1(2), in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and

(c) does not reveal the substance, meaning or purpose of the communication.

transmission data recorder means a device, including a computer program within the meaning of subsection 342.1(2), that may be used to obtain or record transmission data or to transmit it by a means of telecommunication.

41. According to the RCMP's representations, MDI devices were used during the course of 125 investigations over the past five years. Prior judicial authorization was obtained for the deployment of the MDI devices in 113 of those cases – either by a General Warrant under section 487.01 of the *Criminal Code* or by a TDR Warrant under subsection 492.2(1) of the *Criminal Code*.
42. With respect to 7 of the deployments of MDI devices in which the RCMP did not obtain prior judicial authorization, the RCMP claims that it was because of exigent circumstances. In Canadian criminal law, “exigent circumstances” exist where a police officer has reason to believe that a particular action is necessary to prevent imminent loss or destruction of evidence or bodily harm or death to any person.⁷
43. The RCMP provided us with information regarding the specific circumstances of each of these cases. We are of the view that the RCMP has provided sufficient details to establish that it acted in accordance with common law powers to forgo obtaining a warrant in exigent circumstances.⁸
44. In general, we agree with the RCMP's position that the collection of personal information using an MDI device is consistent with section 4 of the *Act* in that it is directly related to an operating program or activity of the institution, since the apprehension of criminals and offenders and others who may be lawfully taken into custody, and the execution of all warrants, and the performance of all duties and services in relation thereto, is the core mandate of the RCMP, as established under the *Royal Canadian Mounted Police Act*.
45. We are of the view, however, that section 4 of the *Act* must be read in a manner that is consistent with the *Charter*, even where the collection of the personal information is directly related to an operating program or activity of an institution. Section 8 of the *Charter* protects individuals against unreasonable search or seizure by the state. Warrantless

⁷ See e.g., *R v Knelsen*, 2012 MBQB 242 at para. 57; *R v DeWolfe* 2007 NSCA 79 at paras. 24-25; *R v Grant*, [1993] SCR 223; and *Criminal Code*, s. 529.3 (definition of “exigent circumstances” for the purpose of entering a dwelling house without a warrant).

⁸ See *R. v. Spencer*, 2014 SCC 43 at paras 71-74.

searches are considered to be *prima facie* unreasonable for the purposes of section 8.⁹ The deployment of an MDI and the resulting collection of personal information by the RCMP constitutes a search and seizure, and as such, prior judicial authorization is required for that activity to be *Charter*-compliant, and for the collection at issue to comply with section 4 of the *Act*.

46. In the 6 instances in which MDI devices were deployed by the RCMP without prior judicial authorization or the presence of exigent circumstances, we do not believe that the collection of personal information in these cases was *Charter*-compliant. We recognize that the presumption that warrantless searches are *prima facie* unreasonable is a rebuttable one;¹⁰ however, no evidence was provided by the RCMP to rebut this presumption, and the onus for doing so rests with them. We are therefore of the view that those instances constitute a contravention of section 4 of the *Act*.
47. Similar to our conclusion with respect to section 4 of the *Act*, in general, we agree with the RCMP's position that paragraph 5(3)(b) of the *Act* applies to personal information that is lawfully collected using MDI devices in that the direct collection from a suspect would compromise an investigation in which covert technologies are utilized. Likewise, the direct collection of personal information from non-suspects of an investigation would likely compromise the investigation. However, in the 6 instances where warrants were not obtained, we have already determined that the collection of personal information constitutes a contravention of section 4 of the *Act* as it was not lawfully collected.
48. Our primary concern in this matter is the collection, use, retention, and disposal of third party personal information, that being the IMSI and IMEI numbers of a vast number of individuals who are not subjects or suspects in an investigation but whose personal identifiers have been, or will be, collected by the RCMP using MDI devices. Knowing where an individual is, or was, at any given time can reveal information about an individual, which can result in the individual(s) being rendered identifiable.¹¹ We therefore sought to determine how the RCMP handled the cellular and mobile device data collected during the deployment of its MDI devices, particularly in response to the complainant's allegation that cell site simulators are used by police to monitor large groups of people.
49. The RCMP Technical Investigation Services demonstrated that the transmission data collected by the MDI equipment is temporarily held on a secured computer that is used during the operation of the MDI. This information is accessible only to the operator(s) of the MDI equipment. Only the unique identifiers (IMSI/IMEI numbers) that have been linked specifically to a suspect of the investigation that has been named in the judicial authorization are provided to the police investigators.

⁹ See *Hunter et al. v. Southam Inc.*, [1984] 2 SCR 145.

¹⁰ *Ibid*; see also *R. v. Collins*, [1987] 1 S.C.R. 265.

¹¹ See "Metadata and Privacy," https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/md_201410.

