St-Denis, Sylvie

From: McCreery, Matthew
Sent: 2017-Apr-13 2:12 PM
To: St-Denis, Sylvie
Subject: FW: Emailing: Questions raised on privacy, trust in our justice system.htm

Here you go.

Cheers.

Matthew McCreery
Counsel | Conseiller juridique
Department of Justice Canada | Ministère de la Justice Canada
284 Wellington Street, Room 3155 | 284 rue Wellington, pièce 3155
Ottawa (Ontario) K1A 0H8
tel. | tél.: (613) 957-4627
fax | téléc.: (613) 941-2002
Email | Courriel: matthew.mccreery@justice.gc.ca
Government of Canada | Gouvernement du Canada

From: McCreery, Matthew
Sent: Thursday, April 13, 2017 12:47 PM
To: Clervoix, Magali <Magali.Clervoix@justice.gc.ca>; Bastien, Melanie <Melanie.Bastien@justice.gc.ca>
Subject: FW: Emailing: Questions raised on privacy, trust in our justice system.htm

Cheers.

Matthew McCreery
Counsel | Conseiller juridique

Department of Justice Canada | Ministère de la Justice Canada
284 Wellington Street, Room 3155 | 284 rue Wellington, pièce 3155
Ottawa (Ontario) K1A 0H8
tel. | tél.: (613) 957-4627
fax | téléc.: (613) 941-2002
Email | Courriel: matthew.mccreery@justice.gc.ca
Government of Canada | Gouvernement du Canada

From: Prescott, D. Mark
Sent: Tuesday, March 21, 2017 9:32 AM
To: JUS.L OTT CIPL Lawyers / Avocat es CDIPRP OTT L.JUS <DL-ILAP_LAWYERS@justice.gc.ca>
Subject: Emailing: Questions raised on privacy, trust in our justice system.htm

published: 2017-03-21
received: 2017-03-21 03:35 (EST)
Montreal Gazette (EARLY)
CITY | A4, Words: 518

Questions raised on privacy, trust in our justice system

by: JESSE FEITH

When the RCMP announced the first batch of arrests resulting from an investigation dubbed Project Clemenza back in 2014, it proudly boasted the force had intercepted more than a million private cellphone messages through the use of wireless signal interception techniques.

The techniques, in part, had allowed it to dismantle two groups operating within the Montreal Mafia, eventually leading to dozens of arrests for charges including drug-trafficking, assault, extortion, kidnapping and arson.

But now federal prosecutors are set to seek a stay of proceedings in the cases on Tuesday, a decision that is being linked back to those intercepted cellphone messages. Though the Crown is not required to divulge why it will cease prosecuting a case, it's believed one of the factors behind the decision is the RCMP's refusal to disclose how it was able to intercept the Blackberry messages in the first place.

It's a decision that not only raises privacy concerns, but one that could also further undermine the public's trust in the criminal justice system, experts said on Monday.

"If that is the core reason, it's a really serious problem," said Christopher Parsons, a research associate with the Citizen Lab at the University of Toronto's Munk School of Global Affairs.

Across the country, Parsons said, law enforcement agencies are using devices known as "IMSI catchers" or as they're called in Canada, "mobile device identifiers."

The devices, widely believed to have been used during Project Clemenza, essentially mimic a cellular tower, allowing law enforcement to gather information and communications from nearby phones that connect to it.

But police have been hesitant to release information about how the devices work, Parsons said.

If the Project Clemenza cases had gone to trial, the Crown would have had to reveal the full extent to which the RCMP relied on the devices, exposing the technique to defence lawyers rightfully trying to determine exactly how accurate and reliable they are.

"I think the police are mindful that these devices are challenging to develop and operate and may not sustain under cross-examination," Parsons said.

"They want to be able to continue using them, and if they're found to be significantly flawed devices, then their perceived value and utility may decrease."

For Pierre de Champlain, a former RCMP intelligence analyst and author of books about organized crime, the decision to stay the charges is also likely to have troubling consequences in Montreal.

"It will certainly further undermine people's trust in the criminal justice system," de Champlain said, adding that anyone should be concerned when the prosecution decides to abandon cases against people with links to organized crime.

De Champlain said it seems as though, is some ways, Project Clemenza is becoming the equivalent of the SharQc trial, in which several alleged Hells Angels members had their charges stayed due to unreasonable delays.

The news probably also came as a relief to a Montreal Mafia that's currently in a state of disarray, de Champlain added, and could give those expected to see their charges stayed a new-found "sense of invisibility."

"Unfortunately," he said, "society is the real loser in all of this." jfeith@postmedia.com Twitter.com/jessefeith

Cyr, Lita

From: Prescott, D. Mark
Sent: 2017-Apr-12 8:57 AM
To: JUS.L OTT CIPL Lawyers / Avocat es CDIPRP OTT L.JUS
Subject: Emailing: Cellphone surveillance technology being used by local police across Canada.htm

published: 2017-04-12 05:00 (EST)

received: 2017-04-12 08:35 (EST)

CBC.ca: Technology & Science

Words: 1,101

Cellphone surveillance technology being used by local police across Canada

At least six police forces across Canada are now using cellphone surveillance technology, but several of them won't say whether they use the devices to eavesdrop on phone calls and text messages.

Calgary police, Ontario Provincial Police and Winnipeg police all confirmed to CBC News they own the devices - known as IMSI catchers, cell site simulators or mobile device identifiers (MDIs) - joining the RCMP, which has used the technology for its own investigations and to assist Toronto and Vancouver police.

While Ontario and Winnipeg police refused to say whether they use the technology to intercept private communications, Calgary police and the RCMP insist they only deploy their IMSI catchers to identify - and occasionally, in the RCMP's case, track - cellular devices.

Police have described the surveillance devices as a "vital tool" used under warrant to help pinpoint suspects, and as a first step toward applying for wiretaps in serious criminal and national security investigations.

But Micheal Vonn, policy director of the B.C. Civil Liberties Association and a legal expert on privacy, says she's concerned there isn't a warrant process specific to IMSI catchers that establishes strict limits on how the technology is used given its potential for mass surveillance.

"It's nothing but a policy choice for some law enforcement not to use the content interception capabilities," said Vonn, referring to features some IMSI catchers have to eavesdrop on any cellphone within a radius of several blocks. It's hard to believe "the tantalizing availability of such technology is not going to be exploited," she said. "It will."

In an unprecedented briefing with reporters last week, the RCMP insisted that its IMSI catchers cannot currently intercept calls, text messages and other private communication.

After a decade of silence, the RCMP revealed it owns 10 IMSI catchers, which were used in 19 criminal investigations last year and another 24 in 2015 - including emergency cases such as kidnappings or imminent threats to public safety.

Survey of police forces

CBC News has since contacted 30 provincial and municipal police forces across Canada to ask how many IMSI catchers they own, the number of operators trained to use them, and how many times the technology was used in 2015 and 2016.

Only Calgary police answered in full.

Ryan Jepson, the head of Calgary police's technical operations section, said his force has owned one IMSI catcher since 2015. It was used in six investigations that year, and eight more in 2016.

He says the device is only deployed by "a very small group of trained operators" within his unit, and is only used to identify suspects' devices - not track their location or collect the content of their communications.

"It's the same as the RCMP. We don't intercept private communications," Jepson said.

Ontario Provincial Police and Winnipeg police each possess at least one IMSI catcher, but declined to discuss:

- Whether their technology is used to capture the contents of communications.

- How many technicians are trained to operate the technology.

- The number of investigations in which the device was used in 2015 and 2016.

Both forces said revealing more information could jeopardize ongoing investigations, court proceedings, and public and officer safety. But Jepson in Calgary disagrees.

"I have no issues with being transparent about it. It was never the intent to be secretive," he said. "It was about being able to protect certain techniques."

Others deny use

Several police forces told CBC News they neither own nor use IMSI catcher technology, including Charlottetown police; the forces in Thunder Bay, Sudbury, Halton and London, Ont.; and in Quebec City, Laval and Gatineau, and the Quebec Provincial Police.

Police in Montreal, Regina, Halifax, Ottawa, Niagara and Windsor, Ont., declined to comment, citing policies not to discuss investigative techniques.

- CBC INVESTIGATES | Someone is spying on cellphones in the nation's capital

And police from York Region, Peel Region, Hamilton, Kingston and Waterloo in Ontario, as well as Victoria and the Royal Newfoundland Constabulary either didn't respond in time for publication, or ignored CBC's requests completely.

Durham Regional Police east of Toronto also ignored repeated requests from CBC to discuss IMSI catcher use, despite applying for a broad federal licence last summer that would allow the force to purchase such a device.

RCMP helps other forces

It's still not clear whether police in Toronto and Vancouver also own and operate their own IMSI catchers, but CBC News has learned that the RCMP has used the technology on behalf of both forces in the past.

Edmonton police said they don't own an IMSI catcher, but declined to say how many times they've used the technology during the past two years - or whether another police force helped them to do so.

The technique has been used in multiple Toronto police investigations, but in Vancouver it may have only been deployed once - in an emergency situation involving a missing person in 2007.

"The Device was used in an attempt to locate or verify the presence of a specific and known cellular phone," wrote Darrin Hurwitz, legal counsel for Vancouver police's access and privacy section, in response to a July 2016 Freedom of Information request from PIVOT Legal Society. "VPD does not own and has never owned this Device."

Vancouver police didn't respond to multiple requests for comment, including about whether the force received additional RCMP assistance or obtained its own device since last summer.

Toronto police spokesperson Mark Pugash wrote in an email that they "do not discuss investigative techniques."

Calls for rules

Watchdog groups have called for specialized warrants and better public reporting of how the devices are being used.

"We want the police to have the appropriate tools," said Vonn of the B.C. Civil Liberties Association. "That they don't have the appropriate oversight and that those tools have the potential for abuse [...] the public cares very much about that."

The Office of the Privacy Commissioner of Canada is investigating the RCMP's use of IMSI catchers, following a complaint filed last year.

"What I can tell you is that we are looking at what type of information the IMSI devices and associated software used by the RCMP are capable of capturing," spokesperson Tobi Cohen wrote in an email. "For instance, can and do they only capture the unique identifiers associated with a mobile device or are they also capable of capturing private voice, text and email communications."

Her office called the lack of transparency "a concern," and supports regular public reporting on the use and effectiveness of new technological powers - something the RCMP has said it could support.

For the online article click here.

Thibeault, Alexandre

From: Thibeault, Alexandre
Sent: April-10-17 11:37 AM
To: Ward, Eric; Prescott, D. Mark; JUS.L OTT CIPL Lawyers / Avocat es CDIPRP OTT L.JUS
Subject: RE: Emailing: Regulate use of surveillance devices by police forces.htm

CONTAINS SOME SOLICITOR-CLIENT PRIVILEGED / DELIBERATIONS / ADVICE

Thank you Eric for sharing.

[redacted]

Alexandre

From: Ward, Eric
Sent: April-10-17 11:20 AM
To: Prescott, D. Mark <Mark.Prescott@justice.gc.ca>; JUS.L OTT CIPL Lawyers / Avocat es CDIPRP OTT L.JUS <DL-ILAP_LAWYERS@justice.gc.ca>
Subject: RE: Emailing: Regulate use of surveillance devices by police forces.htm

CONTAINS SOME SOLICITOR-CLIENT PRIVILEGED / DELIBERATIONS / ADVICE

Thanks Mark.

[redacted]

Eric

From: Prescott, D. Mark
Sent: Monday, April 10, 2017 9:15 AM
To: JUS.L OTT CIPL Lawyers / Avocat es CDIPRP OTT L.JUS <DL-ILAP_LAWYERS@justice.gc.ca>
Subject: Emailing: Regulate use of surveillance devices by police forces.htm

published: 2017-04-10
received: 2017-04-10 07:35 (EST)
Toronto Star.com
OPINION | EDITORIAL COVERAGE | T, Words: 598

Regulate use of surveillance devices by police forces

Editorial

by: Star Editorial Board

Finally, the RCMP has admitted what journalists, parliamentarians, privacy watchdogs and democracy advocates have suspected for years. The federal police force has been surreptitiously using spy technology to collect Canadians' cellular details, including tracking where they are.

As disturbing as that admission is, it's also a welcome step forward. Now that it's acknowledged, citizens and parliamentarians can debate - and legislate - how and when the devices should be used. Until now, it's been the Wild West.

