



Public Safety Sécurité publique
Canada Canada

Senior Assistant Sous-ministre
Deputy Minister adjoint(e) principal(e)

Ottawa, Canada
K1A 0P8

UNCLASSIFIED

DATE:

File No.: NS 6652-O3 / CCM: PS-012578
RDIMS No.: 1972097

MEMORANDUM FOR THE DEPUTY MINISTER

SECTION 191 LICENCES

(Information only)

ISSUE

To provide information on the issuing of section 191 licences under the *Criminal Code of Canada*.

BACKGROUND

Section 191 Licences:

Subsection 191(1) of the *Criminal Code* indicates that: "Everyone who possesses, sells or purchases any electro-magnetic, mechanical or other device or any component thereof knowing that the design thereof renders it primarily useful for surreptitious interception of private communication is guilty of an indictable offence and is liable to imprisonment for a term not exceeding two years".

Subsection 191(2) of the *Criminal Code* allows for specific exemptions to 191(1), namely to:

- (a) a police officer in the course of his employment;
- (b) a person using it in an interception made or to be made in accordance with an authorization;
- (b.1) a person under the direction of a police officer in order to assist that officer in the course of his duties as a police officer;

.../2

s.15(1)(d)(ii)

s.16(1)(b)

s.16(1)(c)

UNCLASSIFIED

- 2 -

- (c) an officer or servant of Her Majesty in right of Canada or a member of the Canadian forces in the course of his duties as such an officer, servant or member;
- (d) any other person under the authority of a licence issued by the Minister of Public Safety and Emergency Preparedness.

In order for a company or an individual to obtain an exemption under subsection 191(2)(d) to possess, sell or purchase enabling devices for the interception of communications, the Minister must issue them a licence. As such, companies and individuals must present a licence application to the RCMP or CSIS for processing which is subsequently sent to Public Safety Canada (PS) for approval. Licences under section 191 are only granted to companies or individuals that provide sources of supply to police departments, the Canadian Forces, or the Canadian government, unless special circumstances exist. Licences issued under subsection 191(2)(d) contain terms and conditions (**TAB A**) relating to the possession, sale or purchase of the device(s) or component(s) as prescribed by the Minister and are generally applied to all licences. Once approved, each licence has an expiration date of up to two years.

PS Agencies Roles:

In the course of undertaking its lawful duties, 

All other licence applications pursuant to section 191 are processed by the Technical Investigation Services Branch of the RCMP. The RCMP is responsible for completing appropriate indices checks for the applying company and its employees, and ensuring that the necessary fees have been received. Once the applications have been verified the licence application is forwarded to PS for review and signature.

PS's Role:

Once an application under section 191 is received, PS's National Security Operations Directorate ensures quality control of the licence application and facilitates the signature process of the licence. The Senior Assistant Deputy Minister of the National and Cyber Security Branch has the delegated authority to sign such licences on behalf of the Minister.

CURRENT STATUS

There has been increased media coverage over the last few months regarding the use of investigative tools such as the StingRay, IMSI Catchers, and other interception devices by law enforcement, intelligence services, and even correctional facilities management. This has also been matched by an increase in *Access to Information* requests.

.../3

s.19(1)
s.15(1)(d)(ii)
s.16(1)(b)
s.16(1)(c)

UNCLASSIFIED

- 3 -

On September 22, 2016, the CBC released an investigative report entitled: “*Shady, Secretive System: Public Safety green-lit RCMP, CSIS spying devices, documents reveal*” (TAB B). The article states that the department “has repeatedly approved CSIS and the RCMP’s use of devices to spy on Canadians’ communications”.

However, it is important to note that the process highlighted in the article is the process departments such as CSIS, RCMP and DND use to ensure that they and their contractors are working in compliance with the *Criminal Code*.

In March 2016, the Globe and Mail reported that Federal prison authorities were under criminal investigation for possible illegal surveillance (TAB C). The investigation centers around Correctional Service Canada’s use of a dragnet surveillance device inside Warkworth Institution. The contractor hired to perform the surveillance at Warkworth [REDACTED] This incident has led to a lawsuit from jail guards and a criminal inquiry by the Ontario Provincial Police.

CONSIDERATIONS

The use of technical investigative tools, such as interception devices, help safeguard Canadians and support priority criminal investigations. The use of any investigative tool is subject to lawful authority, which may refer to judicial authorization; common law; or, the presence of exigent circumstances, such as in relation to recent child abductions or missing persons. Having lawful authority ensures that the important, specific and limited law enforcement purpose weighs both the public safety and privacy interests involved. Priority investigations include those linked to national security, organized crime, or financial crime.

The oversight of any investigative technique used by law enforcement and intelligence agencies is governed by appropriate judicial processes, as set out in criminal law. By law, court orders must be limited and specific to the criminality under investigation, can only be obtained if the statutory requirements are met, and can be subsequently reviewed at trial by the court and the accused. The capabilities of sensitive investigative tools are classified, and the release of such information would negatively and significantly impact public and officer safety and the integrity of the criminal justice system.

[REDACTED]

.../4

UNCLASSIFIED

- 4 -

NEXT STEPS

The department is currently reviewing the application and licensing process in collaboration with legal services and key partners.

Should you require any additional information, please do not hesitate to contact me or Suki Wong, Director General, National Security Operations Directorate at 613-991-3583.

Monik Beauregard

Enclosure(s): (3)

Prepared by:  / Rodrigue Taschereau

The cbc.ca login and signup tools may be temporarily unavailable for some people due to maintenance. We're sorry for the inconvenience.

'Shady, secretive system': Public Safety green-lit RCMP, CSIS spying devices, documents reveal

Government officials refuse to say exactly what interception devices are being approved in Canada

By Laura Wright, [CBC News](#) Posted: Sep 22, 2016 5:00 AM ET Last Updated: Sep 22, 2016 10:18 AM ET

Public Safety Canada has repeatedly approved CSIS and the RCMP's use of devices to spy on Canadians' communications, documents obtained by CBC News reveal.

Canadians have been kept largely in the dark about police and intelligence agencies' surveillance capabilities. But recent revelations in a Montreal court case that police are using electronic tools to scoop up mobile phone signals have prompted some experts to call for greater transparency in the approval and use of technologies that potentially violate privacy.

The new documents reveal Public Safety Canada approved requests from the RCMP, Canadian Security Intelligence Service and the Defence Department granting more than a dozen licences to an unnamed company (or companies) for the purpose of possessing, manufacturing or selling devices "used primarily for the interception of communications."

- Cellphone monitoring device use should be transparent and limited, researchers say
- Goodale hopes new spy oversight committee will be 'spontaneous' with reports

The documents, which are heavily redacted and don't identify the manufacturers or the devices and their capabilities, were shared with CBC News by Ottawa-based investigative researcher Ken Rubin.

"It's a part of the puzzle," Rubin said. "There are too many questions there. All I've uncovered is a link to how this rather shady, secretive system works, and there's no public understanding of it."

Government won't identify devices

The one- and two-year licences were issued beginning in 2015, and in some cases, they extend until 2018. One was granted to CSIS retroactively.

They were granted under Section 191 of the Criminal Code, which says technology for the surreptitious interception of private communications is illegal, unless permission to use such technology is granted by the public safety minister.

The RCMP wouldn't disclose what the licences are for.

"We generally do not comment on specific investigative methods, tools and techniques outside of court," said spokeswoman Cpl. Annie Delisle.

Public Safety Canada spokesman Jean-Philippe Levert also declined to identify the devices.

"Disclosing details such as the specific types of equipment used to conduct investigations may hinder these agencies' effectiveness and their ability to carry out their mandates," he said.

CSIS didn't reply to CBC's request for comment.

Delisle said the RCMP has been appointed to review all licence applications made under Section 191, including doing background checks on the individuals or companies that apply. If they pass the RCMP's vetting process, Public Safety officials are then asked to sign off on the licences.

Some, called "special licences," last for two years. The RCMP said this type allows a company to possess the equipment, which is otherwise illegal to own. The licensee can then demonstrate the equipment to law enforcement and government agencies.

Others are just called "licences" and last for one year. The RCMP said this allows a company to sell the equipment to the government agency that sponsored its application.

While Public Safety and the RCMP won't identify the devices, Rubin says one possibility is what's known as a StingRay, or IMSI catcher. The device can identify and track a person based on their mobile device's specific ID and intercept communications to and from the device.

- [Police secrecy on StingRay cellphone surveillance device challenged](#)
- [Are StingRay cellphone surveillance systems used by Vancouver police?](#)
- [Edmonton police backtrack on StringRay surveillance statement](#)

IMSI catchers have come under heavy scrutiny for the lack of transparency around their use. Canadian police agencies, including the RCMP and the Vancouver and Toronto police forces, have fought in court to withhold saying whether they use them.

But RCMP testimony and court records from a Montreal case show the RCMP does use the technology in [investigations across the country](#). In that court case, it was revealed that police had sought a judge's authorization to use the device

No public record

There is no public record or clear policy on how police use technology for surveillance purposes, something privacy advocates say is a problem.

"It could be any kind of device — it certainly doesn't have to be the StingRay — but who knows what this device is, and that's part of the problem," Rubin said.

Tamir Israel, a privacy lawyer who co-authored a [recent report on IMSI catchers](#), said there are lots of invasive electronic devices out there that police can use.

- [Former CSIS head says Canada should have its own cyber-warriors](#)
- [MPs, senators to oversee security, intelligence agencies under new Liberal bill](#)

"If there was some way to get them [law enforcement agencies and the government] to be more proactive about just explaining to the public what the tools are, we can have a discussion up front," Israel said.

Especially since the government introduced legislation this summer to create a spy watchdog committee, and Public Safety Minister Ralph Goodale said he [wants to hear from Canadians](#) on the topic.

But without more transparency, both Rubin and Israel say that's a challenge.

"We're having these consultations, but we don't know what we're consulting about because we don't know about what the tools are that are being used," Israel said.

Exemptions for public officials

Adding to the confusion is the fact any device that interferes with radio communications, such as an IMSI catcher, requires a company or agency to get authorization from Innovation, Sciences and Economic Development Canada, previously known as Industry Canada.

So theoretically, according to Israel, anyone using such a device would need both a licence from Public Safety and authorization from Innovation Canada.

But that isn't the case for the RCMP and other public officials.

Innovation Canada confirmed that it would have to authorize a person or company to own and use a device like an IMSI catcher. But the department says it hasn't authorized their use in Canada.

However, a spokesperson did say that under Section 54 of the Radiocommunications Regulations, it doesn't actually have to be notified if a public official, peace officer, prosecutor, or officer of the court uses such a device for the investigation of an alleged crime, or for the purposes of international affairs, national defence or security.

That means Innovation Canada only regulates their use for the rest of us, which may explain how the RCMP has been able to use the device in its investigations.

- Police secrecy on StingRay cellphone surveillance device challenged
- Canada's electronic spy service to take more prominent role in ISIS fight

Rubin said that even if the government's system of issuing licences for surveillance technology isn't robust, these documents show that it does, indeed, exist.

"And now that we know it exists, how are you going to explain this to the public?"

View the documents released under Access to Information below:

To print the document, click the "Original Document" link to open the original PDF. At this time it is not possible to print the document with annotations.



Surveillance device used in prison sets off police probe

SUBSCRIBE

SIGN IN

AdChoices



CANADA

Surveillance device used in prison sets off police probe



What started as a desire to locate prisoners' contraband cellphones ended with a warden apologizing to his own staff for inadvertently spying on them.

COLIN FREEZE AND MATTHEW BRAGA
TORONTO
MARCH 14, 2016

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

TRENDING

- 1 RCMP worried about escalating sanctions against parliamentary guards
- 2 Manitoba set to defy federal Liberals, unveil \$25-per-tonne carbon tax
- 3 TSX reaches new record high as energy sector surges
- 4 Apple says iPhone X pre-orders are 'off the charts'; shares jump
- 5 Bush set the stage for the Trumpian upheaval

SUPPORT QUALITY JOURNALISM JUST 99¢ PER WEEK FOR THE FIRST FOUR WEEKS

START TODAY

not blanket exemptions, even if they themselves work to manage
pr

[SUBSCRIBE](#)[SIGN IN](#)[AdChoices](#)

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."

SUPPORT QUALITY JOURNALISM JUST 99¢ PER WEEK FOR THE FIRST FOUR WEEKS

START TODAY

000009



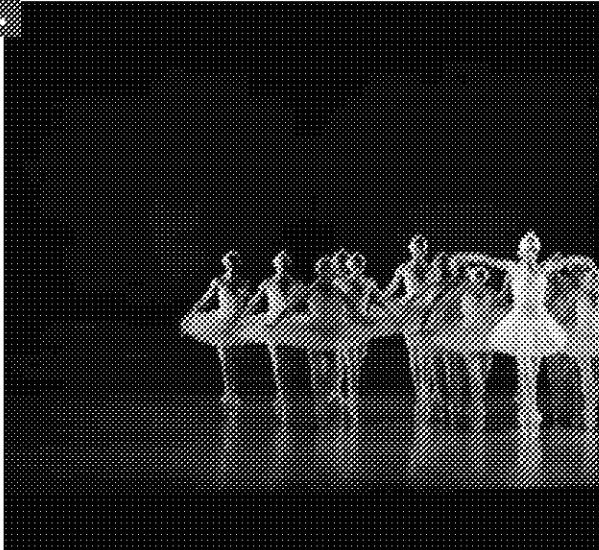
STORY CONTINUES BELOW ADVERTISEMENT

Surveillance device used in prison sets off police probe

SUBSCRIBE

SIGN IN

AdChoices



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.

SUPPORT QUALITY JOURNALISM JUST 99¢ PER WEEK FOR THE FIRST FOUR WEEKS

START TODAY

Some e-mails contradict the warden, stating explicitly that the surveillance device used in prison sets off police probe 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.")

SUBSCRIBE

SIGN IN

AdChoices

At the end of October, the Union of Canadian Correctional Officers took their bosses to court. In a lawsuit, they complained their 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.

With a report from Laura Stone in Ottawa

FOLLOW COLIN FREEZE, ON TWITTER @COLINFREEZE

REPORT AN ERROR LICENSING OPTIONS

63 COMMENTS

SUPPORT QUALITY JOURNALISM

JUST 99¢ PER WEEK FOR THE FIRST FOUR WEEKS

START TODAY



Public Safety Sécurité publique
Canada Canada

Senior Assistant Sous-ministre
Deputy Minister adjoint(e) principal(e)

Ottawa, Canada
K1A 0P8

SECRET (W/A)

DATE:

File No.: PS-13946

MEMORANDUM FOR THE DEPUTY MINISTER

**PRELIMINARY ANALYSIS OF THE NATIONAL SECURITY
CONSULTATION SUBMISSION BY THE PRIVACY COMMISSIONER OF
CANADA AND HIS PROVINCIAL AND TERRITORIAL COUNTERPARTS**

(Information only)

ISSUE

On December 6, 2015, the Privacy Commissioner of Canada and all provincial and territorial privacy commissioners and ombudspersons provided a joint submission to the Government's National Security Consultation. The submission touched on the following consultation topics:

- accountability,
- prevention,
- domestic national security information sharing, and
- investigative capabilities in a digital world.

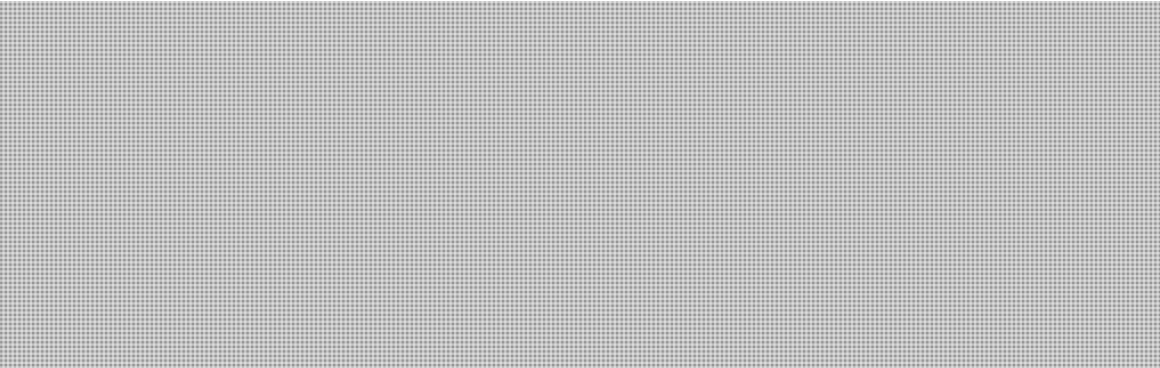
While metadata was discussed in the Green Paper in the context of investigations in a digital world, the submission's comments go beyond this context. The submission also included recommendations related to international information sharing, which is not itself a consultation topic.

