SUPERIOR COURT
Criminal Division

CANADA
PROVINCE OF QUEBEC
DISTRICT OF LAVAL

No: 540-01-063428-141

DATE: November 18, 2015

PRESIDED BY: THE HONOURABLE MR JUSTICE MICHAEL STOBER, J.S.C.

HER MAJESTY THE QUEEN

v.

VITTORIO MIRARCHI

JACK SIMPSON

CALOGERO MILIOTO

PIETRO MAGISTRALE

STEVEN FRACAS

STEVEN D'ADDARIO

RAYNALD DESJARDINS

and

FELICE RACANIELLO

JUDGMENT ON MOTIONS FOR DISCLOSURE OF INFORMATION UPON WHICH THE CROWN IS CLAIMING INVESTIGATIVE TECHNIQUES PRIVILEGE*

---

*The judgment and the related hearings are subject to a non-publication order.
Judgment was rendered orally on November 18, 2015.
All parties were advised that this written judgment would follow.
[NDLE : L'ordonnance de non-publication émise est levée pour les parties non caviardées]

JS1327

[1] Vittorio Mirarchi, Jack Simpson, Calogero Milioto, Pietro Magistrale, Steven Fracas, and Steven D'Addario are jointly charged with the first degree murder, on November 24, 2011, of Salvatore Montagna. They are also charged with conspiracy, between September 16, 2011 and November 24, 2011, to commit the murder of Salvatore Montagna.

[2] Felice Racaniello is charged with being, between November 24, 2011 and November 28, 2011, an accessory after the fact to the murder of Salvatore Montagna.

[3] These charges resulted from police investigations named *Projet Clemenza* and *Projet Inertie*.

[4] Most of the evidence relied upon by the Crown consists of private communications (Pin to Pin, BBM, SMS), primarily Pin to Pin messages, that were intercepted pursuant to judicial authorizations granted under s. 186 of Part VI (Invasion of Privacy) of the *Criminal Code*.[1]

[5] Part of the evidence relied upon by the Crown consists of private communications in the form of emails, chat conversations and text messages (Pin to Pin, BBM and SMS), extracted from several electronic devices particularly cell phones and computers, seized upon the arrests of the accused and at various other locations.

---

[1] No. 500-54-000076-105;
Crown and defence counsel confirm that the original general warrant no. 500-26-062901-107, dated December 17, 2010, contained in Mirarchi's Application Record, Tab 2, authorized (for the period December 17, 2010 to February 4, 2011) the use of the MDI technique. In the three renewals (for the periods February 4, 2011 to February 25, 2012) referred to at par. 3 in both R-25 and R-32, the affiant obtained authorizations to similarly use the MDI technique for the same reasons stated in the affidavit for the original general warrant, contained in Mirarchi's Application Record, Tab 2, Annex, B, par. 1, Annex C, par. 5.2, 5.3.

[6] The defence seeks disclosure of police techniques in intercepting and decoding these communications. As well, the defence seeks disclosure with respect to the police use of a device that captures information and identifies cellular phones in range.

[7] Mirarchi presents a motion regarding the manner of interception of Pin to Pin communications and requests "*disclosure of information that the Crown acknowledges is in its possession or control but that the Crown has not disclosed on the basis of Investigative Privilege*".[2] Mirarchi also presents a motion for "*disclosure of information that is likely relevant in relation to a mobile device identifier (MDI)*".[3] All of the co-accused, except Desjardins, join in these motions.

[8] Both motions proceeded together. However, the MDI motion began at a later date, after its filing on May 5, 2015. The Crown invoked investigative techniques privilege under the common law with respect to both motions. The Crown indicated that it intended to file, at a later date, a motion under s. 37 of the *Canada Evidence Act*, dependent upon the Court's ruling regarding the common law privilege. It was understood that all of the evidence that the Crown intended to present, on investigative techniques privilege or public interest privilege, would be tendered at the present hearings dealing with disclosure and privilege at common law.

[9] Raynald Desjardins was accused jointly of the same charges. On July 6, 2015, he pleaded guilty before a different judge, on a new and separate indictment, to conspiracy to murder; the first degree murder charge was stayed by the Crown (s. 57*9 Cr. C*.). Therefore, Desjardins is no longer a co-accused in these proceedings. His separate

---

2 R-25 was filed on November 11, 2014.
3 R-32 was filed on May 5, 2015.

disclosure motion with respect to the MDI[4] is therefore moot and was struck from the docket.

[10] A first *ex parte* hearing took place, upon an agreed procedure,[5] on November 11, 2014. Inspector Mark Flynn testified. He spoke of particular matters that were not pertinent to the privilege invoked. The Court expressed concerns at a later *ex parte* hearing on December 2, 2014 with respect to uncertainties as to the nature of the information that the Crown wanted to protect with privilege.

[11] Certain delays were inevitable in view of the untimely death on December 24, 2014, of Me Greenspan, lead counsel for Mirarchi.

[12] In view of many anticipated *ex parte* hearings, Crown and all defence counsel proposed the appointment of an *amicus curiae* for these hearings, since defence counsel would be excluded. Thus on May 27, 2015, Me Anil Kapoor was appointed amicus curiae for these two motions. A procedure was adopted for the in camera *ex parte* proceedings which were to follow.[6] Me Kapoor participated in all subsequent hearings - *ex parte* and public - with respect to these two motions. RCMP witnesses - Inspector Mark Flynn, Corporal Josh Richdale and Mr Jocelyn Fortin (civilian member) - testified for the Crown at *ex parte* and public hearings. No witnesses were called by the defence. Numerous documents were filed as exhibits in both the *ex parte* and public hearings of these two motions.

4 R-32a.
5 R-25.1.
6 R-33 en liasse.

[13] Subsequent to the filing of the motions and following earlier hearings on the motions, the parties narrowed the information sought, upon which the Crown invokes common law investigative techniques privilege, as follows.[7]

[14] With respect to the manner of interception of the Pin to Pin and text messages (R-25):

> 1. Location on the travel path of the RCMP's intercept solution, which includes the actions that are necessary to expose the communications to the RCMP equipment to facilitate the intercept;
>
> 2. A demonstration of the interception software that exposes the user interface and the capabilities of the system, which would show what the RCMP is able and not able to do. Crown and defence counsel advise that this question is no longer an issue, thus the Court will not rule on it in this judgment;
>
> 3. Role, if any, of *Research in Motion* (RIM) in the interception and decoding process.

[15] With respect to the mobile device identifier (R-32):

> 1. The manufacturer, make, model and software version for the equipment used by the RCMP while employing the MDI technique and confirmation that the device is a cell site simulator;
>
> 2. While the RCMP is disclosing the signal strength of the targets' devices, it will not disclose the signal strength of the MDI device;
>
> 3. How the MDI device affects the targeted mobile devices; ie. did it force the targeted device to use a 2G network connection; did it turn off encryption on the mobile device; did it force the device to increase its broadcast strength;
>
> 4. A description of the default settings on the MDI device;
>
> 5. If they do exist, the Crown is not willing to provide a copy of any non-disclosure agreement relating to the MDI device;
>
> 6. The results of research conducted by the RCMP on the effect of the MDI on the ability of devices within its coverage area to make and receive calls or SMS messages.

---

[7] R-34.

[16] The Court must decide if the information requested by the defence should be disclosed, in all or in part, to the defence; or whether it should remain non-disclosed, in all or in part, being subject to *Investigative Techniques Privilege*.

[17] For the reasons that follow, the Court grants the motion, in part.

THE FACTS

[18] In addition to the public and *ex parte* testimonies referred to above, as well as exhibits filed, the following documents marked as exhibits outline and explain the police techniques and the request for investigative techniques privilege. These documents are attached as annexes to this judgment:

1. RCMP report; [8]
2. Affidavit of RCMP civilian member Jocelyn Fortin;[9]
3. Affidavit of Corporal Josh Richdale;[10]
4. Affidavit of Inspector Mark Flynn.[11]

[19] The Court finds it useful to reproduce here all or part of these documents as well as summarizing certain information in evidence.

[20] The RCMP report reads as follows:[12]

[redacted]

[redacted]

[redacted]

---

8 EP-32.27, (EP refers to exhibits filed at the *ex parte* hearings).
9 EP-32.14.
10 EP-32.10.
11 EP-32.9.
12 EP-32.27.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[21] Excerpts of the affidavit of **civilian <u>RCMP member Jocelyn Fortin</u>** read as follows:[13]

...

a) Overview

a) <u>Wireless Telecommunication in Canada</u>

3. Different mobile technologies are currently deployed in Canada.
    a. GSM (Global System for Mobile Communications)
    b. UMTS (Universal Mobile Telecommunications System)
    c. LTE (Long Term Evolution)
    d. CDMA (Code Division Multiple Access)
    e. iDen (Trunk-Radio)

4. Around the world, the frequency bands where the cellular mobile technologies are deployed are different for each country. In Canada they are deployed on the following bands
    a. Band 5 – Cellular: 824-849 MHz paired with 869-894 MHz
    b. Band 2 – PCS : 1850-1910 MHz paired with 1930-1990 MHz
    c. Band 4 – AWS : 1710-1755 MHz paired with 2110-2155 MHz
    d. Band 12 – Lo A/B/C: 699-716 MHz paired with 729-746 MHz

[13] EP-32.14.

e. Band 17 – Lo B/C: 704-716 MHz paired with 734-746 MHz (Subset)
f. Band 7 – 2600 : 2500-2570 MHz paired with 2620-2690 MHz

5. Mobile devices use unique identifiers to authenticate themselves with the cellular network. GSM/UMTS/LTE devices use an IMSI (International Mobile Subscriber Identity) and IMEI (International Mobile Equipment Identity). CDMA devices use MSID (Mobile Station ID) and ESN (Electronic Serial Number).

b) Wireless Interception

6. In project Clemenza, the communication content was not intercepted over the air using the MDI.

c) Mobile Device Identifier (MDI)

7. Mobile Device Identifier is a device that may be described as, and is commonly referred to as, an IMSI-Catcher.

8. IMSI-Catchers, are devices that could be used in cellular networks to identify, eavesdrop or locate mobile devices.

9. There are many models of IMSI-Catchers and manufacturers. They all have their differences and features.

10. In order to identify the unknown cellular devices, IMSI-Catchers can be used to gather the unique identifiers of the cellular devices that are in possession of the subjects.

b) RCMP MDI devices

[redacted]

13. The MDIs used by the RCMP are used to
    a. Identify unknown mobile devices that are in possession of known persons
    b. Confirm the possession of a known device in a known person's possession.

c) RCMP MDI techniques and detectability

[redacted]

[redacted]

16. The cellular devices using the UMTS technology are backward compatible with the older GSM technology. UMTS and GSM technologies offer the same quality for voice communications. UMTS offers a higher speed of transmission for data communications.

[redacted]

[redacted]

35. The information mentioned in paragraphs 14,15 and from 17 to 34 about the RCMP MDI technique and its detectability has not been explicitly explained in the documentation provided by the applicant which I have reviewed.

d) IMSI-Catcher Detection Tools Efficiency

[redacted]

[redacted]

51. The information mentioned in paragraphs 36 to 50 about the IMSI-Catchers detection tools efficiency, has not been explicitly explained in the documentation provided by the applicants which I have reviewed. [redacted]

e) Conclusion

52. [redacted] As explained in this affidavit, disclosure of even minor details about the capabilities and limitations of the equipment would provide critical information that would help develop efficient detection tools.

53. The release of sensitive technical information would also allow criminals to modify their behaviors and take countermeasures to thwart the use of this technology.

...

[22] Excerpts of the affidavit of **Corporal Josh Richdale** read as follows:[14]

...

5. The MDI is a device that may be described as, and is commonly referred to as, an "IMSI Catcher"

6. An IMSI catcher is a device used to intercept identification information of mobile devices and to locate mobile devices.

---

[14] EP-32.10.

[redacted]

10. The MDI utilized by the RCMP in project Clemenza was used for two objectives:

    a) To identify unknown devices that are in possession of known persons;

    b) To confirm the possession of a known devices in a known person's possession;

11. To achieve these objectives, the MDI can be operated in two different modes:

    a) Query mode (unofficial term)

    b) Direction Finding mode (unofficial term)

Query Mode

12. In query mode, when activated, the MDI equipment will obtain information that is being transmitted by devices that are in the range of the MDI.

13. Information that is obtained by the MDI is information that mobile devices regularly transmit to the cellular network in order to operate properly. The types of information are:

    a) the International Mobile Subscriber Identifier (IMSI) of the device; and

    b) The International Mobile Equipment Identifier (IMEI) of the device.

14. These identifiers, also give information pertaining to the cellular provider, the country of origin of the provider, the manufacturer of the device, and the make and model of the device.

15. Information related to frequency bands, channels, tower information can also be captured.

Direction Finding mode

18. With the direction finding mode (DF), the MDI will search for the transmitting signal of a specific known device. Once it has captured the signal from the device, the MDI will analyse the signal strength and direction from which the signal is being received which will allow the operator to locate the device.

21. A technical expert, or to a lesser extent any person, who would have access to the information mentioned in **paragraphs 7, 8, 9, 16, 17, 19, and 20** would be able to determine how the MDI machine operates, the frequencies that are relevant to its operation, the cellular technologies that it is capable to work with, and other various and unique characteristics that differentiates the MDI and other IMSI catcher like equipment. This would allow such individuals to develop methods, software, or equipment to detect when the MDI is being used and to adopt certain behaviours that would prevent cellular their devices from being identified.

22. The information provided in **paragraphs 7, 8, 9, 16, 17, 19, and 20** has not been mentioned in any of the public documentation provided by the applicants, which I have reviewed.

23. Publicly available information about IMSI catchers is mostly based on assumptions and the explanations provided about the way they work are general statements that do not

address the underlying functions of how an IMSI catcher really functions in order to capture mobile device information.

Identifying unknown devices in possession of a person

24. Physical surveillance is established on the person of interest.

25. The MDI operator will complete a reading using the query mode at the location where the person of interest is known to be at.

26. Information transmitted from the mobile devices that are within the range of the MDI will be obtained and stored in a database.

27. Once the person of interest moves to a new location, the MDI operator will complete another reading at this new location.

28. This procedure continues as the subject of interest travels to other locations.

29. After completing readings at various locations, the operator will analyze the database containing the obtained information from the various locations. The analysis is basically a process of elimination, and in theory, there should only be the target's cellular devices that are present in all the locations where he travelled.

30. As more readings are completed, and more data is available for analysis, the operator may choose to focus on certain frequencies, use the DF technique or complete more readings as he sees necessary in order to ensure that he has positively identified a cellular device that is in possession of the target.

31. There are no minimum or maximum number of readings or locations required. This will vary based on the situation.

32. The operator may also study the signal strength of possible devices at the time of capture. The signal strength, known as RSSI (Received signal strength indicator), is a value measured in decibels that illustrate the strength of a transmitted signal. The higher the signal strength, the closer the device is to the MDI. The RSSI will be weaker if the device is farther away. This signal strength will allow the operator to corroborate what he is seeing as he is conducting readings. This is similar to the DF technique but based on the analysis of the data that was obtained by the machine.

33. In certain circumstances, once a device has been identified using the query mode, the operator may use the DF mode to further validate his findings.

