

Court of Queen's Bench of Alberta

Citation: R v Amer, 2017 ABQB 651



**Docket: 160544938Q1, 160530259Q1,
15033636Q1, 16074258TQ1
Registry: Calgary**

Between:

160544938Q1

Her Majesty the Queen

Crown

- and -

**Talal Amer, Abdul Rahman Ali Amer, Bader Eddin Amer, Barakat Amer and Tarek
Abdul El-Rafie**

Defendants

And Between:

160530259Q1

Her Majesty the Queen

Crown

- and -

Bader Eddin Amer and Tarek Abdul El-Rafie

Defendants

And Between:

15033636Q1

Her Majesty the Queen

Crown

- and -

Said Raek Abdulbaki and Bader Eddin Amer

Defendants

And Between:

160742581Q1

Her Majesty the Queen

Crown

- and -

Ahed Alwan

Defendant

Restriction on Publication

SEALED – See *Canada Evidence Act*, section 37.

By Court Order in paragraph 64 of this judgment, this judgment is sealed and must not be published or distributed in any way except as directed by this court, and is not to be made available from the court file.

Further, by Court Order, the court file materials referenced in paragraph 65 are also sealed and must not be published or distributed in any way except as directed by this court, and are not to be made available from the court file.

By Court Order in paragraph 67, this judgment AS REDACTED is unsealed, and may be published and distributed. In addition, the transcript of the July 12 and 13, 2017 hearing and the Affidavit of Sgt. Campbell affirmed July 6, 2017, AS REDACTED, are unsealed and may be published and distributed.

**Decision of the
Honourable Mr. Justice G.H. Poelman
Regarding Crown Assertion of Public Interest Privilege**

Table of Contents

I. Introduction.....	4
II. Issues.....	6
III. Evidence.....	6
IV. Legal Principles	11
A. Introduction.....	11
B. Burden of Proof.....	11
C. Investigative Privilege	11
D. “Would Encroach Upon”	12

V. Findings.....	12
A. Introduction.....	12
B. Public Knowledge.....	13
C. Disclosure May Assist Offenders	15
D. Would Encroach Upon Privilege	15
VI. Conclusion	16

I. Introduction

[1] Two of the accused in these case-managed proceedings, Mr. El-Rafie and Mr. Barakat Amer, applied for an order directing, among other things, “disclosure of certain enumerated items relating to the development of any Mobile Device Identifiers (“MDI,” also known as Cell Site Simulator, IMSI catcher, “Stingray,” etc.) as part of Operation Hybrid.” The Crown responded by seeking summary dismissal of the application, arguing that there was no basis upon which the relief could be granted, and that the Defence should not be permitted to call any evidence in support of its motion.

[2] I denied the Crown’s application for summary dismissal on May 26, 2017. I expressed reservations about what the requested information could show, because the apparent theory for which the Defence wanted it might prove highly speculative. Nevertheless, I declined to summarily dismiss the disclosure application with the Defence having no right to put forward evidence in support. The main part of my oral ruling was as follows:

The defence argues that it needs more technical information to make that determination. In any event, the proposed *viva voce* evidence may answer the question in a way that helps determine how speculative the concern about accuracy of negative results might be. The Crown has not convinced me that this inquiry is clearly irrelevant on its face, such that the defence should not be permitted to call any evidence.

I will allow evidence, but only going to the narrow issue of what a negative result might mean in the context of the incidents identified in Sergeant Campbell’s will-state. That will, of course, involve describing exactly what unit was used, what features were activated, and the circumstances in the area that might have affected results.

[3] Following my ruling, on May 28, 2017 the Crown objected to disclosure of the information by certificate under section 37 of the *Canada Evidence Act*, R.S.C. 1985, c. C-5, where it stated that “the disclosure . . . should not be made in the proceedings in which disclosure is sought on the grounds of a specified public interest, namely: police investigative technique privilege.”

[4] The Crown’s certification invoked the procedure set out in section 37. The relevant parts of that section are as follows:

37(1) . . . [A] Minister of the Crown in right of Canada or other official may object to the disclosure of information before a court, person or body with jurisdiction to compel the production of information by certifying orally or in writing to the court, person or body that the information should not be disclosed on the grounds of a specified public interest.

...

(2) If an objection to the disclosure of information is made before a superior court, that court may determine the objection.

...