The chart attached at **TAB A** provides a summary of the report (**TAB B**) with preliminary analysis of which recommendations of the Office of the Privacy Commissioner (**TAB C**) could be implemented and how.

s.21(1)(a)

SECRET (W/A)

- 2 -



In its submission, the Commissioners call for comprehensive reform of the legislative authorities governing the collection and retention of metadata by police and intelligence agencies. The Commissioners take the perspective that metadata has the same privacy interest as the content of communications, and that current practices and safeguards with regard to collection of metadata are insufficient. The Commissioners' specific concerns and recommendations address a range of contemporary metadata-related issues, beyond the scope of the *Green Paper*. This includes the Federal Court's decision regarding the CSIS Operational Data Analysis Centre; police use of IMSI catchers; the surveillance of journalists in Quebec; and metadata collection by the Communications Security Establishment.



NEXT STEPS

The analysis at **TAB A** is preliminary. Officials continue to analyze this and other consultation input and will incorporate into ongoing policy development.

Should you require any additional information, please do not hesitate to contact me at 613-990-4976 or John Davies, Director General, National Security Policy Directorate at 613-991-1970.

Monik Beauregard

Enclosures: (3)

Prepared by: [redacted] / Lindsey Micholuk [redacted]

s.15(1) - Subv

Accountability		
Recommendation	Considerations	Potential Implementation
Oversight		
<p>Ensure all government institutions with a national security role are subject to expert, independent oversight</p> <p>A committee of Parliamentarians provides democratic accountability, but it would also be important to have review by experts with an in-depth knowledge of the operations of national security agencies and of relevant areas of the law are applied so that rights are effectively protected.</p> <p>Expert review bodies should have meaningful independence from the executive, be non-partisan and have institutional expertise, with knowledge of both domestic and international standards and law.</p>		
<p>Review bodies must be able to collaborate</p> <p>Review bodies must be able to share information so that reviews can be performed in a collaborative and effective manner rather than in silos, as is currently the case.</p> <p>Currently, the confidentiality provisions of the <i>Privacy Act</i> prevent the OPC from sharing information about ongoing investigations with other review bodies, such as the Security Intelligence Review Committee, the Office of the CSE Commissioner or the Civilian Review and Complaints Commission for the RCMP.</p>		

s.21(1)(a)

s.69(1)(g) re (a)

SECRET

Confidence of the Queen's Privy Council

Transparency		
Require transparency reporting by government		
There should be reporting requirements on broader privacy issues dealt with by federal organizations as well as specific transparency requirements for lawful access requests made by agencies involved in law enforcement.		

Prevention (No specific recommendations.)
The Commissioners' concerns largely focus on whether prevention activities would involve widespread internet monitoring. The Commissioners noted that while they appreciate that countering radicalization to violence is a legitimate goal, they advocate for a balanced approach which limits the potential chilling effect and focuses prevention activities or detection efforts on what reliable intelligence reveals are credible threats.

Security of Canada Information Sharing Act		
Recommendation	Considerations	Potential Implementation
Justify the need for changes. The federal government should provide a justification for the new information sharing provisions, including a clear explanation, with concrete examples, of how the previous law created barriers to information sharing required for national security purposes.		

s.21(1)(a)

SECRET
Confidence of the Queen's Privy Council

Raise the standard from "relevance" to "necessity."

Low standards authorizing information to be shared where it is merely of "relevance" to national security goals should be addressed. In contrast CSIS may only collect and analyze information that is "strictly necessary." If "strictly necessary" is adequate for CSIS to collect, analyze and retain information, it is unclear why this standard cannot be adopted for *all* departments and agencies with a stake in national security.

A "dual threshold," where a specific threshold is added for collocation that is higher than the threshold for disclosure, may address departmental officials concerns' that front line staff in non-listed departments do not necessarily have the requisite expertise or experience to make real-time and nuanced decisions to what is necessary and proportional for the purposes of carrying out a national security mandate. The onus of the higher threshold would be shifted to the 17 recipient departments that do have capacity to make such decisions in an informed manner.

s.21(1)(a)

SECRET

Confidence of the Queen's Privy Council

Set clear limits around how long information received or shared is to be retained

National security agencies should be required to dispose of information immediately after analyses are completed and the vast majority of individuals have been cleared of any suspected terrorist activities.

Create an explicit requirement for written information sharing agreements

Elements addressed in these information sharing agreements should include, as a legal requirement, the specific elements of personal information being shared; the specific purposes for sharing; limitations on secondary use and onward transfer, and other measures to be prescribed by regulations, such as specific safeguards, retention periods and accountability measures.

s.21(1)(a)

SECRET

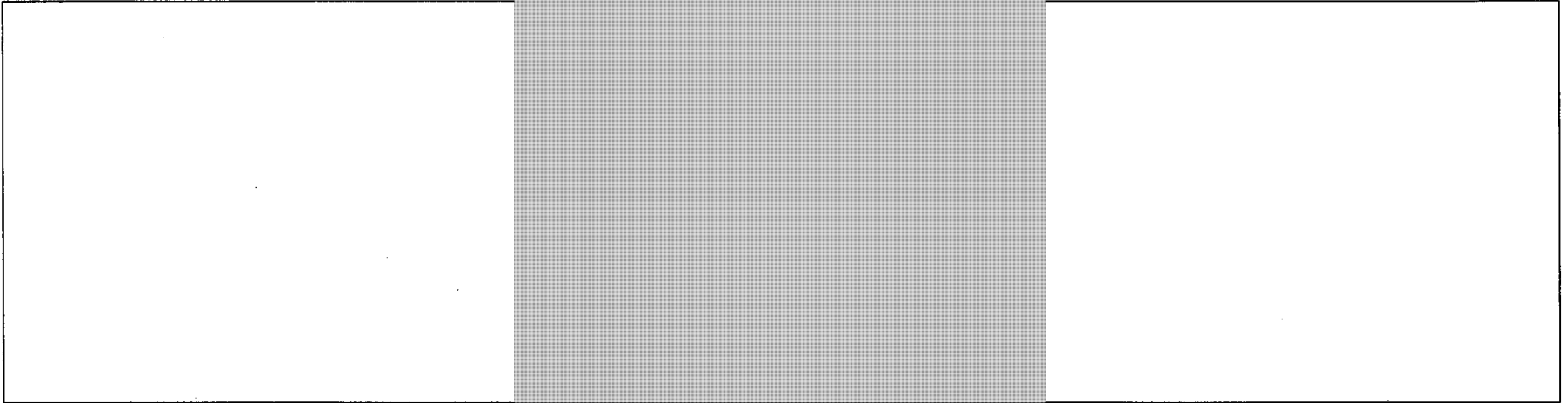
Confidence of the Queen's Privy Council

<p>Create a legal requirement to conduct Privacy Impact Assessments</p> <p>The OPC has been concerned to see how few Privacy Impact Assessments were undertaken in relation to the information sharing provisions created under Bill C-51. Privacy Impact Assessments help to identify privacy risks involving the use of personal information and propose solutions to mitigate them. They are currently required under a government policy, but not under the <i>Privacy Act</i>.</p>		
<p>Consider information sharing beyond Bill C-51</p> <p>The information sharing provisions stemming from Bill C-51 are not the only mechanism by which information-sharing for national security purposes takes place. Safeguards such as necessity and proportionality should apply to all domestic information sharing.</p>		

International Information Sharing		
Recommendation	Considerations	Potential Implementation
<p>Set clear rules to ensure respect for international human rights law</p> <p>Clear statutory rules should be enacted to prevent information sharing from resulting in serious human rights abuses and violations of Canada's international obligations.</p> <p>Consideration should be given to incorporating into law some of the privacy principles agreed to between Canada and the United States under the Beyond the Border Action Plan.</p>		

s.21(1)(a)

SECRET
Confidence of the Queen's Privy Council



Investigative Capabilities in a Digital World		
Recommendation	Considerations	Potential Implementation
Metadata in a Criminal Law Context		
<p>Justify lowering the standards from those recently adopted under Bill C-13</p> <p>Government must provide precise explanations as to why existing thresholds cannot be met, and why administrative authorizations to obtain metadata, rather than judicial authorizations, sufficiently protect Charter rights in cases where there are no exigent circumstances.</p>		
<p>Enhance privacy protections: general considerations</p> <p>Recent cases of metadata collection – for example, by the Communications Security Establishment, CSIS, the RCMP, Quebec provincial police and Montreal police – show that existing standards should, in fact, be tightened and that privacy protections should be enhanced. In many cases, the collection of</p>		

SECRET

Confidence of the Queen's Privy Council

s.21(1)(a)

<p>metadata, including with warrants, has involved innocent people not suspected of wrongdoing.</p> <p>A modernized law must reflect the fact that metadata can reveal personal information that is more sensitive than the data for which warrants have traditionally been required in the pre-digital world. It must also ensure that modern investigative tools do not violate the privacy of law-abiding citizens.</p>		
<p>Maintain the role of judges and better define conditions for access to metadata</p> <p>Maintaining the role of judges in the authorization of warrants for the collection of metadata by law enforcement is critical because they ensure the necessary independence for the protection of human rights.</p> <p>However, it is also incumbent on Parliament to better define the conditions under which the sensitive metadata of Canadians should be available to police forces.</p> <p>On the whole, these criteria should provide law enforcement access to metadata where necessary to pursue their investigations – but only in a way that recognizes the often sensitive nature of this type of information.</p> <p>Conditions should include adopting sufficiently high legal thresholds and criteria for the issuance of court orders. For example, collection of metadata could be limited to cases where all other investigative methods have been exhausted and for violent crimes where public safety may outweigh privacy risks.</p> <p>In cases where these criteria are met, there should be conditions aimed at protecting the privacy of people incidentally targeted by a</p>		

s.21(1)(a)

s.69(1)(g) re (a)

SECRET

Confidence of the Queen's Privy Council

<p>warrant, but not suspected of involvement in a crime. For example, use of the data could be restricted to the crime being investigated, and metadata not related to criminal activity destroyed without delay.</p>		
<p>Justify why new data retention requirements are required beyond current preservation orders</p> <p>Preservation orders are a current tool available by law enforcement to ensure that a communications company's customer data is not deleted during an investigation. The government's discussion paper suggests companies should be required to retain their customers' data without such court orders.</p> <p>The imposition of such an obligation would clearly need to be justified and its scope would need to be proportional. A similar obligation imposed in a European data retention directive was invalidated by the European Court of Justice, in large part because it significantly interfered with fundamental rights and lacked sufficient limits on how law enforcement could use the information.</p>		
<p>Metadata and national security</p>		
<p>Amend the <i>National Defence Act</i></p> <p>Following the review of the CSE's metadata sharing, the Office of the Privacy Commissioner of Canada recommended that the <i>National Defence Act</i> be amended to clarify that the CSE's powers with respect to the collection, use and disclosure of personal information be accompanied by specific legal safeguards to protect the privacy of Canadians.</p>		

s.21(1)(a)

Ensure destruction of incidental personal information

The law should be amended to ensure that where the personal information of individuals not suspected of terrorism is obtained incidentally to the collection of information about threats, the former should be destroyed once it has been determined after analysis that individuals have been cleared of any suspected terrorist activities.

Interception and Encryption

Look for technical solutions before considering a new law

Parliament should proceed cautiously before attempting to legislate solutions. It would be preferable to explore technical solutions which might support discrete, lawfully authorized access to specific encrypted devices, as opposed to imposing general legislative requirements.

The government already has powers under the Protecting Canadians from Online Crime Act which, since 2015, have empowered judges to attach an assistance order to any search warrant, interception order, production order or other form of electronic surveillance. These have been used in investigations to defeat security features or compel decryption keys.

It is also important to further note that federal provisions already exist for telecommunications carriers to build in surveillance capability, retain communications metadata and provide decrypted content to government upon request. These requirements, the Solicitor-General Enforcement Standards, have been a condition of licensing since the mid-1990s.

SECRET

Confidence of the Queen's Privy Council

s.21(1)(a)

As with the assistance order scheme, if these requirements are not being properly implemented or enforced, it would be important for the government to explain where the regime falls short.

If a new law is considered, take a narrow approach

If an obvious technological solution is not found and the government believes legislation is required, amendments should reflect the principles of necessity and proportionality in order to narrow how much information is decrypted; and also that such extraordinary measures should be used as a last resort.

December 5, 2016

National Security Policy Directorate
Public Safety Canada
269 Laurier Avenue West
Ottawa, Ontario K1A 0P8
ps.nsconsultation-consultationsn.sp@canada.ca

Subject: Consultation on Canada's National Security Framework

Dear Sir/Madam:

I, along with my provincial and territorial counterparts, would like to take this opportunity to respond to the Call for Submissions issued on September 8, 2016 in support of the consultation on key elements of Canada's national security laws and policies to ensure they reflect the rights, values and freedoms of Canadians. Our Offices oversee compliance with federal, provincial and territorial privacy legislation and, as such, are responsible for protecting and promoting privacy rights of individuals.

Introduction

We note that the stated purpose of the National Security Green Paper is to “prompt discussion and debate about Canada’s national security framework,” which is broader than the reforms brought about by Bill C-51, the *Anti-Terrorism Act*, 2015. We fully support the need to review the entire framework. Bill C-51 is only part, even a small part, of the national security laws in force in Canada and it would be a mistake to only review the most recent addition to an important edifice. But to do that in a comprehensive way, the focus cannot be only on addressing challenges faced by national security and law enforcement agencies.

National security agencies have an important and difficult mandate in protecting all Canadians from terrorist threats, and we believe they generally strive to do their work in a way that respects human rights. But history has shown us that serious human rights abuses can occur, not only abroad but in Canada, in the name of national security.

In order to ensure our laws adapt to current realities, it is important to consider all that we have learned before and after 2001, including the revelations of Edward Snowden regarding mass surveillance, other known risks regarding the protection of privacy and human rights such as those identified during commissions of inquiry, as well as recent terrorist threats and incidents.

.../2

- 2 -

Key lessons from this history are that the legal framework should include clearer safeguards to protect rights and prevent abuse, that national security agencies must be subject to effective and comprehensive review, and that new state powers must be justified on the basis of evidence.

Accountability

We are in full agreement with the Green Paper's statement that "effective accountability mechanisms are key to maintaining the public's trust in [intelligence and national security] agencies."¹ However, the proposed creation of a new National Security and Intelligence Committee of Parliamentarians as envisaged by C-22, although a welcome step in the right direction, is insufficient. We note that other countries have implemented an oversight model which includes review by a Committee of Parliamentarians, while maintaining review by experts. While the former provides democratic accountability, the latter ensures that in-depth knowledge of the operations of national security agencies and of relevant areas of the law are applied so that rights are effectively protected. There are, however, still gaps in coverage in Canada by expert review bodies. Of the 17 agencies authorized to receive information under the *Security of Canada Information Sharing Act* (SCISA), only three are currently subject to expert review. As well, there are other government institutions which have a role in national security, including the Privy Council Office.

The Green Paper notes that in some countries, expert review takes the form of a consolidated model, meaning one review body is responsible for all relevant government institutions – a so-called "Super-SIRC" – whereas in others, different bodies are limited to reviewing one institution or one aspect of national security activities. We have no strong preference between the two models, so long as all government institutions involved in national security are covered. Furthermore, if there is more than one review body, all bodies must be able to collaborate in their review activities, and no longer operate in silos.

Among the models in place around the world is the US model where one body, the Privacy and Civil Liberties Oversight Board, is responsible for reviewing the activities of a number of national security agencies for compliance with both privacy and other human rights. Importing that concept in Canada might mean creating a "fully consolidated model", where a single body would be responsible for reviewing all government institutions and all areas of the law.