34. The operator will conclude that a device is in possession of a person when he has reasonable grounds to believe so.

Confirming the possession of a known device in a known person's possession

35. Physical surveillance is established on the person of interest.

36. The MDI operator may complete a reading using the query mode at the location where the person of interest is located in order to confirm that the device is in the area and within range of the MDI.

37. The operator will then use the DF mode to focus on the signal of a specific device.

38. The operator will then use techniques common with radio frequency direction finding to locate the device as well as the indicators in the MDI software.

39. With these techniques it is possible to precisely locate the targeted device.

40. Based on the circumstances of the how the targeted device was obtained and location of the person of interest, it is possible to have reasonable grounds to confirm that the device is in possession of the person of interest or very close proximity of the person of interest.

The Range of the MDI

41. The range of the MDI varies depending on physical conditions, environmental conditions and the characteristics of the cellular network in the area in which it is being operated. These factors can result in different ranges, for the same equipment, operated with the same settings, when used in different areas or different times.

42. The MDI operators use their skill based on training and experience to determine when a target is within the range of the MDI equipment. An in-depth analysis of how this is done would allow individuals to develop methods to detect when the equipment is being used and also prevent their devices from being identified.

43. Information in relation to specific range and distance would allow individuals to use counter-surveillance techniques that would allow them to identify the location and whereabouts of MDI equipment. This could not only jeopardize the technique but could put the safety of the MDI operator, or other peace officers, at risk.

Inconclusive Results

44. In some cases, the MDI surveillance is not able to identify or locate a mobile device. This negative result does not exclude the possibility that the person of interest is in possession of a mobile device. In face, in this particular file, subjects under surveillance were clearly seen using a mobile device regularly, while the MDI was unable to capture them. There are many reasons why a mobile phone may not be captured by the MDI such as: the phone can be turned off or the device is out of the MDI range of operation.

45. In project Clemenza I was the primary operator of the MDI equipment on the following dates while working on the associated persons of interest:

COLLAPELLE
2012/01/11
2012/01/16
2012/01/17

IACONETTI
2012-01-20

46. I was also present in training as a passenger on the following dates while working the associated persons of interest:

DESJARDINS:
2011-11-25
2011-11-26

Handling of the captured Data

47. The data that is captured by the MDI is stored in a database. Operators will save the database of their surveillance on a USB key which they keep control and possession of throughout the duration of the file. At the end of the file, the databases are consolidated onto a single media (CD or USB) and kept in a secure location at the RCMP Special I office.

48. The operator will only give IMSI, IMEI and the associated provider information of a number for which they had reasonable grounds to believe as in the possession of the person of interest to the investigating unit. All inconclusive results, information concerning non-targeted persons or other information gathered in the database are not given the investigators and are kept under the control of the RCMP Special I unit.

[23] Excepts of the affidavit of **Inspector Mark Flynn** read as follows:[15]

…

3. The MDI is a device that may be described as, and is commonly referred to as, an "IMSI Catcher". Information with respect to how IMSI catchers work is available on the internet. The MDI utilized by the RCMP has unique capabilities that are not commonly available in the public realm. This includes differences that enable the MDI to identify cellular devices that other IMSI catcher like devices are not capable of identifying;

4. A technical expert, or to a lesser extent any person, who has access to the MDI system or user interface (software) would learn information that would aid them in developing techniques that allow them to detect when this techniques is being deployed;

5. These systems are currently being used to support ongoing criminal investigations. The release of sensitive information has the potential to impact the RCMP's ability to successfully conclude these investigations and future investigations;

[redacted]

[15] EP-32.9.

[redacted]

[24] Evidence discloses that [redacted].[16]

Reasons why the MDI may fail to identify a cellular phone

[25] Evidence has demonstrated that the MDI may fail to identify a cellular phone in circumstances where:

1. the device is off;
2. the target was not in possession of the device;
3. the device was out of range;
4. [redacted]
5. counter-surveillance measures are implemented by the target.[17]

POSITIONS OF THE PARTIES

[26] In addition to their initial written arguments as well as oral pleadings, both Crown[18] and defence[19] have filed supplementary written arguments with respect to issues which have been further streamlined since the motions were filed and pleaded at the outset.[20] The Court briefly summarizes these positions here.

[27] The Court underlines that the Crown and the *amicus curiae* were present at *ex parte* hearings. Neither defence counsel nor the accused were present, thus defence positions and arguments do not reflect evidence heard or documents filed at those *ex parte* hearings.

[28] The Crown's objection to the disclosure of the information is based on the common law claim of investigative privilege. Crown counsel, Me Rouleau, advises that

16 Ex parte testimony of Jocelyn Fortin, July 21, 2015, pp. 33-46, 49-50, July 22, 2015, pp. 33-37.
17 Outline of Crown's final arguments, p.3; MDI technique targeting, R-32.8, p. 12; R-32.9, p.16; e*x parte* testimony of Josh Richdale, July 17, 2015, pp.31-32.
18 EP-32.26.
19 R-34.1.
20 These supplementary arguments followed the filing of a document, R-34, on June 30, 2015 after the Court requested the parties to present the contentious issues clearly and concisely.

this case is the first in Canada in which the issues raised in the two motions have been before the courts.[21]

[29] The Crown considers that the specific information sought is not publicly available.

[30] The Crown qualifies the defence disclosure requests as a "*fishing expedition*" asserting that the information requested is privileged. The Crown contends that it has respected the accused's right to full answer and defence having given satisfactory answers to most of the accused's requests.[22]

[31] In the initial motion R-25, the accused seek an order directing that the Crown provide any disclosure that it is refusing to disclose on the basis of *investigative privilege*.

[32] The defence claims that the undisclosed information is relevant to the accused's position in meeting the Crown's case and in exercising a full answer and defence.

[33] The defence maintains that, with respect to undisclosed information, the accused's full answer and defence interests outweigh the public interest in effective police investigation.

[34] Even if the material can properly be said to be privileged, the defence insists that the right of the accused to make full answer and defence necessitates disclosure.

<u>THE RCMP'S INTERCEPTION OF MESSAGES (R-25)</u> (manner and capabilities)

1. Location on the travel path of the RCMP's intercept solution, which includes the actions that are necessary to expose the communications to the RCMP equipment to facilitate the intercept

[21] *Ex parte* hearing, July 2, 2015, p. 17.
[22] Crown's Reply and Annexes, par. 29.

[35] The Crown contends that if the location of the equipment and interception points were known, individuals would, in this high tech internet world, develop ways and configure devices in order to circumvent interception.

[36] The Crown indicates that disclosure of the travel paths of Pin to Pin messages would not identify the location of the end user.

[37] The defence is concerned that the travel path of Pin to Pin messages might never travel through Canada[23] whereas *Criminal Code* Part VI authorizations only apply to the interception of communications in Canada.

[38] The defence is also concerned that the travel path of Pin to Pin messages may assist the accused in understanding the geographical location of the user.

[39] The defence argues that disclosure of the location of interceptions on the travel path, at the time of the interceptions, over four years ago, would not reveal information about the RCMP's capabilities or interception points at the present time or in the future.

[40] The *amicus curiae* pleads that the precise locations of the interceptions within Canada are not privileged and should be disclosed to the defence.

[41] The *amicus* submits that [redacted] at RIM/BlackBerry and Rogers locations and the diversion of communications to RCMP locations are not privileged and should be disclosed.

2. A demonstration of the interception software that exposes the user interface and the capabilities of the system, which would show what the RCMP is able and not able to do.

[42] Crown and defence counsel advise that this question is no longer an issue.

---

[23] Public testimony of Inspector Flynn, November 11, 2014, p.128.

3. Role, if any, of *Research in Motion* (RIM) in the interception and decoding process

[43] The Crown confirms that [redacted] the global key built into the BlackBerry devices. The RCMP was then able to decode and decrypt intercepted messages.[24]

[44] The Crown states that RIM was [redacted]

[45] The Crown is reluctant to disclose any RIM involvement, stating that to do so may have a negative commercial impact on the company. Such disclosure, according to the Crown, would affect relations between RIM and police investigators.[25]

[46] The defence refers to the existence of an assistance order which compels RIM to assist the police.[26] The defence also refers to "*comfort letters*" [27] in which the RCMP requested RIM's assistance when Pin to Pin messages were intercepted. The defence presumes that RIM had a role in the interception and decoding process.

[47] The defence is of the view that the RCMP had the global encryption key built into BlackBerry devices in order to decode the messages.

[48] The defence contends that: "*If the key did not come from RIM/BlackBerry or RIM/BlackBerry was not involved in the process of providing the RCMP with the tools to unlock or decipher the encrypted messages, the accused cannot have any confidence that the messages were properly deciphered. The MD5-Hash value ensures that the*

[24] *Ex parte* testimony of Mark Flynn, November 11, 2014, pp. 24-25, June 30, 2015, pp. 33-37.
[25] Public testimony of Mark Flynn, November 11, 2014, pp. 81-82.
[26] R-25.6, Affidavit for confirmation order and sealing order in Ontario; see R-25.14, par. 29-31.
[27] R-25.2, R-25.3, R-25.4 and R-25.5.

pre-decoded data and the post-decoded data are the same, but does not ensure that the raw data has been accurately decoded".[28]

[49] The *amicus curiae* contends that the scope of the participation of RIM and Rogers may be disclosed without imperilling police work. [redacted]

[50] The *amicus curiae* submits that the global key which was used to decode messages is not privileged and should be disclosed. He states that although [redacted]

[51] On September 18, 2015, in final argument, Crown counsel, Me Rouleau, produced a document conceding that the existence of the global key to code and decode Pin messages is in the public domain.[29]

THE RCMP'S USE OF THE MOBILE DEVICE IDENTIFIER (R-32)

1. The manufacturer, make, model and software version for the equipment used by the RCMP while employing the MDI technique and confirmation that the device is a cell site simulator

[52] The evidence obtained through police use of the MDI assists the Crown at trial on the issue of identification.

[53] The Crown objects to the disclosure by raising the investigative techniques privilege.

---

[28] R-34.1, p. 3.
[29] EP-32.28.

[54] The Crown argues that the police use of the MDI will not be led before the jury as part of the prosecution's case and hence police detection methods should remain privileged and confidential.

[55] The Crown asserts that the RCMP has never disclosed how it uses MDI devices; nor has it revealed the make, model or how it operates. Although the Crown eventually conceded that certain information regarding the device is in the public domain, some characteristics are not necessarily known.

[56] The Crown claims that this information would single out the specific device used, allowing criminals to bypass the police capacities. The public interest in the protection of investigative techniques should consequently prevail.

[57] The Crown argues that disclosure would tend to identify which devices the RCMP uses and allow individuals in the criminal milieu to avoid them. The Crown also raises the security of police MDI operators in the field.

[58] [redacted]

[59] The defence insists that information regarding the MDI is already public therefore the privilege is not applicable.[30]

[60] The defence submits that challenges to the MDI's accuracy and reliability are central to the accused's defence. Therefore, even if the information were privileged, it must be disclosed because it is necessary for the accused to make full answer and defense.

---

[30] See Tabs in Mirarchi's Application Record.

[61] The defence pleads that the use of the MDI leads to indiscriminate invasions of non-targeted third party privacy rights as per *R. v. Thompson*, [1990] 2 S.C.R. 1111.[31]

[62] The defence pleads that the disclosure of information related to the MDI would facilitate the mandating of an expert regarding the functioning of the device and its reliability.

[63] The defence argues that the information is relevant to the *Garofoli* issues (in particular the "*resort to*" clause) and to the trial (in challenging the Crown's circumstantial case of identification).[32] It is further argued that disclosure would also allow the defence to establish the relevance of any independent evidence about the reliability of the device and its features. As well, disclosure would allow the defence to assess the undisclosed fourth reason why the technique might have failed to identify devices in certain accused's possession leading to police testimony that non-identification is simply inconclusive.[33]

[64] The defence pleads that the information is required to probe whether the affiants made full and frank disclosure upon applications for the general warrant and the authorizations (including renewals) to intercept private communications,[34] pursuant to *R. v. Araujo,* [2000] 2 S.C.R. 992 and *R. v. Morelli*, [2010] 1 S.C.R. 253.

[65] Although the Crown is not presenting evidence to the jury on police use of the MDI, the *amicus curiae* contends that evidence obtained by the police through the MDI is relied upon by the Crown to construct its case. Therefore, he says, on balance, evidence with respect to the MDI should not be protected and must be produced.

---

31 Mirarchi's factum (R-32), par. 36.
32 Mirarchi's factum (R-32), par. 33-35; Mirarchi's supplementary factum, par. 31-46.
33 Mirarchi's supplementary factum, p. 8, par. 13-30.
34 Mirarchi's factum (R-32), par. 32.

2. While the RCMP is disclosing the signal strength of the targets' devices, it will not disclose the signal strength of the MDI device

3. How the MDI device affects the targeted mobile devices; ie. did it force the targeted device to use a 2G network connection; did it turn off encryption on the mobile device; did it force the device to increase its broadcast strength

4. A description of the default settings on the MDI device

[66] According to the Crown, the MDI device [redacted] also capable [redacted] IMEI and IMSI numbers.[35]

[67] The Crown maintains that disclosure of any information related to the signal strength will reveal [redacted][36]

[68] The Crown wishes to maintain privilege over such MDI settings and techniques, as well as those dealing with:

(i) range specifics;

[redacted]

[69] The Crown has stated that this and other information[37] is not in the public domain.

[70] The defence has always claimed that much of this information is public.

[35] *Ex parte* testimony of Josh Richdale, July 17, 2015, p. 8; e*x parte* testimony of Jocelyn Fortin, July 21, 2015, pp. 8, 31, July 22, 2015, pp. 31-32, 87-88, 95-97, July 23, pp. 30-35.

[36] *Ex parte* testimony of Jocelyn Fortin, July 21, 2015, pp. 31-36, July 22, 2015, pp. 3, 16-23, 31-32, 37-38; *ex parte* testimony of Josh Richdale, July 17, 2015, p.12.

[37] EP-32.27; EP-32.10; EP-32.14; *ex parte* testimony of Jocelyn Fortin, July 21, 2015, pp. 51-62, July 22, 2015, pp. 23-47.

[71] The defence argues that the disclosure of default settings and the configuration of the device will assist the accused in fully appreciating the operation and capabilities of the device and the scope and extent to which the manufacturer envisioned the capture of cellular phones by the device. Such disclosure is also relevant to the configuration of the MDI when it was used to target the accused.

[72] The defence further seeks the GPS coordinates when the MDI was used; this information is relevant with respect to whether the target was out of range when the cellular phone details were captured. With respect to range, the defence wants additional specifics of the MDI when using Direction Finding Mode (DFM) in locating a known cellular phone; i.e., can it locate the phone within 2 meters, 5 meters, etc? The defence requires as well all reasons why the MDI may fail to identify a cellular phone.

[73] The defence view is that the signal strength and range of the MDI are relevant and important with respect to the manner of interference and the extent of the invasion of privacy interests of targeted individuals and/or non-targeted innocent third parties' rights. The defence further requests disclosure in order to assess the ability of the police to limit the impact on such third party rights, an issue the accused may pursue in the context of the s. 8 *Charter* motions.[38]

[74] The *amicus curiae* submits that:

- the [redacted] is a matter of investigative privilege and should not be disclosed;
- the [redacted] is a matter of investigative privilege and should not be disclosed;
- although the [redacted] is not privileged and may be safely disclosed, [redacted] is a matter of investigative privilege.