(4.1) Unless the court having jurisdiction to hear the application concludes that the disclosure of the information to which the objection was made under subsection (1) would encroach upon a specified public interest, the court may authorize by order the disclosure of the information.

(5) If the court having jurisdiction to hear the application concludes that the disclosure of the information to which the objection was made under subsection (1) would encroach upon a specified public interest, but that the public interest in disclosure outweighs in importance the specified public interest, the court may, by order, after considering both the public interest in disclosure and the form of and conditions to disclosure that are most likely to limit any encroachment upon the specified public interest resulting from disclosure, authorize the disclosure, subject to any conditions that the court considers appropriate, of all of the information, a part or summary of the information, or a written admission of facts relating to the information.

(6) If the court does not authorize disclosure under subsection (4.1) or (5), the court shall, by order, prohibit disclosure of the information.

(6.1) The court may receive into evidence anything that, in the opinion of the court, is reliable and appropriate, even if it would not otherwise be admissible under Canadian law, and may base its decision on that evidence.

[5] An accused (or his or her counsel) may not attend a section 37 hearing; it is a discrete proceeding separate from the accused's trial: *R v Basi*, 2009 SCC 52, 248 C.C.C. (3d) 257 at para 50. However, a trial judge should adopt reasonable measures to permit defence counsel to make meaningful submissions regarding what occurs in their absence, including submissions on scope of privilege and suggestions of questions to put to witnesses who may be called. In addition, an *amicus curiae* may be appointed: at paras 55-57.

[6] I received briefs of law and books of authorities from counsel from both Mr. El-Rafie and Mr. Amer. They were invited to submit questions, but did not do so. However, at their request I appointed an *amicus curiae* to assist in the hearing. Further, again at Defence counsel's request, I appointed lawyer Anil K. Kapoor for that role. He has extensive experience in both the section 37 procedure and its use in regard to MDI devices. The Crown consented to the appointment of an *amicus curiae* and to Mr. Kapoor being designated to fill that role.

II. Issues

[7] The Crown's section 37 certificate objected to disclosure of:

- a) The make and model of a device deployed by members of the Calgary Police Service ("CPS") in the investigation of these matters and commonly referred to as an MDI or PTDR (certificate at para 2(a));
- b) A description of the features of the aforesaid device (certificate at para 2(b)); and
- c) A description of the circumstances that may cause the MDI/PTDR deployed to fail to identify a mobile device (certificate at para 2(c)).

[8] During the hearing, the Crown advised that it abandoned some of its objections to disclosure. However, it maintained its objection to disclosure of the make and model of CPS's device, and a description of the features by which unique cellphone identifier numbers were detected

[9] As a result of the Crown's position at the hearing, the objection made with respect to paragraph 2(a) of the certificate is maintained, but the objections in paragraphs 2(b) and (c) are abandoned, except to the extent that such information would reveal the [REDACTED] technique used by CPS's device. The Crown maintains that disclosing the make and model would itself disclose the [REDACTED] technique.

[10] Thus, the issue to be addressed on the disclosure application before me is whether the make and model of CPS's MDI and certain specific features of it would "encroach upon a specified public interest" (section 37(4.1)), namely police investigative technique privilege (which I will refer to as "investigative privilege").

III. Evidence

[11] Evidence at the *in camera* hearing consisted primarily of the affidavit and testimony of Sgt. Scott Campbell, a member of CPS. In addition, I have considered an affidavit submitted on behalf of Mr. El-Rafie and Mr. Amer, which contains extensive exhibit documentation in the public domain about how MDIs operate. Those exhibits were used during Sgt. Campbell's testimony and in oral submissions.

[12] Sgt. Campbell has at all relevant times been assigned to the CPS's Electronic Surveillance Team. One of his responsibilities in November 2015 and January 2016 was to supervise deployment of an MDI during the Homicide Unit's investigation "Operation Hybrid." The CPS took delivery of its MDI unit in September 2015. There are several types of MDIs available for purchase by law enforcement, intelligence and military agencies. The one selected by CPS was manufactured by [REDACTED], the model being [REDACTED]. Its software is updated from time to time.

[13] Sgt. Campbell took a thirty-hour training course for operating the unit, which was conducted in Calgary by the manufacturer. It involved field simulation, both at secure locations

and in public. In addition, other staff members who would be operating the unit received training.