While such a model would have some merit, we believe it is preferable to have the activities of national security agencies reviewed both by the Office of the Privacy Commissioner and either a single or multiple dedicated national security review bodies. This creates some

.../3

¹ Our Security, Our Rights: National Security Green Paper, Background Document 2016, p.9

- 3 -

overlap, but it ensures that both national security and privacy can be examined by experts with deep and broad knowledge of both privacy and national security law. Among other factors, there is value in having the privacy impact of the work of national security agencies reviewed by an institution that also reviews the work of other government departments, so that best practices and developments in privacy law can apply across government.

As mentioned, review bodies must be able to share information, including classified and personal information, so that their respective reviews can be performed in a collaborative and effective manner rather than in silos as is currently the case. The detriments to siloed review include duplication of effort with resulting effects on resources, but above all less informed and therefore less effective review by all relevant bodies. Given the OPC's extensive and ongoing work in this area, it should be included among the review bodies granted the authority to share and receive information.

Minister Goodale acknowledged that the OPC is a "key part of the parliamentary oversight and accountability apparatus."² This reflects the fact that information, including personal information, is a necessary ingredient in the work of national security agencies, many of which call information their "lifeline." Currently, the confidentiality provisions of the *Privacy Act* prevent the OPC from sharing information with other review bodies, such as the Security Intelligence Review Committee (SIRC), the Office of the Communications Security Establishment Commissioner (OCSEC) or the Civilian Review and Complaints Commission for the RCMP concerning ongoing investigations into national security practices. A system which proposes removal of silos between government departments for information sharing purposes in the name of national security must provide for the same removal of silos for the review bodies which ensure their activities comply with the law.

In order to be fully effective, review bodies must also be properly resourced. Greatly enhanced national security activities and initiatives in recent years have resulted in much heightened public concerns about privacy, including mass surveillance, but without any consequential increase in funding for the oversight bodies. For the OPC's part, it has been forced to risk manage its limited resources, moving efforts from other mandated activities. This is less than ideal. It is also insufficient to produce effective review and privacy oversight, which are essential to maintain trust in national security activities.

.../4

² Hon. Ralph Goodale (Minister of Public Safety and Emergency Preparedness), appearance before the Standing Committee on Public Safety and National Security, October 6, 2016 (at 1535).

- 4 -

The OPC's research on oversight of security and intelligence agencies has led it to determine that, beyond resourcing, effective review requires meaningful independence from the executive, non-partisanship and institutional expertise, with knowledge of both domestic and international standards and law.³

Prevention

The Green Paper indicates the path to terrorism begins with “radicalization to violence,” and describes a number of preventative activities which can be undertaken to counteract radicalization.⁴ While there is unquestioned value in community engagement, conduct of research and promotion of alternative narratives, we would be concerned if prevention activities, which include detection efforts, involved widespread internet monitoring. By creating a situation where people feel inhibited or censor themselves for fear that their views may be misinterpreted, they may turn away from using this important tool for personal development and for exploring ideas. There is some evidence this may already be happening: a recent study by the US Pew Research Center revealed that nearly nine-in-ten respondents had heard of government surveillance programs to monitor phone use and internet use and of those, a quarter had changed their online habits.⁵

There is a privacy interest in much that we do online, and the expectation of privacy will vary according to the context: a private “direct message” between users on a social media network will likely engage a greater expectation of privacy than, say, a public tweet. Furthermore, the perception exists that person-to-person e-mails are private communications, however vulnerable they are to interception. The intrusiveness of proposed “prevention activities” must take this fact into account. Overall, while we appreciate that countering radicalization is a legitimate goal, we advocate a balanced approach which limits the potential chilling effect and focuses prevention activities or detection efforts on what reliable intelligence reveals are credible threats.

.../5

³ This research included reviews of previous Commissions of Inquiry, reports and research from stakeholders, other review bodies and academic literature.

⁴ Our Security, Our Rights: National Security Green Paper, Background Document, 2016, p. 15

⁵ Americans' Privacy Strategies Post-Snowden, March 2015 (<http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/>)

Domestic National Security Information Sharing

The concerns we have in this area, as articulated in the OPC's previous submissions to the Standing Senate Committee on National Security and Defence⁶ and Standing Committee on Public Safety and National Security of the House of Commons,⁷ remain. We recognize that protecting the security of Canadians is important, and that in order to do so, greater information sharing may sometimes lead to the identification and suppression of security threats. However, the scale of information sharing put in place by SCISA is unprecedented, the scope of the new powers conferred is excessive, particularly as these powers affect ordinary Canadians, and the safeguards protecting against unreasonable loss of privacy are seriously deficient.

(I) NEED FOR EVIDENTIARY BASIS

Given that increased information sharing affects privacy and other rights, the justification for SCISA should be made clear. We have yet to hear a compelling explanation, with practical examples, of how the previous law created impediments to information sharing operationally required for national security purposes. When Bill C-51 was introduced in Parliament, the government maintained that SCISA was necessary because some federal agencies lacked clear legal authority to share information related to national security. The Green Paper speaks to complexity around sharing which can "prevent information from getting to the right institution in time."⁸ These references to the "complexity" of the old law do not explain its shortcomings or how it frustrated the government's national security operations. Situations where legal authority was lacking should be identified, but so far they have not been. A clearer articulation of the problems with the previous law would help define a proportionate solution.

(II) RELEVANCE AS THE LEGAL STANDARD

We remain concerned that SCISA authorizes information to be shared where it is merely of "relevance" to national security goals. Setting such a low standard is a key reason why the risks to law abiding citizens are excessive. Revelations by Edward Snowden have shown how pervasive government surveillance programs can be, including some in place in Canada, and how they can affect all Canadians, not only those suspected of being a terrorist threat. If "strictly

.../6

⁶ OPC's Submission to the Standing Senate Committee on National Security and Defence on Bill C-51, *the Anti-Terrorism Act, 2015* (https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2015/parl_sub_150416/)

⁷ OPC's Submission to the Standing Committee on Public Safety and National Security of the House of Commons on Bill C-51, *the Anti-Terrorism Act, 2015* (https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2015/parl_sub_150305/)

⁸ Our Security, Our Rights: National Security Green Paper, Background Document, 2016, p. 26.

- 6 -

necessary”⁹ is adequate for CSIS to collect, analyze and retain information, as has been the case since its inception, it is unclear to us why this cannot be adopted as a standard for information sharing for *all* departments and agencies with a stake in national security. Necessity and proportionality are the applicable legal standards in Europe. European law permits member states to interfere with a citizen’s protected privacy rights only to the extent that the interference is necessary and proportionate in a democratic society.

As an alternative to adopting a “necessity and proportionality” standard for information-sharing across the board, consideration could be given to adopting dual thresholds, one for the disclosing institutions, and another for the 17 recipient institutions. An important point raised by departmental officials during the current review of SCISA by the Standing Committee on Access to Information, Privacy and Ethics is that because front line staff in non-listed departments do not necessarily have the requisite expertise or experience to make real-time and nuanced decisions as to what is necessary and proportional for purposes of carrying out a national security mandate, the onus of the higher threshold would be shifted to the 17 recipient departments that do have the capacity to make such decisions in an informed manner. The Committee discussed the issue of a “dual threshold” and this would appear a reasonable solution under the following condition. In order to close the triage gap between these two different thresholds, the 17 recipient departments should be responsible for selectively receiving and retaining only information that meets the higher threshold of necessity and proportionality (subject to any further limits imposed by their enabling laws), and under a positive legal obligation to return or destroy information that does not.

It should be noted that any changes made or contemplated which involve Canada’s national security activities could affect the European Union’s assessment of Canada’s status as an adequate jurisdiction towards which the personal data of the European citizens can be transferred. According to the European Court of Justice’s decision in *Schrems*¹⁰, necessity and proportionality are important considerations to maintain that status. This decision could have consequential implications for Canada’s trade relationship with the EU.

(III) DATA RETENTION

An issue of equal importance which the OPC has flagged in previous submissions is the setting of clear limits around how long information received or shared is to be retained. If the government maintains that the sharing of information about ordinary citizens (such as travelers or taxpayers) to one or more of the 17 recipient institutions under SCISA is necessary to undertake

.../7

⁹ S. 12, *Canadian Security Intelligence Service Act* (R.S.C., 1985, c. C-23)

¹⁰ Court of Justice of the European Union, *Maximilian Schrems v Data Protection Commissioner* (6 October 2015) (<http://eur-lex.europa.eu/legal-content/EN/SUM/?uri=CELEX:62014CJ0362>)

- 7 -

analyses meant to detect new threats, national security agencies should be required to dispose of that information immediately after these analyses are completed and the vast majority of individuals have been cleared of any suspected terrorist activities. This would be in keeping with the recent judgment of the Federal Court which held that retention of "associated data" for people who are not a threat to national security was illegal.¹¹

(IV) INFORMATION SHARING AGREEMENTS

We maintain the need for an explicit requirement for written information agreements, as the OPC recommended in the context of Bill C-51.¹² These agreements, far from being cumbersome or unworkable, could be drafted at a level of specificity beyond what the statute provides but still remain general enough to be operationally flexible. They need not be at the individual activity level but rather designed to govern information sharing at the level of programs specific to departments, and could provide more specificity beyond the core standards. Elements addressed in these Agreements should include, as a legal requirement, the specific elements of personal information being shared; the specific purposes for the sharing; limitations on secondary use and onward transfer; and other measures to be prescribed by regulations, such as specific safeguards, retention periods and accountability measures. The OPC has, in the context of *Privacy Act* reform, recommended that it should be notified of all new or amended agreements to share personal information. The OPC should also be given explicit authority to review and comment, and the right to review existing agreements on request by OPC to assess compliance. Finally, departments should be required to publish the existence and nature of information-sharing agreements between departments or with other governments.¹³

(V) PRIVACY IMPACT ASSESSMENTS

An additional tool to determine whether government initiatives involving the use of personal information raise privacy risks is the Privacy Impact Assessment (PIA), which describes and quantifies these risks, and proposes solutions to eliminate or mitigate them to an acceptable level. At the federal level, the obligation to conduct PIAs is currently at the policy level, and is

.../8

¹¹ 2016 FC 1105. See also the discussion at pages 10-11 of the European Court of Justice decision invalidating the 2006 EU Data Retention Directive.

¹² OPC's Submission to the Standing Senate Committee on National Security and Defence on Bill C-51, *the Anti-Terrorism Act, 2015* (https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2015/parl_sub_150416/)

¹³ *Privacy Act* Reform in an Era of Change and Transparency: recommendation 1 (https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl_sub_160322/#toc1_1a)

triggered by a new or substantially modified program or activity.¹⁴ Despite this policy obligation, the OPC was concerned to see how few PIAs were undertaken in relation to SCISA. As such, the OPC has, in the context of advice to Parliament on reforming the *Privacy Act*, recommended that the obligation to conduct PIAs be elevated to a legal requirement rather than a policy one.¹⁵ This is equally applicable in the context of the proposed reform to Canada's national security legal framework.

(VI) RECORD KEEPING

Our detailed views on accountability appear elsewhere in this document, but at this juncture it should be stated that record-keeping is an essential prior condition to effective review. The OPC's advice to Public Safety in the context of the SCISA Deskbook was clear on this point: it called for guidance on the content of records that should be kept, including a description of the information shared and the rationale for disclosure.

(VII) DOMESTIC INFORMATION SHARING UNDER OTHER LAWFUL AUTHORITIES

Finally, SCISA is not the only mechanism by which information-sharing for national security purposes takes place.¹⁶ In principle, we are of the view that the safeguards, in particular necessity and proportionality, which the OPC recommended in its review of SCISA should apply to all domestic information sharing.¹⁷ As noted above, under EU jurisprudence and principles of international law, in a democratic society, intrusive state measures need to be rigorously justified as being both necessary and proportionate.¹⁸

International Information Sharing

One of the most important lessons learned from Canada's anti-terrorism efforts since 9/11 has been that international information sharing can lead to serious human rights abuses, including torture. The existing legal framework must be clarified to reduce these risks to a minimum and

.../9

¹⁴ Treasury Board of Canada Secretariat, *Directive on Privacy Impact Assessment*, effective April 2010. <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308>

¹⁵ *Privacy Act Reform in an Era of Change and Transparency: recommendation 7* (https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl_sub_160322/#toc1_2d)

¹⁶ Cohen, Stanley, "National Security Information Sharing", Chapter 8 from *Privacy, Crime and Terror — Legal Rights and Security in a Time of Peril* (Butterworths, 2005)

¹⁷ OPC, "C-51 and surveillance," Chapter 2 from *2015-2016 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act* (Sept. 2016) –

(https://www.priv.gc.ca/en/opc-actions-and-decisions/reports-to-parliament/201516/ar_201516/#heading-0-0-4)

¹⁸ See footnote 10.

- 9 -

must consider the fact that once information is shared with foreign states, Canada has lost control of that information. In the OPC's submission to the Senate Standing Committee on National Security and Defence on Bill C-44, *An Act to amend the Canadian Security Intelligence Service Act and other Acts*¹⁹ on March 9, 2015, it cited the Supreme Court of Canada decision in *Wakeling v. United States of America*²⁰ which confirmed the importance of accountability and oversight measures to safeguard information shared with foreign states. Absent statutory safeguards, the protection of individuals against the risk of mistreatment would depend on the application of general constitutional principles which have not been defined clearly in the context of information sharing amongst national intelligence agencies.

Parliament also has a role in protecting individuals against violations of human rights. We would suggest that any powers conferred on national security agencies must be exercised in a way that respects Canada's obligations under international human rights law in general and, specifically, the Convention Against Torture. Clear statutory rules should be enacted to prevent information sharing from resulting in a violation of Canada's international obligations. We note Justice O'Connor's recommendation that "information should never be provided to a foreign country where there is a credible risk that it will cause or contribute to the use of torture."²¹

In addition, the Governments of Canada and the United States have developed joint privacy principles in support of the *Beyond the Border Action Plan: A Shared Vision for Perimeter Security and Economic Competitiveness*.²² These principles include reference to ensuring accuracy of information, limiting retention of information collected, ensuring relevance and necessity in the collection of personal information, limiting onward transfer of information to third countries, allowing redress before existing national authorities where a person believes their privacy has been infringed and requiring effective oversight. An issue for consideration is importing some of the principles into law. Our concerns regarding information sharing agreements as articulated above apply equally to international information sharing activities. We would urge that minimum content be defined, and that agreements be reviewed by independent bodies including the OPC.

.../10

¹⁹ OPC's statement before the Senate Standing Committee on National Security and Defence (SECD) on Bill C-44, *An Act to amend the Canadian Security Intelligence Service Act and other Act*, March 9, 2015 (https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2015/parl_20150309/)

²⁰ 2014 SCC 72.

²¹ The recommendation continues: "Policies should include specific directions aimed at eliminating any possible Canadian complicity in torture, avoiding the risk of other human rights abuses and ensuring accountability." *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar*, 2006; recommendation 14, page 345.

²² *Beyond the Border Action Plan: Joint Statement of Privacy Principles*, June 28, 2012 (<https://www.publicsafety.gc.ca/cnt/nws/nws-rlss/2012/20120628-2-en.aspx>)

Investigative Capabilities in a Digital World

The Green Paper rightly claims that law enforcement and national security investigators must be able to work as effectively in the digital world as they do in the physical, and that laws governing the collection of evidence have not kept pace with new technologies. However, from these premises one does not proceed to loosen legal rules or lower standards of protection. To the contrary, safeguards which have long been part of our legal traditions must be maintained yet adapted to the realities of modern communication tools, one of which is that these devices hold and transmit extremely sensitive personal information.

A preliminary observation before entering the discussion of metadata: the Green Paper appears to conflate law enforcement and national security agencies, which are two very distinct and separate mechanisms for ensuring public safety. Law enforcement and intelligence agencies have different mandates and work in different environments. Clarity on this is critical since different rules could be adopted for different manners of investigations. Plainly, the context of use for investigative powers matters a great deal to the privacy of individuals.