Chief Superintendent Jeff Adam acknowledged last week that the RCMP used the so-called stingrays or "mobile device identifiers" multiple times in 19 cases in 2016 and 24 in 2015

He also made clear that other police forces in the country are using the technology. But it's still not known how many times it has been used in total.

Adam said the identifiers are used simply to "identify and locate a suspect in a criminal investigation." But the problem is that the technology doesn't distinguish between suspects in criminal cases and ordinary citizens.

That has privacy experts worried. Stingrays, which imitate a cell phone tower, act like a "drag net" that puts the privacy of potentially tens of thousands of innocent, law-abiding people at risk, warns Ann Cavoukian, the director of the Privacy and Big Data Institute at Ryerson University.

Worse, once the "metadata" - information relating to phone numbers, SIM cards or handset identifiers - is collected it is kept by the RCMP. "Surely the data (that is not needed) should be deleted," Cavoukian sensibly points out.

That's how it works elsewhere. In the United States, the government is required to destroy within 48 hours any information obtained through this kind of surveillance that is unrelated to an investigation. Other countries have laws requiring that all citizens whose data has been incidentally caught up in the net must be informed.

Canada has no such protections, since before last week no one had publicly acknowledged that the devices were being used. At this point, Adam said, the RCMP is required to get judicial authorization before using the devices, except in extremely urgent cases to prevent death or imminent harm.

The technology, he said, is used to identify a user's "basic subscriber information," such as the name and address connected to the phone. Then police can seek additional warrants to track the device or conduct a wiretap to capture communications.

But here too, Cavoukian suggests, there is a need for independent oversight to ensure the technology (never mind the data that is mined) is not abused.

In addition to privacy concerns, the devices also raise safety issues. Because they mimic cell towers, anyone caught in their zone who is dialing 911 would not be able to get through.

That's a risk the RCMP has tried to minimize by advising stingray operators to use the devices for only three minutes at a time and to shut them down if they realize anyone is trying to call 911.

Still, there is a danger that something could go horribly wrong in an emergency.

For the police, the privacy downside to using the devices is outweighed by their usefulness. "This capability can be used to further criminal investigations relating to national security, serious organized crime and other serious Criminal Code offences that impact the safety and security of Canadians," said Adam.

Maybe so, but police should not be given free rein to invade our privacy indiscriminately.

Now that the RCMP has admitted Canadian police forces use these devices, the government must step up to regulate their use and ensure that data gathered from innocent Canadians is destroyed.

Photo: RCMP Chief Superintendent Jeff Adam admits the RCMP and other Canadian police forces use spy technology that gathers cellular information on potentially thousands of people.

Ward, Eric

From: Ward, Eric
Sent: Monday, April 10, 2017 12:21 PM
To: Wong, Normand
Subject: RE: Emailing: Regulate use of surveillance devices by police forces.htm

Categories: Red Category

[redacted]

Happy to discuss anytime.

Eric

From: Wong, Normand
Sent: Monday, April 10, 2017 12:17 PM
To: Ward, Eric <Eric.Ward@justice.gc.ca>
Subject: RE: Emailing: Regulate use of surveillance devices by police forces.htm

[redacted]

Normand Wong
613.941.2341 o
613.791.4669 m

From: Ward, Eric
Sent: 2017-Apr-10 12:07 PM
To: Wong, Normand <Normand.Wong@justice.gc.ca>
Subject: FW: Emailing: Regulate use of surveillance devices by police forces.htm

Hi Normand,

[redacted]

Eric

From: Ward, Eric
Sent: Monday, April 10, 2017 11:20 AM
To: Prescott, D. Mark <Mark.Prescott@justice.gc.ca>; JUS.L OTT CIPL Lawyers / Avocat es CDIPRP OTT L.JUS <DL-ILAP_LAWYERS@justice.gc.ca>
Subject: RE: Emailing: Regulate use of surveillance devices by police forces.htm

CONTAINS SOME SOLICITOR-CLIENT PRIVILEGED / DELIBERATIONS / ADVICE

Thanks Mark.

[redacted]

Eric

From: Prescott, D. Mark
Sent: Monday, April 10, 2017 9:15 AM
To: JUS.L OTT CIPL Lawyers / Avocat es CDIPRP OTT L.JUS <DL-ILAP_LAWYERS@justice.gc.ca>
Subject: Emailing: Regulate use of surveillance devices by police forces.htm

published: 2017-04-10
received: 2017-04-10 07:35 (EST)
Toronto Star.com
OPINION | EDITORIAL COVERAGE | T, Words: 598

Regulate use of surveillance devices by police forces

Editorial

by: Star Editorial Board

Finally, the RCMP has admitted what journalists, parliamentarians, privacy watchdogs and democracy advocates have suspected for years. The federal police force has been surreptitiously using spy technology to collect Canadians' cellular details, including tracking where they are.

As disturbing as that admission is, it's also a welcome step forward. Now that it's acknowledged, citizens and parliamentarians can debate - and legislate - how and when the devices should be used. Until now, it's been the Wild West.

Chief Superintendent Jeff Adam acknowledged last week that the RCMP used the so-called stingrays or "mobile device identifiers" multiple times in 19 cases in 2016 and 24 in 2015

He also made clear that other police forces in the country are using the technology. But it's still not known how many times it has been used in total.

Adam said the identifiers are used simply to "identify and locate a suspect in a criminal investigation." But the problem is that the technology doesn't distinguish between suspects in criminal cases and ordinary citizens.

That has privacy experts worried. Stingrays, which imitate a cell phone tower, act like a "drag net" that puts the privacy of potentially tens of thousands of innocent, law-abiding people at risk, warns Ann Cavoukian, the director of the Privacy and Big Data Institute at Ryerson University.

Worse, once the "metadata" - information relating to phone numbers, SIM cards or handset identifiers - is collected it is kept by the RCMP. "Surely the data (that is not needed) should be deleted," Cavoukian sensibly points out.

That's how it works elsewhere. In the United States, the government is required to destroy within 48 hours any information obtained through this kind of surveillance that is unrelated to an investigation. Other countries have laws requiring that all citizens whose data has been incidentally caught up in the net must be informed.

Canada has no such protections, since before last week no one had publicly acknowledged that the devices were being used. At this point, Adam said, the RCMP is required to get judicial authorization before using the devices, except in extremely urgent cases to prevent death or imminent harm.

The technology, he said, is used to identify a user's "basic subscriber information," such as the name and address connected to the phone. Then police can seek additional warrants to track the device or conduct a wiretap to capture communications.

But here too, Cavoukian suggests, there is a need for independent oversight to ensure the technology (never mind the data that is mined) is not abused.

In addition to privacy concerns, the devices also raise safety issues. Because they mimic cell towers, anyone caught in their zone who is dialing 911 would not be able to get through.

That's a risk the RCMP has tried to minimize by advising stingray operators to use the devices for only three minutes at a time and to shut them down if they realize anyone is trying to call 911.

Still, there is a danger that something could go horribly wrong in an emergency.

For the police, the privacy downside to using the devices is outweighed by their usefulness. "This capability can be used to further criminal investigations relating to national security, serious organized crime and other serious Criminal Code offences that impact the safety and security of Canadians," said Adam.

Maybe so, but police should not be given free rein to invade our privacy indiscriminately.

Now that the RCMP has admitted Canadian police forces use these devices, the government must step up to regulate their use and ensure that data gathered from innocent Canadians is destroyed.

Photo: RCMP Chief Superintendent Jeff Adam admits the RCMP and other Canadian police forces use spy technology that gathers cellular information on potentially thousands of people.

Cyr, Lita

From: Prescott, D. Mark
Sent: 2017-Apr-06 9:15 AM
To: JUS.L OTT CIPL Lawyers / Avocat es CDIPRP OTT L.JUS
Subject: Emailing: RCMP acknowledges using controversial spy tech to track cellphone data.htm

Note the highlighted passage referring to an investigation by the Office of the Privacy Commissioner

published: 2017-04-05

received: 2017-04-06 04:45 (EST)

Canadian Press Newswire

Words: 521

RCMP acknowledges using controversial spy tech to track cellphone data

OTTAWA _ The RCMP confirmed Wednesday what civil liberties groups say has been an open secret for them for some time: that the Mounties use so-called mobile device identifiers, also known as Stingrays, to identify and locate cellphones.

In a rare disclosure of police tactics, the national police force acknowledged in a statement that it used the technology 19 times last year, but insisted that it did so in compliance with the law and with judicial authorization.

The Mounties say the devices can identify and locate cellular devices, such as a mobile phone, enabling police to identify and apprehend a criminal suspect or locate a missing person.

The RCMP does not intercept phone calls, email or text messages, contact lists, images, encryption keys or basic subscriber information, the statement said.

The disclosure, a rarity for the RCMP, followed a CBC report that someone in downtown Ottawa has been using a device known as an "IMSI catcher," which can intercept and identify cellphone metadata.

The CBC report found the device being used in recent months in close proximity to Parliament Hill and the U.S. and Israeli embassies, among other locations.

Brenda McPhail of the Canadian Civil Liberties Association said the technology casts far too broad a net to be used by police, since it captures the data of innocent people who might be in range of the device.

The federal privacy commissioner's office acknowledged Wednesday that it is investigating the use of the IMSI devices following a complaint by OpenMedia, a self-described crowd-sourced civic engagement platform for the Internet community.

The technology works by momentarily connecting to cellphones in its immediate proximity, before returning them to their own networks. It collects metadata associated with the phones, allowing the operator to identify the phone used by the suspect.

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

Except for cases where there is an immediate threat of death or serious harm, police must obtain warrants to use the devices, it added.

McPhail, the association's director of privacy, technology and surveillance, said the RCMP has long refused to confirm or deny that it used Stingrays.

"These devices are not about targeted surveillance, they're indiscriminate," McPhail said.

"They mimic a cellphone tower and they scoop up the data of everybody who has an active cellphone in a large area. In order to find the information of one suspect or a small group of suspects, you're capturing the information of thousands of innocent bystanders at the same time. So it's a dragnet."

She said since the Mounties refused to admit they used the technology, there was no way to discuss the implications.

"Canadians have a right to know when it comes to invasive surveillance technologies not only that they're being used, but that they're being used lawfully," McPhail said.

Added Laura Tribe, executive director of OpenMedia: "Now that the RCMP has come clean, can we finally have the public debate about privacy and accountability that Canadians deserve?"

Cyr, Lita

From: Prescott, D. Mark
Sent: 2017-Apr-06 9:00 AM
To: JUS.L OTT CIPL Lawyers / Avocat es CDIPRP OTT L.JUS
Subject: Emailing: RCMP admit using 'identifier technology' to track cellphones.htm

published: 2017-04-06

received: 2017-04-06 03:25 (EST)

Toronto Star (ONT)

NEWS | A1, Words: 979

RCMP admit using 'identifier technology' to track cellphones

Some privacy advocates want practice scrapped, saying it gathers info on thousands of innocent Canadians

by: Robert Cribb and Jesse Winter Toronto Star

The RCMP used controversial spy technology to track cellphone data in 19 criminal investigations last year - the first official public acknowledgement that the force uses surreptitious devices to collect Canadians' cellular details.

In a rare briefing with reporters from the Toronto Star, CBC and the Globe and Mail Wednesday morning, RCMP Chief Superintendent Jeff Adam said his force owns 10 so-called "mobile device identifier" (MDI) devices with the ability to gather high-level data about the phone's location - but not private communications.

"We will confirm officially that the RCMP possesses and uses mobile identifier technology in order to identify and locate a suspect in a criminal investigation," he said. "This capability can be used to further criminal investigations relating to national security, serious organized crime and other serious Criminal Code offences that impact the safety and security of Canadians."

Adam called the technology a "very important investigative tool for us."

Adam said the devices identify a suspect's cellphone by gathering "very limited" signalling information in a given vicinity and collecting unique identification information from the phone - called International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity numbers (IMEI).

"What the RCMP technology does not do is collect private communications," Adam said.

That includes voice and audio communications, email messages, text messages, contact lists, images, encryption keys or basic subscriber information, he said.

While MDI technology does allow for the collection of personal communications, the RCMP uses equipment that - by policy - does not capture private communications, said Adam. He would not identify the specific model of MDI device the RCMP uses.

But Brenda McPhail, director of privacy, technology and surveillance at the Canadian Civil Liberties Association, said even metadata collection is an invasion of privacy.

"Metadata includes location information. That is intimately personal. The fact that they only collect metadata doesn't let them off the hook," she said.

The same MDI technology used to target a suspect will also gather up the cellular data of many other Canadians, Adam confirmed.