50. The remainder of the transmission data collected during an MDI deployment, that being third party personal information in the form of a log containing IMSI and IMEI numbers, is withheld from the police investigators. It is downloaded onto a USB drive and wiped from the hard drive of the computer on which it was collected. The USB drive is then secured in the Divisional Technical Investigation Services office so that access is restricted. The data is retained in order that it can be produced if ordered by a judge during court proceedings. This may result in a lengthy retention depending on the duration of proceedings, which may include appeals. The data and USB drive on which it has been stored is destroyed at the conclusion of all relevant legal proceedings.
51. This process appears to be consistent with the policy. Specifically, section 5.3 of the policy states that “The logs created by the use of the MDI device will be retained by the Divisional Special “T” unit as exhibits and protected in accordance with the terms and conditions of the General Warrant.” As already mentioned, the RCMP now generally obtains prior judicial authorization the form of a TDR warrant.
52. The RCMP is in the processes of implementing a new version of the policy, a draft copy of which it submitted for our review during the course of our investigation. The new policy is significantly more detailed than the current version. A copy of the draft policy is attached at Appendix C to this report.
53. Both the sample ITO and TDR Warrant we reviewed state that “Any unique identifiers relating to other third parties that have been collected will be preserved and access by anyone other than the operators restricted until ordered otherwise by a court of competent jurisdiction.” We believe that this wording provides adequate protection of the collected personal information. While we note that it is also reflected in the warrant and ITO templates provided by the RCMP, we suggest that the RCMP also consider adding these terms and conditions to the new policy.
54. Based on our review, we are of the view that both the geographic and temporal scope of the deployment detailed in the sample ITO and TDR Warrant were reasonable and provide sufficient details on the collection of third party personal information and the segregation and restriction of access to that information during the course of an investigation.
55. With respect to the MDI devices themselves, based on the demonstration by RCMP Technical Investigation Services and the subsequent analysis of the specific devices used by the RCMP that was conducted by our Technology Analysis Branch, we are of the view that we have sufficient information to verify that they are not capable of intercepting private communications such as voice communications, email messages, text messages, contact lists, images, encryption keys or basic subscriber information.

Findings

56. The complainant was primarily concerned that the RCMP was using MDI devices to monitor large groups of people in a given location and that the devices are capable of

intercepting the content of voice and text communications and extracting encryption keys that are used to protect data on cellular devices.

57. Our investigation established that the MDI devices used by the RCMP are not capable of intercepting private communications such as voice communications, email messages, text messages, contact lists, images, encryption keys or basic subscriber information. Based on our review of the current and draft policies, the sample TDR Warrant and the warrant templates provided by the RCMP, we are satisfied that third party personal information collected by the RCMP under the authority of the warrants is being properly segregated, secured, retained, and ultimately destroyed at the conclusion of court proceedings.
58. Based on the foregoing, we have concluded that this complaint is **not well-founded**, with the exception of the six deployments of MDI devices for which no prior judicial authorization was obtained and exigent circumstances were not present. While the RCMP was operating in good faith based on legal advice it received from the NWECC, given the lack of prior judicial authorization or exigent circumstances, it is our view that those six deployments were not lawfully executed and, therefore, the RCMP's collection of personal information was not compliant with Section 4 of the *Act*. Based on the information received from the RCMP in this matter, we conclude that the complaint is **well-founded** for those six deployments.
59. Although we have concluded that the complaint is well-founded in the case of six MDI deployments, we believe that the RCMP has taken appropriate steps to remedy this situation, since it now requires prior judicial authorization for all MDI deployments unless presented with exigent circumstances, in which case a warrant is not required.

Other

60. During the course of our investigation, the RCMP provided us with unprecedented access to its MDI devices, which was critical in coming to a timely conclusion. We appreciate the RCMP's efforts and high level of cooperation in this matter.
61. We note, however, that the complainant's primary concern was that the RCMP initially would not confirm that it was using cell site simulators. This lack of transparency led to serious concerns about the capabilities of these devices and how they are being used. We strongly encourage the RCMP to continue to make efforts toward openness and accountability in terms of the technologies it employs in its law enforcement activities and the legal authorities it relies on for the use of those technologies.

Canada

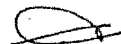
ONTARIO COURT OF JUSTICE

IN THE MATTER OF an application for a warrant to track the location of a mobile device, pursuant to section 492.1(2) of the Criminal Code,

AND IN THE MATTER and a warrant for a transmission data recorder, pursuant to section 492.2 of the Criminal Code

AND IN THE MATTER OF an application for an order denying access to the information pursuant to section 487.3 of the Criminal Code

1. **UPON** reading the information on oath of Cst Craig ELLIOTT, a peace officer and member of the Royal Canadian Mounted Police (RCMP), dated the 16th day of September, 2016.
2. **AND UPON BEING SATISFIED** that the requirements of ss. 492.1(2) and 492.2 of the Criminal Code have been met
3. **IT IS ORDERED** that any peace officer trained for the use of the device, or any person acting under their direction, are authorized to obtain tracking data by covertly using a mobile device identifier (MDI) as a tracking device, to obtain tracking data in relation to the following device
 - a. Mobile device with associated phone number [REDACTED]
4. **IT IS FURTHER ORDERED THAT** any peace officer trained for the use of the device, or any person acting under their direction, are authorized to obtain transmission data while operating the MDI in accordance with this order.