[38] Mirarchi's factum (R-32), par. 36; Mirarchi's supplementary factum, par. 44-46.

[75] The *amicus curiae* further submits that:

- , is not privileged and must be disclosed to the accused;
- are subject to disclosure; he maintains that no privilege attaches to these settings and techniques;
- the use of is not privileged and must be disclosed to the accused.

[76] On September 18, 2015, in final argument, Crown counsel, Me Rouleau, produced a document .[39]

(iv) MDI have a maximum range of 2 kilometers in a rural setting and an average range of 500 meters in a city;

5. If they do exist, the Crown is not willing to provide a copy of any non-disclosure agreement relating to the MDI device

[77] The Crown explains that it does not seek to protect the commercial aspect of the corporate relationship between the RCMP and the MDI manufacturer. It seeks to protect the impact of that relationship on the RCMP's capacities. In the Crown's view, disclosing - could jeopardize the strength of the relationship and compromise future investigations .[40]

[39] EP-32.28.
[40] *Ex parte* testimony of Mark Flynn, June 30, 2015, pp. 2-4, 25-27.

[78] The defence view is that the existence - or not - of a non-disclosure agreement is relevant to the question whether the police are improperly asserting privilege as a result of a private contract, thereby attempting to fetter the accused's constitutional rights and the Court's exercise of discretion.[41]

[79] The *amicus curiae* is of the view that non-disclosure agreements are not captured by *R. v. Stinchcombe,* [1991] 3 S.C.R. 326. He submits that they are neither material nor privileged.

6. The results of research conducted by the RCMP on the effect of the MDI on the ability of devices within its coverage area to make and receive calls or SMS messages

[80] The defence raises claims by the police, in general warrants, that the MDI technique had little impact on third parties and did not interfere generally with the ability to receive calls or send messages; that this has been tested on an *ad hoc* basis by the police. Thus the defence requests any documented information in relation to this issue, if it exists.

[81] The Crown states that testing was done, but no reports were produced.[42] However, the RCMP report[43] does refer to disclosure research as outlined above.

---

41 Mirarchi's factum (R-32), par. 31.

42 *Ex parte* testimony of Mark Flynn, July 2, 2015, pp. 104-106, July 14, 2015, pp. 20-21; public testimony of Mark Flynn, July 16, 2015, pp. 131-134.

43 EP-32.27, p. 4.

PRINCIPLES

The Crown's Duty to Disclose

[82] The Supreme Court has established that the Crown is under a general duty to disclose all information, whether inculpatory or exculpatory, except evidence that is beyond the control of the prosecution (eg. it is unaware or denies its existence), or that is clearly irrelevant, privileged, or delayed due to an ongoing investigation; *R. v. Stinchcombe*, [1991] 3 S.C.R. 326, pp. 335-336, 339-340, 343; *R. v. Dixon*, [1998] 1 S.C.R 244; *R. v. Chaplin*, [1995] 1 S.C.R. 727, par. 21, 30; *R. v. Egger*, [1993] 2 S.C.R. 451, pp. 466-467; *R. v. Taillefer,* [2003] 3 S.C.R. 307, par. 59.

[83] The Crown must disclose all relevant material whether favourable to the accused or not and whether the Crown intends to produce it in evidence or not. It must not withhold information if there is a reasonable possibility that doing so would impair the accused's *Charter*-protected right to make full answer and defence (s. 7), subject to certain exceptions; *R. v. Stinchcombe*, supra, pp. 336, 338, 340, 343; *R. v. Mills*, [1999] 3 S.C.R. 668, par. 69; *R. v. Rose*, [1998] 3 S.C.R. 262, par. 98; *Dersch v. Canada (Attorney General),* [1990] 2 S.C.R. 1505, p. 1514; *R. v. Hutter* (1993), 67 O.A.C. 307; *R. v. Bero*, (2000), 137 O.A.C. 336, par. 31-32.

[84] In *Krieger v. Law Society of Alberta*, [2002] 3 S.C.R. 372, the Supreme Court stated (par. 45) that the exercise of prosecutorial discretion is to be treated with deference by the courts. The Supreme Court indicated (par. 54), however, that while the prosecutor retains the discretion not to disclose irrelevant information, disclosure of relevant evidence is not a matter of prosecutorial discretion but, rather, is a prosecutorial duty.

[85] In *R. v. Anderson*, [2014] 2 S.C.R. 167, par. 45, the Supreme Court held that "*the Crown possesses no discretion to breach the Charter rights of an accused*", and that "*prosecutorial discretion provides no shield to a Crown prosecutor who has failed to fulfill his or her constitutional obligations such as the duty to provide proper disclosure to the defence*".

[86] In *Stinchcombe*, Sopinka J. stated (p. 333):

> I would add that the fruits of the investigation which are in the possession of counsel for the Crown are not the property of the Crown for use in securing a conviction but the property of the public to be used to ensure that justice is done. In contrast, the defence has no obligation to assist the prosecution and is entitled to assume a purely adversarial role toward the prosecution. The absence of a duty to disclose can, therefore, be justified as being consistent with this role.

[87] Failure to disclose undermines the ability of the accused to make full answer and defence. This common law right to make full answer and defence has been elevated to a constitutional right by its inclusion as one of the principles of fundamental justice in s. 7 of the *Charter*; *Dersch v.Canada (Attorney General)*, supra, p. 1514; *Stinchcombe*, p. 336; *R. v. Chaplin*, supra, par. 20-22, 25.

[88] As Sopinka J. pointed out in *Stinchcombe* (p. 336):

> ...The right to make full answer and defence is one of the pillars of criminal justice on which we heavily depend to ensure that the innocent are not convicted. Recent events have demonstrated that the erosion of this right due to non-disclosure was an important factor in the conviction and incarceration of an innocent person. …

[89] The Supreme Court, in *Henry* v. *British Columbia (Attorney General)*, [2015] 2 S.C.R. 214, raised difficulties facing prosecutors:

> I readily acknowledge that disclosure decisions often involve difficult judgment calls. As the intervener Attorney General of Ontario observes, disclosure decisions may require consideration of numerous factors, such as whether the information is subject to special protections for sexual assault complainants, special considerations concerning highly sensitive material, or one of the various privileges that attach to information obtained in the course of a criminal prosecution. Even the basic question of relevance may be difficult to assess before the Crown is made aware of the defence theory of the case, and where disclosure requests are not explained or particularized. Furthermore, disclosure obligations are ongoing, which requires prosecutors to

> continuously evaluate the information in their possession.

[90] "*While the Crown must err on the side of inclusion, it need not produce what is clearly irrelevant*"; *R. v. Chaplin*, supra, par. 22. The Supreme Court further stated in *Chaplin* (par. 22):

> ... One measure of the relevance of information in the Crown's hands is its usefulness to the defence: if it is of some use, it is relevant and should be disclosed — *Stinchcombe*, *supra*, at p. 345. This requires a determination by the reviewing judge that production of the information can reasonably be used by the accused either in meeting the case for the Crown, advancing a defence or otherwise in making a decision which may affect the conduct of the defence such as, for example, whether to call evidence.

[91] On the question of relevance, the Supreme Court, in *Stinchcombe* (pp. 345-346) said:

> ... If the information is of no use then presumably it is irrelevant and will be excluded in the exercise of the discretion of the Crown. If the information is of some use then it is relevant and the determination as to whether it is sufficiently useful to put into evidence should be made by the defence and not the prosecutor. ...

[92] In *R. v. Dixon*, supra, par. 23, 50, the Supreme Court held that the fairness of the trial process would be compromised if the Crown's failure to disclose "*deprived the defence of opportunities to pursue additional lines of inquiry with witnesses or garner additional evidence flowing from the undisclosed material*". The Supreme Court considered the right to disclosure of all relevant material to have a "*broad scope*", however, the Court indicated that material which may have only marginal value to the ultimate issues at trial may be relevant and subject to disclosure, but could not possibly affect the overall fairness of the trial process and would not give rise to a remedy.

[93] Relevance must be assessed in relation both to the charge itself and to the reasonably possible defences; *R. v. Taillefer,* supra, par. 59.

[94] With respect to the burden of proof, the Supreme Court stated, in *Stinchcombe* (p.340):

> The discretion of Crown counsel is, however, reviewable by the trial judge. Counsel for the defence can initiate a review when an issue arises with respect to the exercise of the Crown's discretion. On a review the Crown must justify its refusal to disclose. Inasmuch as disclosure of all relevant information is the general rule, the Crown must bring itself within an exception to that rule.

and in *Chaplin,* par. 25:

> In situations in which the existence of certain information has been identified, then the Crown must justify non-disclosure by demonstrating either that the information sought is beyond its control, or that it is clearly irrelevant or privileged. The trial judge must afford the Crown an opportunity to call evidence to justify such allegation of non-disclosure. As noted in *R. v. Stinchcombe, supra*, at p. 341:

This may require not only submissions but the inspection of statements and other documents and indeed, in some cases, *viva voce* evidence. A *voir dire* will frequently be the appropriate procedure in which to deal with these matters.

...

[underlining added]

[95] "*This may be done by showing that the public interest in non-disclosure outweighs the accused's interest in disclosure*"; *R. v. Durette*, [1994] 1 S.C.R. 469, p. 495.

[96] This obligation to disclose is not absolute.[44] It is subject to Crown discretion with respect to the withholding of information, the timing of disclosure, the law of privilege and the relevance of information. As the Supreme Court stated, upon a trial judge's review of such discretion the Crown must justify its refusal to disclose and bring itself within an exception to the general rule to disclose all relevant information; *Stinchcombe*, pp. 339-340.

[97] Justification for non-disclosure may be based on grounds of privilege at common law or under the *Canada Evidence Act* (sections 37, 38 & 39), in order to protect the confidentiality of the information or evidence.

[44] For some historical perspective on privilege in the context of government documents and the public interest, see *Carey v. Ontario,* [1986] 2 S.C.R. 637.

[98] However, the right to make full answer and defence remains a priority.

[99] Sopinka J. stated (*Stinchcombe*, p. 340):

> The trial judge on a review should be guided by the general principle that information ought not to be withheld if there is a reasonable possibility that the withholding of information will impair the right of the accused to make full answer and defence, unless the non-disclosure is justified by the law of privilege. The trial judge might also, in certain circumstances, conclude that the recognition of an existing privilege does not constitute a reasonable limit on the constitutional right to make full answer and defence and thus require disclosure in spite of the law of privilege. ...

[100] Privilege was defined by David Watt, J.A., as follows:[45]

> A *privilege* is an *exclusionary* rule. It bars evidence that is relevant and material. Unlike other rules of admissibility, for example, hearsay, opinion, and character, a privilege is *not* grounded upon concerns about the unreliability, lack of probative value, or susceptibility to fabrication of the evidence. A privilege is founded upon social values, external to the trial and its process, which are considered of superordinate importance.
>
> Privileges are few and narrowly confined. Their effect, like other admissibility rules, is to foreclose from forensic scrutiny, relevant and material evidence more often than not of significant probative value. They do so on the basis that a social policy, external to the litigation process, is of such overwhelming importance that it *cannot* be sacrificed to ascertain truth in litigation.
>
> [underlining added]

[101] The principles were more recently reaffirmed by the Supreme Court in *R. v. Basi*, [2009] 3 S.C.R.389, par. 1, a case relating to informer privilege:

> Everyone charged with a criminal offence in Canada is constitutionally entitled to full and timely disclosure of all relevant material under the control of the Crown. To withhold that material without justification is to jeopardize impermissibly the right of the accused to make full answer and defence. The entitlement to disclosure must therefore be broadly construed. But it is neither absolute nor unlimited.

[102] Disclosure is such an important duty that a breach exposes the Crown to *Charter* remedies.[46]

---

[45] *Watt's Manual of Criminal Evidence*, Toronto, Carswell, 2013, par. 15.01; see also S. Casey Hill, David M. Tanovich & Louis P. Strezos, *McWilliam's Canadian Criminal Evidence*, 5th ed. Toronto, Canada Law Book, loose-leaf updated 2015, Part III, vol 2, ch. 13-14.

[46] In the context of a civil claim alleging a breach of the Crown's disclosure duty causing harm to the plaintiff, the Supreme Court decided that the claimant has the burden with respect to: whether the prosecutor intentionally withheld information; whether the prosecutor knew or ought reasonably to have known that the information was material to the defence and that the failure to disclose would likely impinge on his or her ability to make full answer and defence; whether withholding the

[103] The Court reminds counsel of the following comments of the Supreme Court in *Stinchcombe* (pp. 340-341):

> The trial judge may also review the Crown's exercise of discretion as to relevance and interference with the investigation to ensure that the right to make full answer and defence is not violated. I am confident that disputes over disclosure will arise infrequently when it is made clear that counsel for the Crown is under a general duty to disclose all relevant information. The tradition of Crown counsel in this country in carrying out their role as "ministers of justice" and not as adversaries has generally been very high. Given this fact, and the obligation on defence counsel as officers of the court to act responsibly, these matters will usually be resolved without the intervention of the trial judge. When they do arise, the trial judge must resolve them. ...

Investigative Techniques Privilege

[104] Protection of investigative techniques is a well established common law privilege. In considering the application of this *case by case,* content based, privilege, presumptively admissible information would be subject to review and balancing (public interest vs. accused's right to make full answer and defence). The analysis requires that the policy reasons for excluding otherwise relevant evidence be weighed on a case by case basis. This differs from a *class* privilege which is based on communication or determined by the nature of a relationship, encompassing informer privilege, solicitor-client privilege and the codified spousal privilege. A class privilege is nearly absolute and related information will be *prima facie* inadmissible; this privilege will only be set aside when the innocence of the accused is demonstrably at stake; *R. v. McClure*, [2001] 1 S.C.R. 445, par. 26-30; *R. v*. *Basi*, supra, par. 22, 37; *R. v. Gruenke,* [1991] 3 S.C.R 263, par. 26; *R. v. Thomas*, [1998] O.J. No. 1400 (Ct. J.), par. 10; *R. v. Trang*, 2001 ABQB 825, par. 64, 75; *R. v. Trang*, 2002 ABQB 19, par. 32-33, 48-51, 55; Pierre Lapointe, *Les privilèges en droit criminel du point de vue du poursuivant* dans Service

---

information violated his or her *Charter* rights; and whether he or she suffered harm as a result; *Henry* v. *British Columbia (Attorney General)*, [2015] 2 S.C.R. 214 , par. 85.

de la formation continue, Barreau du Québec, vol. 298, *Développements récents en droit criminel 2008*, Cowansville, Éditions Yvon Blais, 2008, p. 84.

[105] A court's upholding of investigative techniques privilege may exempt the Crown from disclosing the privileged information and shield the information affected from being admitted in open court; either it is excluded from the trial or, notwithstanding the privilege, the balance may favour disclosure and the information may be subject to protections, such as non-publication orders and/or *in camera* hearings.