(I) METADATA IN A CRIMINAL LAW CONTEXT

Metadata, generated constantly by digital devices, can be far more revealing than the information on the outside of an envelope or found in a phonebook, as it is commonly characterized. For instance, metadata can reveal medical conditions, religious beliefs, sexual orientation and many other elements of personal information.²³ The British signals intelligence agency, GCHQ, has publicly stated that metadata is more revealing than the content of communications²⁴. In short, it can be highly sensitive depending on the context.

Basic subscriber information, which is a form of metadata, is undeniably useful for investigative purposes. The Green Paper suggests it should be available to law enforcement more easily than under current laws because the police, particularly in the early stages of an investigation, do not have enough evidence to be in a position to satisfy a judge that there is reasonable grounds to believe a crime was committed and that the metadata requested would assist in the investigation.

.../11

²³ Office of the Privacy Commissioner, *Metadata and Privacy*, 2014. (https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/md_201410/)

²⁴ Daniel Weitzner, who founded the Internet Policy Research Initiative at the Massachusetts Institute of Technology, considers metadata “arguably more revealing [than content] because it’s actually much easier to analyze the patterns in a large universe of metadata and correlate them with real-world events than it is to go through a semantic analysis of all of someone’s email and all of someone’s telephone calls.” (Daniel Weitzner, quoted in E. Nakashima, “Metadata reveals the secrets of social position, company hierarchy, terrorist cells”, *The Washington Post*, June 15, 2013.)

- 11 -

Bill C-13, the *Protecting Canadians from Online Crime Act*, in force since 2015, has already lowered legal thresholds for accessing metadata. Under it, a production order for "transmission data", transaction records and location tracking can be obtained from a judge on a standard of "reasonable grounds to suspect".²⁵ An order to preserve information or evidence can also be sought on mere suspicion,²⁶ giving law enforcement more time to find information in order to satisfy a judge on reasonable grounds to believe that an order for the production of the content of communications is warranted. The *Criminal Code* and the Supreme Court of Canada's decision in *Spencer*²⁷ even allow for collection in exigent circumstances with no court authorization at all.

We have not seen evidence why these provisions do not give law enforcement adequate tools to do their job. The government is proposing to further reduce safeguards. It has a duty to provide precise explanations as to why existing thresholds cannot be met and why administrative authorizations to obtain metadata, rather than judicial authorizations, sufficiently protect Charter rights absent exigent circumstances.

In our view, recent cases of metadata collection show that existing standards should, in fact, be tightened and that privacy protections should be enhanced. The past few years has seen extensive coverage and public concern over the operations of the Communications Security Establishment²⁸, CSIS²⁹, the RCMP³⁰, the Sûreté du Québec and the Montreal Police (SPVM)³¹ stemming from the collection, use, retention and disclosure of metadata. In many cases, the collection of metadata, including with warrants, involved innocent individuals who were not suspected of criminal activity or of representing a threat to national security.

.../12

²⁵ Criminal Code of Canada, section 487.016 (<http://laws-lois.justice.gc.ca/eng/acts/C-46/page-109.html>)

²⁶ Criminal Code of Canada, section 487.013 (<http://laws-lois.justice.gc.ca/eng/acts/C-46/page-109.html>)

²⁷ R. v. Spencer, 2014 SCC 43, [2014] 2 S.C.R. 212 (<https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do>)

²⁸ Office of the Communications Security Establishment Commissioner Annual Report 2015-2016, p. 20. (<https://www.ocsec-bccst.gc.ca/s21/s68/d365/eng/highlights-reports-submitted-minister#toc-tm-2>)

²⁹ CSIS broke law by keeping sensitive metadata, Federal Court rules, November 3, 2016 <http://www.cbc.ca/news/politics/csis-metadata-ruling-1.3835472>; Le SCRS a illégalement conservé des données personnelles, dit la Cour fédérale, November 3, 2016 <http://www.lapresse.ca/actualites/justice-et-affaires-criminelles/actualites-judiciaires/201611/03/01-5037489-le-scrs-a-illegalement-conserve-des-donnees-personnelles-dit-la-cour-federale.php>

³⁰ Review of the Royal Canadian Mounted Police – Warrantless Access to Subscriber Information https://www.priv.gc.ca/en/opc-actions-and-decisions/reports-to-parliament/201314/201314_pa/#heading-0-0-4

³¹ La SQ a espionné six journalistes: Le ministre de la Sécurité publique ordonne une enquête administrative, le 3 novembre, 2016, <http://www.ledevoir.com/societe/medias/483697/six-journalistes-surveilles-par-la-sq>
Quebec to hold public inquiry into police surveillance of journalists, November 3, 2016 <http://www.theglobeandmail.com/news/national/quebec-to-hold-public-inquiry-into-surveillance-of-journalists/article32657198/>

- 12 -

A modernized law adapted to new technologies must take into consideration the fact that metadata emitted by digital devices can reveal personal information whose sensitivity often exceeds that for which warrants have traditionally been required in the pre-digital world. It must also ensure that the state's modern investigative tools do not violate the privacy of law abiding citizens.

First and foremost, it is important to maintain the role of judges in the authorization of warrants for the collection of metadata by law enforcement. Despite its imperfections, the judicial system ensures the necessary independence for the protection of human rights.

But we also now know that it is probably not enough to rely solely on the judiciary. Indeed, some judges have made this point themselves. In a recent ruling³², Ontario Superior Court Justice John Sproat found he did not have the power to impose privacy protective conditions on a production order involving the metadata of thousands of individuals who happened to be within the vicinity of a number of crimes. He said this responsibility rests with legislators.

We also believe that it is incumbent on Parliament to better define the conditions under which the sensitive metadata of Canadians should be available to police forces. These conditions include adopting sufficiently high legal thresholds and criteria for the issuance of court orders, but also, where these criteria are met, adding limitations to protect the privacy of people who are incidentally targeted by a warrant but are not suspected of involvement in a crime.

The criteria precedent to the issuance of orders would include but may not be limited to the burden of proof (suspicion or belief). On the whole, these criteria should provide law enforcement access to metadata where necessary to pursue their investigations but only in a way that recognizes the often sensitive nature of this type of information. For example, it could be prescribed that the collection of metadata should be a last resort, after all other investigative methods have been exhausted. This is already a condition for access to the content of communications and, as stated, metadata can be more sensitive in nature. Similarly, this type of surveillance could be limited to serious crimes to be prescribed in legislation, for instance crimes of violence where public safety interests may outweigh potential risks to privacy.

In cases where those pre-conditions are met, the law should then add conditions to protect the privacy of people who are incidentally targeted by a warrant but are not suspected of involvement in a crime. Judges could also be authorized to issue case specific limitations, where warranted. For example, there could be restrictions on use and disclosure (only for the

.../13

³² R. v Rogers Communications, 2016 ONSC 70.

investigation of the crime for which the authorization is granted) and limits on retention (metadata related to communications that have no connection with criminal activity should be destroyed without delay).

(II) RETENTION

The Green Paper also suggests facilitating police investigations by adopting in law general data retention requirements which would prevent companies from deleting their customers' data before law enforcement can seek production orders. We note that in 2014, the European Court of Justice (ECJ) issued a decision³³ invalidating the 2006 EU Data Retention Directive,³⁴ largely on the basis that it entailed a significant interference with Europeans' fundamental rights without imposing sufficient limitations on law enforcement's use of the information collected. While the ECJ recognized that the objective of fighting terrorism and serious crime was legitimate, it found that the retention of data for the purpose of possible access by national law enforcement authorities seriously interfered with the right to private life and the protection of personal data, both of which are guaranteed in the Charter of Fundamental Rights ("EU Charter"). Article 52(1) of the EU Charter requires that any limitation on the exercise of guaranteed rights be necessary and proportionate. The ECJ held that the absence of any limit on whose information could be retained or how it could be accessed or used, and the lack of guidance to national authorities in controlling the use of retained data, meant that the Directive entailed "a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what it is strictly necessary."

Preservation demands (to hold information for 21 days) and orders (which preserve information for three months) are a current tool under the *Criminal Code* which can be used. We have not seen evidence why these tools do not work. Introducing a broad retention requirement, not only impedes on human rights, as noted in the ECJ decision, it also increases the risks of breaches to that personal information. Retention requirements, if any, should be scoped narrowly, focussing on serious crime only, and should be for the briefest period of time possible.

.../14

³³ The full ECJ judgement: eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&rid=1

³⁴ Directive 2006/24/EC: <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1480100474890&uri=CELEX:32006L0024>

(III) METADATA IN A NATIONAL SECURITY CONTEXT

Earlier this year, OCSEC reported on inappropriate information sharing conducted by the Communications Security Establishment (CSE).³⁵ In short, due to a filtering technique that became defective, metadata was not being properly minimized (for example, it was not removed, altered, masked or otherwise rendered unidentifiable) before being shared with international “Five Eyes” partners—the signals intelligence agencies of Australia, New Zealand, the United Kingdom and the United States. As noted in our subsequent report³⁶, CSE shared large volumes of metadata with its international partners, some of which may have had a “Canadian privacy interest.”

The OPC made several recommendations following its investigation into the matter, including that CSE conduct a PIA on their metadata program and that the *National Defence Act* be amended not only to clarify the CSE’s powers but that those powers be accompanied by specific legal safeguards with respect to collection, use and disclosure in order to protect the privacy of Canadians. While the government maintains that metadata is essential for identifying threats, this case demonstrates that CSE activities related to metadata can affect the privacy of a large number of Canadians, and that these activities should be governed by appropriate legal safeguards.

In another recent case, the Federal Court found that CSIS had unlawfully retained for an extended period metadata that was not “strictly necessary” to its mandate related to threats to national security.³⁷ In our view, the law should be amended to ensure that where the personal information of individuals who are not suspected of terrorism is obtained incidentally to the collection of information about threats, the former should be destroyed once it has been determined after analysis that individuals have been cleared of any suspected terrorist activities.

(IV) INTERCEPTION AND ENCRYPTION

Context

Encryption represents a particularly difficult dilemma. As the Green Paper sets out in its scenarios, encryption can be a significant obstacle to lawful investigations and even to the

.../15

³⁵ Office of the Communications Security Establishment Commissioner Annual Report 2015-2016, p. 20. (<https://www.ocsec-bccst.gc.ca/s21/s68/d365/eng/highlights-reports-submitted-minister#toc-tm-2>)

³⁶ The OPC’s 2015-2016 Annual Report to Parliament on the *Personal Information Protection and Electronic Documents Act* and the *Privacy Act*: Chapter 2: C-51 and surveillance (https://www.priv.gc.ca/en/opc-actions-and-decisions/reports-to-parliament/201516/ar_201516/#heading-0-0-4)

³⁷ Federal Court of Canada, *In the Matter of An Application by X for Warrants ...*, 2016 FC 1105 ([http://cas-cdc-wwww02.cas-satj.gc.ca/rss/DES%20\(warrant\)%20nov-3-2016%20public%20judgment%20FINAL%20\(ENG\).pdf](http://cas-cdc-wwww02.cas-satj.gc.ca/rss/DES%20(warrant)%20nov-3-2016%20public%20judgment%20FINAL%20(ENG).pdf))

- 15 -

enforcement of judicial orders. As a legal matter, individuals who use it and companies that offer it to their customers are subject to laws and judicial warrants, and these sometimes require access to personal information where legitimately needed in cases where public safety is at risk. On the other hand, as a technological tool, encryption is extremely important, even essential, for the protection of personal information and for the security of electronic devices in use in the digital economy. Unfortunately, the crux of the problem springs from the fact there is no known way to give systemic access to government without simultaneously creating an important risk to the security of this data for the population at large. Laws should not ignore this technological fact.

For contextual purposes, it is useful to distinguish between three primary modes of encryption: (1) traditional, which routinely is applied to systems and infrastructure (e.g. internal e-mail or telecommunications networks), where service providers typically hold the cryptographic key, (2) end-device encryption, such as that found on certain handheld devices and computers, where some service providers hold the key, while other firms do not, and, (3) third-party encryption software or applications (end-to-end encryption) which consumers can freely download to their devices, and where typically only the users control the key. It is the second and third encryption scenarios that pose more challenges in terms of how to address the needs of law enforcement.

International approaches

We fully understand the importance of encryption for a wide range of stakeholders – industry, civil society, citizens and police – who all have an interest in the issue. Cryptographic protections are important for online trust, e-commerce and general privacy protections. Therefore, it is not solely a law enforcement or security issue, with which many jurisdictions continue to grapple with options and regulations.

One instructive case for policy makers to bear in mind was a US law from two decades ago which mandated specific technical intercept requirements (the *Communications Assistance for Law Enforcement Act*). During implementation, in subsequent audits and reports to Congress, it was noted that there were serious cost overruns, administrative difficulties given technical complexities and legal problems stemming from enforcing compliance via inspections.³⁸ Many technical experts also have noted since that the specifics of the law were soon after overshadowed by changes in technology, network architecture and prevalence of social media.

Other countries legislating in this domain have sought to avoid many of those risks through more flexible regulatory approaches or more principle-base, tech-neutral law. For example, in

.../16

³⁸ Implementation of the Communications Assistance for Law Enforcement Act by the Federal Bureau of Investigation (<https://oig.justice.gov/reports/FBI/a0419/index.htm>)

- 16 -

recent years EU states have taken distinct and differing approaches in policy and law, either ruling out backdoor requirements as too great a risk for data protection and security (the Netherlands), opting to legislate specific powers for investigative orders where encryption is encountered - backed by heavy fines (France), or requiring plaintext from companies pursuant to court orders (the UK). These laws were fiercely debated and met with mixed results.

One factor that greatly impedes the efficacy of such laws is that many encryption tools originate from sources and firms abroad and are widely available, including to criminals and terrorists, so would restrictions primarily affect ordinary citizens with limited knowledge of protection tools? The rapid pace of technological change is also an important issue.

Existing Canadian rules

It should be noted that Canada is not without rules which may assist law enforcement agencies in addressing encryption issues. For instance, assistance order provisions came into force in March 2015 with the *Protecting Canadians from Online Crime Act*. That legislation empowers a judge to attach an assistance order³⁹ to any search warrant, interception order, production order or other form of electronic surveillance. These orders compel any named person to help “give effect” to the authorization, and these have been used in investigations to defeat security features or compel decryption keys.⁴⁰ The requirements are backed with serious fines and/or criminal penalties. In the US, companies respond to such orders thousands of times a year, as noted in transparency reporting.⁴¹ However, the use of these orders to compel individuals to hand over the encryption codes that they use on their devices raises the possibility of self-incrimination and therefore *Charter* issues.

It is also important to note that at the federal level, provisions already exist for telecommunications carriers to build in surveillance capability, retain communications metadata and provide decrypted content to government upon request.⁴² If these requirements (the *Solicitor-*

.../17

³⁹ Section 487.02 of the *Criminal Code* (<http://laws-lois.justice.gc.ca/eng/acts/C-46/page-111.html>)

⁴⁰ Clayton Rice, “Apple and ‘Assistance Orders’ in Canada” (Nov. 8, 2015) <http://www.claytonrice.com/apple-and-assistance-orders-in-canada/>; Justin Ling and Jordan Pearson, “Canadian Police Obtained BlackBerry’s Global Decryption Key”, April 12, 2016 (<https://news.vice.com/article/exclusive-canada-police-obtained-blackberrys-global-decryption-key-how>)

⁴¹ Apple, *Report on Government Information Requests*; July 1 - December 31, 2013; (<http://images.apple.com/ca/privacy/docs/government-information-requests-20131231.pdf>)

⁴² Public Safety Canada, SGES, standard 12, Page 6 (2008).

- 17 -

General Enforcement Standards [SGES]⁴³), which have been a condition of licensing since the mid-1990s⁴⁴ are not being properly implemented or enforced, government needs to explain exactly where these standards fall short and why they need modification.

Possible solutions

Parliament should proceed cautiously before attempting to legislate solutions in this complex area. Given the experience and factors noted, we believe it preferable to explore the realm of technical solutions which might support discrete, lawfully authorized access to specific encrypted devices, as opposed to imposing general legislative requirements. At the same time, an open dialogue with the technical community, industry, civil society and privacy experts including the OPC, could provide valuable input; the Green Paper could be the beginning of such a dialogue.