19 Sep 16

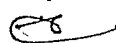
APPENDIX A

5. IT IS FURTHER ORDERED THAT the warrants pursuant to s. 492.1(2) and 492.2 are subject to the following terms and conditions
- a. The MDI will be used to locate and track mobile device with associated phone number [REDACTED] and [REDACTED]
 - b. The MDI will only be used if there are reasonable grounds to believe that data from mobile device with associated phone number [REDACTED] may be obtained
 - c. While searching for the mobile device with associated phone number [REDACTED] the MDI will be activated for no more than three minutes at a time per frequency, with rest periods of at least two minutes between activation per frequency;
 - d. Once mobile device with associated phone number [REDACTED] is located, the MDI may be activated for as much time as necessary to locate the user of the device.
 - e. The MDI will only be activated in the area described as follows; bordering [REDACTED] to the south, [REDACTED] to the West, [REDACTED] to the East and [REDACTED] to the North.
 - f. The MDI will not be activated once the mobile device associated to phone number [REDACTED] is located and the person using it is identified, unless further judicial authorization is obtained
 - g. The only data that will be provided to the investigators will be related to the location of mobile device with associated phone number [REDACTED] Any unique identifiers relating to other third parties that have been collected will be preserved and access by anyone other than the operators restricted until ordered otherwise by a court of competent jurisdiction.

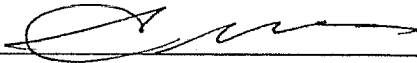


APPENDIX A

6. **THIS COURT ORDERS** that this warrant shall be valid for a period of 60 days, commencing today, the date of issuance.

X, Sealing Order issued. 

Issued today, the 19 day of
September, 2016 by:

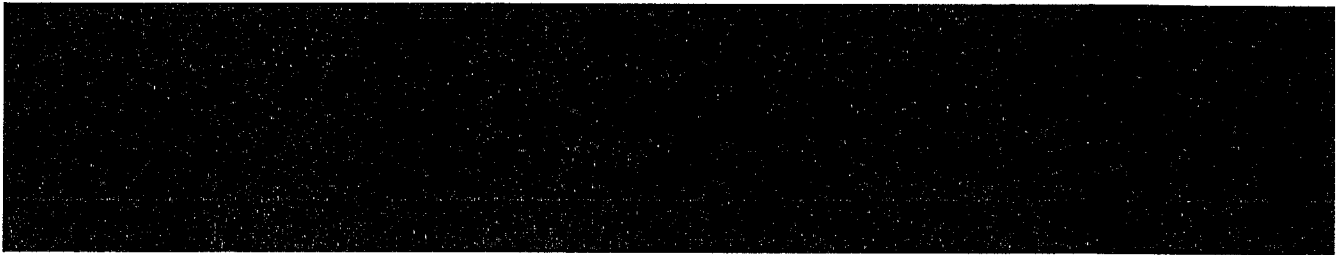


A Justice of the Peace in and for the
Province of Ontario

(ABDUL MALIK)

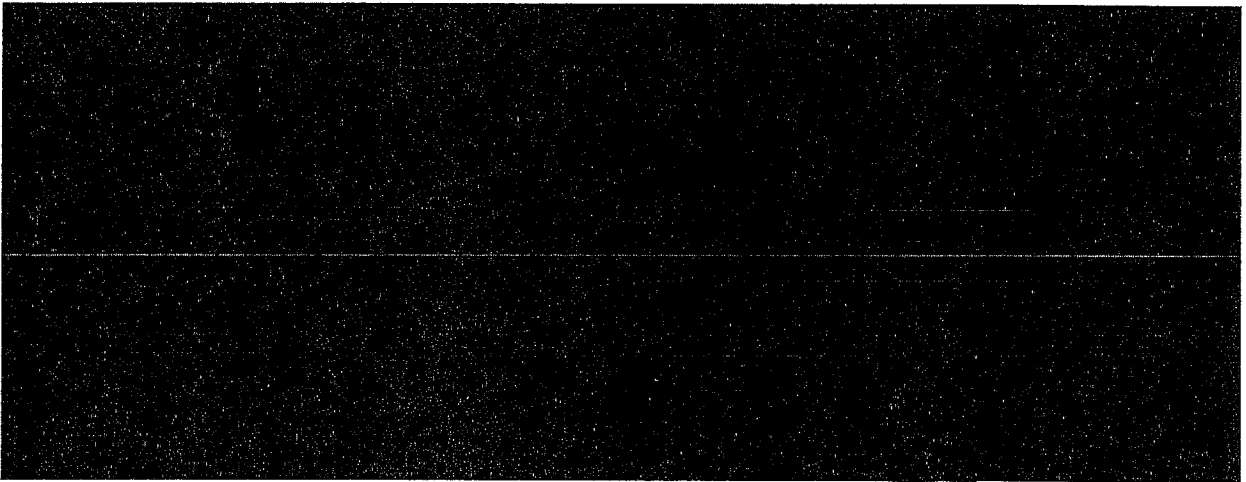
10:27

q.no



CONCLUSION

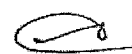
24. Based on the evidence presented in this Information to Obtain, I have reasonable grounds to believe that the offences of Importing into Canada a substance included in Schedule 1 to wit, Cocaine, contrary to Section 6(1) of the Controlled Drugs and Substances Act and Conspiracy to Import a Controlled Substance included in Schedule 1 to wit, cocaine, contrary to section 465(1) of the Criminal Code of Canada have and/or will be committed. I base my belief on the following:



25. Based on the evidence gathered as a result of the Production Order, Transmission Data Recorder Warrant and Tracking Warrant, investigators have been unable to determine the true identity of the person or persons using the mobile device to commit the listed offences. I believe that the person or persons in possession of the mobile device are using common techniques (prepaid phones and payphones) in order to avoid detection and/or to hide their true identity.