[14] CPS's MDI unit was deployed first for Operation Hybrid in November 2015, and again in January 2016. Overall, it has been deployed in fourteen investigations and is still being used.

[15] Other Canadian policing agencies that are known to use MDI units are the Royal Canadian Mounted Police, the Ontario Provincial Police and the Winnipeg Police Service. None have disclosed the make and model of their devices.

[16] There are three modes in which most MDIs, including CPS's device, can be deployed. The direction-finding mode enables the location of a specific cellphone, and can be used to identify missing persons or kidnapping victims who have a cellphone with them. A second mode would be used in a military or tactical operation to block operation of all cellphones within range of, for example, an improvised explosive device, thus avoiding remote detonation. The third mode is the query mode.

[17] In this case, only the query mode was used. It is explained briefly in Sgt. Campbell's affidavit at paragraph 7 as follows:

In Query mode, the CSS [Cell Site Simulator, commonly referred to as an MDI] requests the International Mobile Subscriber Identity (IMSI) number and International Mobile Equipment Identity (IMEI) number from all active mobile communication devices within a given area. The simulator typically receives signals from multiple such devices, and then acquires the unique ID for each handset within the area of influence. The CSS operator attempting mobile communication device identification uses this technique in several locations where the target device is confirmed to be. Using simple subtractive analysis, the CSS operator determines the unique ID from all confirmed locations to identify the unique ID for the target device. In this mode, mobile communication devices leave their home network (i.e. Rogers, Bell, Telus etc.) and attempt to connect with the CSS -exchanging their IMSI and, in some circumstances, their IMEI.

[18] More detail about the technique used by the CPS was given during his testimony. Based on Sgt. Campbell's description, the operation may be summarized as follows:

- a) Each mobile phone, or cellphone, must have credentials to connect to a cellular network. Those networks are divided into areas commonly referred to as local area codes, or "LACs."
- b) Each LAC has a unique identifier. Within each LAC, there may be a number of cell towers. The towers broadcast the LAC's unique identifier to the area.
- c) The subscribers to a network communicate to that network's tower within a LAC. That is the way mobile phone calls are connected and routed to their ultimate destination.
- d) For a mobile phone to connect with the subscribed network, it must communicate its credentials, which include the IMSI and the IMEI.
- e) In Canada, there are different mobile technologies, such as Global System for Mobile Communications ("GSM") and Long-Term Evolution ("LTE").

- f) GSM and LTE devices all use IMSI and IMEI identifier numbers. At least one of these identifier numbers is recorded by a service provider, such as Rogers, as part of a customer's subscription information.
- g) The idea behind MDI technology is that the cellphone will communicate with the most attractive cell tower within range of the phone, and provide as credentials at least one of the identifier numbers. The MDI masquerades as a cell tower and thus the communication is given to it.

All of this information is publicly available.

[19] Many MDI units rely [REDACTED]

[20] The [REDACTED] unit used by CPS employs a different technique.
[REDACTED]

[REDACTED]

[21] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[22] Use of the data collected is made by “subtraction analysis.” Based on “eyes on” surveillance, the MDI is taken within range of the target and activated. This is repeated over a number of locations. The software then determines which unique identifiers appear at each location, giving the investigators presumptive knowledge about what numbers are being used by the target who was gone to each location. This information can be used to support an application to intercept the newly-discovered cellphone number.

[23] In his affidavit, Sgt. Campbell testified that “the [MDI] was used in Operation Hybrid to attempt to identify unknown mobile communication devices in the position of known persons”: at para 6. No such unknown numbers were identified during three sets of deployments against thee targets. Sgt. Campbell testified that the police could not rule out the possibility that numbers already known to be associated with those targets were identified by the MDI. Such results would not have been kept because the MDI deployment was for the purpose of locating unknown numbers not already being intercepted pursuant to court authorization: transcript at 21-22.

[24] Sgt. Campbell explained that in the case of Mr. El-Rafie, the device was deployed as the target travelled to different locations. However, he did not leave a certain area of Calgary, staying at locations within two or three blocks of each other. Thus, the results were not meaningful: Campbell affidavit at para 9.

[25] In the case of Mr. Amer, they were only able to deploy the device at one location and therefore had insufficient information to conduct the subtraction analysis: Campbell affidavit at para 10.