"All of that information is evidence," he said. "The judge is informed of what we got and where we're going to keep it . . . It will not be accessed, other than the target information, again."

Cellphone data collected with the MDI devices is sealed, treated as an exhibit and retained for court purposes and can be later destroyed "in accordance to records management principles," Adam said.

But that assurance isn't good enough for some privacy experts.

Ontario's former privacy commissioner, Ann Cavoukian, said the "drag net" nature of the technology puts the privacy of potentially tens of thousands of innocent, law-abiding people at risk.

"Surely that data should be deleted. It certainly shouldn't be retained, I totally reject that," Cavoukian said. "The data that is secured, that is not needed, why would that data be retained at all?"

Now the director of the Privacy and Big Data Institute at Ryerson University, Cavoukian said the government should be destroying data that's not related to investigations as soon as it's identified and called for much more stringent oversight to ensure that the technology isn't abused.

"Who's auditing this? You need independent eyes on this, someone completely unrelated to law enforcement to do an exhaustive audit and oversight. There's no independent oversight over this," she said.

Joseph Hickey, the executive director of the Ontario Civil Liberties Association, wants to see the technology done away with altogether.

"It's unacceptable," Hickey said.

"It's too broad. It's completely unpredictable who will be caught up in it. We should draw the line at not using this kind of technology. It's hard to imagine how that could be justified in a free and democratic society," Hickey said.

Adam said the technology is used, "in full compliance with Canadian law which includes the charter of rights, the Criminal Code of Canada and proper judicial processes."

In cases where the RCMP believes a suspect is using a cellphone to conduct criminal activity, they can deploy the tool for a few moments at a time to collect cellular device information, said Adam.

Use of the MDI technology can cause interference with cellular signals in the immediate area, including 911 calls, he said.

"The RCMP makes every effort to . . . cause the least disruption to service and public safety," said Adam.

There are 24 RCMP officers certified to use the MDI devices across the country. Judicial authorization is required before using the devices except in "extremely urgent cases," Adam said, including preventing death or imminent harm. In those cases, the RCMP can use this technology and then get a judge's authorization after the fact, he said.

One of the 19 criminal investigations that involved use of the tools last year involved an "exigent circumstance such as a kidnapping," Adam said.

In 2015, RCMP officers used the devices in 24 criminal investigations, he said.

The technology could be deployed numerous times during each of those investigations, Adam confirmed.

"It is one of the only ways to identify a cellphone 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," Adam said.

Some other Canadian police forces have the devices as well, he said, without identifying them.

The use of the spy technology by the RCMP has long been met with silence from the force which has cited privacy around its investigation techniques.

That silence was broken following a CBC-Radio Canada story this week that reported the presence of spy technology being used in the area around Parliament Hill. Using a device that detects the spy equipment, journalists documented readings in December and January in downtown Ottawa, the CBC reported.

The identity of those using the technology is not known. On Tuesday, Public Safety Minister Ralph Goodale announced an investigation by the RCMP and CSIS.

s.21(1)(a)

s.21(1)(b)

Cyr, Lita

From: Jarvis, Brian
Sent: 2017-Apr-05 10:22 AM
To: Prescott, D. Mark; JUS.L OTT CIPL Lawyers / Avocat es CDIPRP OTT L.JUS
Subject: RE: RCMP, CSIS launch investigations into phone spying on Parliament Hill after CBC story - Politics - CBC News

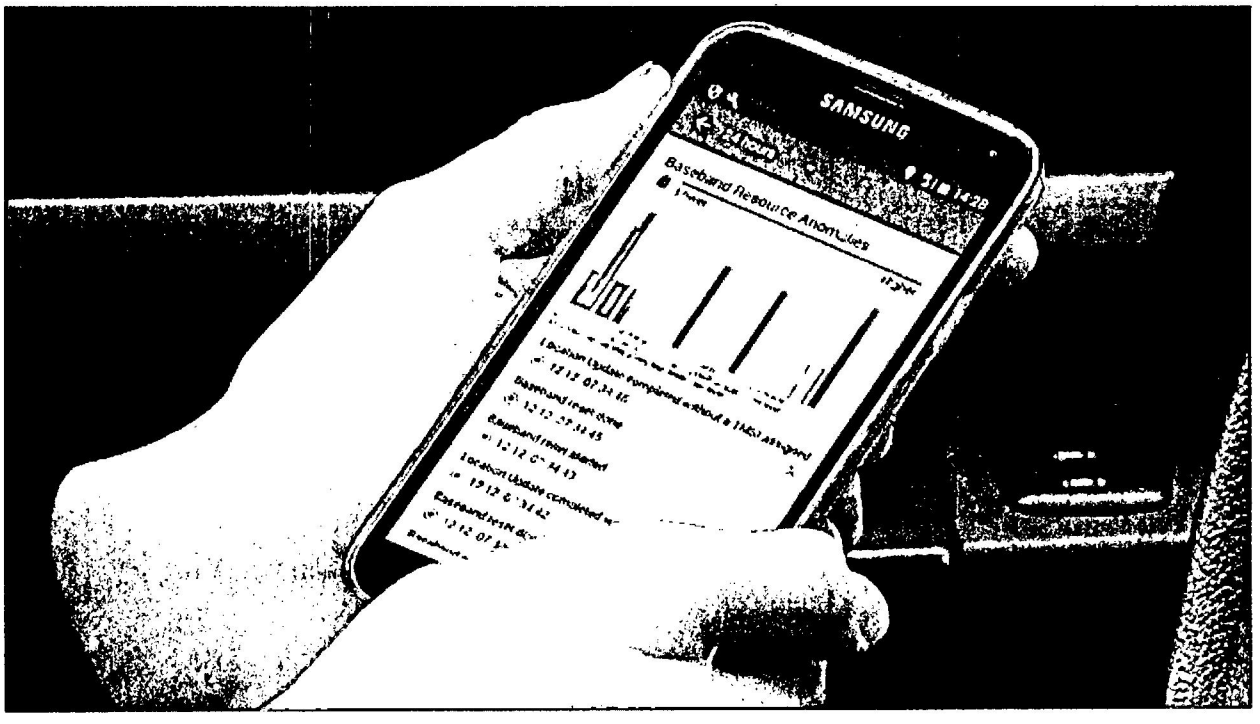
[redacted]

From: Prescott, D. Mark
Sent: April 5, 2017 10:13 AM
To: JUS.L OTT CIPL Lawyers / Avocat es CDIPRP OTT L.JUS <DL-ILAP_LAWYERS@justice.gc.ca>
Subject: FW: RCMP, CSIS launch investigations into phone spying on Parliament Hill after CBC story - Politics - CBC News

http://www.cbc.ca/news/politics/goodale-spying-investigation-phone-1.4055107

RCMP, CSIS launch investigations into phone spying on Parliament Hill after CBC story

Public Safety Minister Ralph Goodale says Canadian agencies not involved in spying



CBC and Radio-Canada purchased a special cellphone that can detect when an IMSI catcher is trying to intercept it. It is made by ESD America. (CBC)

Public Safety Minister Ralph Goodale says the RCMP and CSIS have launched investigations in response to a CBC News/Radio-Canada report, which revealed that someone is using devices that track and spy on cellphones in the area around Parliament Hill.

"Obviously we are very anxious to determine who lies at the source of this activity and that's why both CSIS and the RCMP are investigating," Goodale said.

"We want to make sure that we get to the bottom of this and find out the facts and the RCMP and CSIS are in the best position to do that."

Goodale confirms the spying was not being done by a Canadian agency using International Mobile Subscriber Identity (IMSI) catchers. But he could not say whether those using the IMSI catchers might be domestic organized crime, a foreign intelligence agency or some other source.

- **Someone is spying on cellphones in the nation's capital**
- **Mounties conducted unauthorized surveillance of 2 journalists**
- **Federal officials approved Winnipeg police spying devices**

CBC News and Radio-Canada spent months investigating the use of IMSI catchers in and around Parliament Hill in Ottawa.

The devices work by mimicking a cellphone tower to interact with nearby phones and read the unique ID associated with a phone.

Some catchers can go further

The problem with certain IMSI catchers is they can go a bit further, according to cybersecurity expert Daniel Tobok.

"[Some] can actually intercept your voice communication, your data communication. So your voice calls can be recorded, your text messages could be read," Tobok said in an interview on CBC News Network's *Power & Politics*.

"That is one of the problems. Somebody could actually intercept your communication and have access into your personal information on your phone."

Tobok said some devices can even intercept encrypted communication applications.

"When somebody casts a very large net and intercepts everything that comes through, then they could have time to potentially decrypt the WhatsApps of the world and any other type of encrypted communication. All depends on who you are dealing with," he told host Rosemary Barton.

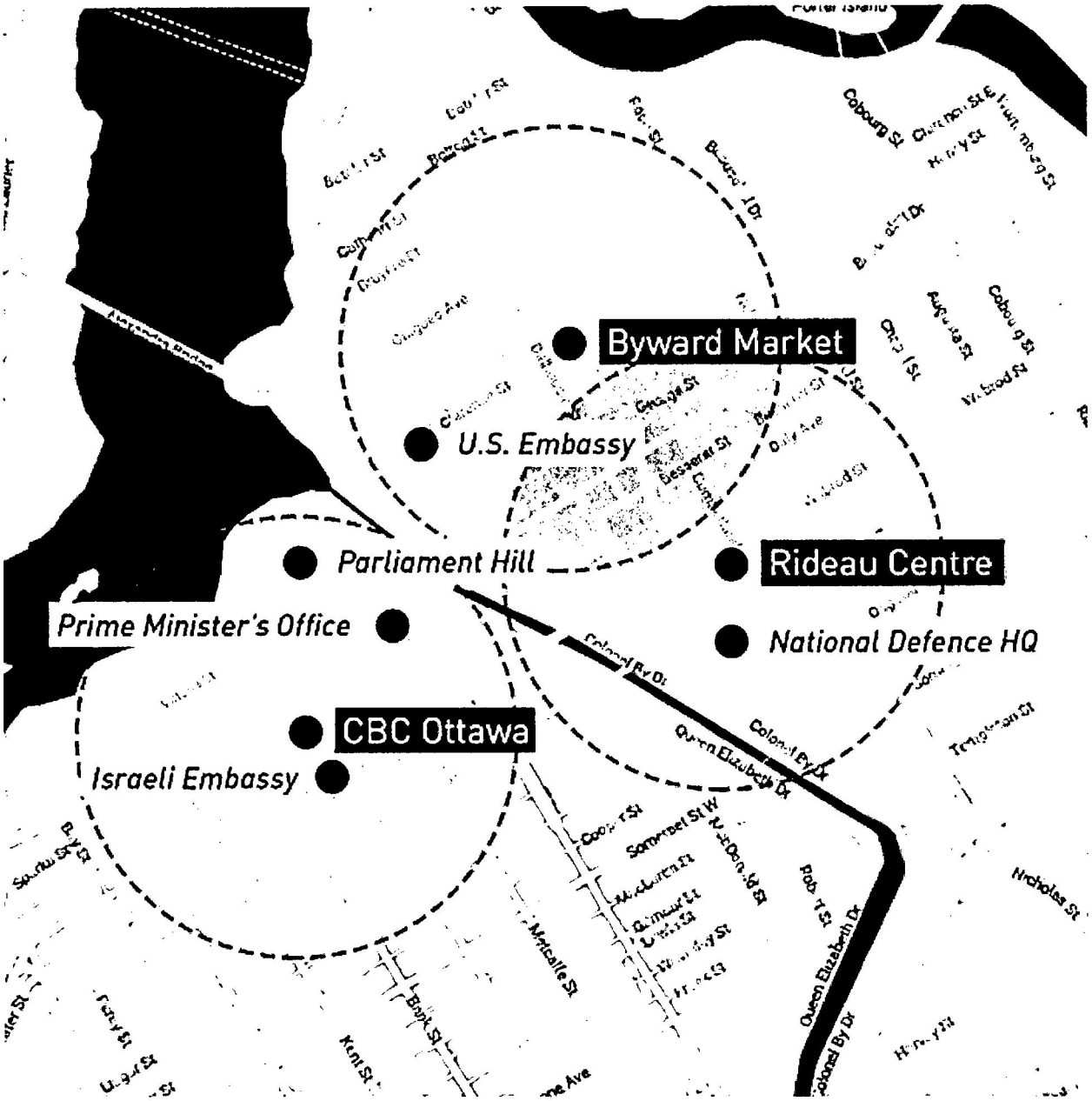
It is unclear what kind of IMSI catcher or catchers are being used in the Ottawa area.