WARRANT FOR TRACKING DEVICE AND TRANSMISSION DATA RECORDER




19 Sept 16.

APPENDIX B

26. I am seeking a tracking warrant and a transmission data recorder warrant in order to use a device commonly known as the mobile device identifier (MDI) to locate and track the mobile device associated to phone number [REDACTED]

[REDACTED] I believe that in order to identify the person or persons involved in the offences listed, the use of the MDI is necessary. The person who uses the mobile device is in current contact with people involved in the drug trade and, as demonstrated from the intercepted communications, is in the process of facilitating the importation of large quantities of drugs into Canada.

27. On September 15th and September 16th, 2016, I spoke with Sgt. Mike ROACH of the RCMP Technical Operations Section and learned that the MDI is a device that when deployed, obtains the unique identifiers of mobile devices or similar devices (any devices using cellular network such as tablets and [REDACTED] within its range. I also learned the following:

- a. The MDI has two purposes. The device can either gather the unique identifiers of the mobile devices within its range or be configured to confirm the location of a specific mobile device. When configured in the latter mode, the MDI will be gathering the unique identifiers of all the mobile devices within its range until the specific mobile device the MDI is looking for is found;
- b. When the MDI obtains unique identifiers, it will obtain unique identifiers from all mobile devices within its range including third party mobile devices of people and objects not part of the investigation. It does not intercept any private communications. The unique identifiers that are collected are numbers that are associated with mobile devices, service providers, and transmission data of the cellular networks. The unique identifiers that the MDI will be searching for are the IMEI and the IMSI. The unique identifiers do not provide identification information of the user or other personal information. Once the MDI finds this specific mobile device, it will only be gathering the transmission data of that mobile device and will only be affecting this mobile device. The MDI uses indicators to show the operator where that mobile device is located;
- c. The purpose of this application is to obtain a tracking warrant to use the MDI to find the mobile device associated to phone number [REDACTED] and ultimately determine the location and identity of the individual who uses it. However, while the MDI is trying to locate the mobile device associated to phone number [REDACTED] it will gather transmission data [REDACTED]



APPENDIX B

of third party devices. We will not be using the transmission data of third party mobile devices of people and objects not part of the investigation;

- d. It is difficult to predict the range of the MDI as it can be affected by different factors, such as the environment, electromagnetic fields, and the weather. When activated within a specific area the MDI may effect devices outside that area depending on the location of the MDI and the factors listed above.

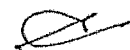
(This is relevant in this particular investigation as investigators are seeking to activate the MDI within a specific area further defined in the Terms and Conditions.)

- e. The MDI is activated in relation to the devices associated to a particular frequency. When the MDI is activated, mobile devices associated to the particular frequency within range of the MDI will have a temporary disruption of service. There is a potential that mobile devices will be affected from their normal operation for the entire duration of the time the MDI is activated. There is a possibility that its deployment could affect 9-1-1 calls of mobile device within its range while trying to locate mobile device associated to phone number [REDACTED] While searching for the target device, the operators will not activate the MDI on any one frequency for more than 3 minutes. The purpose of this practice of switching frequencies up to every 3 minutes is to ensure that no one cell phone is interfered with for more than 3 minutes as each cell phone transmits signals on a particular frequency.

Terms and Conditions

28. Should the warrant be granted the MDI would be used as follows:

- ✓ a. The MDI will be used to locate and track mobile device associated to phone number [REDACTED]
- ✓ b. While the MDI is gathering IMSI/IMEI numbers in attempt to find the target mobile device, the MDI will be activated for no more than three minutes on any one frequency. Once the target mobile device is located, only that mobile device will be affected, and therefore we will activate the MDI for as much _____


12/sep/16

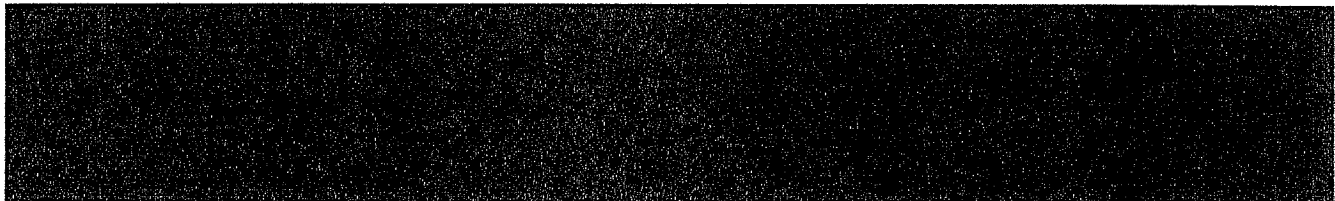
APPENDIX B

time as necessary to locate and identify the person using the mobile device. By stopping the tracking function every three minutes we risk losing the target mobile device and having to start the process over again which would affect the phones of the general public. While connected to the target mobile device it will not be able to make or receive calls, including to 911 ;