[106] This privilege may be invoked pursuant to common law or under s. 37 of the *Canada Evidence Act*, which mainly codifies the common law (sections 38 and 39 go further); Pierre Béliveau and Martin Vauclair, *Traité général de preuve et de procédure pénales*, 20e éd., Cowansville, Éditions Yvon Blais, 2013, p. 332. Section 37 does not eliminate the common law privilege. The Crown here seeks to invoke the common law privilege. If the common law privilege claim is upheld, there is no need for a s. 37 application. If the privilege claim is denied, the Crown may invoke s. 37 and seek a ruling from this Court under s. 37(2); *R. v. Chan*, 2002 ABQB 287, par. 103, 120; *R. v. Trang,* 2002 ABQB 19, par. 48-51; *R. v. Lam,* 2000 BCCA 545, par. 3; *R. v. Pilotte,* (2002), 156 O.A.C. 1, par. 44.

[107] Crown counsel, defence counsel and the *amicus curiae* agree that there is no difference between the considerations underlying an analysis pursuant to either s. 37 of the *Canada Evidence Act* or the common law. The distinction, of course, is that appeals are permitted under the s. 37 procedure on an interlocutory basis, but not under the common law.[47]

[47] Crown's Reply and Annexes, R-25c)i),Tab 1, par. 3; Factum of the amicus curiae, September 8, 2015, par. 24.

[108] Section 38 of the *Canada Evidence Act* refers to sensitive information (*renseignements sensibles*) and potentially injurious information (*renseignements potentiellement préjudiciables*). Section 37 uses different language. The Crown burden is more onerous. Section 37(5) refers to information which *would encroach upon a specified public interest* (*est préjudiciable au regard des raisons d'intérêt public déterminées*). Thus it is easier to have access to information if s. 37 (public interest) is invoked, as opposed to s. 38 (international relations, national defence, national security) or s. 39 (confidences of the Queen's Privy Council for Canada); *R. v. Minisini*, 2008 QCCA 2188, par. 53; *Babcock v. Canada (Attorney General),* [2002] 3 S.C.R. 3, par. 17-19.

[109] However, the Crown does not have to show, under s. 37, that the disclosure of the information would ***necessarily*** encroach upon a specified public interest; *R. v. Minisini*, 2008 QCCA 2188, par. 54; *R. v. Allie*, 2014 QCCS 2381, par. 10, 19.

[110] The mere assertion by the police or the Crown is insufficient to warrant a finding of privilege. Proof of the allegation is required.

[111] In *R. v. Allie, supra,* par. 19, Huot J. stated :

> Évidemment, une simple affirmation du Ministère public à l'effet que la divulgation de renseignements risquerait de dévoiler une technique d'enquête ou de compromettre la sécurité d'un témoin est insuffisante. Une preuve doit être faite à cet effet. Il convient cependant de remarquer que cette dernière n'a pas à démontrer qu'une communication de l'information entraînerait nécessairement l'effet pervers appréhendé. …

[112] Investigative techniques privilege was recognized in *R. v. Meuckon,* [1990] B.C.J. No. 1552 (C.A.). An undercover police officer testified that he simulated the ingestion of cocaine during his contacts with the accused. The defence wanted to show that it could not be done effectively, that he must have ingested the cocaine, and that

his testimony was not credible. Crown privilege was claimed under s. 37 of the *Canada Evidence Act*.

[113] The British Columbia Court of Appeal (par. 25-27) specified the procedure to follow when the privilege is claimed:

> If an objection is made, and the public interest is specified, then the trial judge may examine or hear the information in circumstances which he considers appropriate, including the absence of the parties, their counsel, and the public. Whether the trial judge does hear or examine the information, or whether he does not, the trial judge may then either uphold the claim of Crown privilege or order the disclosure of the information either with conditions or unconditionally.
>
> In my opinion, if the privilege is claimed in a criminal trial, the trial judge must decide first whether the information might possibly affect the outcome of the trial. His decision on that question may well be influenced by whether the trial is being conducted by a judge alone or by a judge and jury. If a decision to uphold the claim of privilege and to prevent the disclosure of the information could not affect the outcome of the trial, then the privilege claim should generally be upheld. But if the decision to uphold the claim of privilege might affect the outcome of the trial, then the trial judge must consider whether the upholding of the claim of privilege would have the effect of preventing the accused from making full answer and defence. If the trial judge concludes that the claim of privilege would have that effect he should then consider giving the Crown the alternative of either withdrawing the claim of privilege or entering a stay of proceedings. If the Crown refuses to do either, then the trial judge may permit the introduction of the evidence though the trial judge may impose whatever safeguards seem appropriate.
>
> In short, the trial judge should consider whether the public interest in allowing the accused to make full answer and defence to a criminal charge can be overridden by the interest asserted by the Crown. The ultimate safeguard of the privileged information lies in the Crown's power to enter a stay of proceedings.
>
> [underlining added]

[114] *Meuckon* was followed in *R. v. Richards*, (1997), 100 O.A.C. 215. The Crown objected to the disclosure of information regarding the location from which a police officer observed, from a nearby observation post, the sale of cocaine by the accused to two undercover officers, as well as their automobile. The accused claimed that the disclosure was relevant to the issue whether he was the trafficker. On the privilege procedure under s. 37 of the *Canada Evidence Act*, the Ontario Court of Appeal stated that the public interest privilege is a creature of the common law rules of evidence, that s. 37 provides a mechanism for its resolution. The Court elaborated (par. 11):

> ...Disclosure of police investigative techniques is subject to a qualified privilege: *R.* v. *Meuckon* (1990), 57 C.C.C. (3d) 193 (B.C.C.A.). Where the claim is made, the judge must first decide whether the information sought is relevant to an issue in the proceedings. Second, if relevant, evidence of the investigative techniques used will not be disclosed if the public interest in effective police investigation and the protection of those involved in, or who assist in such investigation, outweigh the legitimate interests of the accused in disclosure of the techniques.

[115] Binder J. in *R. v. Trang,* 2002 ABQB 19, par. 49-50, explained the rationale behind the privilege:

> The jurisprudence clearly supports a common law privilege in relation to investigative technique, where warranted...
>
> Clearly, disclosure of investigative techniques may in some cases compromise ongoing investigations and put officers or civilians at risk; it might also cause criminal offenders in the future to modify their activities in order to avoid detection. There may be other justifications for non-disclosure of investigative techniques which are specific to the technique in question.

[116] Binder J. then categorized the privilege invoked as a qualified privilege which means it is subject to review and balancing by the Court (par. 55):

> Investigative techniques, ongoing investigations and safety of individuals are well recognized common law privileges. To distinguish them from communication based privilege and avoid the confusion created by the use of communication privilege terminology, I would categorize them as "qualified privileges". In accordance with the jurisprudence, these privileges are subject to review and balancing by the Court of the public interest served by the privilege against the importance of the information to the right of an accused to make full answer and defence.

[117] In *R. v. Toronto Star Newspapers Ltd*., [2005] O.J. No. 5533 (S.C.), par. 14, Nordheimer J. indicated that allowing the investigative technique to remain concealed "*is a basis for secrecy that is, however, fairly narrow in its application and one that of necessity needs to be determined on a case by case basis.*"

[118] The following cases deal with the investigative technique or a similar public interest privilege raised in a variety of cases which illustrate the manner in which judges strike the balance between the public interest in law enforcement and the right of the accused to make full answer and defence; *R. v. Minisini* 2008 QCCA 2188*; R. v. Boucher*, 2006 QCCA 668; *R. v. Pearson*, [2002] J.Q. no 3541 (CA) (certain protective measures agreed to between a witness and/or accomplice and the state);

R. v. Meuckon, [1990] B.C.J. No. 1552 (C.A) (undercover officer's simulated ingestion of cocaine); *R. v. J.J.*, 2010 ONSC 385 (location of concealed police firearm); *R. v. Lam*, 2000 BCCA 545; *R. v. Blair*, [2000] O.J. No. 3079 (C.A.); *R. v. Richards*, (1997), 100 O.A.C. 215; *R. v. Thomas*, [1998] O.J. No. 1400 (Ct. J.) (observation post); *R. v. Toronto Star Newspapers Ltd*., (2005), 204 C.C.C. (3d) 397 (Ont. S.C.) (forensic accountants retained by the Crown or the RCMP regarding victim corporation); *R. v. Gerrard*, (2003), 56 W.C.B. (2d) 564 (Ont. S.C.) (GPS tracking device); *R. v. Allie*, 2014 QCCS 2381 (the installation and components of video cameras and the transmission of images recorded); *R. v. Guilbride*, 2003 BCPC 176 (the location of a satellite tracking device and the circumstances of its installation on a boat); *Bégin v. R*., 2005 QCCA 213; *Hernandez v. R*., [2004] J.Q. 11285 (C.A.); *R. v. Boomer*, (2000) 182 N.S.R. (2d) 49 (N.S.S.C.); *R. v. Smith*, 2009 ABPC 88; *Stetson Motors Corp. v. Peel (Regional Municipality) Police Services Board,* [1996] O.J. No. 4632 (C. J.) (secondary locations of serial (VIN) numbers in automobiles or motorcycles); *R. v. Provenzano*, [2003] O.J. No. 474 (S.C.) (lack of VINs to establish stolen vehicles and parts); *R. v. Desjardins* (1990), 61 C.C.C. (3d) 376 (Nfld. S.C.) and *R. v. Rizzuto*, [1991] N.J. No. 14 (Nfld. S.C.) (police wiretap in hotel rooms used for consultations between accused and their lawyers; privilege raised re witness subpoenas and contents of the packet).

Information Already in the Public Domain

[119] Defence arguments have argued that much of the information which the Crown wishes to protect, with respect to the MDI, is in the public domain.

[120] In *R. v. Durette,* supra, p. 497, with respect to excerpts of a wiretap affidavit that were not redacted, hence public, at a previous trial, the Supreme Court held:

> ... non-disclosure can only be justified on the basis that disclosure will prejudice the interests of

> informants, innocent persons or the law enforcement authorities and that such prejudice overbears the interests of the accused. If, however, the information has ceased to be confidential, then the justification for non-disclosure disappears. ...

[121] The Crown urges the Court to follow certain passages of *Canada (Attorney General) v. Commission of Inquiry into the Actions of Canadian Officials in relation to Maher Arar,* 2007 FC 766. In this case, the Attorney General of Canada applied under s. 38.04 of the *Canada Evidence Act* for an order from the Federal Court prohibiting the disclosure of certain redacted portions of the public report issued by the Commission, on the basis that disclosure of this information would be injurious to international relations, national defence or national security.

[122] Referring to *Babcoc*k v. *Canada (Attorney General),* supra, Noël J. said (par. 54):

> ...
>
> Although *Babcock*, above, deals with section 39 of the CEA, the same principle applies in the section 38 of the CEA context, namely that information in the public domain cannot be protected from disclosure. ...
>
> [underlining added]

[123] He referred (par. 55) to *Attorney General v. Observer Ltd et al,* [1990] 1 A.C. 109 (H.L.) in which Lord Brightman wrote (p. 267):

> The Crown is only entitled to restrain the publication of intelligence information if such publication would be against the public interest, as it normally will be if theretofore undisclosed. But if the matter sought to be published is no longer secret, there is unlikely to be any damage to the public interest by re-printing what all the world has already had the opportunity to read.
>
> [underlining by Noël J.]

[124] Noël J. pointed out limits to the public domain rule (par. 56):

> I note that the rule that information available in the public domain cannot be protected from disclosure is not an absolute. There are many circumstances which would justify protecting information available in the public domain, for instance: where only a limited part of the information was disclosed to the public; the information is not widely known or accessible; the authenticity of the information is neither confirmed nor denied; and where the information was inadvertently disclosed.
>
> [underlining added]

[125] But in *Arar,* the Court was not faced with an individual accused with a crime or threatened by criminal prosecution and imprisonment. Maher Arar is a Canadian citizen, who was never charged with any criminal offence. Thus where an individual faces "*no risk of the stigma of conviction, the justification for such a strict standard is accordingly diminished*",[48] whereas in the present case, the accused (except Racaniello) are charged with first degree murder and conspiracy to commit murder and face the most severe penalties in Canadian criminal law. Therefore, reference to *Arar* is not helpful.

[126] As the Supreme Court reasoned in *Michaud v. Québec*, [1996] 3 S.C.R. 3, par. 49:

> ... Where an individual does not face the jeopardy of the criminal process, I believe that greater weight must be attached to state's interest in confidentiality. ... Pursuant to this contextual approach, we have noted that the content of the legal rights of the *Charter* will often be interpreted more flexibly where the relevant state action does not threaten the individual with the risk of imprisonment. ...

ANALYSIS

[127] The exclusion of defence counsel from the *ex parte* hearings has created an imbalance; however, the participation of Me Kapoor, a competent security-cleared counsel, as *amicus curiae*, has levelled the playing field.

[128] The Court underlines that the cornerstone of the police investigation and the Crown's evidence consists of intercepted Pin to Pin communications, as well as cellular phone identifications captured by the deployment of the MDI device.

[129] In a case such as this one, where all of the accused (except Racaniello) are charged with the most serious offence in the *Criminal Code,* the Court must measure

---

48 *Michaud v. Québec*, [1996] 3 S.C.R. 3, par. 50.

carefully the connection and proximity of crucial relevant information to the ability of the accused to make full answer and defence in the context of a fair trial.

[130] The Crown has a common law duty and a constitutional obligation to disclose information in its possession or control that is likely relevant to the charges against the accused; *R. v. Stinchcombe*, supra. The accused have a statutory right pursuant to s. 650(3) of the *Criminal Code*, and a constitutional right under s. 7 of the *Canadian Charter of Rights and Freedoms*, to make full answer and defence. Thus the accused's right to make full answer and defence and the entitlement to full disclosure are entrenched in s. 7 of the *Charter*. The accused also have a constitutional right under s. 11(d) of the *Charter* to be presumed innocent until proven guilty according to law in a fair and public hearing by an independent and impartial tribunal.

[131] Sufficient disclosure leads to meaningful instructions to defence counsel and, it is expected, a more efficient and fair trial.

[132] Investigative techniques privilege invoked by the Crown would deny such disclosure of information that the accused would ordinarily be entitled to receive.

[133] The state does not have a constitutional right to privilege**.**

[134] It is agreed by Crown and defence counsel that the privilege invoked in this matter is a case by case privilege, which is based on content, rather than a class privilege which is based on the nature of the relationship (informer privilege; solicitor-client privilege).

[135] The significance of the police role in the maintenance of law and order and the protection of the public is indisputable. In carrying out this role "*the state's interest in protecting the confidentiality of its investigative methods and police informers remains*

compelling. The reality of modern law enforcement is that police authorities must frequently act under the cloak of secrecy to effectively counteract the activities of sophisticated criminal enterprises".[49] At the same time, there continues to be a concern about the limits of acceptable police action.[50]

[136] In determining whether the privilege should apply to the information, in all or in part, the Court must examine the relevance, and connection or proximity, of the information in question, to the accused's right to make full answer and defence.

[137] The Crown must do more than simply assert investigative privilege. It is not all information that is so sensitive that it is worthy of the shield of privilege.

[138] In deciding which - disclosure or privilege - outweighs the other, the Court must balance the state interests in protecting sensitive investigative techniques in effective law enforcement against the accused's right to make full answer and defence at a fair trial.