Devices detected around Parliament Hill

Reporters used a device that detects IMSI catchers created by the German company GSMK. While it looks like a regular cellphone, the CryptoPhone emits an alert when a fake cellphone antenna intercepts its signal.

Media in the United States, Norway and Australia have done similar tests, but this is the first time it has been conducted by a media outlet in Canada.

During tests in December and January, the CryptoPhone set off alerts at locations around Parliament Hill, including the nearby Byward Market, the Rideau Centre shopping mall and CBC offices in downtown Ottawa.



The locations in black are where CBC/Radio-Canada detected IMSI catchers in Ottawa. The circles show the range the IMSI catchers could cover. (CBC)

Because IMSI catchers have a radius of about half a kilometre in an urban setting, the IMSI catchers CBC detected could reach territory including Parliament Hill, the Prime Minister's Office in Langevin Block, National Defence headquarters, as well as the U.S. and Israeli embassies.

CBC News and Radio-Canada then used even more sophisticated equipment called an Overwatch Sensor that confirmed the presence of an IMSI catcher close to Parliament Hill.

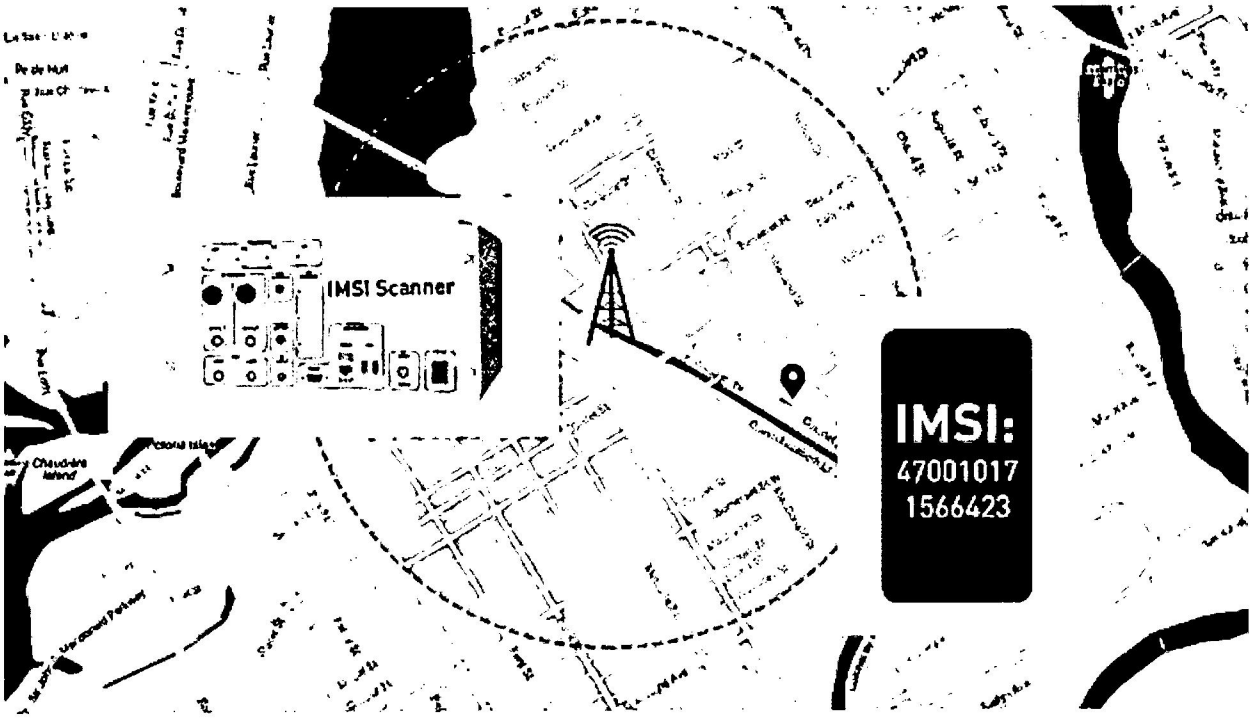
Sweeping sensitive areas and perimeters is definitely something the RCMP and CSIS should be doing, said Tobok.

Your identity can be 'harvested'

"As you are getting to what we call sensitive areas in the business, your phones, your potential identity is being harvested just to see if you are on a particular list ... Washington is very well known for this. Anywhere around Capitol Hill they usually know your IMI number and who's coming, who's going within a particular radius," said Tobok.

Goodale said that like most police and security services around the world, Canadian law enforcement and intelligence agencies use the technology in the course of their work, but only in compliance with the law.

"Both CSIS and the RCMP have the legal, and privacy, issues that are involved here under active ongoing assessment and reassessment to ensure that in a field where technology is rapidly changing all the time, that our Canadian agencies like CSIS and the RCMP are always staying squarely within the four corners of the law," Goodale said.



IMSI catchers pretend to be a cellphone tower to attract nearby cell signals. When it does, it can intercept the unique ID number associated with your phone, the International Mobile Subscriber Identity or IMSI. That number then can be used to track your phone. (CBC)

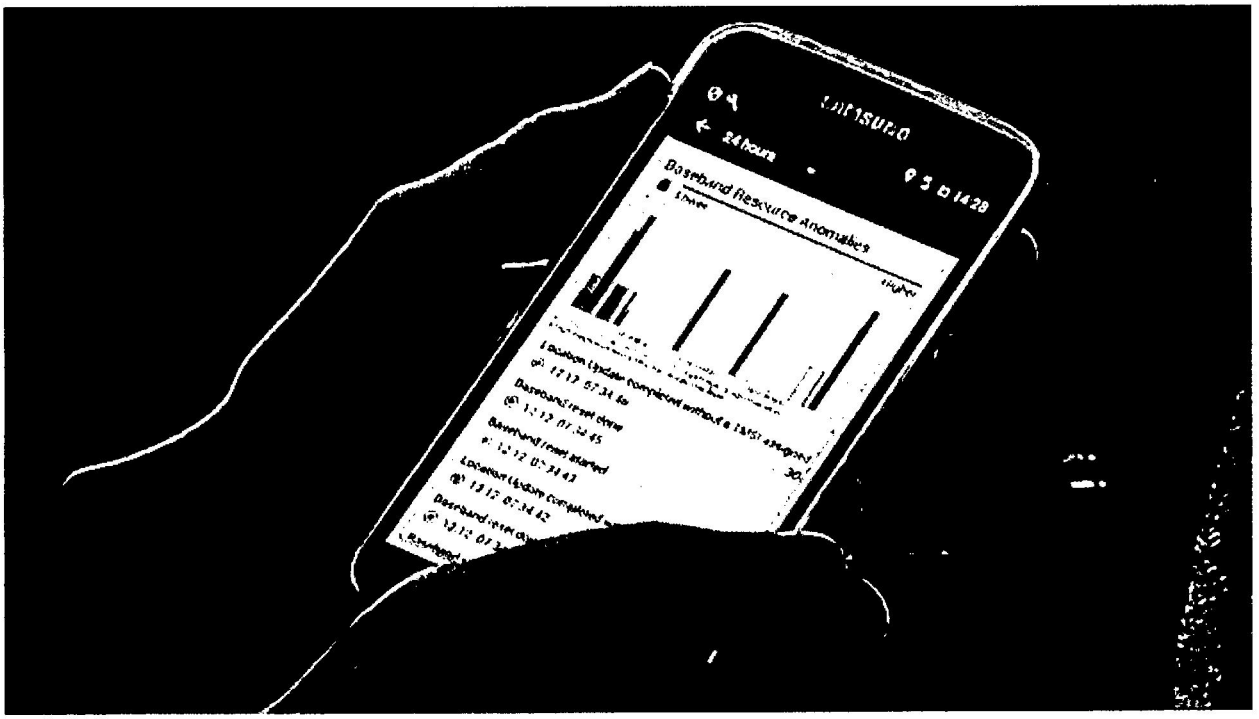
Cyr, Lita

From: Prescott, D. Mark
Sent: 2017-Apr-05 10:13 AM
To: JUS.L OTT CIPL Lawyers / Avocat es CDIPRP OTT L.JUS
Subject: FW: RCMP, CSIS launch investigations into phone spying on Parliament Hill after CBC story - Politics - CBC News

http://www.cbc.ca/news/politics/goodale-spying-investigation-phone-1.4055107

RCMP, CSIS launch investigations into phone spying on Parliament Hill after CBC story

Public Safety Minister Ralph Goodale says Canadian agencies not involved in spying



CBC and Radio-Canada purchased a special cellphone that can detect when an IMSI catcher is trying to intercept it. It is made by ESD America. (CBC)

Public Safety Minister Ralph Goodale says the RCMP and CSIS have launched investigations in response to a CBC News/Radio-Canada report, which revealed that someone is using devices that track and spy on cellphones in the area around Parliament Hill.

"Obviously we are very anxious to determine who lies at the source of this activity and that's why both CSIS and the RCMP are investigating," Goodale said.

"We want to make sure that we get to the bottom of this and find out the facts and the RCMP and CSIS are in the best position to do that."

Goodale confirms the spying was not being done by a Canadian agency using International Mobile Subscriber Identity (IMSI) catchers. But he could not say whether those using the IMSI catchers might be domestic organized crime, a foreign intelligence agency or some other source.

- **Someone is spying on cellphones in the nation's capital**
- **Mounties conducted unauthorized surveillance of 2 journalists**
- **Federal officials approved Winnipeg police spying devices**

CBC News and Radio-Canada spent months investigating the use of IMSI catchers in and around Parliament Hill in Ottawa.

The devices work by mimicking a cellphone tower to interact with nearby phones and read the unique ID associated with a phone.

Some catchers can go further

The problem with certain IMSI catchers is they can go a bit further, according to cybersecurity expert Daniel Tobok.

"[Some] can actually intercept your voice communication, your data communication. So your voice calls can be recorded, your text messages could be read," Tobok said in an interview on CBC News Network's *Power & Politics*.

"That is one of the problems. Somebody could actually intercept your communication and have access into your personal information on your phone."

Tobok said some devices can even intercept encrypted communication applications.

"When somebody casts a very large net and intercepts everything that comes through, then they could have time to potentially decrypt the WhatsApps of the world and any other type of encrypted communication. All depends on who you are dealing with," he told host Rosemary Barton.

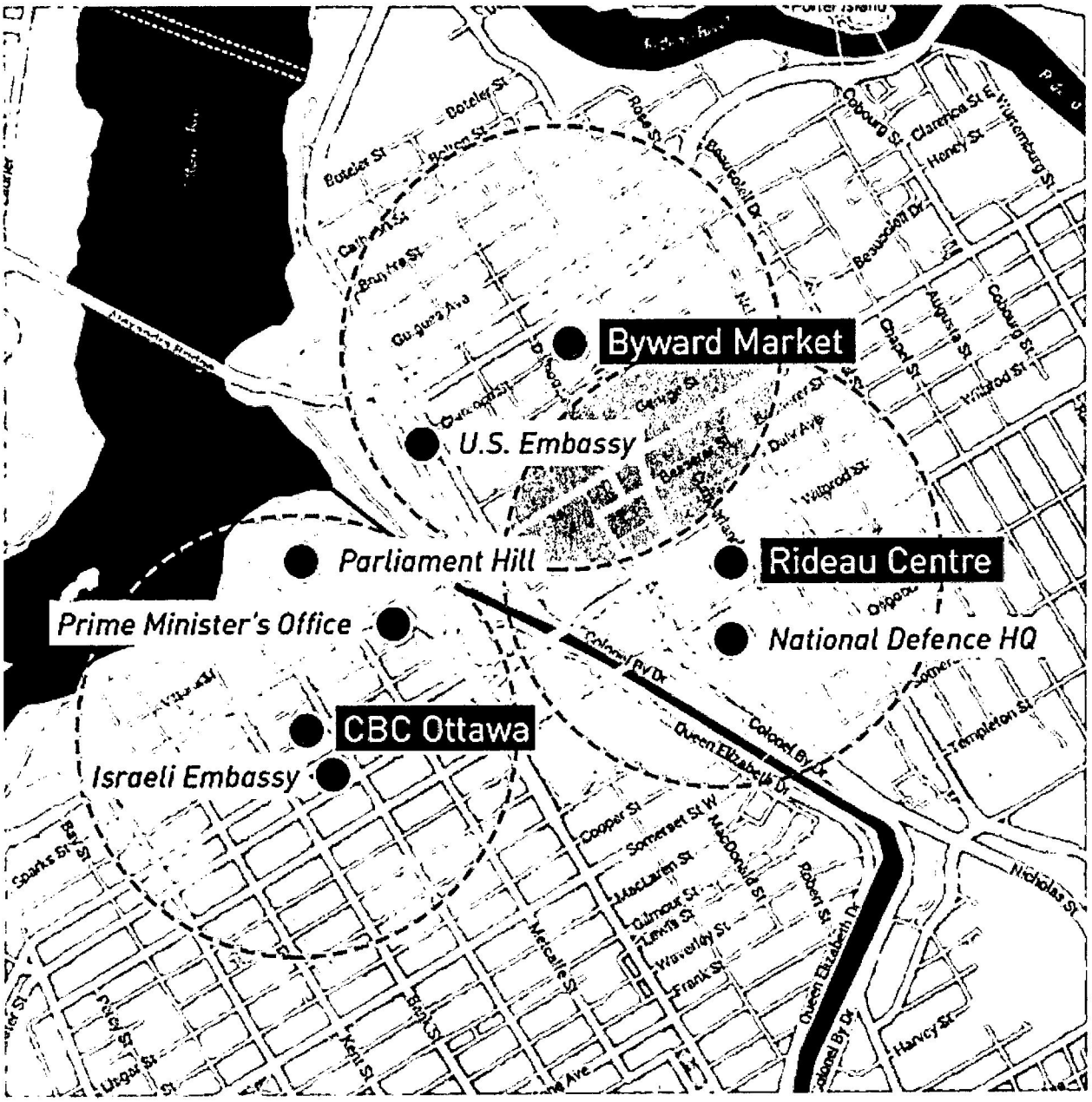
It is unclear what kind of IMSI catcher or catchers are being used in the Ottawa area.