However, if the government feels that a legislative solution is required, we believe that amendments should reflect and articulate the principles of necessity and proportionality⁴⁵, so as to narrow how much information is decrypted, and that such extraordinary measures should be used as a last resort.

(V) TRANSPARENCY REPORTING

Another aspect missing from the Green Paper concerns transparency reporting, which is an important part of ensuring balance and accountability. Since 2009, the OPC has advocated for a reporting regime on personal information disclosures to government by commercial organizations. The OPC has addressed these calls to Parliament, government bodies, companies and industry associations. Its 2013 PIPEDA Reform paper called for a reporting regime to be enacted, as did the Office's recommendations to Parliament on Bill S-4, the *Digital Privacy Act* in 2014-2015.⁴⁶ These recommendations call upon commercial organizations to be open about the number, frequency and type of lawful access requests they respond to.

.../18

⁴³ Duncan Campbell, "Intercepting the Internet", *The Guardian*, April 29, 1999. (<http://www.theguardian.com/technology/1999/apr/29/onlinesupplement3>)

⁴⁴ These are jointly overseen and administered by Public Safety Canada, Innovation Science and Economic Development (ISED) and Canadian Radio and Telecommunications Commission.

⁴⁵ Christopher Kuner, "Encryption and the rule of law" 38th Annual Conference of Data Protection and Privacy Commissioners (Marrakech, Morocco), p. 3. (<https://icdppc.org/wp-content/uploads/2015/03/Dr-Christopher-Kuner.pdf>)

⁴⁶ Bill S-4, An Act to amend the *Personal Information Protection and Electronic Documents Act* and to make a consequential amendment to another Act (the *Digital Privacy Act*), the OPC's Submission to the Standing Committee on Industry, Science and Technology, March 11, 2015.

- 18 -

In the past few years, six telecommunications companies (Rogers, TELUS, TekSavvy, MTS Allstream, Sasktel and Wind) in Canada each began to publish annual reports which provide statistical details on various forms of customer name/address checks by government, court orders and warrants, as well as emergency requests from police in life threatening situations. These categories are generally described in the reports with specific examples, as well as a description of the applicable legal authorities involved. With the OPC's assistance, the Department of Innovation, Science and Economic Development has provided an additional set of guidelines to encourage consistent reporting.

Transparency reporting limited to the private sector is insufficient and it is frankly abnormal that government institutions are not legally required to report on these issues, subject of course to limitations required to protect investigative methods. The OPC has therefore recommended strengthening reporting requirements on broader privacy issues dealt with by federal organizations as well as specific transparency requirements for lawful access requests made by agencies involved in law enforcement. There are various models and approaches for developing such reporting. On the public sector side for example, the *Annual Report on the Use of Electronic Surveillance* tabled annually in Parliament since 1977 (pursuant to Criminal Code section 195) has provided a reporting framework on transparency for very sensitive law enforcement investigations.

Timely, accurate statistical information on government requests and access of personal information – in the form of clear transparency reports at regular intervals – can form the basis for rational consumer choices and build citizen confidence in a growing digital economy and its interface with the state for law enforcement and security purposes. Public debates and decisions on privacy need grounding in facts and legal reality. Good transparency reporting based on evidence can support these discussions.

Conclusion

This exercise stems from a government commitment to repeal the problematic elements of Bill C-51, the *Anti-terrorism Act, 2015*, a commitment whose objective was to strike a better balance between security and human rights. As stated at the outset, we support the broader approach under which the entire security framework is to be reviewed, because problematic elements of this framework are not all found in Bill C-51. For instance, commissions of inquiry were conducted to review national security activities in the aftermath of 9/11 and have concluded that Canada had violated fundamental rights.

Now that it is clear the government wishes to take this opportunity to consider new state powers, we feel it is important that we not forget the lessons of history. One of these lessons is that once conferred, new state powers are rarely relinquished. While we applaud the government's wish to reconsider recent amendments with a view to strengthening human rights.

.../19

- 19 -

protections, we trust this same philosophy will apply to the potential expansion of investigative tools. Government should only propose and Parliament should only approve such expansion if it is demonstrated to be necessary, not merely useful or convenient, and proportionate. For its part, proportionality will depend on the adoption of strong and effective legal safeguards, standards and oversight.

This consultative exercise is a positive step, and we welcome the opportunity to continue the discussion about how best to ensure that Canada's national security framework truly protects Canadians and their privacy.

Sincerely,

A handwritten signature in black ink, appearing to read 'D. Therrien', with a stylized flourish at the end.

Daniel Therrien
Privacy Commissioner of Canada

.../20



Drew McArthur
Acting Information and Privacy
Commissioner for British
Columbia



Jill Clayton
Information and Privacy
Commissioner of Alberta



Ronald J. Kruzeniski, QC
Information and Privacy
Commissioner of Saskatchewan



Charlene Paquin, Ombudsman
Manitoba



Brian Beamish
Information and Privacy
Commissioner of Ontario



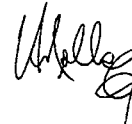
M^e Jean Chartier
President
Commission d'accès à
l'information du Québec



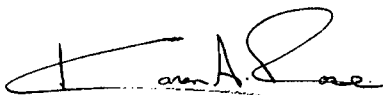
Catherine Tully
Information and Privacy
Commissioner for Nova Scotia



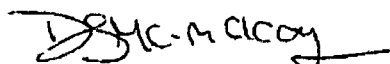
Anne E. Bertrand, Q.C.
Access to Information and
Privacy Commissioner
New Brunswick



Donovan Molloy, QC,
Information and Privacy
Commissioner
Office of the Information and
Privacy Commissioner for
Newfoundland and Labrador



Karen A. Rose
Information and Privacy
Commissioner of Prince Edward
Island



Diane McLeod-McKay
Yukon Information and Privacy
Commissioner



Elaine Keenan-Bengtts, LL.B.,
B.A.
Information and Privacy
Commissioner of Nunavut and
the Northwest Territories



Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

[Home](#) → [OPC News](#) → [News and announcements](#)

→ [Backgrounder: Privacy and Canada's national security framework](#)

Backgrounder

Privacy and Canada's national security framework

OTTAWA, December 6, 2016 – Privacy Commissioner of Canada Daniel Therrien and his provincial and territorial counterparts have provided Public Safety Canada with a formal submission to the federal government's review of Canada's national security framework. Here are some of key themes and recommendations in the submission:

Metadata in a criminal law context

Metadata, generated constantly by digital devices, can be far more revealing than the information on the outside of an envelope or in a phonebook, as it is commonly characterized by law enforcement. For instance, metadata can reveal medical conditions, religious beliefs, sexual orientation and many other elements of personal information. We also saw recently that it can identify journalistic sources.

Basic ISP subscriber information – which can include name, email address, and IP address (but not the content of communications) – is a form of metadata and can clearly be useful for investigative purposes.

The federal government's discussion paper suggests this information should be available to law enforcement more easily. Yet, Bill C-13, the *Protecting Canadians from Online Crime Act* lowered legal thresholds for accessing metadata when it came into force in 2015.

Under that legislation, a production order for "transmission data", transaction records and location tracking can be obtained from a judge on "reasonable grounds to suspect." It is unclear why these provisions do not give law enforcement adequate tools to do their job. Do police officers really need access to metadata on less than a reasonable suspicion?

Recommendations:

- **Justify lowering the standards from those recently adopted under Bill C-13**

Government must provide precise explanations as to why existing thresholds cannot be met, and why administrative authorizations to obtain metadata, rather than judicial authorizations, sufficiently protect Charter rights in cases where there are no exigent circumstances.

- **Enhance privacy protections: general considerations**

Recent cases of metadata collection – for example, by the Communications Security Establishment, CSIS, the RCMP, Quebec provincial police and Montreal police – show that existing standards should, in fact, be tightened and that privacy protections should be enhanced. In many cases, the collection of metadata, including with warrants, has involved innocent people not suspected of wrongdoing.

A modernized law must reflect the fact that metadata can reveal personal information that is more sensitive than the data for which warrants have traditionally been required in the pre-digital world. It must also ensure that modern investigative tools do not violate the privacy of law-abiding citizens.

- **Maintain the role of judges and better define conditions for access to metadata**

Maintaining the role of judges in the authorization of warrants for the collection of metadata by law enforcement is critical because they ensure the necessary independence for the protection of human rights.

However, it is also incumbent on Parliament to better define the conditions under which the sensitive metadata of Canadians should be available to police forces.

On the whole, these criteria should provide law enforcement access to metadata where necessary to pursue their investigations – but only in a way that recognizes the often sensitive nature of this type of information.

Conditions should include adopting sufficiently high legal thresholds and criteria for the issuance of court orders. For example, collection of metadata could be limited to cases where all other investigative methods have been exhausted and for violent crimes where public safety may outweigh privacy risks.

In cases where these criteria are met, there should be conditions aimed at protecting the privacy of people incidentally targeted by a warrant, but not suspected of involvement in a crime. For example, use of the data could be restricted to the crime being investigated, and metadata not related to criminal activity destroyed without delay.

- **Justify why new data retention requirements are required beyond current preservation orders**

Preservation orders are a current tool available by law enforcement to ensure that a communications company's customer data is not deleted during an investigation. The government's discussion paper suggests companies should be required to retain their customers' data without such court orders.

The imposition of such an obligation would clearly need to be justified and its scope would need to be proportional. A similar obligation imposed in a European data retention directive was invalidated by the European Court of Justice, in large part because it significantly interfered with fundamental rights and lacked sufficient limits on how law enforcement could use the information.

Metadata and national security

The British signals intelligence agency, GCHQ, has publicly stated that metadata is more revealing than the content of communications. It is therefore very useful in national security investigations. Yet the Snowden revelations, and various incidents in Canada, have demonstrated that metadata collection can include law abiding citizens. These represent examples of mass surveillance.

In Canada, two recent incidents are worth mentioning. First, the oversight authority for the Communications Security Establishment (CSE) – the Office of the CSE Commissioner – revealed in its 2014-15 annual report that metadata had been shared illegally with international security partners without being properly minimized. More recently, the Federal Court held that CSIS had unlawfully retained, for analytical purposes, the metadata of persons who were not threats to national security.

Recommendations:

- **Amend the *National Defence Act***

Following the review of the CSE's metadata sharing, the Office of the Privacy Commissioner of Canada recommended that the *National Defence Act* be amended to clarify that the CSE's powers with respect to the collection, use and disclosure of personal information be accompanied by specific legal safeguards to protect the privacy of Canadians.

- **Ensure destruction of incidental personal information**

The law should be amended to ensure that where the personal information of individuals not suspected of terrorism is obtained incidentally to the collection of information about threats, the former should be destroyed once it has been determined after analysis that individuals have been cleared of any suspected terrorist activities.

Interception and Encryption

The widely publicized battle between Apple and the FBI over investigators' access to the locked cellphone of a mass shooter in California brought the difficult issue of interception and encryption to the forefront in recent months.

The government's discussion paper notes that encryption can be a significant obstacle to lawful investigations and even to the enforcement of judicial orders. People who use encryption and companies that offer it to customers are subject to laws and judicial warrants, and these sometimes require access to personal information legitimately needed in cases where public safety is at risk.

However, encryption is also extremely important, even essential, for the protection of personal information and for the security of electronic devices such as smart phones. Unfortunately, there is no known way to give systemic access to government without simultaneously creating an important risk for the population at large. In addition, encryption often originates from foreign sources and is widely available, including to criminals and terrorists, so a Canadian law may have no impact on suspects while reducing the privacy and security protections needed by ordinary users of digital services.

Recommendations:

- **Look for technical solutions before considering a new law**

Parliament should proceed cautiously before attempting to legislate solutions. It would be preferable to explore technical solutions which might support discrete, lawfully authorized access to specific encrypted devices, as opposed to imposing general legislative requirements.

The government already has powers under the *Protecting Canadians from Online Crime Act* which, since 2015, have empowered judges to attach an assistance order to any search warrant, interception order, production order or other form of electronic surveillance. These have been used in investigations to defeat security features or compel decryption keys.

It is also important to further note that federal provisions already exist for telecommunications carriers to build in surveillance capability, retain communications metadata and provide decrypted content to government upon request. These requirements, the *Solicitor-General Enforcement Standards*, have been a condition of licensing since the mid-1990s.

As with the assistance order scheme, if these requirements are not being properly implemented or enforced, it would be important for the government to explain where the regime falls short.

- **If a new law is considered, take a narrow approach**

If an obvious technological solution is not found and the government believes legislation is required, amendments should reflect the principles of necessity and proportionality in order to narrow how much information is decrypted; and also that such extraordinary measures should be used as a last resort.

Domestic information sharing

Protecting the security of Canadians is clearly an important goal and greater information sharing may sometimes lead to the identification and suppression of security threats.

However, the scale of information sharing permitted following the passage of Bill C-51, the *Anti-Terrorism Act*, 2015, is unprecedented; the scope of the new powers created is excessive – and may affect ordinary Canadians; and the safeguards protecting against unreasonable loss of privacy are seriously deficient.

Authorizing the sharing of information based on a standard of “relevance” to the detection of threats is a key reason why risks to law abiding citizens are excessive. For instance, the information of ordinary travelers or taxpayers could be shared with a view to detecting threats among them. And SCISA, the *Security of Canada Information Sharing Act*, does not mandate the destruction of this information once the vast majority of individuals, after analysis, have been cleared of any suspected terrorist activity.

Recommendations:

- **Justify the need for changes**

The federal government should provide a justification for the new information sharing provisions, including a clear explanation, with concrete examples, of how the previous law created barriers to information sharing required for national security purposes.

- **Raise the standard from “relevance” to “necessity”**

Low standards authorizing information to be shared where it is merely of “relevance” to national security goals should be addressed. In contrast CSIS may only collect and analyze information that is “strictly necessary.” If “strictly necessary” is adequate for CSIS to collect, analyze and retain information, it is unclear why this standard cannot be adopted for *all* departments and agencies with a stake in national security.

- **Set clear limits around how long information received or shared is to be retained.**

National security agencies should be required to dispose of information immediately after analyses are completed and the vast majority of individuals have been cleared of any suspected terrorist activities.

- **Create an explicit requirement for written information sharing agreements.**

Elements addressed in these information sharing agreements should include, as a legal requirement, the specific elements of personal information being shared; the specific purposes for sharing; limitations on secondary use and onward transfer, and other measures to be prescribed by regulations, such as specific safeguards, retention periods and accountability measures.

- **Create a legal requirement to conduct Privacy Impact Assessments**

The OPC has been concerned to see how few Privacy Impact Assessments were undertaken in relation to the information sharing provisions created under Bill C-51. Privacy Impact Assessments help to identify privacy risks involving the use of personal information and propose solutions to mitigate them. They are currently required under a government policy, but not under the *Privacy Act*.

- **Consider information sharing beyond Bill C-51**

The information sharing provisions stemming from Bill C-51 are not the only mechanism by which information-sharing for national security purposes takes place. Safeguards such as necessity and proportionality should apply to all domestic information sharing.

International Information Sharing

International information sharing can lead to serious human rights abuses, including torture. This was demonstrated during the commissions of inquiry held in the aftermath of new security measures adopted following the tragic events of 9/11. The existing legal framework must be clarified to reduce these risks to a minimum.

Recommendations:

- **Set clear rules to ensure respect for international human rights law**

Clear statutory rules should be enacted to prevent information sharing from resulting in serious human rights abuses and violations of Canada's international obligations.

Consideration should be given to incorporating into law some of the privacy principles agreed to between Canada and the United States under the Beyond the Border Action Plan.

Oversight

The government's proposal to create a new National Security and Intelligence Committee of Parliamentarians is a step in the right direction, but is insufficient to ensure effective oversight. Expert review is critical.

All government institutions involved in national security should be the subject of expert review. This includes all of the 17 agencies authorized to receive information following the passage of Bill C-51 and, among others, the Privy Council Office.

Recommendations:

- **Ensure all government institutions with a national security role are subject to expert, independent oversight**

A committee of Parliamentarians provides democratic accountability, but it would also be important to have review by experts with an in-depth knowledge of the operations of national security agencies and of relevant areas of the law are applied so that rights are effectively protected.

Expert review bodies should have meaningful independence from the executive, be non-partisan and have institutional expertise, with knowledge of both domestic and international standards and law.