[139] The Court underlines that the Crown is not seeking privilege in connection with an ongoing investigation.

[140] The Crown, in its written reply to the MDI motion,[51] comments on case by case privilege. However, the Crown then supports its argument with quotes from a section entitled "*Le Privilège de la Protection des Témoins*" in an article by Pierre Lapointe, *Les privilèges en droit criminel du point de vue du poursuivant,*[52] in which the author deals with informer class privilege. The policy and basis of the two classes of privilege are

[49] *Michaud v. Québec*, [1996] 3 S.C.R. 3, par. 51.
[50] *R. v. Mentuck,* [2001] 3 S.C.R. 442, par. 51.
[51] Crown's Reply to Motions Concerning MDI Technique (R-32 & R-32a), par. 27.
[52] Published in *Développements récents en droit criminel 2008*, Barreau du Québec, vol. 298, Cowansville, Éditions Yvon Blais, 2008, p. 97.

fundamentally different. The extent of the trial judge's power is not the same with respect to the two classes. Furthermore, the Crown states in its written reply that police investigative techniques have "*consistently, across jurisdictions, been protected by the Courts*".[53] This is not accurate.

[141] Investigative techniques privilege has been rejected in certain cases and accordingly, the investigative technique was disclosed.

[142] In *R. v. Toronto Star Newspapers Ltd*., (2005), 204 C.C.C. (3d) 397 (Ont. S.C.), the Crown invoked investigative technique privilege. Nordheimer J. rejected the argument (par. 15-16):

> In this case, the Crown has adopted an interpretation of investigative technique that is both remarkably broad in its scope and extremely vague in its boundaries. ...
>
> I do not accept that revealing that forensic accountants have been retained by the Crown or the RCMP to assist in a case of alleged commercial fraud would come as a surprise to anyone nor do I see how its revelation would render that investigative technique ineffective in the future. I also fail to see how the revelation of the analyses done by those accountants could impair this or future investigations. There is nothing to suggest that BDO Dunwoody is using some novel or unique form of forensic accounting that has not, until now, been applied to such an investigation. …

see also *R. v. Provenzano*, [2003] O.J. No. 474 (S.C.); *R. v. Lam*, 2000 BCCA 545, par. 41-44; *R. v. Desjardins* (1990), 61 C.CC. (3d) 376 (Nfld S.C.) and *R. v. Rizzuto*, [1991] N.J. No. 14 (Nfld S.C.).[54]

[143] In other cases, for example, the privilege was upheld with respect to the location of secondary serial or VIN numbers in automobiles or motorcycles, as the evidence of the secondary VIN number would not affect the ability of the accused to make full answer and defence. This is a far different situation than that in which information would

---

[53] Crown's Reply to Motions Concerning MDI Technique (R-32 & R-32a), par. 27.

[54] Although in another context, see also *Montréal (Ville de) v. Perreault***,** 2013 QCCS 1667, par. 54, with respect to the public accessibility of safety mechanisms on police holsters.

allow the defence to challenge the existence and accuracy of the Pin to Pin messages and the identity of the communicators. These messages go to the core of allegations of guilt.

[144] The following excerpts from these VIN cases are noteworthy:

In *Hernandez v. R.*, [2004] J.Q. 11285 (C.A.), par. 75-76, the Quebec Court of Appeal[55] reasoned:

> Il importe de bien saisir la portée de cette opération manufacturière; elle permet d'établir la véritable identité du véhicule et de le relier à son propriétaire légitime. En soi, ces numéros de série secondaires ne font pas la preuve que le véhicule fut volé et encore moins, le cas échéant, par qui le vol fut commis.
>
> …en soi, le numéro et son emplacement ne permettent pas d'établir la culpabilité de l'accusé.

Similar comments were made by Goodfellow J. in *R. v. Boomer* (2000), 182 N.S.R. (2d) 49 (N.S.S.C.), par. 59:

> It should be noted that the primary purpose of the secondary VIN numbers is not to prove that the motor vehicle was stolen or that it was stolen by the accused or that it is a stolen vehicle in the possession of the accused. The primary purpose is to determine the true registered owner and in so doing, this does not inhibit an accused from asserting the Crown's onus of proof beyond a reasonable doubt and maintaining the establishment of the true registered owner does not establish a lack of colour, right or interest of the accused's consent, etcetera, in the possession of the motor vehicle, nor does it establish the motor vehicle itself has been stolen, ectetera.
>
> [underlining added]

Finally in *R. v. Smith*, 2009 ABPC 88, (par. 19, 20), Rosborough J. stated:

> In the context of the system of secondary VIN identification, the balancing function must take into account the limited effect of that evidence on the accused's ability to make full answer and defence. In essence, secondary VIN identification systems operate to establish the true identity of a motor vehicle. They do not prove that the vehicle was stolen. They do not prove that the accused knew it was stolen. They do not prove that the accused had possession of the motor vehicle. And they do not prove that the accused took, obtained, removed or concealed anything or otherwise undertook any dealings with the motor vehicle for a fraudulent purpose or with the intent to defraud a person. The impact of this evidence on the accused's ability to make full answer and defence is significantly limited.
>
> The impact of secondary VIN evidence on the right to make full answer and defence is also more limited than evidence surrounding other confidential police investigative techniques.

---

[55] See also *Bégin v. R.*, 2005 QCCA 213, par.15-18.

> Surveillance or observation posts may operate to identify the accused as the perpetrator of a crime. They may provide proof of commission of the crime itself. It is for this reason that observation post privilege is qualified so as to permit questioning about, for example, the observer's distance from the object of his observation or the presence of obstructions to visibility. See: *Ripe for Resolution: A Critique of the Surveillance Post Privilege, op cit*.
>
> [underlining added]

[145] These excerpts distinguish the application of investigative techniques privilege in those cases from the present matter in which the requested privilege would shield information which is the foundation of the prosecution.

[146] The effect on full answer and defence in the VIN cases is far different from the present case where the Crown's position would block the defence from mounting any effective challenge to the existence and accuracy of the Pin to Pin messages and the identity of the communicators. Without this evidence, the Crown has publicly stated that it has no case and the accused (except possibly Simpson, although the Crown's position is unclear) will be acquitted. These messages therefore, are the essence of this case. If they are inaccurate or unreliable as a result of the decryption process, or if the identification via MDI of the senders and recipients of messages is unreliable, the outcome of the trial is affected. These are compelling circumstances.

[147] The Crown asserts that their investigative techniques identified the accused using specific cell phones at specific times. However, the Crown claims privilege over interception travel paths, decryption of intercepted messages, the type of MDI device and its capacities.[56] These techniques, particularly the global key and the MDI, may contain exculpatory information yet the Crown refuses to disclose this information on the basis of privilege.

---

[56] Mirarchi's Factum (R-32), par. 42.

[148] Defence counsel should not be compelled, at this stage, to demonstrate the specific use to which they might put information which they have not even seen.[57] Defence counsel have not seen or heard evidence put forward at the *ex parte* hearings.

[149] The Crown focuses on the public interest, being "*the protection of the capacity of the state to investigate and fight criminality*".[58] The prevailing preoccupation of the police is that those individuals in the criminal milieu will become aware of police investigative methods and will then be able to develop methods to expose and circumvent law enforcement's ability to intercept, thereby avoiding detection and endangering the community.[59]

[150] However, when a police technique is a central feature behind evidence obtained against the accused, the public interest does not weigh the balance in favour of a privilege overriding the accused's right to make full answer and defence and their entitlement to disclosure of all relevant information. [60]

[151] Moreover, the foundation for invoking investigative privilege is undermined once the police method or technique is publicly known. While the deployment of a publicly known technique may be sensitive, the actual technique itself is not.

[152] Many police techniques, some with a statutory basis, are so well known that a claim of privilege would not stick. For example, investigative techniques such as wiretap, various bugs, radar, videos, and breathalyzers, undercover officers and informers, police infiltration, surveillance, covert entries, and Mr. Big operations have

---

57 *R. v .Durette*, [1994] 1 S.C.R. 469, p. 499.
58 Crown's Reply and Annexes, R-25c)i),Tab 1, par. 2.
59 *Ex parte* testimony of Mark Flynn, June 30, 2015, pp. 2-3.
60 With respect to security certificates under the scheme in the *Immigration and Refugee Protection Act*, see *Canada (Citizenship and Immigration) v. Harkat*, [2014] 2 SCR 33, par. 56; *Charkaoui v. Canada,* [2007] 1 S.C.R. 350, par. 19-20; *Charkaoui v. Canada,* [2008] 2 S.C.R. 326, par. 50.

been in the public domain for many years and involve inherent risk and danger to the police. Scientific analyses such as DNA and fingerprint comparison have also been in the public domain for many years. Accused individuals have been challenging the collection of evidence obtained via these public techniques on an ongoing basis. Notwithstanding this public knowledge, crimes have been detected as a result of these techniques for decades. The use of a particular technique may be confidential, but it is not necessarily privileged. Besides, police investigative techniques in crime detection, and actions taken by those individuals attempting to avoid crime detection, evolve alongside changes in technology. What is unknown or novel today is not as time marches on. The Court points out that this investigation took place four years ago.

[153] At the outset of these proceedings, the RCMP and the Crown asserted that all of the information over which privilege was claimed was not publicly known. As proceedings on the motion progressed and police witnesses were challenged on cross-examination, the RCMP and the Crown now acknowledge that much of the information is largely public but that its utilization by the RCMP is not known.[61]

[154] Upon review of the applicable jurisprudential and doctrinal principles referred to above, as regards this common law privilege claim, the Court balances the following factors:

1. the sensitivity of the investigative technique and the impact disclosure would have on the present case and on future investigations;
2. the length of time that has passed since the investigative technique was utilized;
3. the circumstances in which, and the extent to which the investigative technique has been made public; whether the technique is truly public or whether the accused learned of it through improper means;

---

[61] Factum of the *amicus curiae*, September 8, 2015, par. 29; EP-32.28.

4. the good faith or bad faith of law enforcement and/or the Crown in invoking the privilege; whether the privilege claim is motivated by something other than a genuine concern for the secrecy of the information;

5. the nature of the criminal charge weighing against the accused;

6. the effect of disclosure or non-disclosure on the public perception of the administration of justice;

7. whether the information sought is relevant to an issue in the proceedings to the extent that it may possibly affect the outcome of the trial;

8. if relevant, whether the public interest in effective police investigation and the protection of those involved in such investigations, outweigh the interests (public and individual) in protecting the legitimate right of the accused to receive disclosure of information with respect to the investigative police techniques, in the exercise of the accused's right to make full answer and defence;

9. in considering relevancy,

   (i) the proximity and connection of the information to triable issues;
   (ii) whether there is other evidence of guilt unrelated to the information;
   (iii) whether the information is the source of the sole evidence incriminating the accused.[62]

[155] In deciding whether to disclose information under s. 37 of the *Canada Evidence Act*, s. 37(5) requires the Court to balance whether the public interest in disclosure outweighs in importance the specified public interest that would be encroached upon. The Court is of the view that the factors referred to with respect to a common law privilege claim would apply equally under s. 37.[63]

---

[62] *R. v. Meuckon*, [1990] B.C.J. No. 1552 (C.A.), par. 25-27; *R. v. Richards*, (1997), 100 O.A.C. 215, par.11; *R. v. Trang*, 2002 ABQB 19, par. 55; *Attorney General of Canada v. Commission of Inquiry into the Actions of Canadian Officials in relation to Maher Arar and Maher Arar, 2007 FC 766,* par. 55 (reference to the judgment of Scott J. of the Chancery Division, referred to and upheld by the House of Lords in *Attorney General v. Observer Ltd et al*, [1990] 1 AC 109); Alan W. Bryant, Sidney N. Lederman, Michelle K. Fuerst, *The Law of Evidence in Canada*, 4th ed., Markham, LexisNexis Canada, 2014, par. 15.46; S. Casey Hill, David M. Tanovich & Louis P. Strezos, *McWilliam's Canadian Criminal Evidence*, 5th ed. Toronto, Canada Law Book, 2013, loose-leaf updated 2015, Part III, vol. 1, ch. 13-14.

[63] Crown's Reply and Annexes, R-25c)i),Tab 1, par. 3; Factum of the *amicus curiae*, September 8, 2015, par. 24.

[156] On the brink of trial, and in the event of a rejection of a claim of investigative privilege, the Crown has alternatives, such as: conducting the trial and disclosing the information over which privilege is sought; continuing without the information in question; or protecting the information in question by measures such as publication bans and/or *in camera* hearings, or finally, by staying proceedings.[64] Inspector Flynn referred to a case where the RCMP preferred to protect police techniques rather than continue with the prosecution.[65]

[157] In the special context of s. 38 of the *Canada Evidence Act*, the Court refers to the following remarks of the Supreme Court in *R. v. Ahmad*, [2011] S.C.R. 110, par. 2, 78:

> We acknowledge at the outset that in some situations, the prosecution's refusal to disclose relevant (if sensitive or potentially injurious) information in the course of a criminal trial may on the facts of a particular case prejudice the constitutional right of every accused to "a fair and public hearing" and the separately guaranteed right "to be tried within a reasonable time" (*Charter* , ss. 11 (*d*) and (*b*), respectively). Where the conflict is irreconcilable, an unfair trial cannot be tolerated. Under the rule of law, the right of an accused person to make full answer and defence may not be compromised. …
>
> …
>
> As we have stated, co-operative arrangements between the prosecution and the defence are to be encouraged, as they have the potential to greatly facilitate complex trials for all parties involved and to reduce the strain on judicial resources. However, the defence is under no obligation to cooperate with the prosecution and if the end result of non-disclosure by the Crown is that a fair trial cannot be had, then Parliament has determined that in the circumstances a stay of proceedings is the lesser evil compared with the disclosure of sensitive or potentially injurious information.

[64] *R. v. Parmar,* [1987] O.J. No. 567 (S.C.), par. 47-49, aff'd by [1989] O.J. No. 2314 (C.A.).
[65] *Ex parte* testimony of Mark Flynn, July 2, 2015, pp. 49-50.

THE RCMP'S INTERCEPTION OF MESSAGES (R-25) (manner and capabilities)

1. Location on the travel path of the RCMP's intercept solution, which includes the actions that are necessary to expose the communications to the RCMP equipment to facilitate the intercept

[158] The Crown has filed, on public record, material in its Reply and Annexes including a report from Inspector Flynn[66] regarding the RCMP BlackBerry intercept System used to intercept Pin to Pin and BBM communications in *Projet Clemenza*; as well as an expert report from Sergeant Patrick Boismenu[67] regarding the accuracy of messages intercepted.