Devices detected around Parliament Hill

Reporters used a device that detects IMSI catchers created by the German company GSMK. While it looks like a regular cellphone, the CryptoPhone emits an alert when a fake cellphone antenna intercepts its signal.

Media in the United States, Norway and Australia have done similar tests, but this is the first time it has been conducted by a media outlet in Canada.

During tests in December and January, the CryptoPhone set off alerts at locations around Parliament Hill, including the nearby Byward Market, the Rideau Centre shopping mall and CBC offices in downtown Ottawa.



The locations in black are where CBC/Radio-Canada detected IMSI catchers in Ottawa. The circles show the range the IMSI catchers could cover. (CBC)

Because IMSI catchers have a radius of about half a kilometre in an urban setting, the IMSI catchers CBC detected could reach territory including Parliament Hill, the Prime Minister's Office in Langevin Block, National Defence headquarters, as well as the U.S. and Israeli embassies.

CBC News and Radio-Canada then used even more sophisticated equipment called an Overwatch Sensor that confirmed the presence of an IMSI catcher close to Parliament Hill.

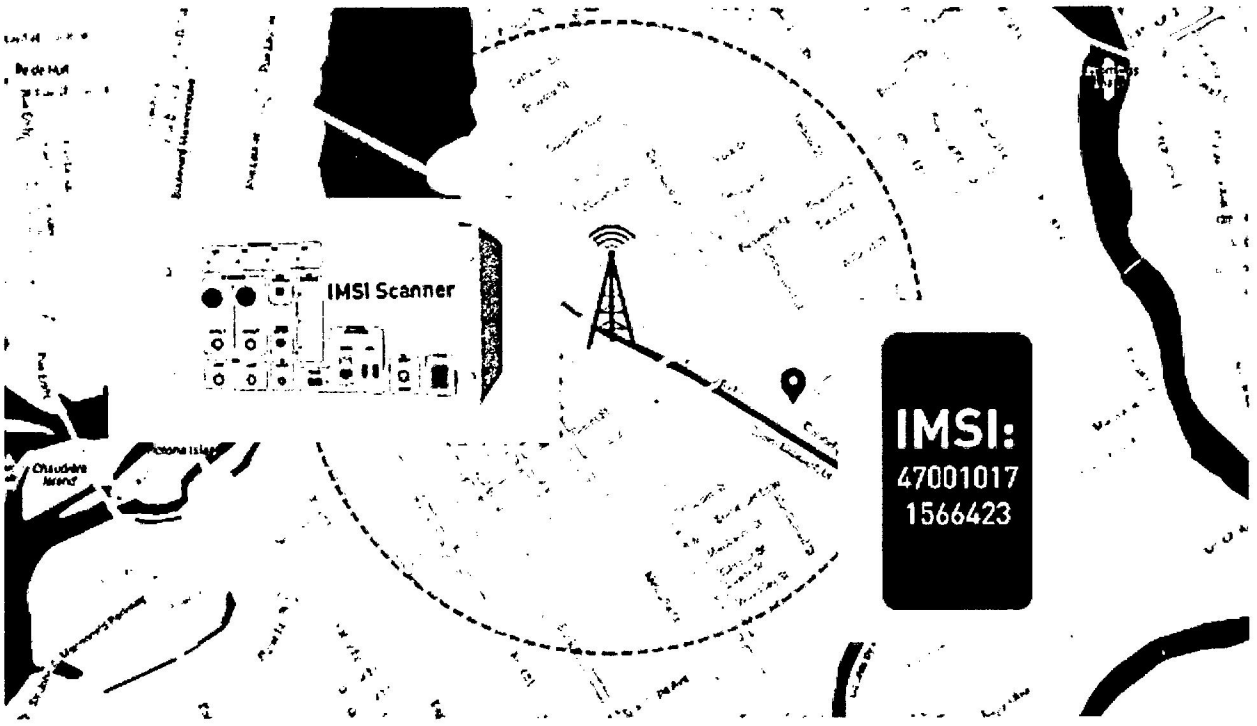
Sweeping sensitive areas and perimeters is definitely something the RCMP and CSIS should be doing, said Tobok.

Your identity can be 'harvested'

"As you are getting to what we call sensitive areas in the business, your phones, your potential identity is being harvested just to see if you are on a particular list ... Washington is very well known for this. Anywhere around Capitol Hill they usually know your IMI number and who's coming, who's going within a particular radius," said Tobok.

Goodale said that like most police and security services around the world, Canadian law enforcement and intelligence agencies use the technology in the course of their work, but only in compliance with the law.

"Both CSIS and the RCMP have the legal, and privacy, issues that are involved here under active ongoing assessment and reassessment to ensure that in a field where technology is rapidly changing all the time, that our Canadian agencies like CSIS and the RCMP are always staying squarely within the four corners of the law," Goodale said.



IMSI catchers pretend to be a cellphone tower to attract nearby cell signals. When it does, it can intercept the unique ID number associated with your phone, the International Mobile Subscriber Identity or IMSI. That number then can be used to track your phone. (CBC)

Prescott, D. Mark

From: McCreery, Matthew
Sent: April 4, 2017 9:19 AM
To: Prescott, D. Mark; JUS.L OTT CIPL Lawyers / Avocat es CDIPRP OTT L.JUS
Subject: RE: Emailing: Someone is spying on cellphones in the nation's capital.htm

Matthew McCreery
Counsel | Conseiller juridique
Department of Justice Canada | Ministère de la Justice Canada
284 Wellington Street, Room 3155 | 284 rue Wellington, pièce 3155
Ottawa (Ontario) K1A 0H8
tel. | tél.: (613) 957-4627
fax | téléc.: (613) 941-2002
Email | Courriel: matthew.mccreery@justice.gc.ca
Government of Canada | Gouvernement du Canada

From: Prescott, D. Mark
Sent: Tuesday, April 04, 2017 8:44 AM
To: JUS.L OTT CIPL Lawyers / Avocat es CDIPRP OTT L.JUS <DL-ILAP_LAWYERS@justice.gc.ca>
Subject: Emailing: Someone is spying on cellphones in the nation's capital.htm

published: 2017-04-03 17:00 (EST)
received: 2017-04-04 04:35 (EST)
CBC.ca: Canada
Words: 1,480

Someone is spying on cellphones in the nation's capital

A months-long CBC News/Radio-Canada investigation has revealed that someone is using devices that track and spy on cellphones in the area around Parliament Hill.

The devices are known as IMSI catchers and have been used by Canadian police and security authorities, foreign intelligence and even organized crime.

The devices, sometimes known by the brand name of one model, StingRay, work by mimicking a cellphone tower to interact with nearby phones and read the unique ID associated with the phone - the International Mobile Subscriber Identity, or IMSI.

That number can then be used to track the phone and by extension the phone's user. In some instances, IMSI catchers can even be used to gain access to a phone's text messages and listen in on calls.

At the heart of Canadian government

To do the investigation, our journalists used a device that detects IMSI catchers created by the German company GSMK. While it looks like a regular cellphone, the CryptoPhone emits an alert when a fake cellphone antenna intercepts its signal.

Media in the United States, Norway and Australia have done similar tests, but this is the first time it's been used by a media outlet in Canada.

During tests in December and January, the CryptoPhone set off alerts at locations around Parliament Hill, including the nearby Byward Market, the Rideau Centre shopping mall and CBC offices in downtown Ottawa.

Because IMSI catchers have a radius of about half a kilometre in an urban setting, the IMSI catchers CBC detected could reach territory including Parliament Hill, the Prime Minister's Office in Langevin Block, National Defence headquarters, as well as the U.S. and Israeli embassies.

We then used even more sophisticated equipment called an Overwatch Sensor that confirmed the presence of an IMSI catcher close to Parliament Hill.

Who is behind it?

We wanted to know more about who might be using the IMSI catcher or catchers that we detected, so we asked the U.S. supplier of the CryptoPhone to analyze the alerts we were getting.

ESD America specializes in counterintelligence and its clients include U.S. Homeland Security.

"Consistently you've been seeing IMSI catcher activity, definitely," said CEO and co-founder Les Goldsmith, when we took our results to the company's Las Vegas office.

We described the part of the city in which we detected the IMSI catchers - full of politicians, political staffers and civil servants.

"Somebody could be listening to calls right now and [the phone owners] have no idea," he said.

As for who might be behind it, Goldsmith says IMSI catchers are used by law enforcement, federal agencies as well as organized crime and foreign intelligence.

Based on the configurations suggested by CBC's results, he believes the IMSI catchers detected in Ottawa could be foreign made.

"We're seeing more IMSI catchers with different configurations and we can build a signature. So we're seeing IMSI catchers that are more likely Chinese, Russian, Israeli and so forth," he said.

Foreign spies?

We also showed our results to an expert in Canadian security.

He knows a lot about IMSI catchers and comes from a Canadian security agency. We agreed to conceal his identity in order not to jeopardize that security work.

The expert found the results of our investigation disturbing.

"That an MP or a person who works on Parliament Hill could be exposed, that they could be a victim of this type of attack- it undermines our sovereignty," he said.

Based on his experience, he sees two very different potential explanations for the results. One domestic, the other foreign.

He said Russia has used IMSI catchers in Canada before.

"We learned that Russian intelligence was parked near CSIS with equipment on board to do IMSI catching. After X number of days or weeks, they're capable of identifying the IMSI numbers that belong to intelligence officers because the phones were spending eight hours a day in the same spot."

He said when the Russians would do their next clandestine operation, they would use an IMSI catcher to see if any of the numbers associated with Canadian intelligence were nearby. If there were, they would call off the operation.

The Russian Embassy rejects any allegation that Russians have used IMSI catchers in Ottawa.

"Any suggestions as to that kind of activities are bogus and baseless," said an embassy spokesperson.

A representative from the Chinese Embassy told us it was "not only unreasonable but even irresponsible" to suggest that country would be involved in the activity.

Israel said it had no knowledge of the issue, and the United States declined to comment.

Canadian spies?

Our security expert suggested the IMSI catchers we saw might be the work of a domestic agency, like Canada's electronic spy agency, the Communication Security Establishment.

"One possibility is that the Communications Security Establishment has been mandated to monitor the network for protection purposes, in a defensive way," he said.

CSE said it's not allowed to do that.

"To be clear, by law, CSE is not permitted to direct its activities at Canadians anywhere or at anyone in Canada, " a spokesperson said in a statement, adding that CSE respects the law.

Police use of IMSI catchers

Last June it was revealed the RCMP uses IMSI catchers in its work. A Quebec Superior Court lifted a publication ban to reveal police were using the technology as part of an investigation into the 2011 death of Salvatore (Sal the Ironworker) Montagna, a high-ranking member of a New York crime family killed outside Montreal.