- **Review bodies must be able to collaborate**

Review bodies must be able to share information so that reviews can be performed in a collaborative and effective manner rather than in silos, as is currently the case.

Currently, the confidentiality provisions of the *Privacy Act* prevent the OPC from sharing information about ongoing investigations with other review bodies, such as the Security Intelligence Review Committee, the Office of the CSE Commissioner or the Civilian Review and Complaints Commission for the RCMP.

- **Review bodies must be properly resourced**

In order to be fully effective, review bodies must also be properly resourced. Although public concern about privacy has increased in recent years, and the budgets of national security agencies have grown significantly, there has not been a consequential increase in funding for oversight bodies. The OPC, for example, has been forced to risk manage limited resources, moving efforts from other mandated activities. This is less than ideal and insufficient for effective review and privacy oversight.

Transparency

A key aspect missing from the government's discussion paper is the issue of transparency reporting, which is important to ensure balance and accountability.

Transparency reporting limited to the private sector is currently insufficient. It is also unacceptable that government institutions are not legally required to report on these issues (in a manner that protects investigative methods.)

Public debates and decisions on privacy need grounding in facts and legal reality. Timely, accurate statistical information on government requests and access of personal information can support such discussions and also form the basis for informed consumer choices.

Recommendation:

- **Require transparency reporting by government**

There should be reporting requirements on broader privacy issues dealt with by federal organizations as well as specific transparency requirements for lawful access requests made by agencies involved in law enforcement.

See also:

- [News release: Don't repeat past mistakes, Privacy Commissioner warns as government reviews national security framework \(/en/opc-news/news-and-announcements/2016/nr-c_161206/\)](#)

[Submission to the Consultation on Canada's National Security Framework \(/en/opc-actions-and-decisions/submissions-to-consultations/sub_psc_161205/\)](#)

[Statement \(/en/opc-news/speeches/2016/s_d_20161206/\)](#)

- 30 -

For more information, please contact:

[Tobi Cohen \(mailto:Tobi.Cohen@priv.gc.ca\)](mailto:Tobi.Cohen@priv.gc.ca), Office of the Privacy Commissioner of Canada
Tobi.Cohen@priv.gc.ca

Date modified:

2016-12-06

**Pages 52 to / à 77
are not relevant
sont non pertinentes**

[REDACTED] (PS/SP)

From: Jeffrey Morris <jeffrey.morris@rcmp-grc.gc.ca>
Sent: Friday, February 24, 2017 3:42 PM
To: [REDACTED] (PS/SP)
Subject: Re: question

[Redacted]

s.15(1) - Subv

As mentioned, please see attached.

Available to discuss.

Jeff

>>> "[Redacted] (PS/SP)" [Redacted]@canada.ca> 2017/02/24 2:01 PM >>>
Hey Jeff,

PS Comms received the RCMP's media lines re: CSS and is asking us about the status of the ISED/RCMP review.

Comms wants to know about the links between the work on CSS and the GP consults. The answer of course is that there are thematic links, and although the GP didn't include specific discussion of CSS, a number of stakeholders raised the issue.


Regardless, if you're able to provide me a sense of the state of play on your review with ISED that would be helpful context both for my shop and for Comms, as we haven't been too looped-in on this so far.

Thanks very much,

[Redacted]

[Redacted]

Policy Analyst
National and Cyber Security Branch
Public Safety Canada
[Redacted]@canada.ca
613-990-2715

 <p>Royal Canadian Mounted Police</p>	<p>Gendarmerie royale du Canada</p>	<p>ES&ML No:17-01-012 No. des SE&LM: CCM# : 17-000418</p>	<p>Security Classification : Classification sécuritaire : PROTECTED B (Not for further distribution)</p>
---	-------------------------------------	---	---

**BRIEFING NOTE
 TO THE MINISTER OF
 PUBLIC SAFETY AND
 EMERGENCY PREPAREDNESS**

**NOTE D'INFORMATION
 AU MINISTRE DE LA
 SÉCURITÉ PUBLIQUE ET DE
 LA PROTECTION CIVILE**

ISSUE

To brief on the Royal Canadian Mounted Police's (RCMP) intention to publicly acknowledge and provide general information on its use of cell-site simulators for law enforcement purposes.

BACKGROUND

When necessary to identify a suspect's mobile device during serious criminal investigations, the RCMP may be required to use a tool called a cell-site simulator (CSS). Mobile device identification (MDI) is a crucial investigative technique that provides valuable assistance to support key public safety and law enforcement objectives. The RCMP uses CSS technology to assist in criminal investigations relating to national security, serious and organized crime, and other serious *Criminal Code* offences that impact the safety and security of Canadians. During these complex investigations, the RCMP will frequently encounter criminals who utilize multiple disposable cellular devices to mask their illegal activities. The use of a CSS to identify a target's mobile device is often the only method that allows investigators to gather this valuable evidence and further an investigation.

The RCMP utilizes a CSS to attract and collect limited information from cellular devices, such as mobile phones. In response to the signals emitted by a CSS, the operator attempts to enable cellular devices within range of the tool to identify the CSS as the most attractive cellular tower in the area. In turn, the CSS attracts and collects limited information from the cellular devices, including International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI) data, which helps to identify a cellular device used by a target (suspect) under investigation. With the exception of exigent circumstances (e.g. to prevent imminent bodily harm), the RCMP seeks prior judicial authorization to use CSS technology, and only uses the MDI technique where the collected information is required to further an investigation and cannot otherwise be obtained. At minimum, a judge must be satisfied that there are reasonable grounds to suspect that an offence has been or will be committed, and that the information obtained through a CSS will assist in the investigation of the offence. In 2015, the RCMP only used CSS technology in connection with 24 priority criminal investigations, and only one of these cases involved exigent circumstances.

In addition to collecting limited information, a CSS may cause limited cellular interference for devices within range of the tool. This potential impact may include individuals and cellular devices who are not the target (suspect) of the investigation but are within range of the CSS. The RCMP deploys CSS technology in a manner to minimize cellular interference and the potential impact of this investigative technique on Canadians. This includes deploying CSS technology for short duration periods and frequently changing cellular frequencies. In rare instances, the deployment of the tool may cause limited cellular interference to 911 calls for some mobile devices with older cellular technology. While evolving technology has significantly minimized this risk, the RCMP always identifies this potential impact of CSS technology when seeking judicial authorization, and ensures that CSS deployment either mitigates or minimizes any potential negative effects. The RCMP does not use any ancillary, collected data from non-targets (third parties) and immediately destroys this information following court



Royal
Canadian
Mounted
Police

Gendarmerie
royale
du
Canada

ES&ML No:17-01-012

No. des SE&LM:

CCM# : 17-000418

Security Classification :
Classification sécuritaire :

PROTECTED B (Not for further distribution)

proceedings, including appeal periods, and any specific orders from a judge.

Contrary to recent media coverage, the RCMP's CSS technology is not capable of collecting the contents of any form of private communication, including voice and audio communications, email messages, text messages, contact lists, images, encryption keys or any other content information from cellular devices. The CSS technology also does not provide any basic subscriber information (e.g. name, home address) associated with the subscriber account for a cellular device.

CURRENT STATUS

Public Strategy on RCMP's Use of Cell-Site Simulator (CSS) Technology

The RCMP's use of CSS technology has been the subject of recent misperception and confusion by the Canadian public and media, such as false information on the type and scope of information collected through this tool. To date, the RCMP has publicly refused to either confirm or deny its use of CSS technology. This position, and the assertion of privilege in court proceedings, has been maintained to protect the RCMP's operational use of the tool (i.e. protecting sensitive tradecraft, techniques and operational capabilities for law enforcement and national security purposes) and prevent or minimize potential exploitation by the criminal element. However, recent court disclosures (e.g. "Project Clemenza" court case in Montreal involving organized crime) have included information on the RCMP's use of CSS technology, which is now in the public domain. There is also publicly available information on CSS technology and law enforcement operational use in general, and a strong public interest in this technology from privacy and civil liberty stakeholders.

The RCMP is committed to operating CSS technology in full compliance with the laws of Canada and the *Canadian Charter of Rights and Freedoms*. To strike a more appropriate balance between public transparency and protecting sensitive investigative techniques for CSS operational use, the RCMP intends to publicly acknowledge and provide general, publicly accessible information on its use of CSS technology. While the public information will be general in nature, certain details and sensitive information will continue to be safeguarded (not disclosed), including the full version of the RCMP's operational policy on CSS technology. These safeguards will continue in order to protect the integrity of CSS technology for investigative purposes, and prevent the criminal element from evading law enforcement surveillance and detection. This public strategy will enhance the RCMP's transparency on its use of investigative tools, improve the public's understanding of CSS technology, and help to correct any public confusion and misperceptions. This public shift is consistent with the approach taken by the United States Department of Justice and the Department of Homeland Security, which publicly announced and published information in fall 2015 on the use of CSS technology by U.S. component agencies, including the Federal Bureau of Investigation.

There are two (2) key policy and administrative developments that are underway and apply to the RCMP's use of CSS technology:

1) **Innovation, Science and Economic Development Canada (ISED) Authorization**

Throughout 2016 and 2017, the RCMP and Innovation, Science and Economic Development Canada (ISED) have worked together to analyze the *Radiocommunication Act* and determine the appropriate legal framework for the use of CSS technology by Canadian law enforcement, pursuant to that Act.



Royal Canadian Mounted Police

Gendarmerie royale du Canada

ES&ML No:17-01-012

No. des SE&LM:

CCM# : 17-000418

Security Classification :
Classification sécuritaire :

PROTECTED B (Not for further distribution)

Prior to this analysis, the RCMP used CSS technology under what the Force reasonably considered to be lawful means to seek and obtain judicial authorization, and pursue serious criminal activity through the use of CSS technology. The RCMP also has an exemption order under the *Radiocommunication Act*, which exempts the RCMP from prohibitions under the Act against the use of jammers. However, in late 2016, the RCMP and ISED determined that CSS technology is not considered to be a "jammer" as defined in the *Radiocommunication Act*, and that the RCMP's current exemption order for jammers did not apply to operating this tool. Since that time, the RCMP has continued to diligently work with ISED to determine the appropriate ISED authorization instrument for CSS technology. The RCMP and ISED are now in the process of finalizing a separate authorization for the RCMP to operate "radio apparatus" as defined in the *Radiocommunication Act*, which may communicate with cellular devices and obtain "transmission data" as defined in the *Criminal Code*. This new authorization is expected to be finalized in the coming weeks and will apply to the RCMP's lawful use of CSS technology, in addition to ongoing judicial authorization requirements. The RCMP has also been engaging other Canadian police services to inform them of ISED authorization requirements for operating CSS technology in Canada, pursuant to the *Radiocommunication Act*.

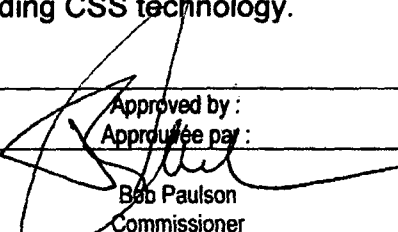
2) Office of the Privacy Commissioner of Canada (OPC) Investigation

In April 2016, the RCMP received notification from the Office of the Privacy Commissioner of Canada (OPC) that an investigation was being launched in response to a complaint that the RCMP "is contravening the collection provision of the *Privacy Act* by collecting personal information using 'StingRay' or similar devices [CSS technology] known as IMSI catchers; and, has refused to either confirm or deny that it uses International Mobile Subscriber Identity catchers as investigative tools." The RCMP has fully cooperated with the OPC in this matter, and has provided a detailed explanation of its CSS operations and policies. The OPC is also aware of the RCMP's intention to move towards a more transparent, public strategy with respect to its use of CSS technology. The OPC recently informed the RCMP that it expects to complete the investigation by March 2017.

NEXT STEPS

The RCMP will publicly acknowledge and provide general information on its use of CSS technology following the above-noted ISED authorization requirements. It is anticipated that this information will be made publicly available on the RCMP external website by no later than April 2017. The RCMP's shift towards greater transparency for CSS operations will garner media and public attention. The RCMP continues to work with Public Safety Canada and ISED to coordinate a public communications strategy on this issue. The strategy will center on clarifying the RCMP's use of CSS technology, and the judicial oversight and other safeguards that are in place to comply with the laws of Canada, including privacy.

Given the complexity and high profile nature of this issue, the RCMP welcomes representatives from the Minister's office to visit the RCMP's Technical Operations facilities in Ottawa for an in-person briefing on how it develops and deploys specialized technical services in criminal investigations, including CSS technology.

Approved by : Approuvé par :	Date
 Bob Paulson Commissioner	FEB 07 2017

Question Period Note / Note pour la Période des questions

INTERCEPTION OF OR INTERFERENCE WITH COMMUNICATIONS

ISSUE: CBC article regarding International Mobile Subscriber Identity catchers near Parliament Hill.

PROPOSED RESPONSE:

- **We recognize the concerns of potential illegal interception activities, and their potential implication on our democratic institutions, media freedoms and the privacy of Canadians.**
- **I can assure Canadians that our law enforcement and intelligence agencies can only act in support of their legislative mandates to ensure the safety and security of Canada.**
- **Their activities must be in strict accordance with federal laws including the Charter of Rights and Freedoms, the Criminal Code, and must recognize and respect the constitutional rights of all Canadians.**
- **We take these reports seriously, whether they are conducted by individuals or foreign actors and we are committed to detecting and pursuing such activities.**
- **While we do not generally comment on operational matters, the activity that was reported on April 3 does not involve a Canadian agency like the RCMP or CSIS.**
- **Yesterday, to enhance transparency around the use of investigative techniques, the RCMP confirmed its use of technology to identify mobile devices during serious and priority investigations.**
- **The RCMP's use of this technology is limited, only used with prior judicial authorization or in exigent circumstances to prevent imminent harm, and does not involve the collection of any private communications.**
- **The RCMP takes strong measures to protect public safety and privacy rights when using this technique, and complies fully with the Charter of Rights and Freedoms, criminal laws and regulations.**
- **Data collected from this technique is retained only until after the conclusion of court proceedings and is done so to ensure the RCMP adheres to the principles of fundamental justice. The Court has considered and supported this retention requirement.**

INTERCEPTION OF OR INTERFERENCE WITH COMMUNICATIONS

BACKGROUND:

On April 3, 2017, the CBC reported that technology was being used in downtown Ottawa to track cellular (mobile) devices. The media coverage alleges that the technology, commonly known as International Mobile Subscriber Identity (IMSI) catchers (preferred term is Mobile Device Identifier (MDI technology), was used by an unknown party to track mobile devices. Follow-up media coverage occurred on April 4, which included comments from the Minister of Public Safety. The Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Services (CSIS) are investigating the alleged use of IMSI catchers in downtown Ottawa. The investigation is ongoing.

Similar media coverage and investigations have recently taken place in the United States:

<http://www.ibtimes.co.uk/someone-could-be-secretly-spying-mobile-communications-white-house-pentagon-who-1612274>.

Prohibiting unlawful use of IMSI Catchers

There are federal statutes that prohibit the unlawful use of IMSI catchers and other technologies used to intercept or interfere with communications. For the unlawful use of IMSI catchers, the *Radiocommunication Act* includes prohibitions involving the unlawful interference or obstruction of radiocommunication, and the unlawful possession and operation of radio apparatus. Penalties under this Act include imprisonment (not exceeding one year) and fines.

The *Criminal Code* includes prohibitions involving the unlawful possession or use of devices to intercept private communications. Penalties under the *Code* include imprisonment not exceeding two years (possession) and five years (use).

Federal use of IMSI Catchers

The use of IMSI catchers by the RCMP and CSIS must be lawful, Charter compliant and subject to appropriate judicial oversight.

In April 2017, the RCMP will engage Canadian media outlets to publicly confirm and provide general information on its use of IMSI catchers. This will be done to improve transparency and correct public misperceptions on the RCMP's use of this technology.

The RCMP's use of technology to identify cellular devices is limited, only used with prior judicial authorization or in exigent circumstances to prevent imminent harm, and does not involve the collection of any private communications. The RCMP will continue to safeguard certain operational details on this technology to prevent criminals from evading law enforcement, and to prevent National Security Targets here and abroad from deploying countermeasures and detecting counter intelligence operations.

