April 5,2017

10:00 AM (Eastern)

The RCMP invited reporters from CBC News, Toronto Star and the Globe and Mail to a 'technical briefing' in what the force described as "the interest of transparency" to discuss publicly for the first time their use of Mobile Device Interceptors, also known as IMSI catchers.

PRESENT (by phone):

RCMP: Jeff Adam, RCMP Chief Superintendent, Technical Investigation Services
CBC: Dave Seglins, Brigitte Bureau, Catherine Cullen
Toronto Star: Robert Cribb
Globe and Mail: Colin Freeze

Chief Supt. Jeff Adam (RCMP): The historical background on this is that the RCMP has been trying to get ourselves into a position where we can become a little bit more transparent and a little bit more accountable in some of the technical investigative techniques that we use in a criminal investigation as authorized under Canadian Law

There have been some hiccups in our attempts to get out in front of some of the information that's out there. However today is the day when we're going to get to pull the trigger on it.

And so I'm here to talk a little bit about some media coverage of some of our techniques and technology. And again, it is with the intent of informing canadians and to relieve potential misconceptions about the RCMP mobile device identifier technique commonly known as an IMSI catcher or mistakenly as a Stingray or any of those other terms that are floating around out there.

So there has been some recent media coverage relating to mobile device identifiers, which is the RCMP term for this. And it has gotten significant attention in the media.

Though we will confirm officially that the RCMP possesses and uses mobile device identifier technology in order to identify and locate a suspect of a criminal investigations' mobile device.

This capability can be used to further criminal investigations relating to national security, serious and organized crime and other serious criminal code offences that impact the safety and security of canadians.

We use that MDI technology in full compliance with Canadian laws which include the charter of rights, the criminal code of Canada and proper judicial processes as established by either jurisprudence and or common law in the courts

Except in the extremely urgent cases — for example to prevent death or imminent harm, the RCMP can use this technology but then gets the judge's authorization after the fact — in the fact where it's not urgent we get it before.

There are a very limited number of authorized and trained RCMP operators who can use the MDI technology and its use is subject to very strict rules, senior management approval and judicial authorization prior to its use and deployment

So this is a very important investigative tool for us and in order to identify a suspect’s cellular device such as a mobile phone. It helps us identify an unknown cellular device used by a target under investigation by collecting very limited signalling information or for other policing matters such as identifying the location of a known cellular device linked to, for example, a missing person.

In simple terms, when a trained officer deploys MDI technology it attracts and momentarily connects cell phones in the immediate vicinity before returning them to their own networks it then blocks further attempts by those devices to attack, or sorry, to connect to the technology.

The technology collects international mobile subscriber identity — I-M-S-I, or IMSI — and international mobile equipment identity numbers — IMEI — those data associated with the phones which allow the operator to identify the phone used by the subject

The IMSI and IMEI number are international standardized unique numbers that identify a mobile device and subscriber respectively

What the RCMP technology does not do is collect private communications. In other words it does not collect voice and audio communications, email messages, text messages, contact lists, images, encryption keys or basic subscriber information

The information that is not relevant to the investigation is secured along with the information that is relevant pursuant to criminal code authorities and requirements imposed by the judiciary in other words the data is sealed, treated as an exhibit. The judge is properly informed as to what was collected, it is retained for court and appeal periods and any specific orders by judiciary before it is destroyed in accordance to records management principles.

So this technology is a vital tool in providing valuable assistance to criminal investigations and other policing duties it is one of the only ways to identify a cell phone used by a subject which then can lead to further judicial authorizations to get the subscriber information and then further authorizations to conduct further investigation in the criminal investigation

After getting authorization from the senior criminal officer and then a judge, the mobile device identifier, MDI, is deployed for a short period of time to attract and collect that limited information from cellular devices in the vicinity. That data is used to identify the cellular device used by the suspect.

So we've maintained the use of this device only in serious cases. And only when there are proper grounds to believe that a suspect is using an unknown cell phone to conduct criminal activity.

It does require a judge's authorization and there are strict reporting requirements for each use by the RCMP.

For example in 2016 the RCMP used the MDI technology in 19 criminal investigations. One of those was involving exigent circumstances such as a kidnapping.