[159] With respect to the location on the travel path of the RCMP's interceptions, a review of the evidence at the *ex parte* hearings demonstrates that interceptions took place [redacted][70] In an excerpt of his testimony that was not redacted, Inspector Flynn said that "*information is then forwarded to our Ottawa office where it is decoded and rendered intelligible*".[71]

[160] Inspector Flynn testified that *"to intercept the communications as they travel a normal path, is very sensitive to us because if somebody knows where that equipment is deployed, they would, in this Internet enabled world, be able to develop solutions to circumvent some of those*".[72] He later responded:

> THE COURT: Q You're not talking about geographical location, you're talking about the systems that are being used regardless of where the RCMP has their equipment.
>
> Inspector Mark FLYNN: That is correct. Sometimes there is geographical consideration, but it is

66 R-25c)i)a), Tab 2.
67 R-25c)i)b), Tab 6.
68 RCMP report, EP-32.27, pp. 1-2; *ex parte* testimony of Mark Flynn, June 30, 2015, pp. 42-43.
69 RCMP report, EP-32.27, pp. 1-2.
70 RCMP report, EP-32.27, p. 2.
71 *Ex parte* testimony of Mark Flynn, June 30, 2015, p. 43; see also Crown's Reply and Annexes, R-25c)i)a), Tab 2, par. 11-24 (Inspector Flynn's report, which is not redacted).
72 Public testimony of Mark Flynn, November 11, 2014, p. 78.

more the virtual path that is the most significant.[73]

[161] Inspector Flynn further testified that the interception location does not assist in establishing the location of the user of the BlackBerry device, with respect to Pin to Pin and BBM communications, and is not relied upon for that purpose.[74]

[162] Moreover, four years later in 2015, as Me Kapoor states, "*there is no longer an investigative imperative to have the RCMP equipment installed* [redacted][75]

[163] The following exchange at the *ex parte* hearing explains:

Justice Michael STOBER: Q161. Why did you have to go [redacted]

Inspector Mark FLYNN [redacted] We could go anywhere along the communication path, [redacted]

Justice Michael STOBER: Q162. [redacted]

Inspector Mark FLYNN: [redacted]

Justice Michael STOBER: Q163. [redacted]

Inspector Mark FLYNN: That is correct.[76]

…

Justice Michael STOBER: Q166. [redacted]

[73] Public testimony of Mark Flynn, November 11, 2014, p. 87.
[74] *Ex parte* testimony of Mark Flynn, June 30, 2015, pp. 56-57; public testimony of Mark Flynn, November 11, 2014, p. 83; public testimony of Mark Flynn, November 17, 2014, pp. 139, 143-145.
[75] EP-32.29, (written argument of *amicus curiae*, September 14, 2015), p. 7.
[76] *Ex parte* testimony of Mark Flynn, June 30, 2015, pp. 42-43.

Inspector Mark FLYNN: [redacted]

Justice Michael STOBER: Q167. [redacted]

Inspector Mark FLYNN: That's correct.[77]

[164] The RCMP requested RIM's assistance when Pin to Pin messages were intercepted. The Court refers to the Quebec *Authorization to Intercept Private Communications*,[78] as well as RCMP Cst. Jason Morton's affidavit upon an application for a *Confirmation Order and Sealing Order*,[79] with respect to compliance with the assistance portion of the Quebec Authorization, in Ontario. Crown and defense counsel confirm that a confirmation order was issued by the Ontario Superior Court on October 5, 2010. Furthermore, "*comfort letters"* were sent from the RCMP to RIM, pursuant to the authorization, requesting RIM's assistance in taking the appropriate steps and proceeding with configurations to ensure successful interceptions of certain devices.[80]

[165] The fact that RIM or telecommunications service providers allowed RCMP access to equipment to expose target communications to the RCMP BlackBerry intercept and processing system is not privileged and must be disclosed.

[166] Inspector Flynn testified about the impact of a disclosure order [redacted] He also spoke of the negative publicity[81] and the effect on

---

77 *Ex parte* testimony of Mark Flynn, June 30, 2015, p. 43.
78 R-25.14, par. 12, 29-31.
79 R-25.6, par. 12.
80 R-25.3, R-25.4, R-25.5.
81 *Ex parte* testimony of Mark Flynn, November 11, 2014, p. 3, June 30, 2015, pp. 59-60; public testimony of Mark Flynn, November 11, 2014, pp. 81-82.

[redacted] These matters are not pertinent and do not give rise to privilege.

[167] Although the RCMP prefers not to disclose that interception equipment was installed [redacted] and that the intercepted information was forwarded to Ottawa for decrypting, these are not matters that fall under the umbrella of investigative privilege and must be disclosed.

[168] The Court finds that disclosure of these facts would allow the defence to evaluate the scope and impact, if any, of such information. In the Court's view, this would not impair law enforcement's ability to investigate and detect crime, nor would it jeopardize this or future police investigations.

[169] With respect to *police actions that are necessary to expose the communications to the RCMP equipment to facilitate the intercept,* the Court underlines that Crown counsel and the RCMP have agreed to a demonstration in the presence of defence counsel. Counsel advise the Court that this demonstration took place on November 4, 2015. Therefore, the Court is of the view that, at least at the present time, its intervention on this point is not required.

2. A demonstration of the interception software that exposes the user interface and the capabilities of the system, which would show what the RCMP is able and not able to do

[170] As mentioned, Crown and defence counsel have agreed to such a demonstration, thus this question is no longer an issue. Such a demonstration would assist the defence in understanding how the RCMP equipment intercepted the communications.

3. Role, if any, of *Research in Motion* (RIM) in the interception and decoding process

[171] As mentioned, the RCMP requested RIM's assistance when Pin to Pin messages were intercepted. The Court has referred to the judicial authorization to intercept, the application for a confirmation order in Ontario,[82] and *comfort letters.*

[172] However, these letters or judicial authorizations did not require RIM [redacted]

[173] No court order or comfort letters were produced regarding Rogers.

[174] The Court holds that the extent of the participation of RIM and Rogers, or other telecommunications service providers, if any, may be disclosed without jeopardizing this or future police investigations.

[175] A major concern for the RCMP [redacted] is to avoid negative publicity for RIM and to protect its collaborative relationship with RIM on technical issues which contribute to the interception process. It is not a good marketing to work with the police, according to Inspector Flynn.[83] He stated: [redacted][84]

[176] Inspector Flynn further stated:

[redacted]

---

82 Crown and defence counsel confirm that a confirmation order was issued by the Ontario Superior Court on October 5, 2010.

83 Public testimony of Mark Flynn, November 11, 2014, pp. 81-82.

84 *Ex parte* testimony of Mark Flynn, June 30, 2015, p. 34.

85 *Ex parte* testimony of Mark Flynn, November 11, 2014, p. 3.

[177] The Court notes that the only witness heard on this issue was Inspector Flynn; his testimony on this point was self-serving and weak. No witness was called from RIM.

[178] The Court cannot decide the issue of privilege, upon considerations as to whether an adverse impact on RIM's business interests or commercial success will diminish its willingness to cooperate with the RCMP. These concerns must give way to the accused's ability to make full answer and defence.

[179] The Court has concerns with testimony of Inspector Flynn when questioned as regards his view of the various justice system participants and whether they could be trusted with the information sought. This testimony was in relation to a hypothetical situation presented by Me Kapoor, the *amicus curiae,*[86] in which information sought by the defence in R-32 was disclosed, and the part of the proceedings dealing with that information is held *in camera* before jury and a publication ban ordered. Inspector Flynn testified that:

(i) with respect to the Crown, he relied on their professional ethics and good faith;

(ii) he trusted the Court staff;

(iii) he trusted the presiding Judge;

(iv) with respect to the defence lawyers, he did not know their "*histories*" or "*personalities*" and "*would need time to think about it";* even if defence counsel, had security clearance at the highest level, as is the case with the *amicus*, he was still not comfortable;

(v) he did not know the jury, the reputation of the jury, the persons selected;

(vi) he was concerned with dissemination and future use by the accused.[87]

[180] When asked if the choice were to stay the prosecution or to disclose the information, he said that he would need more time to think about that. However, upon

---

[86] See EP-32.29 (written argument of the *amicus curiae*, September 14, 2015), p. 10.

[87] *Ex parte* testimony of Mark Flynn, July 2, 2015, pp. 68-69, 137-141.

further questioning by the *amicus*, he seemed open to considering disclosure at trial with the implementation of certain protections.[88]

[181] Such evidence raises the question, "*who are the decision-makers on the privilege issues - the Crown or the police*"?

[182] In his testimony, Inspector Flynn distinguished SMS text messages from BBM, Pin to Pin and email messages. Both travel through towers but on different pathways. SMS text messages travel on a cellular telephone data connection pathway; telecommunications service providers such as Bell or Rogers manage the connectivity - the pathway of the communication - and the server. BBM, Pin to Pin and email messages travel on an Internet connection pathway; telecommunications service providers, such as Bell or Rogers, manage the connectivity - the pathway of the communication - whereas RIM manages the servers. Wi Fi is another means to send Pin to Pin, BBM or emails.[89] With Pin to Pin and BBM messages sent or received, both devices used during the period of this investigation had to be BlackBerrys.[90]

[183] Pin to Pin and BBM messages travelling through BlackBerry Internet Server (BIS) are encrypted with a global encryption key built into the device. The global key is the same for all BlackBerry devices. It secures communications between these devices. Messages from the sender to a recipient are converted by a BlackBerry encrypting algorithm. The message is then decrypted through this global key in order to be readable and comprehensible. PGP is an additional protective security layer.[91] The

---

88 *Ex parte* testimony of Mark Flynn, July 2, 2015, pp. 140-146.

89 Public testimony of Mark Flynn, November 11, 2014, pp. 43-52,125-133, November 17, 2014, pp. 79, 83-85, 102.

90 *Ex parte* testimony of Mark Flynn, June 30, 2015, p. 45.

91 Crown's Reply and Annexes, R-25c)i)a), Tab 2, par. 5, (Inspector Flynn's report); public testimony of Mark Flynn, November 11, 2014, pp. 50-51, November 17, 2014, pp. 86-87.

Court notes that the Crown initially objected on privilege grounds to a question as to whether PGP protected Pin to Pin communications.[92] However, at a later date, Inspector Flynn, in cross-examination stated that he was not claiming privilege on this point; the Crown did not intervene.[93]

[184] Messages travelling through BlackBerry Enterprise Server (BES) are encrypted by the BES administrator responsible for those users who are participants in the BES; in these cases, a different unique key is utilized.[94] However, it has been explained at the *ex parte* hearing [redacted].[95]

[185] In the present case, the RCMP installed equipment to intercept the accused's messages. MD5 Hash tags are an algorithm that established the continuity of the messages thereby ensuring the integrity of the data as it arrived. [redacted] The RCMP was then able to decrypt digital intercepted messages in order that they be converted into the readable and comprehensible format in which the originator of the message created it. [redacted] The fact that "*[t]he RCMP uses a system to decode and render the intercepted data into human readable communication*" has been disclosed to the defence.[96]

---

92 Public testimony of Mark Flynn, November 17, 2014, pp. 168-169.
93 Public testimony of Mark Flynn, July 16, 2015, pp. 66-67.
94 Crown's Reply and Annexes, R-25c)i)a), Tab 2, par. 6, (Inspector Flynn's report).
95 *Ex parte* testimony of Mark Flynn, November 11, 2014, pp. 25-27.
96 Crown's Reply and Annexes, R-25c)i)a), Tab 2, par. 8, 11-24, 30-31 (Inspector Flynn's report); public testimony of Mark Flynn, November 11, 2014, pp. 57-58, 64-72, 119-121, November 17, 2014, pp. 157-167; see also *ex parte* testimony of Mark Flynn, November 11, 2014, pp. 24-26, June 30, 2015, pp. 33-37; in another context, see Mirarchi's Application Record, Tab 4, Exhibit L - Daehyun Strobel, *IMSI Catcher*, Seminararbeit, Ruhr-Universitat Bochum, July 13, 2007, par. 2.1 & 2.6.

[186] In his public testimony, Inspector Flynn said:

> ...So, would I properly identify which traffic was associated with a particular device, would intercept that traffic, forward it to various communication paths where we then had equipment that would verify the filtering, take that communication, reverse the process that was applied by the device and turn it back into an intelligible product. ...
>
> ...the majority of the components that are involved in intercepting and rendering the communications readable is developed...by the RCMP.
>
> ...We have to reverse the encryption, the encoding and so on, that was applied to the communications when it was first sent by the sender...[97]

[187] Inspector Flynn testified that [redacted] only.[99] Inspector Flynn's testimony with respect to [redacted] as well as on other matters, is vague and not consistent throughout. In and of itself, it is not sufficiently reliable to support a privilege claim.

[188] The fact that BlackBerry devices contain a global cryptographic key is in the public domain.[100] By resorting to the global key, the RCMP was able to decrypt the intercepted messages.

[189] No evidence has been produced at either the *ex parte* or public hearings indicating that [redacted] RIM/BlackBerry's global key.

[190] The process of decrypting messages is of prime importance to the accused.[101] Since the global key unlocks Pin to Pin messages containing crucial evidence against

---

97 Public testimony of Mark Flynn, November 11, 2014, pp. 58, 60, 68.
98 *Ex parte* testimony of Mark Flynn, November 11, 2014, p. 24.
99 *Ex parte* testimony of Mark Flynn, June 30, 2015, pp. 33-36.
100 R-25.9, p. 4 (Government of Canada document on Security of BlackBerry Pin-to-Pin Messaging).
101 R-34.1, p. 3.

the accused that form the basis of first degree murder charges, an argument contesting the relevance and proximity of this information is rejected.

[191] The Court adopts the following comments of the *amicus curiae* in his written argument:

> … Essentially, the Crown will lead PIN to PIN messages before the jury in a translated language, English. The actual PIN to PIN message *was* delivered in a foreign language (code). The RCMP translated those messages to English. The Crown now says that the defence cannot have access to how the translation occurred. Yet, the Crown will lead the messages to the jury without proving their accuracy. By suppressing the global key information, any attempt to determine the efficacy and accuracy of the content of the PIN to PIN messages is frustrated.[102]

[192] On balance, the global key must be disclosed and a privilege claim rejected.

[193] The remaining question is how the RCMP obtained the key [redacted] Inspector Flynn, in his disclosed report on the BlackBerry Intercept System, discusses this RCMP process and compares it to the process of converting the noises heard on a phone line, when a fax is sent, into a printed image on paper.[103]

[194] The Court finds that, on balance, [redacted] are protected by investigative privilege and must not be disclosed. It is the key itself that is relevant and closely

[102] EP-32.29, (written argument of the *amicus curiae*, September 14, 2015), p. 4.

[103] Crown's Reply and Annexes, R-25c)i)a), Tab 2, par. 8, 11-24, 30-31; public testimony of Mark Flynn, November 11, 2014, pp. 47, 60, 68, November 27, 2014, p. 43.

connected to the core issues and hence to full answer and defence, [redacted]

[195] The Court holds that, on balance, the global key - the algorithm and/or formula - which was applied in order to render intelligible, unintelligible data, is not subject to investigative privilege and must be disclosed. Without the key, the accused would not be able to conduct a forensic analysis on their own. They would be required to take a leap of faith that the "*translation*" of the intercepted messages by the RCMP is accurate.

[196] In the same way, imagine the scenario where an ancient hieroglyphic or cuneiform tablet is translated into English or French. Of course, the original version in the ancient language must be disclosed to the defence. How the translators obtained the tool to translate the ancient language is not significant; what is significant is the actual translator's tool, say the *Rosetta Stone* or an equivalent which translated unintelligible messages into English or French. The same reasoning would apply to intercepted Pin to Pin messages - unintelligible in their original form but rendered intelligible with the global key.

[197] It is this tool which must be disclosed.