IMSI catchers used by the RCMP do not involve the interception of private communications, and collect limited information only (non-content) from cellular devices. The *Radiocommunication Act* is therefore the most applicable federal statute to authorize and prohibit IMSI catchers with respect to RCMP general use. The *Criminal Code* is the most applicable legislative instrument with respect to obtaining prior judicial authorization (absent exigent circumstances) for the RCMP to deploy an IMSI catcher. Pursuant to the *Radiocommunication Act*, authorization is required to install, operate and possess radio apparatus designed to communicate with mobile devices on commercial mobile networks to obtain "transmission data" (as defined in the *Criminal Code*) associated with a mobile device or the mobile network. This authorization may apply to IMSI catchers depending on the capabilities of the technology. The RCMP has obtained the respective authorization from Innovation Science and Economic Development Canada (ISED). This authorization occurred recently in 2017 following ISED and RCMP analysis throughout 2016 and 2017 to determine the most appropriate legal framework for the use of IMST catchers, pursuant to the *Radiocommunication Act*.

Information (third party data) obtained through IMSI catchers is destroyed after court proceedings, appeal periods, and/or any specific orders from a judge. This retention policy is upheld by case law. On June 27, 2016, the Ontario Superior Court of Justice issued a decision in a Toronto Police Service case, in which RCMP provided technical support ("Project Battery"), which upheld the law enforcement use of IMSI catchers.

Specifically, the court found that an IMSI catcher "*undoubtedly interferes to some extent with the privacy interests of third parties...these are minor and temporary interferences with privacy when balanced against the strong public interest in facilitating the investigation of very serious crimes...*". The court also identified that the RCMP: "*were bound to withhold all innocent third parties' cell phone serial number data from the investigators.*" With respect to destroying third party data, the court stated: "*I agree that destruction of this data, while cases remain pending before the Court, would only invite s. 7 Charter issues. However, once all cases are complete, the RCMP should consider destroying this irrelevant data...*"

OPC investigation

On April 7, 2016, the RCMP received correspondence from the Office of the Privacy Commissioner (OPC) dated April 1, 2016, that indicated that the OPC had launched an investigation in response to a complaint the OPC had received that alleged that the RCMP "is contravening the collection provision of the *Privacy Act* by collecting personal information using 'StingRay' or similar devices known as IMSI catchers; and, has refused to either confirm or deny that it uses [IMSI] catchers as investigative tools."

The investigation is ongoing and the RCMP continues to fully cooperate with the OPC.

CONTACTS:

Prepared by
RCMP – Jeffrey Morris

Tel. no.

613-843-4494

Approved by
RCMP

Tel. no.

613-843-4494

QUESTION PERIOD NOTE

Date: April 5, 2017

Classification: UNCLASSIFIED

Branch / Agency: RCMP

Question Period Note / Note pour la Période des questions

INTERCEPTION OF OR INTERFERENCE WITH COMMUNICATIONS

ISSUE: CBC article regarding International Mobile Subscriber Identity catchers near Parliament Hill.

PROPOSED RESPONSE:

- We recognize the concerns of potential illegal interception activities, and their potential implication on our democratic institutions, media freedoms and the privacy of Canadians.
- I can assure Canadians that our law enforcement and intelligence agencies can only act in support of their legislative mandates to ensure the safety and security of Canada.
- Their activities must be in strict accordance with federal laws including the Charter of Rights and Freedoms, the Criminal Code, and must recognize and respect the constitutional rights of all Canadians.
- We take these reports seriously, whether they are conducted by individuals or foreign actors and we are committed to detecting and pursuing such activities.
- While we do not generally comment on operational matters, the activity that was reported on April 3 does not involve a federal Canadian agency like the RCMP or CSIS.

INTERCEPTION OF OR INTERFERENCE WITH COMMUNICATIONS

BACKGROUND:

On April 3, 2017, the CBC reported that technology was being used in downtown Ottawa to track cellular (mobile) devices. The media coverage alleges that the technology, commonly known as International Mobile Subscriber Identity (IMSI) catchers (preferred term is Mobile Device Identifier (MDI technology), was used by an unknown party to track mobile devices.

Follow-up media coverage occurred on April 4, which included comments from the Minister of Public Safety.

The Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Services (CSIS) are investigating the alleged use of IMSI catchers in downtown Ottawa. The investigation is ongoing.

Similar media coverage and investigations have recently taken place in the United States:

<http://www.ibtimes.co.uk/someone-could-be-secretly-spying-mobile-communications-white-house-pentagon-who-1612274>.

Prohibiting unlawful use of IMSI Catchers

There are federal statutes that prohibit the unlawful use of IMSI catchers and other technologies used to intercept or interfere with communications. For the unlawful use of IMSI catchers, the *Radiocommunication Act* includes prohibitions involving the unlawful interference or obstruction of radiocommunication, and the unlawful possession and operation of radio apparatus. Penalties under this Act include imprisonment (not exceeding one year) and fines.

The *Criminal Code* includes prohibitions involving the unlawful possession or use of devices to intercept private communications. Penalties under the *Code* include imprisonment not exceeding two years (possession) and five years (use).

Federal use of IMSI Catchers

The use of IMSI catchers by the RCMP and CSIS must be lawful, Charter compliant and subject to appropriate judicial oversight.

In April 2017, the RCMP will engage Canadian media outlets to publicly confirm and provide general information on its use of IMSI catchers. This will be done to improve transparency and correct public misperceptions on the RCMP's use of this technology.

The RCMP's use of technology to identify cellular devices is limited, only used with prior judicial authorization or in exigent circumstances to prevent imminent harm, and does not involve the collection of any private communications. The RCMP will continue to safeguard certain operational details on this technology to prevent criminals from evading law enforcement, and to prevent National Security Targets here and abroad from deploying countermeasures and detecting counter intelligence operations.

IMSI catchers used by the RCMP do not involve the interception of private communications, and collect limited information only (non-content) from cellular devices. The *Radiocommunication Act* is therefore the most applicable federal statute to authorize and prohibit IMSI catchers with respect to RCMP general use. The *Criminal Code* is the most applicable legislative instrument with respect to obtaining prior judicial authorization (absent exigent circumstances) for the RCMP to deploy an IMSI catcher. Pursuant to the *Radiocommunication Act*, authorization is required to install, operate and possess radio apparatus designed to communicate with mobile devices on commercial mobile networks to obtain "transmission data" (as defined in the *Criminal Code*) associated with a mobile device or the mobile network. This authorization may apply to IMSI catchers depending on the capabilities of the technology. The RCMP has obtained the respective authorization from Innovation Science and Economic Development Canada (ISED). This authorization occurred recently in 2017 following ISED and RCMP analysis throughout 2016 and 2017 to determine the most appropriate legal framework for the use of IMST catchers, pursuant to the *Radiocommunication Act*.

OPC investigation

On April 7, 2016, the RCMP received correspondence from the Office of the Privacy Commissioner (OPC) dated April 1, 2016, that indicated that the OPC had launched an investigation in response to a complaint the OPC had received that alleged that the RCMP "is contravening the collection provision of the *Privacy Act* by collecting personal information using 'StingRay' or similar devices known as IMSI catchers; and, has refused to either confirm or deny that it uses [IMSI] catchers as investigative tools."

The investigation is ongoing and the RCMP continues to fully cooperate with the OPC.

CONTACTS:

Prepared by
RCMP – Jeffrey Morris

Tel. no.

613-843-4494

Approved by
PETER HENSCHEL,
DEPUTY COMMISSIONER
SPECIALIZED POLICING
SERVICES, RCMP

Tel. no.

613-843-4494

INTERCEPTION DE COMMUNICATIONS PRIVÉES

SUJET : Article de la CBC concernant des intercepteurs d'IMSI près de la Colline du Parlement

RÉPONSE SUGGÉRÉE :

- **Nous comprenons l'inquiétude que suscitent les activités de possible interception clandestine et les conséquences qu'elles pourraient avoir sur nos institutions démocratiques, sur la liberté de presse et sur la vie privée des Canadiens.**
- **Je tiens à rassurer la population canadienne que nos organismes de renseignement et d'application de la loi ne peuvent agir qu'au soutien de leurs mandats légitimes pour assurer la sécurité des Canadiens.**
- **Leurs activités doivent respecter scrupuleusement les lois fédérales, notamment la *Charte des droits et libertés* et le *Code criminel*, et elles doivent tenir compte des droits constitutionnels de tous les Canadiens et les respecter.**
- **Nous prenons très au sérieux le signalement de telles activités, qu'elles soient tenues par des particuliers ou par des étrangers, et nous nous engageons à les détecter et à en amener les responsables devant les tribunaux.**
- **Bien que nous n'ayons pas l'habitude de commenter les dossiers opérationnels, sachez que l'activité qui a fait l'objet d'un reportage le 3 avril n'est pas le fait d'un organisme fédéral canadien, comme la GRC ou le SCRS.**

INTERCEPTION DE COMMUNICATIONS PRIVÉES

CONTEXTE :

Le 3 avril 2017, la CBC a diffusé un reportage faisant état de l'utilisation au centre-ville d'Ottawa de moyens technologiques pour suivre des appareils cellulaires (mobiles). Selon le journaliste, la technologie, appelée capteurs d'IMSI (données d'identité internationale d'abonné mobile – préférablement identificateurs d'appareils mobiles) a été utilisée par une partie inconnue pour suivre des appareils mobiles.

Le dossier a fait l'objet d'un suivi médiatique le 4 avril, qui présentait des commentaires du ministre de la Sécurité publique.

La Gendarmerie royale du Canada (GRC) et le Service canadien du renseignement de sécurité (SCRS) enquêtent sur l'utilisation alléguée de capteurs d'IMSI au centre-ville d'Ottawa. L'enquête se poursuit.

Il y a eu récemment aux États-Unis aussi des reportages et des enquêtes semblables :

<http://www.ibtimes.co.uk/someone-could-be-secretly-spying-mobile-communications-white-house-pentagon-who-1612274>.

Interdiction de l'utilisation clandestine de capteurs d'IMSI

Il existe des lois fédérales qui interdisent l'utilisation clandestine de capteurs d'IMSI et d'autres technologies servant à intercepter des communications. La *Loi sur la radiocommunication* comporte des interdictions concernant l'action clandestine de brouiller ou d'entraver la radiocommunication et la possession ou l'exploitation illégale d'appareils radio. Cette loi prévoit des peines d'emprisonnement (ne dépassant pas un an) et des amendes.

Le *Code criminel* comporte des interdictions concernant la possession et l'utilisation illégale de dispositifs conçus pour intercepter clandestinement des communications privées. Le Code prévoit des peines d'emprisonnement ne dépassant pas deux ans (possession) et cinq ans (utilisation).

Utilisation fédérale des capteurs d'IMSI

L'utilisation de capteurs d'IMSI par la GRC et le SCRS doit être légale, conforme à la Charte et assujettie à une surveillance judiciaire adéquate.

En avril 2017, la GRC confirmera aux bureaux de presse canadiens son utilisation de capteurs d'IMSI. À cette occasion, elle fournira des renseignements généraux à cet égard, afin d'accroître la transparence et de corriger les fausses impressions répandues dans la population sur l'utilisation que la GRC fait de cette technologie.

L'utilisation par la GRC de la technologie de détection d'appareils cellulaires est limitée, elle repose forcément sur une autorisation judiciaire préalable ou sur une situation d'urgence pour éviter un danger imminent, et ne comprend pas le prélèvement de communications privées. La GRC continuera de protéger certains détails opérationnels liés à cette technologie afin d'éviter que des criminels se soustraient à l'application de la loi et d'éviter que des cibles de la Sécurité nationale, ici et ailleurs, mettent en place des contre-mesures et détectent des opérations de contre-espionnage.

Les capteurs d'IMSI qu'utilise la GRC ne servent pas à intercepter des communications privées mais à tirer seulement des renseignements limités (non liés au contenu) des appareils cellulaires. C'est donc la *Loi sur la radiocommunication* qui, des lois fédérales, s'applique surtout pour autoriser et interdire les capteurs d'IMSI pour l'usage général qu'en fait la GRC. Le *Code criminel* est l'instrument législatif sur lequel repose l'obtention de l'autorisation judiciaire préalable (sauf en situation d'urgence) pour permettre à la GRC de déployer un capteur d'IMSI. Conformément à la *Loi sur la radiocommunication*, il faut une autorisation pour installer, faire fonctionner ou posséder un appareil radio conçu pour communiquer avec des appareils mobiles dans des réseaux mobiles commerciaux afin d'obtenir des « données de transmission » (suivant la définition du *Code criminel*) associées à un appareil mobile ou au réseau mobile. Cette autorisation peut s'appliquer à des capteurs d'IMSI selon la capacité de la technologie. La GRC a obtenu l'autorisation nécessaire d'Innovation, Sciences et Développement économique Canada (ISDE). Cette autorisation s'est concrétisée récemment en 2017 après qu'ISDE et la GRC ont fait en 2016 et 2017 l'analyse nécessaire pour déterminer le cadre légal qui conviendrait le mieux à l'utilisation de capteurs d'IMSI, conformément à la *Loi sur la radiocommunication*.

Enquête du Commissariat à la protection de la vie privée

Le 7 avril 2016, la GRC a reçu du Commissariat à la protection de la vie privée une missive datée du 1^{er} avril 2016 indiquant que le CPVP avait ouvert une enquête en réponse à une plainte reçue au CPVP dans laquelle il est allégué que la GRC contrevient aux dispositions de la *Loi sur la protection des renseignements personnels* en recueillant des renseignements personnels à l'aide de StingRay ou d'appareils semblables connus comme des capteurs d'IMSI et qu'elle refuse de confirmer ou d'infirmer son utilisation de capteurs d'IMSI comme outils d'enquête.

L'enquête se poursuit et la GRC continue de coopérer pleinement avec le CPVP.

CONTACTS :

Préparée par
GRC – Jeffrey Morris

N° de tél.

613-843-4494

Approuvée par
RCMP

N° de tél.

613-843-4494

Question Period Note / Note pour la Période des questions

INTERCEPTION OF PRIVATE COMMUNICATIONS

ISSUE: CBC article regarding IMSI catchers near Parliament Hill.

PROPOSED RESPONSE:

- **Our government is committed to keeping Canadians safe while protecting rights and freedoms.**
- **Under Section 191 of the Criminal Code, it is illegal to import, manufacture or possess interception devices unless specific exemptions apply.**
- **The use of all technical investigative tools by the RCMP is governed by the law and the Charter and subject to judicial control.**
- **Court orders are limited and specific to the criminality under investigation, and can only be obtained if statutory requirements are met.**
- **The RCMP must inform judges of the potential impact of investigative tools when seeking authorization, and use them in accordance with the limits set out by the court.**
- **The Privacy Commissioner has indicated that he has launched an investigation in relation to certain investigative tools reportedly used by the RCMP, and I welcome that. The RCMP is cooperating with the Privacy Commissioner in this matter.**

INTERCEPTION OF PRIVATE COMMUNICATIONS

BACKGROUND:

The use of technical investigative tools, such as interception devices (e.g.: IMSI Catchers), help safeguard Canadians and support priority criminal investigations.

Subsection 191(1) of the *Criminal Code* indicates that: "Everyone who possesses, sells or purchases any electro-magnetic, mechanical or other device or any component thereof knowing that the design thereof renders it primarily useful for surreptitious interception of private communication is guilty of an indictable offence and is liable to imprisonment for a term not exceeding two years".

Subsection 191(2) of the *Criminal Code* allows for specific exemptions to 191(1), namely to:

- (a) a police officer in the course of his employment;
- (b) a person using it in an interception made or to be made in accordance with an authorization;
- (b)(1) a person under the direction of a police officer in order to assist that officer in the course of his duties as a police officer;
- (c) an officer or servant of Her Majesty in right of Canada or a member of the Canadian forces in the course of his duties as such an officer, servant or member;
- (d) any other person under the authority of a licence issued by the Minister of Public Safety and Emergency Preparedness.

The use of interception devices by law enforcement or security agencies is limited and specific to the criminality under investigation, and can only be obtained if statutory requirements are met. The RCMP must inform judges of the potential impact of investigative tools when seeking authorization, and use them in accordance with the limits set out by the court.