- c. The MDI will only be deployed in an area where there are reasonable grounds to believe that transmission data from mobile device associated to phone number [REDACTED] may be obtained. Current transmission data obtained through the Transmission Data Recorder Warrant and the Tracking Warrant have isolated the location of the device to the Scarborough area of Toronto. The MDI in this instance will only be activated in the area described as follows; bordering [REDACTED] to the south, [REDACTED] to the West, [REDACTED] to the East and [REDACTED] to the North.³¹
- d. The MDI will not be activated once the mobile device associated to phone number [REDACTED] is located and the person using it is identified; unless further judicial authorization is obtained
- e. The only transmission data that will be provided to the investigators will be related to the location of mobile device associated to phone number [REDACTED]. Any unique identifiers relating to other third parties that have been collected will be preserved and access by anyone other than the operators restricted until ordered otherwise by a court of competent jurisdiction.

Scope of the Warrant

29. Further to section 492.1(3), I am requesting that any activity related to the tracking device shall be authorized to be done covertly. The success of this investigation is dependent upon secrecy. I believe the usefulness of the tracking device would be rendered futile, if the targets of this investigation, or anyone associated to them, were aware that a tracking device was activated, or used in relation to the named mobile device. I also believe that covert authority is necessary to ensure the safety



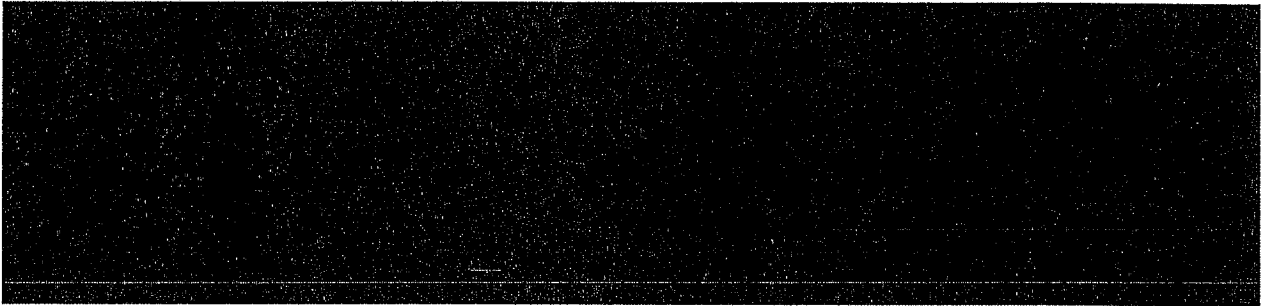
12/24/16

APPENDIX B

of the peace officers, or any person acting under their authority, involved in the activation, use, maintenance and monitoring of the tracking device.

Application to Obtain a Sealing Order

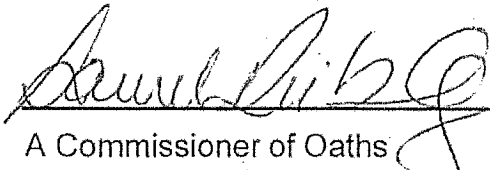
30. Pursuant to Section 487.3(1) of the Criminal Code, it is requested that all documents filed in support of this Order, including the Order itself, be placed in a packet and sealed. It is further requested that the packet be kept in the custody of the court in a place where the public has no access and shall not be dealt with except in accordance with the terms and conditions as specified in the Order or under the provisions of Section 487.3(4) of the Criminal Code.



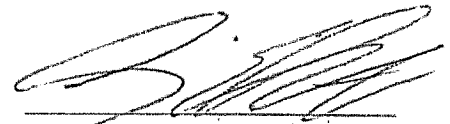
Duration


32. In order to gather sufficient information and evidence, I am requesting that the warrant be valid for a period of 60 days starting on the day it is issued.

SWORN before me at the City of)
Toronto in the Province of)
Ontario, this 16th day of)
September, 2016.)


A Commissioner of Oaths)
in and for the Province of Ontario)

LAUREL REIBLING, a Commissioner, etc.,
Province of Ontario, for the Government of Canada,
Department of Public Safety
and Emergency Preparedness.
Expires October 20, 2017.


Cst Craig ELLIOTT


19. / Sep / 16

Canada

██████████
ONTARIO COURT OF JUSTICE
██████████

IN THE MATTER OF an application for a warrant to track the location and movement of a device; pursuant to section 492.1(2) of the Criminal Code.

AND IN THE MATTER OF an application for a transmission data recorder warrant, pursuant to section 492.2(1) of the Criminal Code.

IN THE MATTER OF an application for an Order Denying Access to Information (Sealing Order), pursuant to section 487.3 of the Criminal Code.

INFORMATION ON OATH

Cst Craig ELLIOTT

██████████
██████████
██████████
██████████

CE
19/08/16



RCMP CSS Policy on MDI Activities

For information regarding this policy, contact Royal Canadian Mounted Police (RCMP) Technical Investigation Services (TIS).