[26] Sgt. Campbell had no recollection about the deployment for target Qyrin Edwards (who is not an accused in these proceedings). In his affidavit, he testified that he was advised that the

operator “did not obtain data from a sufficient number of unique locations to conduct a meaningful subtractive analysis”: Campbell affidavit at para 11.

[27] Apart from these specific incidents, Sgt. Campbell testified in his affidavit at paragraph 8 to a number of reasons an MDI may fail to capture a cellphone:

- a) The device has been turned off (that is, powered off – it does not actually have to be transmitting or receiving a communication to be detected);
- b) The device was out of range of the MDI (which in an urban environment is anywhere from 200-500 metres);
- c) The device was not transmitting (for example, if put on airplane mode, which shuts off the transmitter);
- d) The device remained on the home network (which Sgt. Campbell understood may occur by some internal programming on the device);
- e) The known person did not possess an unknown device (which is really more of a reporting issue, in that in this case the investigators did not report on or retain records about obtaining identifier numbers for known numbers used by targets); and
- f) The general operating environment (which includes obstructions such as buildings, weather, and radio frequency interference caused by other devices transmitting on the same frequencies the MDI is using).

[28] Sgt. Campbell explained that even where situations appear to be ideal for MDI deployment as far as can be determined by investigators’ observations, there may be factors which prevent the MDI from receiving the identifier numbers from targets using unknown numbers. He also testified that it would be impossible to recreate the situation the operators faced in Operation Hybrid when they deployed the MDI. There are a broad range of unknown or impossible-to-duplicate factors, such as variations in location, weather, other radio frequency traffic being used, other devices (such as a refrigerator, which produces radio frequency), and other people present within the range: transcript at 79.

[29] In his affidavit, Sgt. Campbell testified that “disclosure of the make, model and software version of the simulator will enable persons engaged in criminal activity to research its capabilities and take steps to defeat it”: at para 5. In his *in camera* testimony, he stated that “if the public were to understand our specific device and, potentially, the technology and software that runs our device, there’s the possibility . . . of people being able to defeat it, either by understanding how it works and physically defeating it or by potentially hiring somebody or somebody developing further technology that would allow them to defeat it”: transcript at 17.

[30] CPS has done no investigation on the efficacy of frustrating its MDI’s operation. Sgt. Campbell is aware that there are attempts to frustrate the operation of MDIs. Examples are Snoop Snitch and CryptoPhone, both of which are advertised as having the ability to detect the use of MDI units. Sgt. Campbell does not know whether these technologies are effective or, in particular, whether they could detect deployment of CPS’s MDI device: transcript at 71-72.

IV. Legal Principles

A. Introduction

[31] The effect of section 37(4.1) of the *Canada Evidence Act* is that upon a certified objection by a Minister of the Crown or other official, there can be no disclosure order if the court concludes that the requested information “would encroach upon a specified public interest,” in this case investigative privilege.

[32] There are two questions to be addressed in interpreting this provision: (1) what constitutes investigative privilege, and (2) what is meant by the phrase “would encroach upon.”

B. Burden of Proof

[33] The parties agree that the Crown has the onus of establishing, on a balance of probabilities, that investigative privilege applies to the MDI information it seeks to withhold. As was stated in *R v Mirarchi*, 2015 QCCS 6628: “The mere assertion by the police or the Crown is insufficient to warrant a finding of privilege. Proof of the allegation is required”: at para 110.

C. Investigative Privilege

[34] Police investigative technique privilege is a “case-by-case” (or case-specific) form of privilege, as contrasted with a class privilege. At common law, case-specific privilege is qualified and involves balancing competing interests (usually some public interest against an accused’s right to full answer and defence): *Mirarchi* at para 104; *Michaud v Quebec (Attorney General)*, [1996] 3 S.C.R. 3, 109 C.C.C. (3d) 289 at paras 47-48; and *R v Richards* (1997), 115 C.C.C. (3d) 377 (Ont. C.A.) at para 11. In section 37, the balancing of interests is expressly required by subsection 5.

[35] Investigative privilege reflects the state’s interest in preserving the confidentiality of its investigations and investigative techniques: *Michaud* at para 48; *R v Durette*, [1994] 1 S.C.R. 469, 88 C.C.C. (3d) 1 at 53. It protects against the risk that “disclosure of investigative techniques . . . might . . . cause criminal offenders in the future to modify their activities in order to avoid detection”: *R v Trang*, 2002 ABQB 19, 168 C.C.C. (3d) 145 at para 50. As Mr. Kapoor said in his *amicus curiae* brief: “The underlying concern animating the application of the privilege is that if the criminal element learns the police technique, they will be able to avoid detection and thereby public safety will be undermined”: at para 12.