So as I stated already the governance around the use of this technology is very strict, senior officer approval and a valid judicial authorization are required before the technology is deployed except in those extreme urgent cases where the police reasonably believe that there is a need to deploy the technology to prevent imminent harm or death

Now, in addition the RCMP is cooperating completely with the office of the federal privacy commissioner in their investigation relating to the RCMP possession and use of this technology.

Authorization to use this technology under the Radiocommunications Act has been issued by innovation science and economic development canada and this MDI technology, we know, that it might cause limited cellular interferences for some devices within range of the tool.

The RCMP makes every effort to deploy the technology in a way that causes the least disruptions to service and public safety

And that is the conclusion of the prepared remarks.

CBC: You gave us some stats from 2016 about the number of criminal investigations that MDIs were employed in. Do you have any any other figures for previous years?

RCMP: I do. Not at my fingertips. I'll include those. I know the number was in the vicinity of the mid-20 range. So less, but not a significant drop.

RCMP spokesperson Harold Pfleiderer: It was 24 in 2015.

CBC: 24 investigations in 2015. Do you have the number for 2014?

RCMP: No we don't.

CBC: And when you say in a criminal investigation, that could be multiple uses correct?

RCMP: That's correct.

CBC: So do we have any idea how many times it's been deployed.

RCMP: So the — No we don't at this time, and some of those investigations are ongoing now so I wouldn't be answering that question anyway.

CBC: Now, you're talking about RCMP use of this. Does RCMP assist other forces in the use of this technology?

RCMP: In some cases we have been asked to assist and have rendered assistance to other canadian police forces. And the same requirements for judicial authority before deployment are followed.

CBC: And part of the question comes from—because other law enforcement agencies, local, municipal, even provincial police forces, have not been as forthcoming as you guys have today, which is wonderful—we don't know, do they operate independently? Are they allowed to do that independently? Or does the RCMP have a supervisory or assistance role?

RCMP: So the RCMP does not have a supervisory role on the use of this technology.

CBC: Okay, so do you ever deploy them on behalf of other agencies? CSIS, CSE?

RCMP: I cannot answer that question.

CBC: How has the use of MDIs changed over time? Like, in the last 5-10 years, I mean, are you using them more? Less?

RCMP: There have been changes in the criminal code and judicial authorities that govern the use and deployment of these. So as the law has changed the use and controls around the use of this and deployment of the device have changed in accordance with those authorities.

So for example the TDRW, the transmission data record warrant, is a new thing to us in the last couple of years, and we have adapted to fulfill the requirements under the criminal code for the use of the device in relation to the TDRW.

Now in so far as the deployment of it for criminal investigations, again, we use it only in serious organized crime, or serious criminal offences, or exigent circumstances or national security investigations.

And the use of that will ebb and flow in relation to the number of investigations that are ongoing, likely proportionately

CBC: So I want to ask about the kind of crimes in a sec, but just in terms of the new warrant being brought in, does that mean it was being used more in the past, and it's slightly less now? Say over the span of five years?

RCMP: No, so the changes—I don't believe so. I only have the data now for '16 and '15. Except for a very brief period of time, there was a period of a couple months where there was a national wiretap experts group which was composed of Justice and prosecutions personnel, had made a determination that there was no warrant required which was subsequently discarded and the TDRW is being used.

Globe: Sorry, just to interject, the TDRW warrant is basically a metadata warrant. Are you saying that the MDI can go beyond IMSI/IMEI identifiers and collect logs of call-to-call and the like? Is that—that is what I'm interpreting here, is that the MDIs don't, aren't simply limited to IMSIs and IMEI identifier, and if you want to court and got a TDRW you could use the device to log transactions occurring through a [inaudible] or have I misunderstood?

RCMP: So the last sentence is correct, you have misunderstood. The RCMP MDI technology does not capture any communications, any of the things that I listed, which I can go over again if you wish, which is PIN messages, audio voice communications, email messages, text messages, or basic subscriber information, or has been reported, encryption keys.

So to reaffirm the RCMP MDI equipment does not collect any of that information or have access to it.

Globe: Right. Okay. So the application of a—what does a TDRW give you that you didn't have before then? What is the use of that warrant say that you can do—

RCMP: The TDRW is the judicial authority under which we collect the IMSI and IMEI information.

Globe: Before that you used a general warrant power. Would that be fair to say?