APPENDIX C
Interim Policy 2017-06-27

OM - Ch. XX.XX Mobile Device Identification Activities

Directive Amended: 2017-03-23

For information regarding this policy, contact Technical Investigation Services.

1. Definitions
2. Policy
3. General
4. Assistance to Outside Agencies
5. Identifying the Unique identifiers of Unknown Devices
6. Locating a Specific Mobile Device
7. Training and Testing
8. Technical Investigation Services Responsibilities
9. Investigator Responsibilities
10. Special "I" Unit Commander Responsibilities
11. CSS operator Responsibilities
12. Handling of data collected during deployments
13. Disclosure
14. Court

1. Definitions

1.1. IMEI means International Mobile Equipment Identity

1.2. IMSI means International Mobile Subscriber Identity

1.3. MDI activities means Mobile Device Identification activities. MDI is an effect produced using a Cell Site Simulator (CSS). MDI activities have two primary functions:

1) To identify the unique identifiers for unknown mobile device(s) being used by the subject(s) of an investigation.

2) To physically locate a specific mobile device when the unique identifiers are already known.

1.4. CSS data means the unique identifiers of a mobile device, device make and model, and cellular network information. CSS data does not include voice or audio communications, text messages, email messages, encryption keys, contact lists, images, or any other forms of private communications or content. See section 2.2.

APPENDIX C
Interim Policy 2017-06-27

1.5. CSS operator means an employee of the RCMP Technical Investigation Services Branch, as well as an employee of the RCMP who falls under the direction of that Branch, who is appropriately trained and authorized to install, operate and possess a CSS

1.6. "Private Communication" is defined in section 183 of the *Criminal Code*.

1.7. Unique Identifiers are serial numbers that are unique to mobile devices. Unique identifiers include, but are not necessarily limited to IMSI and IMEI.

1.8. Exigent circumstances are circumstances where it is necessary to prevent imminent bodily harm or death to any person.

2. Policy

2.1. Mobile Device Identification (MDI) is an investigational technique used to enhance public safety in support of criminal investigations relating to national security, serious crime and organized crime, and other serious *Criminal Code* offences that impact the safety and security of Canadians. A CSS conducting MDI activities will only be deployed by a trained operator in accordance with a judicial authorization, unless there are exigent circumstances. The MDI technique would only be used where the collected information cannot otherwise be obtained. Prior to any deployment of the CSS, approval is required from the Officer in Charge (OIC) of Criminal Operations, or his/her delegate.

2.2. The CSS used by the RCMP when conducting MDI activities is not capable of collecting, or intercepting, voice or audio communications, text messages, email messages, encryption keys, contact lists, images, or any other forms of private communications or content from a mobile device.

2.4. The CSS data is protected information and will only be accessed for the purpose of an investigation, or for court proceedings as required by law. This information will be stored in a Protected "B" environment during the course of the investigation on the investigation file or, in the case of third party information, within Technical Investigation Services. See section 12- Handling of data collected during deployments.

3. General

3.1. The MDI effect is produced using a CSS. Mobile devices in the proximity of the CSS identify the CSS as the most attractive cellular tower in the area and then identify themselves to the CSS using unique identifiers in the same way that they would with a network tower.

3.2 When using the CSS to locate a mobile device, there are two stages. In the first stage, the CSS attracts nearby mobile devices to obtain the unique identifiers, so that it can find the targeted mobile device. During the second stage, once the targeted device contacts the CSS, the CSS stops attracting other devices and is able to only affect the targeted device. The CSS will then provide a direction and estimated distance to the targeted mobile device.

3.3 The CSS operator will only operate the CSS when a security plan is in place to ensure safety of the CSS operator, the persons assisting the CSS operator, and the techniques used during the deployment of the CSS.

3.4 All operational, training and testing deployments of CSS technology will be recorded and kept as per sections 12.3.a and 12.2.d of this policy.

APPENDIX C
Interim Policy 2017-06-27

4. Assistance to Outside Agencies

4.1. Approval from the OIC of Criminal Operations or delegate, a judicial authorization, and a security plan is required before MDI activities are deployed to assist a non-RCMP agency.

4.2. MDI activities can be deployed on behalf of a non-RCMP agency without a judicial authorization in exigent circumstances. An explanation of the exigent circumstances will be provided to the CSS operator and approval from the OIC of Criminal Operations or delegate is required.

4.3. The CSS equipment deployed while assisting a non-RCMP agency with MDI activities, will be operated by an RCMP CSS operator.

5. Identifying the Unique Identifiers of Unknown Devices

5.1. CSS operators will ensure that the CSS is used in accordance with the conditions specified in the judicial authorization.

5.2. The CSS conducting MDI activities is deployed to gather the unique identifiers of the mobile devices within its range, or to confirm if the subject of an investigation is using a specific mobile device.

5.3. The MDI activities should only be deployed to confirm that the subject of an investigation is in possession of a specific device when the location of that subject is known.

5.4. The CSS should only be deployed in an area where there are reasonable grounds to believe that the subject of the investigation is located.

5.5. MDI activities should only be conducted at as many locations as is necessary to provide the CSS operator with enough information to identify, through a process of elimination, the common unique identifier that belongs to a mobile device believed to be in the possession of a person named in the judicial authorization.