[36] Furthermore, the Crown agrees with Mr. Kapoor’s description in his *amicus curiae* brief of how to determine whether the privilege exists over certain information:

An important factor to take into account when assessing if a particular police technique is sensitive is to ask if it is a publicly known technique. For example, the police utilize many techniques to assist their investigations, many of which are well known and part of our criminal law daily experience and are not the subject of privilege. [Footnote: “For example, the use of breathalyzers, radar guns, surveillance, the Mr. Big Technique, employing agents, undercover operatives, the use of covert entries and many more.”] What is privileged and what is not turns, in part, on the extent of public knowledge about the investigative technique. Where the operation of a device is widely known or publicized by the police, the underlying rationale for the application of the privilege weakens: at para 11.

[37] I am not aware of any authority that defines the elements of investigative privilege. However, based on factors giving rise to the privilege and its purpose (addressed in various cases), I conclude that investigative privilege covers information that (1) is used by police in their law enforcement functions; (2) is not publicly known; and (3) if disclosed, may assist offenders to interfere with or defeat police investigative functions.

D. “Would Encroach Upon”

[38] The Crown submitted that under the section 37 regime the court should take a broad approach to recognizing investigative privilege at the initial stage articulated in section 37(4.1). It argued that the notion of “encroaching” upon a privilege connotes something less than an overriding of privilege. Further, it argued that the balancing of interests contemplated in section 37(5) permits more latitude in determining whether privilege exists because a mere finding of privilege does not necessarily preclude disclosure.

[39] I am not persuaded by the Crown’s arguments. In its plain sense, an encroachment is a form of entry or trespass. For example, *The Canadian Oxford Dictionary*, 2nd ed. (2004) defines “encroach”, when followed by “upon”, as “intrude, esp. on another’s territory or rights” or “advance gradually beyond due limits.” Applying this definition, “would encroach upon” suggests a circumstance where the privilege is overridden. My interpretation is reinforced by the use of “encroachment” in section 37(5) in a context that clearly refers to an infringement, because in some cases it allows disclosure after privilege has been found, upon conditions “that are most likely to limit any encroachment upon the specified public interest resulting from disclosure.”

[40] The balancing of interests provision in section 37(5) is not helpful to the Crown’s argument either. The case-specific privilege at common law also requires consideration of competing interests for granting protection over investigative privilege. It is a step that follows the initial determination of whether disputed information falls within the scope of the privilege.

[41] It would be more accurate to say that concealing an investigative technique “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”: *R v Toronto Star Newspapers Ltd.*, [2005] O.J. No. 5533 (S.C.) at para 14, quoted in *Mirarchi* at para 117. However, its narrow application is reflected in the limited scope of the privilege as set out in the authorities to which I referred earlier, and the test I articulated based on them, set out above.

V. Findings

A. Introduction

[42] I summarized the elements required to establish investigative privilege as applying to information that (1) is used by police in their law enforcement functions; (2) is not publicly known; and (3) if disclosed, may assist offenders to interfere with or defeat police investigative functions.

[43] It is beyond dispute that CPS uses an MDI device as part of its law enforcement functions. Accordingly, the first factor is satisfied. What needs to be addressed are the second and third factors: the degree of public knowledge about that device, and whether the information requested may assist offenders in interfering with or defeating police activity. Finally, it must be

addressed whether any special significance should be given to the requirement in section 37(4.1) that disclosure “*would encroach*” (emphasis added) upon the privilege.