RCMP: That's correct.

CBC: I want to get to the—because you're on a point here that talks about the functions of the MDI. You say the RCMP's MDI equipment don't do it, and don't have access to it. But is some of the technology you use capable of it?

RCMP: If some of the technology capable of what, sorry, Dave?

CBC: You say that the RCMP MDI equipment does not capture PIN, audio, voice, email, text, and you don't have access to it. But is the equipment capable of it?

RCMP: Not the RCMP equipment

CBC: Can I just ask quickly, with the PIN-to-PIN information though, the MDI technology is part of, it's a step in the process of ultimately gaining access to those communications is it not?

RCMP: That's correct. So that is the step by which we identify the device that we would then have to apply judicial authority to obtain the subscriber information, and then pursue into further investigation, undertake an intercept of communications, knowing which device and who's using it, in order to get that PIN-to-PIN information. So there's multiple steps of the investigation, and multiple authorities before we actually get to context, if we are allowed to under authority.

CBC: So you mentioned at one point that except for a brief period no warrants were required during a brief. When was that?

RCMP: So the recommendation from the National Wiretap Experts Group— and that was not binding, so there was differences between what was required in the different provinces under the crown councils, so I cannot even say how many were used without warrant. I know there was a period where the recommendation was that we didn't have to have one, which was subsequently changed after, I think it was, a period of around four months.

CBC: And around what period? Two-three years ago? Do you know when?

RCMP: No, I'll get that information and flip it out. *(***Later RCMP statement indicates March - October 2015.)*

CBC: So back to what they can and can't do. What is it of the RCMP, like we know that certain models can intercept phone calls and text messages. What is it in the RCMP's equipment that restricts those abilities? Is it a policy decision? Is it a physical thing on the actual kind of equipment you have? What limits you from using it for the additional potentials of what we know some MDIs can do?

RCMP: So the RCMP has acquired the capability of only receiving the IMEI and IMSI information. If we were to acquire additional, it's both hardware and software, which we have not

obtained. So the policy is not to obtain, and we don't have the devices—the MDIs that we have, do not have the capability of acquiring anything other than the IMSi and IMEI information.

STAR: Jeff, what do you have exactly? What is the model or what is the exact device that you use?

RCMP: So I'm not going to answer that question Rob.

GLOBE: But you did say referring to them as Stingrays is erroneous? So presumably not Harris Corporation devices? Is that correct?

RCMP: So what I said—No it's not. What I said was that, in the media, they have been referred to as Stingrays, which is just a brand name. So I'm not confirming or denying that we have such a device. Or any other device.

GLOBE: Right, okay, I got you.

CBC: So how about this. How many MDIs under a large umbrella description of potentially various kinds of devices, how many MDIs does the RCMP own?

RCMP: Ten.

STAR: Are they all the same?

RCMP: Sorry?

STAR: Rob Cribb here. All the same devices? All the same models?

RCMP: I'm not going to answer that.

STAR: How many officers—you mentioned there's a limited numbers of officers that are trained on it. How many are there?

RCMP: So there's 24 that are currently certified in Canada.

CBC: And where they stationed—

STAR: And the devices themselves—

RCMP: Across Canada.

GLOBE: Sorry that's RCMP officers only?

RCMP: That's correct.

GLOBE: Do you know if any other municipal forces own their own devices or have their own certified technicians?

RCMP: I do know that other municipal forces own a device, or devices, and therefore would have their own technicians. But those questions and answers will have to be relayed to them.

CBC: You said the RCMP does not own equipment that can listen in on conversations and read text messages. Do you work with other associations, other organizations, that do have this and lend you the equipment?

RCMP: The premise of that was, we were talking about MDI equipment. So the RCMP does not own MDI equipment that can intercept communications, other than IMSI and IMEI information.

CBC: I understand that. But does it happen that you work with CSIS for instance and that they have this equipment and can help you out if you need more information than what the MDI can provide?

RCMP: So the authority to use the MDI is granted under a judicial authorization that allows us to capture IMSI and IMEI information with that device under that authority. If we were to pursue subsequent authorities on the interception of the communication under part six of the criminal code of Canada. But it is not under the MDI.

GLOBE: Would it be illegal for me to go out and get an MDI and use it to collect the same IMSI and IMEI data? Would that be a violation of the criminal code?