5.6. Excluding sections 6.3 and 6.4 in this policy, the CSS will be activated for no more than three minutes at a time per frequency/channel, with rest periods of at least two minutes between activation on the same frequency/channel.

5.7. Only the unique identifiers that the CSS operator believes upon reasonable grounds to be associated to the subject of an investigation will be provided to the investigating unit. Any unique identifiers belonging to third parties not involved in the investigation will be withheld from the investigating unit and secured as Protected "B" information.

5.8 The CSS data is protected information and will only be accessed for the purpose of an investigation, or for court proceedings as required by law. See section 12- Handling of data collected during deployments

6. Locating a Specific Mobile Device

6.1. A tracking warrant is required to locate a specific mobile device, unless there are exigent circumstances. This does not apply to 5.3 as the location of the subject and device is already known.

APPENDIX C
Interim Policy 2017-06-27

6.2. CSS operators will ensure that the CSS is deployed in accordance with the conditions specified in the judicial authorization.

6.3. During the first stage of using a CSS to locate a known device, as it attracts nearby mobile devices to obtain the unique identifiers, the CSS can be operated longer than three minutes on the same frequency/channel until it attracts and identifies the targeted mobile device. The CSS can be operated longer than three minutes on the same frequency/channel during the first stage of operation, as long as the CSS is not in a stationary position and it is permitted within the judicial authorization.

6.4. During the second stage of the locating function, only the targeted mobile device is affected, as its direction and distance from the CSS is obtained. There is no time restriction, unless it is ordered within the judicial authorization. See also 3.2 of this Policy.

7. Training and Testing

7.1. CSS deployment for CSS training and/or testing purposes requires the approval of the OIC of Criminal Operations or delegate, or the Director General of Technical Operations. This approval can be delegated to the line officer of the unit conducting the training/testing.

7.2. A warrant cannot be obtained for training and/or testing as there is no investigation of an offence. The CSS will not be deployed for training and/or testing during an investigation and evidence is not to be collected. Any data collected while training and/or testing will not be used in support of an investigation and, will be immediately destroyed.

7.3. When conducting training, MDI activities will be supervised by a trained CSS operator.

7.4. When deploying the CSS for training and/or testing of MDI activities, the equipment will be operated in a way that minimizes interference with third party devices. The minimization clauses listed in the Technical Investigation Services approved wording for judicial authorizations will be used as a guide to minimizing the interference on third party devices. Contact Technical Investigation Services for the most recent wording.

7.5. All deployments of the CSS for the purposes of training and/or testing MDI activities, will be recorded in accordance with section 3.4 of this policy. The records will include confirmation that any data collected is destroyed during or immediately after the training or testing activity is complete.

8. Technical Investigation Services Responsibilities

8.1. Develop and maintain policy and standard operating procedures relating to CSS technology.

8.2. Approve the type/make/model and installation of CSS equipment that will be used by the RCMP.

8.3. Evaluate the operational effectiveness of RCMP CSS systems across Canada that are conducting MDI activities.

8.4. Conduct research and development on CSS technology.

8.5. Provide CSS operator training.

8.6. Provide approved template wording for use in Information To Obtain documents and warrants.

APPENDIX C
Interim Policy 2017-06-27

8.7. Ensure that records are maintained in accordance with the authorization relating to the deployment of CSS equipment and the management of collected data.

9. Investigator Responsibilities

9.1 Contact the local Special "I" unit to determine if deployment of the MDI activities is appropriate for the investigation.

9.2. Contact the local Special "I" unit to obtain the most recent approved wording for a judicial authorization and affidavit.

9.3. Obtain approval from the OIC of Criminal Operations or delegate to deploy the CSS for the purpose of MDI activities.

9.4. Develop a security plan to ensure safety of the CSS operator, the persons assisting the CSS operator, and the techniques used during the deployment of the CSS during MDI activities.

9.5. Complete form 1067 requesting Special "I" services and forward to the local Special "I" unit along with the signed judicial authorization, approval from OIC of Criminal Operations or delegate, and the security plan. Ensure language used in form 1067 is classified at Protected "B" or lower.

10. Special "I" Unit Commander Responsibilities

10.1. Ensure only trained persons who are authorized by Technical Investigation Services operate the CSS equipment.

10.2. Ensure all CSS data is handled, stored, audited and disposed of in accordance with section 12 of this policy.

10.3 Ensure all CSS operational, training and testing deployments and destruction of collected data are recorded in accordance with Section 2.4, 3.4, 7.2 and 7.5 of this policy.

10.4 Ensure that any operational deployments of the CSS are in accordance with this policy, appropriate judicial authorization and Technical Investigation Services directives.

11. CSS Operator Responsibilities

11.1. Ensure that they are trained and authorized by the Officer in Charge (OIC) of Criminal Operations, or his/her delegate, to operate the CSS device.

11.2. Maintain the CSS equipment in accordance with manufacturer recommendations and as instructed by Technical Investigation Services.

11.3. Ensure that installation of the CSS complies with safety code six radio frequency exposure limits for the CSS operator and all others that may be in proximity of the CSS equipment during operation.