Court documents show the RCMP:

- Purchased its first IMSI catcher in 2005.

- Has used IMSI catchers in numerous investigations.

- Keeps information about the cellphones of ordinary Canadians detected in the course of some investigations.

- Recognizes phones may be affected while an IMSI catcher is in use, including possible delays in reaching 911.

The documents also show the RCMP obtained court authorization to use the IMSI catcher, which the RCMP refer to as a mobile device interceptor, or MDI.

Recent court proceedings may also shed light on the degree to which police are reluctant to discuss their use of the devices. Last month, lawyers for the federal government issued stays of proceedings against three dozen suspects out of the nearly 50 people rounded up in an operation targeting the Montreal Mafia.

A Crown prosecutor told reporters one of the reasons was that evidence gathered by the RCMP raised "unprecedented legal questions," but declined to say more.

Some privacy experts believe the Crown is concerned about whether their use of IMSI catchers - including debates about how the data is collected - will hold up in court.

Municipal police forces use the technology as well. The Vancouver police have acknowledged they borrowed an RCMP IMSI catcher in 2007 and said they would use the technology again.

CBC News obtained documents showing that in 2016, Winnipeg police, Durham Regional Police, Ontario Provincial Police and the Canadian Security Intelligence Service had also gotten a licence from federal public safety officials to purchase an IMSI catcher.

Who is using IMSI catchers in Ottawa?

We reached out to police, security agencies, embassies and the federal government to ask if they were involved in the IMSI catchers we detected.

The Department of National Defence said it had no knowledge of IMSI catchers being used on the dates we saw activity.

The Department of Public Safety, the Ottawa Police Service, the RCMP and CSIS all gave similar responses: They don't discuss specific investigative techniques but they do follow the law, respect the Charter of Rights and Freedoms and adhere to the appropriate judicial processes.

The detection of the devices is troubling to Teresa Scassa, Canada Research Chair in Information Law at the University of Ottawa.

Even if the technology is being used by public authorities, Scassa sees reason to be concerned.

She points to a lack of transparency if Canadians are only learning in 2017 that the RCMP has had an IMSI catcher since 2005.

She also said it's not clear whether the authorities always get a warrant. Even when they do, there are still questions about what happens to the information of other people caught up in the investigation, Scassa said.

"Is it destroyed? Is it retained? Is it used for other purposes? It's not always clear that warrants contain conditions that require something specific to be done with the information afterwards."

Given that many groups may have access to IMSI catchers, Scassa argues there is a lot more the government could be doing to protect Canadians' privacy.

She believes agencies that use IMSI catchers should be required to get a warrant whenever the devices are used, destroy information that is intercepted but not related to the investigation and to report to the privacy commissioner about some key pieces of information, like how often they are used and in what context.

For the online article click here.

Cyr, Lita

From: Thibeault, Alexandre
Sent: 2017-Apr-04 8:47 AM
To: Brady, Megan; Bucknall, Jennifer; Clervoix, Magali; Cyr, Lita; Jarvis, Brian; Khanna, Mala; Kratchanov, Denis; Lalonde, Carie; Letarte, Lyne; McCreery, Matthew; Morrison, Mark; Prescott, D. Mark; Rondeau, Claudette; Roy, Nicole; Thibeault, Alexandre; Ward, Eric
Subject: CBC - Someone is spying on cellphones in the nation's capital

Good morning team,

For your information, see this interesting CBC investigative article, on IMSI catchers in downtown Ottawa:

> **Someone is spying on cellphones in the nation's capital**
> *A CBC/Radio-Canada investigation has found cellphone trackers at work near Parliament Hill and embassies*
>
> http://www.cbc.ca/beta/news/politics/imsi-cellphones-spying-ottawa-1.4050049

Alexandre

Alexandre Thibeault

Avocat, Centre du droit à l'information et à la protection des renseignements personnels, Secteur du droit public et des services législatifs
Ministère de la Justice Canada / Gouvernement du Canada
284, rue Wellington, ÉCE-3072, Ottawa (Ontario) K1A 0H8
alexandre.thibeault@justice.gc.ca / Tél. 613-957-4914

Counsel, Centre for Information and Privacy Law, Public Law and Legislative Services Sector
Department of Justice Canada / Government of Canada
284 Wellington Street, EMB-3072, Ottawa, ON K1A 0H8
alexandre.thibeault@justice.gc.ca / Tel. 613-957-4914

Cyr, Lita

From: Prescott, D. Mark
Sent: 2017-Apr-04 8:44 AM
To: JUS.L OTT CIPL Lawyers / Avocat es CDIPRP OTT L.JUS
Subject: Emailing: Someone is spying on cellphones in the nation's capital.htm

published: 2017-04-03 17:00 (EST)

received: 2017-04-04 04:35 (EST)

CBC.ca: Canada

Words: 1,480

Someone is spying on cellphones in the nation's capital

A months-long CBC News/Radio-Canada investigation has revealed that someone is using devices that track and spy on cellphones in the area around Parliament Hill.

The devices are known as IMSI catchers and have been used by Canadian police and security authorities, foreign intelligence and even organized crime.

The devices, sometimes known by the brand name of one model, StingRay, work by mimicking a cellphone tower to interact with nearby phones and read the unique ID associated with the phone - the International Mobile Subscriber Identity, or IMSI.

That number can then be used to track the phone and by extension the phone's user. In some instances, IMSI catchers can even be used to gain access to a phone's text messages and listen in on calls.

At the heart of Canadian government

To do the investigation, our journalists used a device that detects IMSI catchers created by the German company GSMK. While it looks like a regular cellphone, the CryptoPhone emits an alert when a fake cellphone antenna intercepts its signal.

Media in the United States, Norway and Australia have done similar tests, but this is the first time it's been used by a media outlet in Canada.

During tests in December and January, the CryptoPhone set off alerts at locations around Parliament Hill, including the nearby Byward Market, the Rideau Centre shopping mall and CBC offices in downtown Ottawa.

Because IMSI catchers have a radius of about half a kilometre in an urban setting, the IMSI catchers CBC detected could reach territory including Parliament Hill, the Prime Minister's Office in Langevin Block, National Defence headquarters, as well as the U.S. and Israeli embassies.

We then used even more sophisticated equipment called an Overwatch Sensor that confirmed the presence of an IMSI catcher close to Parliament Hill.

Who is behind it?

We wanted to know more about who might be using the IMSI catcher or catchers that we detected, so we asked the U.S. supplier of the CryptoPhone to analyze the alerts we were getting.

ESD America specializes in counterintelligence and its clients include U.S. Homeland Security.

"Consistently you've been seeing IMSI catcher activity, definitely," said CEO and co-founder Les Goldsmith, when we took our results to the company's Las Vegas office.

We described the part of the city in which we detected the IMSI catchers - full of politicians, political staffers and civil servants.

"Somebody could be listening to calls right now and [the phone owners] have no idea," he said.

As for who might be behind it, Goldsmith says IMSI catchers are used by law enforcement, federal agencies as well as organized crime and foreign intelligence.

Based on the configurations suggested by CBC's results, he believes the IMSI catchers detected in Ottawa could be foreign made.

"We're seeing more IMSI catchers with different configurations and we can build a signature. So we're seeing IMSI catchers that are more likely Chinese, Russian, Israeli and so forth," he said.

Foreign spies?

We also showed our results to an expert in Canadian security.

He knows a lot about IMSI catchers and comes from a Canadian security agency. We agreed to conceal his identity in order not to jeopardize that security work.

The expert found the results of our investigation disturbing.

"That an MP or a person who works on Parliament Hill could be exposed, that they could be a victim of this type of attack- it undermines our sovereignty," he said.

Based on his experience, he sees two very different potential explanations for the results. One domestic, the other foreign.

He said Russia has used IMSI catchers in Canada before.

"We learned that Russian intelligence was parked near CSIS with equipment on board to do IMSI catching. After X number of days or weeks, they're capable of identifying the IMSI numbers that belong to intelligence officers because the phones were spending eight hours a day in the same spot."

He said when the Russians would do their next clandestine operation, they would use an IMSI catcher to see if any of the numbers associated with Canadian intelligence were nearby. If there were, they would call off the operation.

The Russian Embassy rejects any allegation that Russians have used IMSI catchers in Ottawa.

"Any suggestions as to that kind of activities are bogus and baseless," said an embassy spokesperson.

A representative from the Chinese Embassy told us it was "not only unreasonable but even irresponsible" to suggest that country would be involved in the activity.

Israel said it had no knowledge of the issue, and the United States declined to comment.

Canadian spies?

Our security expert suggested the IMSI catchers we saw might be the work of a domestic agency, like Canada's electronic spy agency, the Communication Security Establishment.

"One possibility is that the Communications Security Establishment has been mandated to monitor the network for protection purposes, in a defensive way," he said.

CSE said it's not allowed to do that.

"To be clear, by law, CSE is not permitted to direct its activities at Canadians anywhere or at anyone in Canada, " a spokesperson said in a statement, adding that CSE respects the law.

Police use of IMSI catchers

Last June it was revealed the RCMP uses IMSI catchers in its work. A Quebec Superior Court lifted a publication ban to reveal police were using the technology as part of an investigation into the 2011 death of Salvatore (Sal the Ironworker) Montagna, a high-ranking member of a New York crime family killed outside Montreal.

Court documents show the RCMP:

- Purchased its first IMSI catcher in 2005.

- Has used IMSI catchers in numerous investigations.

- Keeps information about the cellphones of ordinary Canadians detected in the course of some investigations.

- Recognizes phones may be affected while an IMSI catcher is in use, including possible delays in reaching 911.

The documents also show the RCMP obtained court authorization to use the IMSI catcher, which the RCMP refer to as a mobile device interceptor, or MDI.

Recent court proceedings may also shed light on the degree to which police are reluctant to discuss their use of the devices. Last month, lawyers for the federal government issued stays of proceedings against three dozen suspects out of the nearly 50 people rounded up in an operation targeting the Montreal Mafia.

A Crown prosecutor told reporters one of the reasons was that evidence gathered by the RCMP raised "unprecedented legal questions," but declined to say more.

Some privacy experts believe the Crown is concerned about whether their use of IMSI catchers - including debates about how the data is collected - will hold up in court.

Municipal police forces use the technology as well. The Vancouver police have acknowledged they borrowed an RCMP IMSI catcher in 2007 and said they would use the technology again.

CBC News obtained documents showing that in 2016, Winnipeg police, Durham Regional Police, Ontario Provincial Police and the Canadian Security Intelligence Service had also gotten a licence from federal public safety officials to purchase an IMSI catcher.

Who is using IMSI catchers in Ottawa?

We reached out to police, security agencies, embassies and the federal government to ask if they were involved in the IMSI catchers we detected.

The Department of National Defence said it had no knowledge of IMSI catchers being used on the dates we saw activity.

The Department of Public Safety, the Ottawa Police Service, the RCMP and CSIS all gave similar responses: They don't discuss specific investigative techniques but they do follow the law, respect the Charter of Rights and Freedoms and adhere to the appropriate judicial processes.

The detection of the devices is troubling to Teresa Scassa, Canada Research Chair in Information Law at the University of Ottawa.

Even if the technology is being used by public authorities, Scassa sees reason to be concerned.

She points to a lack of transparency if Canadians are only learning in 2017 that the RCMP has had an IMSI catcher since 2005.

She also said it's not clear whether the authorities always get a warrant. Even when they do, there are still questions about what happens to the information of other people caught up in the investigation, Scassa said.

"Is it destroyed? Is it retained? Is it used for other purposes? It's not always clear that warrants contain conditions that require something specific to be done with the information afterwards."

Given that many groups may have access to IMSI catchers, Scassa argues there is a lot more the government could be doing to protect Canadians' privacy.

She believes agencies that use IMSI catchers should be required to get a warrant whenever the devices are used, destroy information that is intercepted but not related to the investigation and to report to the privacy commissioner about some key pieces of information, like how often they are used and in what context.

For the online article click here.

Prescott, D. Mark

From: Jarvis, Brian
Sent: March 24, 2017 2:47 PM
To: JUS.L OTT CIPL Lawyers / Avocat es CDIPRP OTT L.JUS
Subject: RE: Emailing: Questions raised on privacy, trust in our justice system.htm

From: Prescott, D. Mark
Sent: March 21, 2017 9:32 AM
To: JUS.L OTT CIPL Lawyers / Avocat es CDIPRP OTT L.JUS <DL-ILAP_LAWYERS@justice.gc.ca>
Subject: Emailing: Questions raised on privacy, trust in our justice system.htm

published: 2017-03-21
received: 2017-03-21 03:35 (EST)
Montreal Gazette (EARLY)
CITY | A4, Words: 518

Questions raised on privacy, trust in our justice system

by: JESSE FEITH

When the RCMP announced the first batch of arrests resulting from an investigation dubbed Project Clemenza back in 2014, it proudly boasted the force had intercepted more than a million private cellphone messages through the use of wireless signal interception techniques.