RCMP: The Criminal Code Section 191.1 states that the use, possession, trafficking of devices for primary purpose is to intercept private communications is illegal, unless—

GLOBE: Okay, but—

RCMP: —unless authorized under lawful authority.

GLOBE: Right, but, does an IMSI or an IMEI, you know, number, elevate to a private communication.

RCMP: I not sure I get the follow-up question.

GLOBE: Well private communication was often interpreted to mean a conversation, an email exchange. Does privacy attach itself to my IMEI or IMSI number on my handset, particularly if I'm a private actor who can't do anything with it? You know, could you prosecute me if I went out and got one of these things for intercepting private

communications when in fact I'm not getting anybody's private communications, when I'm not hearing anything or reading anything, I'm just getting a number?

RCMP: So there's a whole pile of nested assumptions in there. If we keep this within the framework of the RCMP MDI technology. And if you had that same technology, then you would be in violation of the Radiocommunications Act that is administered by ISED — Innovation, Science and Economic Development.

GLOBE: Right. So that's a — you said that the RCMP has gotten approval to use these devices from ISED. Do you know when that approval came?

RCMP: The exact date?

GLOBE: Or a ballpark.

RCMP: Within the last two months.

GLOBE: The reason I ask is because—sorry, it's the last two months. But I think the RCMP has had these devices for a decade. There has been testimony to that effect. So was the RCMP afoul of the Radiocommunications Act except for the last two months?

RCMP: So leading up to a point in the beginning of March - about a year ago actually, the RCMP when the new Radiocommunications Act came into force, questioned whether or not our technology was in fact included under our exclusion that is covered by jamming.

There was some belief that it might be, and some belief that is was not. When we queried industry canada then, or ISED now, it took us quite a bit of time to come to the conclusion that in fact our equipment was not covered under the exemption.

So when we were working with innovation, science and economic development, ISED, they agreed that they would be working with us in order to allow us the use of that technology and it took some time for us to get the authority, the actual authorization.

During that period of time it is understood by the RCMP and ISED that we were, in fact, in potential violation of the Radiocommunications Act, but based on the fact that we were working with them and in cooperation it was not an issue.

GLOBE: There was a 2011 memo circulated within the RCMP that is now in public domain information, talking about 3 minutes on, 2 minutes off rule. Can you say why that that rule was put in place and whether that rule is still in place?

RCMP: So the rule was put in place to minimize the interference from the other people in the area and all cellphones within the area.

So what we didn't want to do was turn on this MDI technology and have phones automatically migrate to it and stay there.

So we both instituted the once connected block and then in order to minimize interference and the risk of interference we decided to use it on a limited time per frequency and came upon the time of about 3 minutes.

That policy remains in effect in order to minimize the interference to other people.

GLOBE: Right, and the 911 calls, was that a consideration and does that remain a consideration?

RCMP: It is and does and was. Some, and few now, older phones may be disrupted if they are attempting to make a 9-11 call during that very limited period of time in which the MDI technology is operating.

In order to, again, further limit the possibility for that for under public safety we decided that we would maintain that time limit. And that's frankly all the time we need.

STAR: Jeff, have there been any examples brought to your attention or the RCMP's where, in fact, that occurred? Where- 9-11 calls were in fact disrupted?

RCMP: None that i'm aware of and i'm not sure the user would know.

STAR: Well the call wouldn't go through, would it?

RCMP: Right, but they wouldn't know why, and we wouldn't get that report.

CBC: So what you're describing is there's a couple levels here. You've described in some details the kind of warrants and the judicial authorization needed to use the device. You've also indicated that until two months ago, having licensing under the act to possess and use the technology, there' that level. Similar to Colin's question about himself, if someone is using the device without a license, near government buildings, does that pose a national security risk?

RCMP: That's the investigation that we're undertaking.

CBC: No no, this is hypothetical.

RCMP: Because we're investigating the answer would be yes.

CBC: Sorry, the answer is, yes, it would be a national security concern?

RCMP: Absolutely.

CBC: And what, is that a concern?

RCMP: Well there's a variety of levels. Not everyone uses the equipment in the way the RCMP does. And as stated. And it is publicly known that there is equipment out there that is not limited in its capturing of communications between devices and so therefore it is a security risk when it is used in the proximity to government and or any other commercial enterprises for the purposes of industrial espionage for example.