11.4. Ensure that a radio frequency exposure monitoring device approved by Technical Investigation Services is in operation during the deployment of MDI activities, so the CSS operator(s) and assisting persons can be warned of excessive exposure levels. Should a warning be given by the device, the CSS deployment will be halted until the radio frequency exposure problem is identified and corrected.

APPENDIX C
Interim Policy 2017-06-27

11.5. Ensure that approval has been obtained from the OIC of Criminal Operations, or delegate, and a valid judicial authorization exists before the CSS equipment is deployed.

11.6. Review the judicial authorization to ensure that it contains wording that has been approved by the OIC of Technical Investigation Services or delegate. Report any deviations of standardized wording or conditions of operation to Technical Investigation Services.

11.7. Review the judicial authorization to ensure that all conditions within that authorization are followed.

11.8. Operate the CSS in accordance with the authorization provided by Industry, Science, and Economic Development Canada.

11.9 Ensure all CSS operational; training and testing deployments and destruction of collected data are recorded in accordance with Section 2.4, 3.4, 7.2 and 7.5 of this policy.

12. Handling of data collected during deployments

12.1 Handling of data collected during operational deployments-Special I Unit Commander Responsibilities

12.1.a Third party data, collected incidental to an operational deployment, will not be provided to the investigation but will be kept securely, apart from the file, at the Division's Technical Investigation Services (Special I) office. The location of third party data will be reported to the investigation file and Crown, in the event it is required for court disclosure.

12.1.b. All data (CSS database) collected during CSS operational deployments, including third party data, will be secured as Protected "B" and, handled in a manner consistent with any other exhibits.

12.1.c The Division Criminal Operations Officer will ensure regular audits are conducted at least once yearly, to ensure third party data collected during CSS deployments no longer required for potential disclosure relating to ongoing prosecutions, is appropriately destroyed.

12.1.d The computer or hard drive upon which the data is stored during operation of the CSS will be secured at all times and, the data contained within will be handled as "Protected B" information. The computer or hard drive will only be accessible to trained and authorized CSS operators.

12.1.e Copies of data collected during CSS operation will not be kept on a shared drive unless;

12.1.e.i) The shared drive is classified as a Protected "B" environment and;

12.1.e.ii) Access to the shared drive can be restricted to CSS operators who are authorized to access copies for operational purposes, and;

12.1.e.iii) The shared drive is capable of recording the date/time of access, individual who accessed and record of access activity.

12.2 Handling of data collected during operational deployments- Operator Responsibilities

APPENDIX C
Interim Policy 2017-06-27

12.2.a The operator who collects the data, including any third party data collected incidental to the deployment, will be responsible for ensuring the continuity and security of the device and the data collected, during his/her operation of the CSS.

12.2.b All data, including third party data, collected during the investigation will be downloaded from the CSS device database at the end of each CSS operator's tour of duty and, secured as an exhibit.

12.2.c In addition to the data downloaded from the CSS by the operator as an exhibit, there may be a requirement to keep the originally collected data on the device, for comparison purposes during an ongoing investigation. Collected data that is kept on the device for this purpose will be deleted as soon as practicable, and in any case, at the conclusion of the investigation by the responsible operator. A record will be made of the deletion by the operator in the CSS master log.

12.2.d In addition to the operator's own notes, the operator(s) will ensure every CSS has a master log which provides detail of the "chain of custody", (continuity) of data collected during each CSS deployment. This log will contain the following:

12.2.d.i Date, time, of each CSS deployment

12.2.d.ii File number/Project name for which the data was collected

12.2.d.iii Name of operator, date and time(s) of collection of the data.

12.2.d.iv Date, time and location where the downloaded collected data, (including incidental third party data) are secured as exhibits.

12.2.d.v Date and time of deletion of collected data from the CSS device's database.

12.2.d.vi Date and time of destruction of the third party data, (following an order of the Court or conclusion of the investigation/prosecution), and name of person who can attest to destruction.

12.2.e Each operator will provide a report to the investigation on his/her involvement in the security and continuity of all data collected during CSS deployments including, third party data. This report will be provided as soon as practicable or, at minimum, upon the conclusion of the use of the CSS within the investigation.

12.3 Collection and handling of data collected during training/testing deployments

12.3.a Any data incidentally collected during training will be destroyed immediately upon conclusion of the training/testing deployment. The CSS master log will record the following:

12.3.a.i Date and time of training/testing

12.3.a.ii Name of operator

12.3.a.iii Name of manager who approved the training/testing deployment

12.3.a.iv Date and time of destruction of collected data

13. Disclosure

13.1. CSS data will be disclosed as required by law.

APPENDIX C
Interim Policy 2017-06-27

13.2. The CSS data will be vetted by a CSS operator as necessary in order to protect sensitive investigative techniques and operational capabilities for law enforcement purposes.

13.3. The OIC of Technical Investigation Services, or delegate, will review the disclosure package before it is provided to the courts in order to ensure compliance with disclosure policy.

14. Court

14.1. TIS will be advised prior to any CSS operator being called to provide evidence/testimony in court.

14.2. The CSS operator will only testify regarding the operation of the device.

14.3. TIS NHQ will arrange for persons to provide testimony on how the device operates should it be required by the courts.