The techniques, in part, had allowed it to dismantle two groups operating within the Montreal Mafia, eventually leading to dozens of arrests for charges including drug-trafficking, assault, extortion, kidnapping and arson.

But now federal prosecutors are set to seek a stay of proceedings in the cases on Tuesday, a decision that is being linked back to those intercepted cellphone messages. Though the Crown is not required to divulge why it will cease prosecuting a case, it's believed one of the factors behind the decision is the RCMP's refusal to disclose how it was able to intercept the Blackberry messages in the first place.

It's a decision that not only raises privacy concerns, but one that could also further undermine the public's trust in the criminal justice system, experts said on Monday.

"If that is the core reason, it's a really serious problem," said Christopher Parsons, a research associate with the Citizen Lab at the University of Toronto's Munk School of Global Affairs.

Across the country, Parsons said, law enforcement agencies are using devices known as "IMSI catchers" or as they're called in Canada, "mobile device identifiers."

The devices, widely believed to have been used during Project Clemenza, essentially mimic a cellular tower, allowing law enforcement to gather information and communications from nearby phones that connect to it.

But police have been hesitant to release information about how the devices work, Parsons said.

If the Project Clemenza cases had gone to trial, the Crown would have had to reveal the full extent to which the RCMP relied on the devices, exposing the technique to defence lawyers rightfully trying to determine exactly how accurate and reliable they are.

"I think the police are mindful that these devices are challenging to develop and operate and may not sustain under cross-examination," Parsons said.

"They want to be able to continue using them, and if they're found to be significantly flawed devices, then their perceived value and utility may decrease."

For Pierre de Champlain, a former RCMP intelligence analyst and author of books about organized crime, the decision to stay the charges is also likely to have troubling consequences in Montreal.

"It will certainly further undermine people's trust in the criminal justice system," de Champlain said, adding that anyone should be concerned when the prosecution decides to abandon cases against people with links to organized crime.

De Champlain said it seems as though, is some ways, Project Clemenza is becoming the equivalent of the SharQc trial, in which several alleged Hells Angels members had their charges stayed due to unreasonable delays.

The news probably also came as a relief to a Montreal Mafia that's currently in a state of disarray, de Champlain added, and could give those expected to see their charges stayed a new-found "sense of invisibility."

"Unfortunately," he said, "society is the real loser in all of this." jfeith@postmedia.com Twitter.com/jessefeith

Prescott, D. Mark

From: Prescott, D. Mark
Sent: March 21, 2017 9:32 AM
To: JUS.L OTT CIPL Lawyers / Avocat es CDIPRP OTT L.JUS
Subject: Emailing: Questions raised on privacy, trust in our justice system.htm

published: 2017-03-21

received: 2017-03-21 03:35 (EST)

Montreal Gazette (EARLY)

CITY | A4, Words: 518

Questions raised on privacy, trust in our justice system

by: JESSE FEITH

When the RCMP announced the first batch of arrests resulting from an investigation dubbed Project Clemenza back in 2014, it proudly boasted the force had intercepted more than a million private cellphone messages through the use of wireless signal interception techniques.

The techniques, in part, had allowed it to dismantle two groups operating within the Montreal Mafia, eventually leading to dozens of arrests for charges including drug-trafficking, assault, extortion, kidnapping and arson.

But now federal prosecutors are set to seek a stay of proceedings in the cases on Tuesday, a decision that is being linked back to those intercepted cellphone messages. Though the Crown is not required to divulge why it will cease prosecuting a case, it's believed one of the factors behind the decision is the RCMP's refusal to disclose how it was able to intercept the Blackberry messages in the first place.

It's a decision that not only raises privacy concerns, but one that could also further undermine the public's trust in the criminal justice system, experts said on Monday.

"If that is the core reason, it's a really serious problem," said Christopher Parsons, a research associate with the Citizen Lab at the University of Toronto's Munk School of Global Affairs.

Across the country, Parsons said, law enforcement agencies are using devices known as "IMSI catchers" or as they're called in Canada, "mobile device identifiers."

The devices, widely believed to have been used during Project Clemenza, essentially mimic a cellular tower, allowing law enforcement to gather information and communications from nearby phones that connect to it.

But police have been hesitant to release information about how the devices work, Parsons said.

If the Project Clemenza cases had gone to trial, the Crown would have had to reveal the full extent to which the RCMP relied on the devices, exposing the technique to defence lawyers rightfully trying to determine exactly how accurate and reliable they are.

"I think the police are mindful that these devices are challenging to develop and operate and may not sustain under cross-examination," Parsons said.

"They want to be able to continue using them, and if they're found to be significantly flawed devices, then their perceived value and utility may decrease."

For Pierre de Champlain, a former RCMP intelligence analyst and author of books about organized crime, the decision to stay the charges is also likely to have troubling consequences in Montreal.

"It will certainly further undermine people's trust in the criminal justice system," de Champlain said, adding that anyone should be concerned when the prosecution decides to abandon cases against people with links to organized crime.

De Champlain said it seems as though, is some ways, Project Clemenza is becoming the equivalent of the SharQc trial, in which several alleged Hells Angels members had their charges stayed due to unreasonable delays.

The news probably also came as a relief to a Montreal Mafia that's currently in a state of disarray, de Champlain added, and could give those expected to see their charges stayed a new-found "sense of invisibility."

"Unfortunately," he said, "society is the real loser in all of this." jfeith@postmedia.com Twitter.com/jessefeith

Kimberley Pearce - [redacted]

From: Dave Cobey
To: Fontaine, Martine
Date: 2016/11/17 6:11 PM
Subject: [redacted]
CC: Adam, Jeff; Bradshaw, Kelly; Pearce, Kimberley; Robin, John; Scriven...
Attachments: [redacted]

Hi Martine,

[redacted]

Please don't hesitate to call or email if you require additional information.

Cheers,
Dave

[redacted]

Pages 42 to / à 106

are withheld pursuant to sections

sont retenues en vertu des articles

21(1)(a), 21(1)(b), 23

of the Access to Information Act

de la Loi sur l'accès à l'information

s.16(2)(c) s.21(1)(a) s.21(1)(b) s.23

Kimberley Pearce - [redacted]

From: Dave Cobey
To: Bradshaw, Kelly; Robin, John
Date: 2016/10/12 5:21 PM
Subject: [redacted]
CC: Beaulieu, Alexandre; Cameron, Wallace; Desrosiers, Heather; Dewar, Mi...
Attachments: [redacted]

John / Kelly,

[redacted]

- Tomorrow's daily meeting is at **9 a.m.** in the A/Comm's meeting room. Conf. call coordinates are: **613-960-7514 / 877-413-4790, Conf. ID:** [redacted]

Cheers,
Dave

Pages 108 to / à 231

are withheld pursuant to sections

sont retenues en vertu des articles

21(1)(a), 21(1)(b)

of the Access to Information Act

de la Loi sur l'accès à l'information

Page 232

is withheld pursuant to sections

est retenue en vertu des articles

21(1)(a), 21(1)(b), 23

of the Access to Information Act

de la Loi sur l'accès à l'information

Page 233

is withheld pursuant to sections

est retenue en vertu des articles

21(1)(a), 21(1)(b)

of the Access to Information Act

de la Loi sur l'accès à l'information

Prescott, D. Mark

From: Jarvis, Brian
Sent: September 15, 2016 1:46 PM
To: * CIPL Lawyers / Avocat (es) CDIPRP
Subject: Report on IMSI catchers

https://citizenlab.org/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf

Prescott, D. Mark

From: Prescott, D. Mark
Sent: September 13, 2016 9:43 AM
To: * CIPL Lawyers / Avocat (es) CDIPRP
Subject: Emailing: Lift secrecy on surveillance devices, privacy experts urge.htm

Provided by **NewsDesk** **http://www.infomedia.gc.ca/allcontent/** Fourni par **InfoMédia**

Published | Publié: 2016-09-13
Received | Reçu: 2016-09-13 3:59 AM

Globe and Mail
News, Page: A1

Lift secrecy on surveillance devices, privacy experts urge

COLIN FREEZE

Canada must acknowledge, and then constrain, the government's use of portable surveillance devices that can indiscriminately dredge data from people's smartphones without them knowing, privacy experts say.

Everything that is known or suspected about the government's use of these machines - called "IMSI catchers," "cell-site simulators" or "Stingrays" - is chronicled in a comprehensive, first-of-its-kind, 130-page report written by privacy experts and released to The Globe and Mail.

Federal police have used these devices for more than a decade, but the practice was confirmed only this year in a series of stories in The Globe. Now, researchers Christopher Parsons and Tamir Israel say it's time for civil society to debate the pros and cons of IMSI catchers, even if many government agencies still won't discuss them.

"This ongoing secrecy has the effect of delaying important public debates," the report says.

The report was commissioned by the Telecom Transparency Project and the Canadian Internet Policy & Public Interest Clinic. They received grants from the Open Society Foundation, privacy activist Frederick Ghahramani, a Social Sciences and Humanities Research Council Postdoctoral Fellowship Award, and the Munk School of Global Affairs at the University of Toronto.

The report follows Public Safety Minister Ralph Goodale's announcement last week that he is soliciting the public's views on the powers of police and spy agencies. Other countries, such as Germany, have been more open about their use of IMSI catchers.

An "IMSI," which stands for "international mobile subscriber identity," is a unique serial number now affixed to every smartphone's chip set. It is one of several digital identifiers that police build modern investigations around if they can tie a specific number to a specific suspect.

Mr. Goodale's department posted a backgrounder stating that police are frustrated by criminals' anonymous use of computers and phones. Canada may need to pass laws that facilitate the flow of customer data - including IMSI data - from telecommunications corporations, the government backgrounder suggests.

Yet mention of the technological equalizers that allow police to bypass corporate gatekeepers have been left out of the government's consultation exercise. For some pro-privacy advocates, this is the conversation Canadians should be having.

"IMSI catchers pose a particularly insidious threat to real-world anonymity," write Mr. Parsons and Mr. Israel, who are part of digital-research labs at the Universities of Toronto and Ottawa respectively. Their paper, which is titled Gone Opaque, points out that corporations that manufacture IMSI catchers often swear police to non-disclosure agreements.

They suggest the scope of IMSI catchers is currently limited only by the imaginations of government agents who use them.

"They can be deployed to geolocate and identify individuals in private homes, to see who visits a medical clinic or a religious meeting, or to identify travelling companions," the research paper says.

"They can be deployed permanently at border crossings, airports or bus depots, or distributed at various points of a city so that movement becomes effectively impossible without a record of it being created."

Officials won't say much about IMSI catchers. Freedom of Information requests filed in several provinces have been rebuffed with can-neither-confirm-nor deny statements. The Toronto Police Service has avowed publicly that it doesn't have such a device, even though its detectives recently used one. Montreal prosecutors tried to suppress discussion of an IMSI catcher in a criminal trial, telling judges they didn't want to broadcast the police playbook to mobsters.

Most dramatically, federal prison officials at the Warkworth Institution in Ontario appear to be under criminal investigation for unlawful use of an IMSI catcher. An effort that aimed to contain contraband phones outraged prison guards, after their warden conceded their personal conversations may have been inadvertently intercepted by such a device.

Mr. Parsons and Mr. Israel point out that Germany releases annual statistics on that government's use of IMSI catchers, and that the U.S. Department of Justice has posted the rules that American authorities must abide by.

In Canada, RCMP-led surveillance teams are understood to control IMSI-catcher technology and lend it out to smaller police forces shadowing specific suspects. But IMSI catchers also pull digital identifiers from the phones of everybody in proximity, raising many privacy questions.

"Collateral impact is inherent in the functioning of IMSI catchers," the research paper says, pointing out that a U.S. court recently imposed a 48-hour deadline on police to destroy bystander data.

No such deadline is known to exist for RCMP-led teams, whose officers get approvals from judges after swearing catch-all "general-warrant" applications.

Mr. Parsons and Mr. Israel argue that specialized, higher-threshold warrants for IMSI catchers are needed.