B. Public Knowledge

[44] Based on the evidence and submissions, I conclude that there is public knowledge of the CPS’s MDI use in the following areas:

- a) The CPS has at least one MDI device (as disclosed, for example, in an interview with *The Globe and Mail* newspaper).
- b) A broad outline of how MDIs operate is publicly known. They simulate cell towers. Because cellphones must connect to cell towers to link to a network, the cellphones’ unique identification numbers are captured by an MDI unit (as they would be by a cell tower).
- c) Specifically in query mode, an MDI requests the identifier numbers from all active cellphones in its range; it then receives signals from these devices, which respond as they would to a cell tower. Thus, the MDI acquires the unique identifiers for each handset within its range.

d) [REDACTED]

[45] Thus, it could be argued that all elements of CPS’s MDI investigative technique are publicly known. However, the Crown argues that it is not known that the CPS’s MDI uses the [REDACTED] method, and the fact that information about the [REDACTED] procedure may be publically accessible is not the same (especially in the internet age) as a police service verifying its accuracy or confirming publicly that this is

the procedure they use. It is not necessarily well-known. The only public information about which Sgt. Campbell was aware that discussed the [REDACTED] technique is the [REDACTED].

[46] These are legitimate points. While information about basic MDI technology may be readily accessible, avoidance measures might need to take into account specific details of each device used. For example, the Defence submitted that “the dominant company in digital cellular surveillance market is Harris Corporation, who introduced its ‘StingRay’ product in 2003”: May 12, 2017 brief at para 17. That is not CPS’s product.

[47] Further, it is one thing to locate information about how MDIs are reported to operate. Information on almost anything can be obtained by persistent inquiry. It is another thing for CPS to state, under court order and perhaps by sworn evidence, what MDI device it uses and how it operates. Confirming what otherwise has a degree of uncertainty confers more useful knowledge.

[48] Additionally, a successful privilege claim does not require proof that the information cannot be accessed any way other than by disclosure. As Mr. Kapoor submitted: “What is privileged and what is not turns, in part, on the *extent* of public knowledge about the investigative technique”: *amicus curiae* brief at para 11 (emphasis added). The extent of public knowledge falls on a continuum, and is an important, but not the sole, factor in determining privilege.

[49] It is telling that the materials submitted on behalf of Mr. El-Rafie and Mr. Amer included an extensive collection of materials showing that MDI technology is publically known. While those materials contain basic information about the technology, they do not go beyond the notion, to quote one reference, that “a Stingray pretends to be a legitimate cell tower, forcing all nearby devices to connect”: Article from *The Globe and Mail* (September 15, 2014), Exhibit N to the Affidavit of Melissa George. [REDACTED]

[50] [REDACTED]

[51] [REDACTED]

[52] The [REDACTED] reinforces my earlier point that the mere fact of information being in the public domain does not mean it is well known. The well-known information, based on the materials submitted to me, focuses on the most prevalent forms of MDI, such as Harris Corporation’s StingRay. Sgt. Campbell testified that [REDACTED]

[REDACTED]

This supports the CPS's assertion of privilege over the make and model of its device.

C. Disclosure May Assist Offenders

[53] The third factor in determining whether investigative privilege applies is whether the requested information may assist offenders to interfere with or defeat police investigative functions.

[54] As I indicated in my summary of the evidence, Sgt. Campbell is aware that devices exist to detect deployment of MDI units. He is not aware of their efficacy generally, nor whether they would work in particular against CPS's model.

[55] Mr. Kapoor submitted that I must consider whether the Crown has met its burden of proof in establishing investigative privilege. He emphasized that the underlying point of investigative privilege is consequential: the question is not whether the information is secret, but what would result from its disclosure. He argued that the risk of persons engaged in criminal activity using this information to defeat MDI technology is speculative. He suggested that the Crown should have provided evidence on whether current countersurveillance products would detect deployment of [REDACTED]'s MDI device, either by introducing test results or by expert opinion evidence.

[56] Requiring that degree of certainty would be too heavy an onus in making out a privilege claim, in my view. The cases do not require proof that disclosure will enable offenders, as a result thereof, to defeat law enforcement objectives. Nor is proof of probable harm needed. This aspect of the test operates to limit the investigative privilege according to its proper purpose; not every police secret will be privileged. But where the evidence supports a genuine, reasonably-based concern about adverse effects on law enforcement functions, the test is met.

[57] I conclude that the make and model information (and related details) concerning CPS's MDI unit fall within investigative privilege. The public knows that CPS has an MDI device, but does not know its particular method of [REDACTED] obtaining cellphone identifiers, information that is not common among all such devices, and perhaps not used by Harris Corporation products (or at least not publicly known to be used). Sgt. Campbell has, on behalf of CPS, expressed genuine and reasonably-based concerns that public confirmation as to how the device operates will facilitate more effective, focused counter surveillance efforts. It is reasonable to be concerned that accurate knowledge of unique features of a particular MDI device will facilitate more effective avoidance techniques. It asks too much to require the Crown to prove this.