CBC: Are there any protective measures in place to protect government communications from such technology, broadly?

RCMP: Yes, of course. 90% of the communications that are undertaken by the government of canada are encrypted.

CBC: Are Stingrays ever installed in key fixed locations to ensure the location of government buildings for instance?

RCMP: I'm not ...not going to answer precisely in relation to that particular brand name…

CBC: Or any other MDI devices or IMSI catchers.

RCMP: So we have secure installations that for the purposes of the confidentiality of the discussions we don't allow cellphones to enter into that area. There are detecting devices that are stationary that would be fixed in order to signal on a very very limited range the presence of a cell phone.

CBC: Could you described what kinds of installations?

RCMP: Well, I can say that wherever there would be a secure conversation ie. in certain government establishments, embassies, where they are tempted to restrict the egress of confidential information—

GLOBE: But these devices don't have a range of 500m or whatever the standard piece or RCMP kit would have? It's more limited than that?

RCMP: Well, if you were to think about how the use of it would be—if I install this equipment with a range of 500m I'd never have an end to the alarms going off. So it would have to be of a very limited range for the purposes of what it's trying to protect.

CBC: In terms of counter surveillance on this stuff, you're aware of Cryptophones? And you know what that is? It's a thing that can help detect the use of an MDI. What can you say about what those counter surveillance tools that can detect an MDI, what are the strengths and weaknesses of those kind of devices are?

RCMP: Generally speaking, if I was to for example say that our light rail system in Ottawa was functional, and you were going to try and use the cellphone underground on the subway, the relay station to which your station would connect could show up on a device such as the Cryptophone as a potential IMSI grabber. So it would take a great deal of analysis to look at what exactly the results were from the data, by an expert, that might not be associated to any particular brand, to determine whether or not these activity that was captured in the data was actually either a real possibility of a simulated cell tower, or a false positive based on all those other things that are out there."

CBC: But Mr. Adam I think you will agree that the Cryptophone that was used was one of the most reliable tools, especially, like you say, when it is backed up by professionals looking at the data, and being backed up by an Overwatch Sensors such as the ones that Homeland Security use in Washington to have more precise location of IMSI catchers. So if we have all of that, I think you will agree that the data is pretty secure.

RCMP: I can't speak to that. That's outside of my understanding.

GLOBE: I heard reference to tracking mode, when an MDI is used in a tracking mode as opposed to the generalized indiscriminate range. Does that mean anything to you? An MDI being used in tracking mode, or there's been two distinct modes in which an MDI can be employed?

RCMP: So I did reference, that we do use it to identify an unknown cellular device. it can also be used to locate a known cellular device. Which was possibly what you were referring to in the tracking. So in the case of a missing person, where their cellphone number and cell device is known, we can get the IMEI number or IMSI number from the company, from Rogers or the telco, and then locate the phone by using this same technology, the MDI technology.

GLOBE: And that would have an obvious application in exigent circumstances you described. It may also have an application in a criminal investigation. it's not tied to one sensibility or another, it's just a capability.

RCMP: That's correct. And so the use of the actual tracking on that would be a actual higher authority level. So if we were using the technology to track a device, the threshold is reasonable grounds to believe, which is a warrant for tracking.

GLOBE: Right, that's the specific tracking warrant power that was also relatively new on the books, right?

RCMP: That's correct.

CBC: So actually on that, has the standard of evidence required to get authorization changed? Meaning was, at one point under general warrant, a reasonable grounds to suspect changed to reasonable grounds to believe?

RCMP: So that's a difficult question to answer because of the way that the new powers have been put in, that they didn't exist before. So depending on which way you go with the device, either into the tracking mode or into the try and identify the unknown cell technology, it's different. So it's hard to say whether or not it's changed—well it has changed obviously, but it hasn't been elevated or lowered depending on which way you go.

CBC: So can you just help remind us, what threshold is needed for which application?

RCMP: So for the transmission data recorder warrant, it is a reasonable grounds to suspect. When using it as a tracking device it is reasonable grounds to believe.

CBC: And the believe is the higher threshold, right?

RCMP: That's correct.