[198] The defence should have the global key - the algorithm and/or formula - in order to challenge the decryption of the messages obtained and/or to request an analysis by an expert in order to determine if such an analysis is the same or different as that carried out by the police.

THE MOBILE DEVICE IDENTIFIER (R-32)

1. The manufacturer, make, model and software version for the equipment used by the RCMP while employing the MDI technique and confirmation that the device is a cell site simulator

5. If they do exist, the Crown is not willing to provide a copy of any non-disclosure agreement relating to the MDI device

[199] The police obtained a general warrant[104] authorizing use of the MDI. As well, three renewals to a judicial authorization to intercept private communications authorized the use of the MDI.[105]

[200] The Crown is not claiming privilege with respect to the bare fact that the MDI was used in the investigation of this case.

[201] RCMP documents disclosed at the public hearing of this MDI motion expose its use by the RCMP generally and in this investigation.[106]

[202] [redacted].[107]

[203] Defence counsel has filed, in its Application Record, an affidavit of Me Megan Savard,[108] an associate of Me Addario, in which she outlines material on the MDI which

---

104 No. 500-26-062901-107; see the general warrant (for the period December 17, 2010 to February 4, 2011), and the affidavit contained in Mirarchi's Application Record, Tab 2, Annex B, par. 1, Annex C, par. 5.2 and 5.3.

105 No. 500-54-000076-105; in the three renewals (for the periods February 4, 2011 to February 25, 2012) referred to at par. 3 in both R-25 and R-32, the affiant obtained authorizations to similarly use the MDI technique for the same reasons stated in the affidavit for the original general warrant contained in Mirarchi's Application Record, Tab 2, Annex, B, par. 1, Annex C, par. 5.2, 5.3.

106 R-32.3, p. 2; Mirarchi's Application Record, Tab 3.

107 EP-32.25.

108 Mirarchi's Application Record, Tab 4.

is available to the public and includes academic literature and conferences,[109] media reports,[110] transcripts of U.S. litigation,[111] U.S. legislation[112] and Harris marketing material for cell site simulators available on the American Civil Liberties Association website[113] as a result of *a Freedom of Information Act* request.

[204] The MDI simulates a cellular tower in order to capture and identify known and unknown cellular phones in the possession of targeted individuals.[114] The MDI may also capture known and unknown cellular phones in the possession of an untargeted individual. The police separate non-searched information.115 [redacted]

[205] Investigative privilege cannot be invoked to safeguard the commercial interests [redacted], no more than it can be invoked to safeguard the commercial interests of RIM. [redacted]

---

109 Mirarchi's Application Record, Tab 4, Exhibit A - Stephanie K. Pell & Christopher Soghoian, *Your Secret StingRay's No Secret Anymore (*2014), Vol. 28, No. 1 Harvard J.L. & Tech. 1; R-32, Tab 4, Exhibit C - Stephanie K. Pell & Christopher Soghoian *A Lot More Than a Pen Register, and Less Than a Wiretap* (2013), 16 Yale J.L. & Tech. 134; see also, Tab 4, Exhibit L - Daehyun Strobel, *IMSI Catcher*, Seminararbeit, Ruhr-Universitat Bochum, July 13, 2007.

110 Mirarchi's Application Record, Tab 4, Exhibit H - Jennifer Valentino-Devries, The Wall Street Journal, September 22, 2011; Tab 4. Exhibit J - Matthew Braga, The Globe and Mail, September 15, 2014, Exhibit K - Ryan Gallagher and Rajeev Syal, The Guardian, October 30, 2011.

111 Mirarchi's Application Record Tab 4, Exhibit M - Testimony of Tallahassee police officer Christopher Corbitt, (August 23, 2010) in *State of Florida v. James L. Thomas,* case no. 2008-CF- 3350A (Circuit Court, 2nd Judicial Circuit, Leon County, Fla.).

112 Mirarchi's Application Record, Tab 4, Exhibit N.

113 Mirarchi's Application Record, Tab 4, Exhibit P.

114 Mirarchi's Application Record, Tab 2, Annex B, par. 1, Annex C, par. 5.2 and 5.3 (Information to obtain a general warrant); Tab 3, p. 3, par. 4, p. 11, par. 2 (Rapport d'enquête technique-RCMP/GRC).

115 Mirarchi's Application Record, Tab 2, Annex C, par. 5.2, subpar. 99 ((Information to obtain a general warrant), Tab 3, p. 6, par. 19 (Rapport d'enquête technique-RCMP/GRC).

116 EP-32.14, par. 28-31; *ex parte* testimony of Josh Richdale, July 17, 2015, pp. 5-9; *ex parte* testimony of Jocelyn Fortin, July 21, 2015, pp. 12-14, 56-57.

[redacted]

[206] [redacted]

[redacted]

...

[redacted]

[underlining added]

[207] The Court refers to par. 8 of Inspector Flynn's affidavit in which he states:

[redacted]

---

117 *Ex parte* testimony of Mark Flynn, June 30, 2015, pp. 2-17, July 2, 2015, pp.2-3; *ex parte* testimony of Jocelyn Fortin, July 22, 2015, pp. 61-77; factum of the *amicus curiae,* September 8, 2015, pp. 11-12.

118 *Ex parte* testimony of Mark Flynn, November 11, 2014, pp. 17-21.

119 Factum of the *amicus curiae*, September 8, 2015, p. 5.

120 *Ex parte* testimony of Mark Flynn, November 11, 2014, p. 19.

[underlining added]

[208] in cross-examination, Inspector Flynn stated that he was Furthermore, in cross-examination, Inspector Flynn testified that he was [122] He did mention, in cross-examination, :

[underlining added]

[209] Inspector Flynn testified in cross-examination that, [124] He testified that he was assuming without having any personal knowledge to make the affirmations in examination-in-chief or in his affidavit. This exaggerated,

[121] EP-32.9.
[122] *Ex parte* testimony of Mark Flynn, July 2, 2015, pp. 34-35.
[123] *Ex parte* testimony of Mark Flynn, July 2, 2015, p. 36.
[124] *Ex parte* testimony of Mark Flynn, July 2, 2015, pp. 62-63.
[125] *Ex parte* testimony of Mark Flynn, July 2, 2015, pp. 35-41.

contradictory testimony is not convincing. Without the precisions raised in cross-examination by Me Kapoor, the Court would have been left with:

[redacted]

[210] [redacted].[128]

[redacted]

[211] [redacted]

126 EP-32.1; EP-32.2.
127 EP-32.4 to EP-32.7.
128 EP-32.2, p. 3.
129 EP-32.2, p. 3.

[212] Therefore, by signing this document, [redacted] sold to the RCMP could be disclosed in a criminal case as per Supreme Court of Canada judgments and the *Canadian Charter of Rights and Freedoms.*

[213] [redacted].

[redacted]

[underlining added]

[214] The Court underlines [redacted] was informed of section 37 of the *Canada Evidence Act* and agreed to be bound by Canadian law.[131]

[215] Thus police and prosecutorial authorities are certainly attempting to keep this information confidential; however, the laws of Canada must prevail with respect to a Canadian criminal case in which the police have obtained evidence through the use of [redacted].

[216] The Court rejects the Crown's argument claiming that [redacted] If the products were so sensitive that confidentiality and non-disclosure were a *sine qua non,* and in view of police and Crown reference to involvement of the [redacted] then one would expect the higher-ups and the legal departments [redacted] to have envisaged potential disclosure in criminal

130 EP-32.5.
131 *Ex parte* testimony of Mark Flynn, July 2, 2015, pp. 45-47.

cases, especially considering the uses and purposes for which the products [redacted][132]

[217] The Court notes that the only witnesses heard regarding the MDI were police officers; as mentioned [redacted]

[218] Various emails were produced between RCMP representatives, such as Jocelyn Fortin, [redacted] These emails and telephone calls were not protected by enhanced security any more than any ordinary email transmissions or telephone calls. According to Jocelyn Fortin's testimony, high security email or telephone lines were not used.[134]

[219] [redacted][135]

---

132 [redacted]

133 EP-32.3; EP-32.8; EP-32.16 to EP-32.22; EP-32.23; EP-32.24.

134 *Ex parte* testimony of Jocelyn Fortin, July 22, 2015, pp. 74-86, July 23, 2015, pp. 19-31.

135 *Ex parte* testimony of Mark Flynn, July 14, 2015, pp. 25-26.

[220] One would think that, if confidentiality and privilege were of utmost importance as Crown counsel and RCMP witnesses are claiming, special care and strict security measures would have been utilized in order to avoid any breach and disclosure of such sensitive communications. Ironically, the Court points out the secure channels in which *ex parte* exhibits and transcripts have been delivered to the Court, the Crown and the *amicus.*

[221] [redacted] the guarantee of a fair trial or the right to make full answer and defence. In criminal cases in which evidence has been obtained with [redacted] extent to which privilege will apply in Canada.

[222] [redacted] do not trigger investigative techniques privilege.[136]

[223] Accordingly, [redacted] are not privileged. However, they are not subject to disclosure rules laid out in *R. v. Stinchcombe, supra,* pp.335-336, 338-340, 343, as they are not relevant to full answer and defence. In other words, is there a reasonable possibility that this information will be useful to the accused in making full answer and defence? I think not; see also *R. v. Chaplin,* supra, par. 22, 30; *R. v. Dixon*, supra; *R. v. Raza*, [1998] B.C.J. No. 3246 (B.C.S.C.).

[224] In *R. v. Egger*, supra, p. 467, the Supreme Court stated:

> One measure of the relevance of information in the Crown's hands is its usefulness to the

[136] *R. v. Toronto Star Newspapers Ltd.,* [2005] O.J. No. 5533 (S.C.), par. 30.

> defence: if it is of some use, it is relevant and should be disclosed — *Stinchcombe*, *supra*, at p. 345. This requires a determination by the reviewing judge that production of the information can reasonably be used by the accused either in meeting the case for the Crown, advancing a defence or otherwise in making a decision which may affect the conduct of the defence such as, for example, whether to call evidence.

[225] This specific issue therefore is moot. Any questions to witnesses on such topics at trial would have to be relevant.

[226] As mentioned, while the Crown retains the discretion not to disclose irrelevant information, disclosure of relevant evidence is not a matter of prosecutorial discretion but, rather, is a prosecutorial duty; *Krieger v. Law Society of Alberta*, supra, par. 54.

[227] [redacted].[138]

[228] The Crown has disclosed that the police used the MDI; any further disclosure with respect to the specifications and manner of use, it claims, is said to be privileged. Much of this information over which protection is sought is in the public domain,[139] the Crown and the police objecting to disclosure of its use in the police investigation of this case. As Me Kapoor states in his oral argument, that is the equivalent of stating that they used a car without stating it has an engine; or, in the Court's view, if they disclosed the engine, without stating the specifics of the engine.

[229] The evidence obtained through police use of the MDI assists the Crown at trial on the issue of identification. The Crown states that it is not relying upon the MDI in

---

137 *Ex parte* testimony of Mark Flynn, July 2, 2015, p. 2.
138 *Ex parte* testimony of Mark Flynn, June 30, 2015, p. 11.
139 EP-32.28; EP-32.25; Mirarchi's Application Record.

order to make its case before the jury. The Crown argues that the police use of the MDI will not be led before the jury and hence police detection methods, such as the specifics of the MDI, should remain privileged, secret and confidential. The Court rejects this argument.

[230] The Crown intends on presenting to the jury the fruits of this police technique. It is therefore relevant and is captured by *Stinchcombe* rules of disclosure.

[231] Again how could such crucial evidence on questions of identity, and authorship and reception of Pin to Pin messages, not be subject to challenge by the defence. Defense counsel, Me Addario, has demonstrated, during the hearings, how challenging the MDI is significant to the issue of identification and thus to a fair trial and full answer and defence.[140] The defence should have the possibility to mandate an expert in order to analyze and challenge the accuracy of MDI-obtained information and evidence.

[232] Thus, the Court holds that the Crown must disclose the following information, with respect to the MDI used in the police investigation of this case. This information is not protected by investigative privilege: the manufacturer, make, model and software version for the equipment used by the RCMP while employing the MDI technique [redacted]

[redacted]

[140] Public testimony of Josh Richdale, July 23-24, 2015; see also R-32.8; R-32.9.

2. While the RCMP is disclosing the signal strength of the targets' devices, it will not disclose the signal strength of the MDI device

3. How the MDI device affects the targeted mobile devices; ie. did it force the targeted device to use a 2G network connection; did it turn off encryption on the mobile device; did it force the device to increase its broadcast strength

4. A description of the default settings on the MDI device

[233] Much of the information [redacted] and their specifications is in the public domain; as demonstrated in documents filed by the defence,[141] and the Crown.[142]

[234] Inspector Flynn acknowledges the public nature of the MDI in documents filed by the defence.[143] However, he testifies that this information does not include all of the details regarding the deployment of the device.[144] Inspector Flynn does not give details about the public nature of [redacted] Other witnesses do provide such details.

[redacted] Jocelyn Fortin compared [redacted] He recognizes that much of the operation of the MDI is public with the exception of the following [redacted]

[236] Although Mr Fortin asserted that the covert nature of the RCMP use of an MDI would be compromised by disclosure, he acknowledged that the RCMP has no

---

141 Mirarchi's Application Record.
142 R-32.28.
143 Mirarchi's Application Record.
144 *Ex parte* testimony of Mark Flynn, July 14, 2015, pp. 5-20.
145 *Ex parte* testimony of Jocelyn Fortin, July 21, 2015, pp. 58-62, July 22, 2015, p. 27, July 23, 2015, pp. 54-62.

empirical basis for that position and notwithstanding information in the public domain, [redacted] he confirmed that the MDI remains an effective device.[146]

[237] In the circumstances, Mr Fortin's assertion is not a proper basis upon which the defence can be denied information that the Crown is constitutionally obliged to provide.[147]

CERTAIN QUESTIONS WITH RESPECT TO THE MDI

[redacted]

[238] [redacted][148]

[239] Corporal Richdale initially claimed that the [redacted] - was not in the public domain. This explains the redacting of paragraphs related to these techniques in his affidavit. Upon questioning by Me Kapoor, *amicus curiae*, Corporal Richdale in his *ex parte* testimony, was [redacted] Corporal Richdale had not been aware of [redacted] in the public domain. Corporal Richdale then candidly conceded that the redacted paragraphs 7-9, 16-17 in his affidavit,[151] over which privilege was invoked, contain information that is

146 *Ex parte* testimony of Jocelyn Fortin, July 22, 2015, pp.103-105.
147 Factum of the *amicus curiae*, September 8, 2015, p. 7.
148 EP-32.14, par. 28-31; *ex parte* testimony of Jocelyn Fortin, July 21, 2015, pp. 12-14, 56-57.
149 EP-32.13 [2009] EWHC 418 (Pat).
150 EP-32.12; [2012] EWCA Civ 7.
151 EP-32.10.

publicly known.[152] He added that the RCMP did not want people to know that [redacted][153]

[240] Jocelyn Fortin also said [redacted] technique are in the public domain. [redacted][154] However, he feels that privilege attaches because people do not know of certain features of the manner of deployment in this case or that the RCMP uses the device. He wants to ensure that the police cannot be detected.[155]

[241] Me Kapoor indicated that, he easily found [redacted] himself, the previous evening while preparing for the hearing the next day. The Court was surprised that the witness had not been made aware, with prior assistance of RCMP lawyers or researchers, [redacted] The Court was more surprised that a team of eight Crown lawyers were either not aware, or chose not to bring this information forward.