[58] I also consider that CPS is willing to disclose significant details about the operation of its MDI device in query mode, and how it was used in surveillance in these cases. They have limited their claim of privilege to a few narrow details, giving up the claim on what they agree is already public information.

D. Would Encroach Upon Privilege

[59] Mr. Kapoor urged me to pay special regard to the requirement in section 37(4.1) that for privilege to apply, the court must conclude that disclosure "*would* encroach upon a specified public interest" (emphasis added). He suggested that this is a further element required to establish investigative privilege, requiring evidence of the consequences of disclosure.

[60] In my view, section 37(4.1) does not change the scope of investigative privilege as established in the cases. Stober J.S.C. said in *Mirarchi* that “Crown counsel, defence counsel and the *amicus curiae* agree that there is no difference between the considerations underlying an analysis pursuant to s. 37 of the *Canada Evidence Act* or the common law”: at para 107. I agree with that conclusion. In another case, when considering a request for disclosure about protection measures under a witness protection program, the Quebec Court of Appeal held that even though section 37 imposes a heavier burden on the Crown than sections 38 or 39, it does not require the Crown to demonstrate that disclosure will necessarily endanger the witness or the program, only that disclosure might impair all those interests: *R v Minisini*, 2008 QCCA 2188, 66 C.R. (6th) 306 as summarized in David Watt, *Watt's Manual of Criminal Evidence 2016* (Toronto: Carswell, 2016) at 1126.

[61] The statute only asks whether disclosure of the information “would encroach upon a” privilege. I have already found that the requested information falls within investigative privilege. Thus, it follows that disclosure of the information would encroach upon that privilege, because a privilege is breached whenever the protected information is divulged.

VI. Conclusion

[62] For the reasons given, I conclude that the Crown has proved that disclosure of the information to which it objects would encroach upon police investigative technique privilege. Thus, I prohibit disclosure of the information covered by the objection, unless in later proceedings I authorize disclosure after undertaking the balancing considerations required in section 37(5).

[63] Subject to submissions from counsel to clarify the scope of privilege, I find that the prohibited disclosure encompasses the make, model and software of the MDI device deployed by CPS in the cases subject to these case management proceedings, and any further information which would have the effect of disclosing the technique by which the MDI obtains cellphone identifier information [REDACTED].

[64] As this matter was heard *in camera* pursuant to section 37 of the *Canada Evidence Act* and deals with the determination of privilege over information, this judgment is sealed and must not be published or distributed in any way, except as directed by this court, and is not to be made available from the court file. These reasons are to be distributed only to Mr. Holtby and Mr. Kapoor.

[65] I have already ordered that the audio recording and transcripts from July 12 and 13, 2017 are sealed. Also sealed are exhibits 1 and 2 from the hearing, the affidavit of Sgt. Campbell affirmed July 6, 2017, and the briefs of the Crown and of the *amicus curiae*, both filed July 11, 2017. These materials must not be published or distributed in any way, except as directed by this court, and are not to be made available from the court file.

[66] This sealing order and publication ban may be modified at a later date by order of this court.

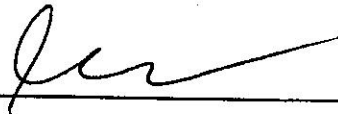
[67] This decision, the transcripts from July 12 and 13, 2017, and the affidavit of Sgt. Campbell affirmed July 6, 2017 have been redacted and edited (with editing underlined) pursuant to my decision dated October 27, 2017, which decision is sealed and subject to a publication ban. By way of update to paragraphs 64 and 65 above, I order that this decision as redacted and edited

is unsealed, and may be published and distributed. In addition, the transcript of the July 12 and 13, 2017 hearing and the affidavit of Sgt. Campbell affirmed July 6, 2017, as redacted and edited, are unsealed and may be published and distributed.

Heard on the 12th and 13th day of July, 2017.

Dated at the City of Calgary, Alberta this 15th day of August, 2017.

Redacted, edited and amended at the City of Calgary, Alberta this 30th day of October, 2017.



G.H. Poelman
J.C.Q.B.A.

Appearances:

Brian Holtby, Q.C.
for the Crown

Anil Kapoor, Kapoor Barristers
Amicus Curiae