STAR: You talked about strict reporting requirements for each use of the devices. And then you mentioned those two numbers — 19 cases last year, and 24 cases in 2015. Can you just talk about what those requirements are? To whom are those reports made? Those are not public right?

RCMP: Not yet. Those are currently reporting into my office.

STAR: So each time an officer goes out into the field and uses one of these, there would be a document, a form, a warning, a something that's filed, and it goes to you, is that right?

RCMP: Well, to my office, yes. So we are tracking the use of this. This is sensitive technology.

STAR: Until today, these numbers have not not been made public, is that right?

RCMP: Not to my knowledge.

STAR: And when you say not yet, is there an intention to in fact publish these numbers?

RCMP: Currently, we provide information under section, I think it's, 195 or 95, I'll have to look that up, under the Criminal Code on the interception of communication warrants, and a variety

of other things that are reported to government. We're not averse to reporting to a degree on the number of times this technology is used, but there is as of yet no requirement to do so.

STAR: Can you give us any details on either the 19 cases last year or the 24 from 2015 in terms of the efficacy of this technology in your pursuit of these suspects? Can you give us some sense as to, in fact, at the end of the day, how useful it was?

RCMP: This technology is key to furthering our investigative objectives. Now there have been, and will always be, some technical glitches here and there between devices and cell towers et cetera, but generally speaking, it is very effective, and very helpful for our criminal investigations.

STAR: Has evidence ended up in court? Have you got the bad guys? What can you say?

RCMP: The ability for us — okay, so there's layers there — to identify the cell device is successful. To in order to then go ahead and get an additional authority to get the basic subscriber information, and then yet again, further authorities, which is very very rigorous and strict control, on the interception of the communication that are to and from that device, that is dependent also on something you're very familiar with is the going dark problem, as to whether or not we can intercept that information, and whether or not the information is in a readable, understandable, comprehensible format.

RCMP MEDIA: Okay this is Harold we'll take one or two more questions and then we'll have to wrap it up, thank you.

CBC: So I want to ask about privacy protection because a lot of the critics are worried about all of the non-targeted or non-suspect information that gets collected. What happens to all the data that's collected, whether it be the metadata or otherwise of innocent Canadians, what can you say to that?

RCMP: So when we deploy the technology, we will get the IMEI information from all the phones that are in proximity and that do connect to our device. Through investigative protocols we finally get to the point where we can identify which of those captured IMSI/IMEI information are the target that we're looking for. All of that information is evidence. That is all because of the authorities and because of the requirements of the criminal code, the judge is informed of what we got, and where we're going to keep it. This is an exhibit. There are very very precise and strict guidelines on exhibit handling, because remember, the ultimate aim is to get this data into court as evidence. So all of the evidentiary guidelines, all of the controls, all of the accesses are followed by our exhibit handling processes, which are subject to scrutiny by the court. So the data, once it is seized lawfully to the judge, will be secured and locked up for criminal court purposes. It will not be accessed, other than the target information, again.

CBC: Mr. Adam did you ever while you were doing investigations, you or the RCMP come across foreign agencies using them?

RCMP: Using which, sorry?

CBC: Using IMSI catchers or MDI or Stingrays or whatever you want to call them. Did you ever come across foreign agencies using that kind of technology.

RCMP: I am not personally aware of any, but I can't rule that out.

GLOBE: Can I ask whether these devices—whether you sign non disclosure information with the vendors and whether any such agreements are fundamentally incompatible with your obligations to produce fair, full, and frank evidence in court? Because we have seen prosecutions go sideways over involving MDIs and there's speculation that the police's inability to discuss these things may have a downstream effect on the police's ability to put bad guys in jail.

RCMP: So, generally speaking, I'm not going to talk about any particular court case. What is important here is that, as recent events here in Ottawa have told us, is that countermeasures to investigative techniques, we don't want to assist the criminal element in figuring out how to conduct countermeasures. Furthermore, any disclosure of specific tradecraft and/or technology may cause serious risk to investigators if the criminal element can identify and locate people using MDI equipment. So there are obvious concerns about releasing technical data.

RCMP MEDIA: Okay so thank you everybody, I hope this was useful to you, and we will see what we can forward to you within the next hour as to the Jeff's statements and everything. Right now we might only have it in English but whatever please go through me I'll be in touch with you through email...