[242] Pursuant to evidence at the hearing and the unredacted paragraphs 12 and 18 of Corporal Richdale's affidavit,[156] Query Mode and Direction Finding Mode are in the public domain. Corporal Richdale acknowledged [redacted].[158] The Court underlines Me Addario's cross-examination of Corporal Richdale, an MDI operator in

152 See Corporal Richdale's PowerPoint, EP-32.11a.
153 EP-32.10; *Ex parte* testimony of Corporal Richdale, July 17, 2015, pp. 42-65.
154 *Ex parte* testimony of Jocelyn Fortin, July 21, 2015, pp. 56-57, July 22, 2015, pp. 99-103.
155 *Ex parte* testimony of Jocelyn Fortin, July 22, pp. 99-103, July 23, 2015, pp. 30-36, pp. 54-61.
156 EP-32.10.
157 *Ex parte* testimony of Josh Richdale, July 17, 2015, pp. 16-17, 47-53.
158 [redacted]

this case. It was demonstrated how a functioning MDI did not capture a BlackBerry cellular phone which was in use at the same time.[159]

[243] Accordingly, [redacted] is not privileged and must be disclosed to the accused. The fact that the MDI [redacted] is not privileged and has been disclosed to the accused.[160]

[redacted]

[244] [redacted] are not privileged and must be disclosed.

[245] On the other hand, [redacted] is not publicly known and disclosure, according to Mr Fortin, would facilitate detection of the MDI.[162] Such information, although ordinarily subject to disclosure, does not sufficiently affect full answer and defence or the outcome of the trial, and is privileged. In practical terms, knowing this fact would not have any impact because the MDI operator could [redacted]; it is not, as Me Kapoor says, "*baked* " into the MDI device.

159 Public testimony of Josh Richdale, July 23-24, 2015; see also R-32.8; R-32.9.
160 R-32.28.
161 Factum of the *amicus curiae,* September 14, 2015, p. 12; *ex parte* testimony of Jocelyn Fortin, July 21, 2015, pp. 51-55; EP-32.14, par. 22-27.
162 *Ex parte* testimony of Jocelyn Fortin, July 21, 2015, pp. 51-56, July 22, 2015, pp. 24-27, 43-44.

(iii) Range

[246] Police witnesses have explained how certain factors such as environmental conditions, buildings, and tunnels, may interfere with reception in the utilization of the MDI. Range was also outlined but in general terms both in testimonies and in the RCMP report (maximum of 2 km in a rural setting; an average of 500 m in a city).[163] Corporal Richdale testified [redacted][164]

[247] The Crown has raised how disclosing range specifics affects the security of police MDI operators in the field. Other than vague generalities, evidence does not support this concern.[165] Police work is known to have inherent risks. Police undercover and infiltration methods are dangerous but they are utilized nonetheless.

[248] It would be entirely unfair for the accused to be unable to know the range of the MDI in more specific detail in order to challenge the capturing of cellular phones and the resulting identification of such devices which, in turn, led to intercepted Pin to Pin messages which are the foundation of these first degree murder and conspiracy charges.

[249] Consequently, the range of the MDI is subject to disclosure and on balance, investigative techniques privilege is rejected.

[redacted]

[250] [redacted]

[163] EP-32.27, p. 4; e*x parte* testimony of Mark Flynn, July 2, 2015, pp. 3-12.
[164] *Ex parte* testimony of Josh Richdale, July 17, 2015, pp. 15-17, July 20, 2015, pp. 11-12; EP-32.28.
[165] *Ex parte* testimony of Jocelyn Fortin, July 22, 2015, p. 6.

[251] [redacted].[166]

[252] [redacted][168]

[253] [redacted].[169]

[254] [redacted] provides an additional explanation for the non capture, by the MDI, of accused's cellular phones. Whilst the Crown wants to protect a technique that benefits police investigations, such information is subject to disclosure rules. Although there is a cogent argument for investigative techniques privilege, the technique and its frailties go to the heart of full answer and defence; it is relevant and closely linked to

---

166 *Ex parte* testimony of Jocelyn Fortin, July 21, 2015, p. 17.

167 *Ex parte* testimony of Jocelyn Fortin, July 21, 2015, pp. 10-11, 14-15, 27-31, July 22, 2015, pp. 27-28.

168 [redacted]

169 This is the fourth undisclosed reason in R-32.8, p.12; R-32.9, p. 16; and in Mirarchi's Supplementary Factum, par. 13; *ex parte* testimony of Corporal Richdale, July 20, 2015, pp. 7-12.

issues in this case. Furthermore, [redacted] disclosure of [redacted] technique would allow the Crown to answer defence arguments that the MDI did not identify the accused's cellular phone because the phone was not at the location in question.[170]

[255] [redacted] on January 16, 2012. [redacted][171] Therefore, since that date, this issue may be hypothetical.

[redacted]

[256] [redacted][172].

[170] Factum of the *amicus curiae*, September, 14, 2015, p. 14.
[171] *Ex parte* testimony of Corporal Richdale, July 20, 2015, pp. 9-11.
[172] EP-32.14, p. 3; *ex parte* testimony of Jocelyn Fortin, July 21, 2015, pp. 20-27, 33-34, July 22, 2015, pp. 33-37, 41.

[257] Such information would ordinarily be subject to disclosure. The Court finds that that, on balance, [redacted] cellular phones is not material, at the present time, in a way that would affect the right to full answer and defence or the outcome of the trial. Therefore, [redacted] should be protected by investigative techniques privilege and must not be disclosed.

[redacted]

[258] [redacted][173].

[259] [redacted].

[260] [redacted].

[173] EP-32.14, par. 31-34; *ex parte* testimony of Jocelyn Fortin July 21, pp. 56-62, July 22, 2015, p. 27.

[261] [redacted][175]

[262] After balancing, [redacted] - does not sufficiently affect the ability to make full answer and defence or the outcome of the trial. Accordingly, it is protected by investigative techniques privilege.

(vii) MDI detection devices

[263] Testimony and affidavits explain that the [redacted] Furthermore, such devices are in the public domain as confirmed by Jocelyn Fortin. Mr Fortin searched these devices on the Internet and elsewhere.[176]

[264] Information relating to these devices must therefore be disclosed.

[265] There is no valid reason to attach investigative techniques privilege to [redacted]

CONCLUSIONS

[266] The Crown claims that police investigative techniques utilized in this case are subject to a qualified privilege applied on a case by case basis.

[267] For the Crown to suggest that the accused are conducting a "*fishing expedition*"[177] as they do not need the material that the Crown seeks to protect with the cloak of investigative techniques privilege, or that it is not relevant, would suggest

174 *Ex parte* testimony of Jocelyn Fortin, July 21, 2015, pp. 57-61.
175 *Ex parte* testimony of Corporal Richdale, July 20, 2015, p. 12.
176 *Ex parte* testimony of Jocelyn Fortin, July 21, 2015, pp. 31-34, July 22, 2015, pp. 14-23; EP-32.14, par. 36-51.
177 Crown's Reply and Annexes, p. 7, par. 21, p. 8, par. 29.

gutting the flesh and bones of a fair defence. The Court has no difficulty rejecting this position.

[268] Trial judges are under a duty to protect the accused's constitutional right to a full and fair defence.[178]

[269] The Court finds that the investigative techniques in question are the principal, if not the only source of the sole evidence proving the guilt of the accused. Without the evidence which is derived from these techniques, the Crown has conceded it has no case (except perhaps regarding Simpson, although the Crown's position has varied and seems uncertain).

[270] The Court concludes that the accused have a legitimate interest in receiving disclosure of information that goes to the heart of this prosecution and may affect the outcome of this case.

[271] Such information may affect defence strategy, for example, the extent of cross-examinations and whether to tender evidence.

[272] Having regard to all the circumstances, the Court concludes, subject to what follows, that the interests of the accused in having a fair trial where they are able to make full answer and defence, outweigh the public interest in protecting police investigative techniques.

[273] To decide otherwise and allow the interest asserted by the Crown and the police to override the accused's right to make full answer and defence would impact negatively on the administration of justice and how the public perceives it.

---

[178] *R. v. Ahmad,* supra, par. 34.

[274] With respect to the location on the travel path of the RCMP's interceptions, the Court has stated that the information does not fall under the umbrella of privilege and would not impair law enforcement's ability to investigate and detect crime. Although the RCMP prefers not to disclose that interception equipment was installed at locations referred to [redacted] and that the intercepted information was forwarded to Ottawa for decrypting, the Court holds that this information must be disclosed.

[275] The Court concludes that the extent of the participation of RIM and Rogers, or other telecommunications service providers, if any, is not subject to privilege and must be disclosed.

[276] The fact that RIM or telecommunications service providers allowed RCMP access to equipment to expose target communications to the RCMP BlackBerry intercept and processing system is not privileged and must be disclosed.

[277] In view of a police demonstration referred to above (par. 169-170 of this judgment), the Court will not rule, at least at the present time, with respect to *actions that are necessary to expose the communications to the RCMP equipment to facilitate the intercept.*

[278] The Court has found that *Research in Motion* (RIM) [redacted] it is not privileged and must be disclosed.

[279] The Court concludes that the RCMP [redacted]

, is subject to investigative techniques privilege and must not be disclosed.

[280] However, the global key itself - the algorithm and/or formula is not protected by investigative techniques privilege and must be disclosed.

[281] With the exception of , the Court concludes that the information sought by the defence concerning the mobile device identifier (MDI) is not subject to investigative techniques privilege and must be disclosed.

[282] Being mindful of the rights of the accused to make full answer and defence, the Court concludes that the public interest asserted by the Crown weighs in favour of applying the investigative techniques privilege in order to protect information with respect to

[283] In order for the accused to make full answer and defence, if convincing evidence arises, for example, through a defence expert with respect to areas in which the Court has maintained investigative techniques privilege, counsel may seek leave of the Court to revisit these specific issues at that time, as the trial unfolds.

[284] The Court holds that, with respect to non-disclosure clauses the balance weighs in favour of rejecting privilege. However, it has not been shown how have the relevance required, that they are meaningful to the accused in making full answer and defence. If

not relevant, the Crown is not compelled to disclose this information pursuant to the rules laid out in *R. v. Stinchcombe,* supra.

[285] Even if the Court were to consider as privileged that information which it holds in this judgment is not privileged, the Court would still conclude that disclosure is required as the accused's right to make full answer and defence and to establish innocence by raising reasonable doubt remain paramount. An unfair trial is not an option.[179]

[286] In order to avoid any uncertainty, the Court will order that the RCMP disclose to the accused any research which the RCMP claims has already been disclosed.[180]

[287] In view of the Court's conclusions, counsel may jointly agree or make separate submissions as to whether evidence or information, upon which the investigative techniques privilege has not been upheld, will be presented or raised at trial *in camera* or in public (s. 486 *Cr. C.*), whether counsel should be required to make undertakings with respect to the disclosed information in question and/or whether non-publication bans or other measures should be ordered.

[179] *R. v. Ahmad*, supra, par. 68, 65; *R. v. Stinchcombe*, supra, p. 340; *R. v. Meuckon*, supra, par. 26.
[180] EP-32.27, p. 4.

FOR THESE REASONS, THE COURT:

[288] **GRANTS** the motions, in part;

[289] **DECLARES** that the following information sought by the accused in motion R-25, with respect to the periods in which these investigative techniques were deployed, is not protected by investigative techniques privilege pursuant to common law:

(i) the location on the travel path of the RCMP's intercept solution;

(ii) the role, if any, of *Research in Motion* (RIM) in the interception and decoding process;

(iii) the global key [redacted];

save and except: [redacted]; investigative techniques privilege applies to information relating thereto.

[290] **ORDERS** the disclosure, by the Crown, of the following information sought by the accused in motion R-25, with respect to the periods in which these investigative techniques were deployed:

(i) the location on the travel path of the RCMP's intercept solution;

(ii) the role, if any, of *Research in Motion* (RIM) in the interception and decoding process;

(iii) the global key [redacted];

save and except: [redacted] investigative techniques privilege applies to information relating thereto.

[291] **DECLARES** that the following information sought by the accused in motion R-32, regarding the mobile device identifier (MDI), with respect to the periods in which this

investigative technique was deployed, is not protected by investigative techniques privilege pursuant to common law:

(i) the manufacturer, make, model and software version for the equipment used by the RCMP while employing the MDI technique and confirmation that the device is a cell site simulator;

(ii) the signal strength of the MDI device;

(iii) how the MDI device affected targeted mobile devices;

(iv) a description of the default settings on the MDI device;

(v) the results of research conducted by the RCMP on the effect of the MDI on the ability of devices within its coverage area to make and receive calls or SMS messages;

save and except: [redacted] investigative techniques privilege applies to information relating thereto.

[292] **ORDERS** the disclosure, by the Crown, of the following information sought by the accused in motion R-32 regarding the mobile device identifier (MDI), with respect to the periods in which this investigative technique was deployed:

(i) the manufacturer, make, model and software version for the equipment used by the RCMP while employing the MDI technique and confirmation that the device is a cell site simulator;

(ii) the signal strength of the MDI device;

(iii) how the MDI device affects targeted mobile devices;

(iv) a description of the default settings on the MDI device;

save and except: [redacted] investigative techniques privilege applies to information relating thereto.

[293] **ORDERS** the disclosure, by the Crown, of the following research referred to in the RCMP report:[181]

a. the MDI may impact the ability of a cellular phone operating within its range to dial 911;

b. the MDI may impact the ability of cellular phones to make and receive calls while the MDI is operating;

c. the MDI does not impact any ongoing calls;

d. the practical range of the device.

_____

MICHAEL STOBER, J.S.C.

[181] EP-32.27, p. 4.

Me Robert Rouleau
Me Alexis Gauthier
Me Julie-Maude Greffe
Me Marie-Christine Godbout
Me Geneviève Rondeau-Marchand
Me Frédérique Le Colletter
Crown Counsel

Me Anil Kapoor
Amicus Curiae

Me Frank Addario
Me Michael W. Lacy
Me William Thompson
Me Maxime Hébrard
Counsel for Vittorio Mirarchi

Me Dominique Shoofey
Counsel for Calogero Milioto

Me Giuseppe Battista, Ad.E.
Me Mathieu Corbo
Counsel for Steven Fracas

Me Ronnie MacDonald
Counsel for Jack Simpson

Me Robert Polnicky
Counsel for Pietro Magistrale

Me Annie Émond
Me Jacques Larochelle
Counsel for Steven D'Addario

Me Marc Labelle
Me Kim Hogan
Counsel for Raynald Desjardins

Me Jeffrey K. Boro
Me Bruce Engel
Counsel for Felice Racaniello

Dates of hearing: November 11, 13, 17 et 27, December 1, 2 et 8, 2014, June 30, July 2, 14, 16, 17, 20, 21, 22, 23, 24, September 8, 9, 11, 14, 17, 18 et 28, November 18, 2015.
Transcribed and revised: December 8, 2015