The authors argue that authorities should also routinely notify bystanders if their phone data have been inadvertently captured. "Given the potential for IMSI catchers to massively track Canadians who have done nothing wrong other than be near the surveillance device, it is imperative to ensure the aforementioned measures are in place."

Cyr, Lita

From: Prescott, D. Mark
Sent: 2016-Sep-13 9:43 AM
To: * CIPL Lawyers / Avocat (es) CDIPRP
Subject: Emailing: Lift secrecy on surveillance devices, privacy experts urge.htm

Published | Publié: 2016-09-13
Received | Reçu: 2016-09-13 3:59 AM

Globe and Mail
News, Page: A1

Lift secrecy on surveillance devices, privacy experts urge

COLIN FREEZE

Canada must acknowledge, and then constrain, the government's use of portable surveillance devices that can indiscriminately dredge data from people's smartphones without them knowing, privacy experts say.

Everything that is known or suspected about the government's use of these machines - called "IMSI catchers," "cell-site simulators" or "Stingrays" - is chronicled in a comprehensive, first-of-its-kind, 130-page report written by privacy experts and released to The Globe and Mail.

Federal police have used these devices for more than a decade, but the practice was confirmed only this year in a series of stories in The Globe. Now, researchers Christopher Parsons and Tamir Israel say it's time for civil society to debate the pros and cons of IMSI catchers, even if many government agencies still won't discuss them.

"This ongoing secrecy has the effect of delaying important public debates," the report says.

The report was commissioned by the Telecom Transparency Project and the Canadian Internet Policy & Public Interest Clinic. They received grants from the Open Society Foundation, privacy activist Frederick Ghahramani, a Social Sciences and Humanities Research Council Postdoctoral Fellowship Award, and the Munk School of Global Affairs at the University of Toronto.

The report follows Public Safety Minister Ralph Goodale's announcement last week that he is soliciting the public's views on the powers of police and spy agencies. Other countries, such as Germany, have been more open about their use of IMSI catchers.

An "IMSI," which stands for "international mobile subscriber identity," is a unique serial number now affixed to every smartphone's chip set. It is one of several digital identifiers that police build modern investigations around if they can tie a specific number to a specific suspect.

Mr. Goodale's department posted a backgrounder stating that police are frustrated by criminals' anonymous use of computers and phones. Canada may need to pass laws that facilitate the flow of customer data - including IMSI data - from telecommunications corporations, the government backgrounder suggests.

Yet mention of the technological equalizers that allow police to bypass corporate gatekeepers have been left out of the government's consultation exercise. For some pro-privacy advocates, this is the conversation Canadians should be having.

"IMSI catchers pose a particularly insidious threat to real-world anonymity," write Mr. Parsons and Mr. Israel, who are part of digital-research labs at the Universities of Toronto and Ottawa respectively. Their paper, which is titled Gone Opaque, points out that corporations that manufacture IMSI catchers often swear police to non-disclosure agreements.

They suggest the scope of IMSI catchers is currently limited only by the imaginations of government agents who use them.

"They can be deployed to geolocate and identify individuals in private homes, to see who visits a medical clinic or a religious meeting, or to identify travelling companions," the research paper says.

"They can be deployed permanently at border crossings, airports or bus depots, or distributed at various points of a city so that movement becomes effectively impossible without a record of it being created."

Officials won't say much about IMSI catchers. Freedom of Information requests filed in several provinces have been rebuffed with can-neither-confirm-nor deny statements. The Toronto Police Service has avowed publicly that it doesn't have such a device, even though its detectives recently used one. Montreal prosecutors tried to suppress discussion of an IMSI catcher in a criminal trial, telling judges they didn't want to broadcast the police playbook to mobsters.

Most dramatically, federal prison officials at the Warkworth Institution in Ontario appear to be under criminal investigation for unlawful use of an IMSI catcher. An effort that aimed to contain contraband phones outraged prison guards, after their warden conceded their personal conversations may have been inadvertently intercepted by such a device.

Mr. Parsons and Mr. Israel point out that Germany releases annual statistics on that government's use of IMSI catchers, and that the U.S. Department of Justice has posted the rules that American authorities must abide by.

In Canada, RCMP-led surveillance teams are understood to control IMSI-catcher technology and lend it out to smaller police forces shadowing specific suspects. But IMSI catchers also pull digital identifiers from the phones of everybody in proximity, raising many privacy questions.

"Collateral impact is inherent in the functioning of IMSI catchers," the research paper says, pointing out that a U.S. court recently imposed a 48-hour deadline on police to destroy bystander data.

No such deadline is known to exist for RCMP-led teams, whose officers get approvals from judges after swearing catch-all "general-warrant" applications.

Mr. Parsons and Mr. Israel argue that specialized, higher-threshold warrants for IMSI catchers are needed.

The authors argue that authorities should also routinely notify bystanders if their phone data have been inadvertently captured. "Given the potential for IMSI catchers to massively track Canadians who have done nothing wrong other than be near the surveillance device, it is imperative to ensure the aforementioned measures are in place."

s.21(1)(a) s.21(1)(b) s.23

Kimberley Pearce - [redacted]

From: Maury Medjuck
To: Morris, Jeffrey
Date: 2016/06/30 10:28 AM
Subject: [redacted]
CC: Lynam, Chris; Pearce, Kimberley
Attachments: [redacted]

Received this morning. [redacted]

>>> Jeffrey Morris 2016/06/29 3:36 PM >>>
Hi Maury,

[redacted]

Regards,
Jeff

Pages 242 to / à 293

are withheld pursuant to sections

sont retenues en vertu des articles

21(1)(a), 21(1)(b), 23

of the Access to Information Act

de la Loi sur l'accès à l'information

Kimberley Pearce - [redacted]

From: Maury Medjuck <Maury.Medjuck@rcmp-grc.gc.ca>
To: Kimberley.Pearce@rcmp-grc.gc.ca
Date: 2016/06/14 12:04 PM
Subject: [redacted]
Attachments: [redacted]

Sent from my BlackBerry 10 smartphone on the Rogers network.

From: Joe Oliver <Joe.Oliver@rcmp-grc.gc.ca>
Sent: Sunday, June 12, 2016 11:26 AM
To: Peter Henschel
Cc: Chris Lynam; Taunya Goguen; Jeff Adam; Maury Medjuck
Subject: [redacted]

Deputy -

[redacted]

Page 295

is withheld pursuant to sections

est retenue en vertu des articles

21(1)(a), 21(1)(b), 23

of the Access to Information Act

de la Loi sur l'accès à l'information

[redacted]

Joe

>>> Maury Medjuck 2016/06/10 2:38 PM >>>
Joe,

[redacted]

Maury

>>> Mike Roach 2016/06/10 8:39 AM >>>
Hi,

[redacted]

Mike

Pages 297 to / à 519
are withheld pursuant to sections
sont retenues en vertu des articles

13(1)(c), 23

of the Access to Information Act
de la Loi sur l'accès à l'information

Cyr, Lita

From: Prescott, D. Mark
Sent: 2016-Mar-15 9:49 AM
To: * CIPL Lawyers / Avocat (es) CDIPRP
Subject: Emailing: Surveillance device used in prison sets off police probe.htm

Published | Publié: 2016-03-15
Received | Reçu: 2016-03-15 2:37 AM

Globe and Mail
News, Page: A1

Surveillance device used in prison sets off police probe

COLIN FREEZE, MATTHEW BRAGA - TORONTO

Federal prison authorities are under criminal investigation for possible illegal surveillance, The Globe and Mail has learned. The probe centres on Correctional Service Canada's use of a dragnet surveillance device inside a penitentiary.

Fallout from the 2015 surveillance incident, involving a device that CSC officials called a "cellular grabber," has led to a lawsuit from jail guards and a criminal inquiry by the Ontario Provincial Police.

Under the Criminal Code, indiscriminate surveillance campaigns can be deemed crimes that merit prison sentences. Federal security officials do not get blanket exemptions, even if they themselves work to manage prisons.

The case at hand started with a desire to locate prisoners' contraband cellphones, but ended up with a warden apologizing to his own staff for inadvertently spying on them.

The make and model of the device in question are being withheld from the public, which generally is familiar with such machines by names such as "Stingrays," "cell-site simulators" or "IMSI catchers."

"IMSI catchers are not localized. It would get anything that's in range and won't discriminate," explained Tamir Israel, a lawyer at the Canadian Internet Policy and Public Interest Clinic.

On Monday, The Globe and Mail reported on the RCMP's courtroom bid to keep its use of a similar device secret.

In the winter of 2015, officials at Warkworth Institution, a medium-security prison in Ontario, grew alarmed by prisoner drug overdoses. On Jan. 20, one CSC official sent an internal e-mail, according to federal court documents related to the civil suit, saying "there are phones all over the institution and this is how they are organizing the introduction of contraband."

Officials in Ottawa, records show, put out a request for an outsider who could perform "surveys of radio traffic" to "confirm the presence of cellular phones inside institutions." The winning contractor, according to federal court documents, was a Quebec-based engineer named Peter Steeves, who said he could do the job for $7,500 in fees, plus $2,000 in travel expenses.

Contacted Monday by The Globe and Mail, Mr. Steeves said he is no expert in the legalities of interception. "I'm just a guy trying to make a living - I really don't know the law," he said.

Asked about the police probe, he said, "I know I have to go for an interview. I have been told it's a criminal investigation."

Access to information records show that last April, a device was shipped to CSC from Florida.

Details are mostly being withheld, but it weighed 38 kilograms and its manufacturer was a Britain-based surveillance machinery firm, Smith Myers.

The "pilot program" at the Warkworth Institution started rolling out in the late spring. By August, CSC officials arranged an internal meeting to review the "cellular grabber to better understand its capacity," according to an e-mail now filed in court.

Officials wanted to know "how to force" a phone to communicate its specific location, or how to list phones on a map of the prison.

Before long, CSC officials began asking for even more specifics - such as how to figure out whether phones were sending texts or calls. On Sept. 3, one official asked for the "total activities of cellular devices from inmates, staff ..." Prison guards learned of the program, and pushed back.

"How does this device bend a radio signal ... to eliminate the inclusion of staff areas?" one guard asked in an e-mail to his bosses.

By the end of September, Warkworth's warden, Scott Thompson, sent an apologetic e-mail to all staff, according to Access to Information records.

"Unfortunately, I knew that by trying to intercept what the inmates were doing, I would also be provided information about cellular devices being used in non-inmate areas," his e-mail said. The warden relayed that the device "provides make, phone numbers and sim-card numbers" and, also, "recorded all voice and text conversations."

With that, he assured his jail guards that any of their inadvertently captured communications wouldn't be used against them.

"I am sorry if this information causes stress to any of you," he said.

Some CSC e-mails contradict the warden, stating explicitly that the device did not capture any conversations beyond three text messages intercepted in a bid used to showcase its capabilities. (On Monday, the contractor, Mr. Steeves, told The Globe that the device "does not capture voice at all.") At the end of October, the Union of Canadian Correctional Officers took their bosses to court. In a lawsuit, they complained their privacy rights had been violated - and that CSC had spied upon them.

"Look - we're all about getting the contraband out. We're in. If there's technology to do that, we're there," explained Jason Godin, a union vice-president in an interview. "But, God damn it," he said, "... you can't spy on private conversations of staff members."

Mr. Israel suggests that the correctional officials who acquired the device were likely operating in a legal vacuum.

"Because no agency to my mind has openly acknowledged to using these in court, no court has provided guidance as to what the [legal] authorities should be," he said. Some federal officials, he added, "may be under the impression they can just deploy these IMSI catchers without any authorization at all."

CSC officials have recently stopped giving statements to lawyers pursuing the civil suit.

According to Federal Court filings, that's because they have become worried to have learned there is now also a criminal probe.

"The Ontario Provincial Police is currently conducting a criminal investigation into the monitoring of cellphones at Warkworth Institution," reads a motion filed earlier this month.

Because OPP detectives are now interviewing CSC officials, the latter "have significant concerns about providing affidavits while an investigation is under way."

Spokespersons for the OPP and CSC won't comment on the specifics of the investigation.

Correctional officials originally defended their use of the device by saying they had "authority to monitor and intercept communications to ensure the security of institutions." But they have stopped saying this now that they face civil and criminal investigations for alleged unlawful surveillance of jail guards.

Court filed e-mails show that, in the end, CSC seized only three contraband cellphones smuggled into Warkworth.

Matthew Braga is special to The Globe and Mail, with a report from Laura Stone in Ottawa