The illegal use of interception devices could be pursued under the *Criminal Code*, including incarceration.

CONTACTS:

Prepared by

Tel. no.

Approved by
MONIK BEAUREGARD

Tel. no.
613-990-4976

INTERCEPTION DE COMMUNICATIONS PRIVÉES

SUJET : Article de la CBC concernant des intercepteurs d'IMSI près de la Colline du Parlement

RÉPONSE SUGGÉRÉE :

- **Notre gouvernement s'est engagé à assurer la sécurité des Canadiens tout en protégeant les droits et les libertés.**
- **En vertu de l'article 191 du *Code criminel*, il est illégal d'importer, de fabriquer ou d'avoir en sa possession des dispositifs d'interception, sauf si des exemptions précises s'appliquent.**
- **L'utilisation par la GRC de tous les outils d'enquête technique est régie par loi et la Charte et elle est assujettie à un contrôle judiciaire.**
- **Les ordonnances des tribunaux se limitent à la criminalité précise visée par l'enquête et elles ne peuvent être obtenues que s'il est satisfait aux exigences législatives.**
- **La GRC doit informer les juges de l'incidence potentielle des outils d'enquête lorsqu'elle demande l'autorisation de les utiliser, et elle doit utiliser ceux-ci dans les limites établies par le tribunal.**
- **Le commissaire à la protection de la vie privée a indiqué avoir ouvert une enquête sur l'utilisation présumée de certains outils d'enquête par la GRC, et j'en suis heureux. La GRC collabore avec le commissaire à la protection de la vie privée dans ce dossier.**

INTERCEPTION DE COMMUNICATIONS PRIVÉES

CONTEXTE :

L'utilisation d'outils d'enquête technique, comme les dispositifs d'interception (p. ex. intercepteurs d'IMSI), contribue à protéger les Canadiens et à soutenir les enquêtes criminelles prioritaires.

Selon le paragraphe 191(1) du *Code criminel* : « [e]st coupable d'un acte criminel et passible d'un emprisonnement maximal de deux ans quiconque possède, vend ou achète un dispositif électromagnétique, acoustique, mécanique ou autre ou un élément ou une pièce de celui-ci, sachant que leur conception les rend principalement utiles à l'interception clandestine de communications privées. »

Le paragraphe 191(2) du *Code criminel* prévoit des exemptions relatives au paragraphe 191(1) :

Le paragraphe (1) ne s'applique pas aux personnes suivantes :

- a) un policier en possession d'un dispositif, d'un élément ou d'une pièce visés au paragraphe (1) dans l'exercice de ses fonctions;
- b) une personne en possession d'un dispositif, d'un élément ou d'une pièce visés au paragraphe (1) qu'elle a l'intention d'utiliser lors d'une interception qui est faite ou doit être faite en conformité avec une autorisation;
- b.1) une personne en possession d'un dispositif, d'un élément ou d'une pièce d'un dispositif, sous la direction d'un policier, afin de l'aider dans l'exercice de ses fonctions;
- c) un fonctionnaire ou préposé de Sa Majesté du chef du Canada ou un membre des Forces canadiennes en possession d'un dispositif, d'un élément ou d'une pièce visés au paragraphe (1) dans l'exercice de ses fonctions en tant que fonctionnaire, préposé ou membre, selon le cas;
- d) toute autre personne en possession d'un dispositif, d'un élément ou d'une pièce visés au paragraphe (1) en vertu d'un permis délivré par le ministre de la Sécurité publique et de la Protection civile.

Les organismes de sécurité et d'exécution de la loi peuvent utiliser, de façon limitée, les dispositifs d'interception uniquement dans le cadre d'une enquête criminelle, et ce, dans la mesure où les exigences prévues par la loi sont respectées. La GRC doit informer les juges de l'incidence potentielle des outils d'enquête lorsqu'elle demande l'autorisation de les utiliser, et elle doit utiliser ceux-ci dans les limites établies par le tribunal.

L'utilisation illégale de dispositifs d'interception peut faire l'objet de poursuites en vertu du *Code criminel* et donner lieu à une peine d'emprisonnement.

CONTACTS :

Préparée par

[REDACTED]

N° de tél.

[REDACTED]

Approuvée par
MONIK BEAUREGARD

N° de tél.
613-990-4976

INTERCEPTION OF PRIVATE COMMUNICATIONS

- Our government is committed to keeping Canadians safe while protecting rights and freedoms.
- Under Section 191 of the Criminal Code, it is illegal to import, manufacture or possess interception devices unless specific exemptions apply.
- The use of all technical investigative tools by the RCMP is governed by the law and the Charter and subject to judicial control.
- Court orders are limited and specific to the criminality under investigation, and can only be obtained if statutory requirements are met.
- The RCMP must inform judges of the potential impact of investigative tools when seeking authorization, and use them in accordance with the limits set out by the court.
- The Privacy Commissioner has indicated that he has launched an investigation in relation to certain investigative tools reportedly used by the RCMP, and I welcome that. The RCMP is cooperating with the Privacy Commissioner in this matter.

BACKGROUND

The use of technical investigative tools, such as interception devices (e.g.: IMSI Catchers), help safeguard Canadians and support priority criminal investigations.

Subsection 191(1) of the *Criminal Code* indicates that: “Everyone who possesses, sells or purchases any electro-magnetic, mechanical or other device or any component thereof knowing that the design thereof renders it primarily useful for surreptitious interception of private communication is guilty of an indictable offence and is liable to imprisonment for a term not exceeding two years”.

Subsection 191(2) of the *Criminal Code* allows for specific exemptions to 191(1), namely to:

- (a) a police officer in the course of his employment;
- (b) a person using it in an interception made or to be made in accordance with an authorization;
- (b)(1) a person under the direction of a police officer in order to assist that officer in the course of his duties as a police officer;
- (c) an officer or servant of Her Majesty in right of Canada or a member of the Canadian forces in the course of his duties as such an officer, servant or member;
- (d) any other person under the authority of a licence issued by the Minister of Public Safety and Emergency Preparedness.

The use of interception devices by law enforcement or security agencies is limited and specific to the criminality under investigation, and can only be obtained if statutory requirements are met. The RCMP must inform judges of the potential impact of investigative tools when seeking authorization, and use them in accordance with the limits set out by the court.

The illegal use of interception devices could be pursued under the *Criminal Code*, including incarceration.

Name of PCO Policy Analyst. Nom de l'analyste du BCP :

Secretariat. Secrétariat :

Telephone number. Numéro de téléphone :

INTERCEPTION OF OR INTERFERENCE WITH COMMUNICATIONS

- We recognize the concerns of potential illegal interception activities, and their potential implication on our democratic institutions, media freedoms and the privacy of Canadians.
- I can assure Canadians that our law enforcement and intelligence agencies only act in support of their legislative mandate to ensure the safety and security of Canada.
- Their activities must be in strict accordance with the Charter of Rights and Freedoms, the Criminal Code, and must recognize and respect the constitutional rights of all Canadians.
- We take these reports seriously, whether they are conducted by individuals or foreign actors and as indicated by the Minister of Public Safety, we are investigating them.
- Last week, to enhance transparency around the use of investigative techniques, the RCMP confirmed its use of technology to identify mobile devices during serious and priority investigations.
- The RCMP's use of this technology is limited, only used with prior judicial authorization or in exigent circumstances to prevent imminent harm, and does not involve the collection of any private communications.

- The RCMP takes strong measures to protect public safety and privacy rights when using this technique, and complies fully with the Charter of Rights and Freedoms, criminal laws and regulations.
- Data collected from this technique is only retained until the conclusion of court proceedings, as required by the courts, and is done to ensure the RCMP adheres to the principles of fundamental justice.
- I understand that other Canadian police services have also confirmed their use of technology to identify mobile devices during investigations.
- There are federal laws with appropriate oversight and conditions in place to ensure the lawful use of investigative techniques by police and security agencies.
- These measures help ensure the appropriate balance between privacy rights and the need to keep Canadians safe.

INTERCEPTION DE COMMUNICATIONS PRIVÉES

- Nous reconnaissons les préoccupations du risque d'interception illégale et par les répercussions éventuelles de telles activités sur nos institutions démocratiques, sur la liberté des médias et sur la protection de la vie privée des Canadiens.
- Je peux assurer les Canadiens que les organisations canadiennes de police et de renseignement n'agissent que dans le cadre de leur mandat législatif, pour assurer la sûreté et la sécurité du Canada.
- Leurs activités doivent être rigoureusement conformes à la Charte des droits et libertés, au Code criminel et doivent respecter les droits constitutionnels de tous les Canadiens.
- Nous prenons ce dossier au sérieux, qu'il provienne d'acteurs ou individus ou des acteurs étrangers et, tel qu'indiqué par le ministre de la Sécurité publique, ce dossier est sous enquête.

BACKGROUND

- On April 3, 2017, the CBC reported that technology was being used in downtown Ottawa to track cellular (mobile) devices. The media coverage alleges that the technology, commonly known as International Mobile Subscriber Identity (IMSI) catchers (preferred term is Mobile Device Identifier (MDI technology)), was used by an unknown party to track mobile devices.
- Follow-up media coverage occurred on April 4, which included comments from the Minister of Public Safety.
- The Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Services (CSIS) are investigating the alleged use of IMSI catchers in downtown Ottawa. The investigation is ongoing.
- Similar media coverage and investigations have recently taken place in the United States: <http://www.ibtimes.co.uk/someone-could-be-secretly-spying-mobile-communications-white-house-pentagon-who-1612274>.

Prohibiting unlawful use of IMSI Catchers

- There are federal statutes that prohibit the unlawful use of IMSI catchers and other technologies used to intercept or interfere with communications. For the unlawful use of IMSI catchers, the *Radiocommunication Act* includes prohibitions involving the unlawful interference or obstruction of radiocommunication, and the unlawful possession and operation of radio apparatus. Penalties under this Act include imprisonment (not exceeding one year) and fines.
- The *Criminal Code* includes prohibitions involving the unlawful possession or use of devices to intercept private communications. Penalties under the *Code* include imprisonment not exceeding two years (possession) and five years (use).

Federal use of IMSI Catchers

- The use of IMSI catchers by the RCMP and CSIS must be lawful, Charter compliant and subject to appropriate judicial oversight.
- In April 2017, the RCMP will engage Canadian media outlets to publicly confirm and provide general information on its use of IMSI catchers. This will be done to improve transparency and correct public misperceptions on the RCMP's use of this technology.
- The RCMP's use of technology to identify cellular devices is limited, only used with prior judicial authorization or in exigent circumstances to prevent imminent harm, and does not involve the collection of any private communications. The RCMP will continue to safeguard certain operational details on this technology to prevent criminals from evading law enforcement, and to prevent National Security Targets here and abroad from deploying countermeasures and detecting counter intelligence operations.

- IMSI catchers used by the RCMP do not involve the interception of private communications, and collect limited information only (non-content) from cellular devices. The *Radiocommunication Act* is therefore the most applicable federal statute to authorize and prohibit IMSI catchers with respect to RCMP general use. The *Criminal Code* is the most applicable legislative instrument with respect to obtaining prior judicial authorization (absent exigent circumstances) for the RCMP to deploy an IMSI catcher. Pursuant to the *Radiocommunication Act*, authorization is required to install, operate and possess radio apparatus designed to communicate with mobile devices on commercial mobile networks to obtain “transmission data” (as defined in the *Criminal Code*) associated with a mobile device or the mobile network. This authorization may apply to IMSI catchers depending on the capabilities of the technology. The RCMP has obtained the respective authorization from Innovation Science and Economic Development Canada (ISED). This authorization occurred recently in 2017 following ISED and RCMP analysis throughout 2016 and 2017 to determine the most appropriate legal framework for the use of IMST catchers, pursuant to the *Radiocommunication Act*.

Information (third party data)

Information (third party data) obtained through IMSI catchers is destroyed after court proceedings, appeal periods, and/or any specific orders from a judge. This retention policy is upheld by case law. On June 27, 2016, the Ontario Superior Court of Justice issued a decision in a Toronto Police Service case, in which RCMP provided technical support (“Project Battery”), which upheld the law enforcement use of IMSI catchers.

Specifically, the court found that an IMSI catcher “undoubtedly interferes to some extent with the privacy interests of third parties...these are minor and temporary interferences with privacy when balanced against the strong public interest in facilitating the investigation of very serious crimes...”. The court also identified that the RCMP: “were bound to withhold all innocent third parties’ cell phone serial number data from the investigators.” With respect to destroying third party data, the court stated: “I agree that destruction of this data, while cases remain pending before the Court, would only invite s. 7 Charter issues. However, once all cases are complete, the RCMP should consider destroying this irrelevant data...”

OPC investigation

- On April 7, 2016, the RCMP received correspondence from the Office of the Privacy Commissioner (OPC) dated April 1, 2016, that indicated that the OPC had launched an investigation in response to a complaint the OPC had received that alleged that the RCMP “is contravening the collection provision of the *Privacy Act* by collecting personal information using ‘StingRay’ or similar devices known as IMSI catchers; and, has refused to either confirm or deny that it uses [IMSI] catchers as investigative tools.”
- The investigation is ongoing and the RCMP continues to fully cooperate with the OPC.

Use of IMSI catchers by other Canadian police services

On April 12, 2017, the CBC confirmed that other Canadian police services, including Calgary Police Service, Winnipeg Police Service and the Ontario Provincial Police use IMSI catchers.

Lawful use of IMSI catchers

The lawful use of an IMSI catcher requires authorization from Innovation Science and Economic Development Canada (ISED), pursuant to the *Radiocommunications Act*. Absent exigent circumstances, the RCMP also obtains judicial authorization prior to using an IMSI catcher.

The provisions under the *Criminal Code* (section 191) apply to devices that are primarily use for and capable of intercepting "private communications", i.e. the actual content of electronic communications. The RCMP's IMSI catchers are incapable of collecting private communications, and therefore these provisions do not apply to the RCMP's use of this technology.

Pursuant to the *Criminal Code* (section 191 (2) (a)), police services are exempted from criminal prohibitions involving the possession of a device used to intercept private communications.

Name of PCO Policy Analysts: [REDACTED]

Secretariat: Security and Intelligence

Telephone number: [REDACTED]

s.15(1) - Subv

2016-2017 Supplementary Estimates (B)

RCMP INVESTIGATIVE TOOLS AND TECHNIQUES

PROPOSED RESPONSE:

- **Our government is committed to keeping Canadians safe while respecting rights and freedoms, and we welcome discussion about how best to achieve this dual objective.**
- **The RCMP may use technical investigative methods to conduct priority criminal investigations and lawfully obtain digital evidence.**
- **The use of investigative tools by the RCMP is governed by the law, including the *Charter*, and is subject to appropriate judicial processes. Court orders are limited and specific to the criminality under investigation, and can only be obtained if the statutory requirements are met.**
- **The RCMP must inform judges of the potential impact of investigative tools when seeking authorization, and use them in accordance with the limits set out by the court.**
- **When considering whether to use particular technology, officers are expected to weigh the need to prevent imminent bodily harm, preserve life and investigate serious crimes against potential impacts on third parties.**
- **On April 7, 2016, the Privacy Commissioner indicated to the RCMP that, in response to a written complaint, he has launched an investigation in relation to certain investigative tools reportedly used by the Force. The RCMP continues to cooperate with the Privacy Commissioner in this important and ongoing matter.**

Backgrounder:

The RCMP's Use and Safeguarding of Investigative Tools

The RCMP uses technical investigative tools under its mandate to safeguard Canadians and conduct priority criminal investigations. Use of any investigative tool is subject to lawful authority, which may refer to judicial authorization; common law; or, the presence of exigent circumstances, such as those in relation to recent child abductions or missing persons. Having lawful authority ensures that the important, specific and limited law enforcement purpose weighs both the public safety and privacy interests involved. Priority investigations include those linked to national security, organized crime, or financial crime. The oversight of any investigative technique used by the RCMP is governed by the appropriate judicial processes, as set out in criminal law, including the *Criminal Code of Canada*. By law, court orders must be limited and specific to the criminality under investigation, can only be obtained if the statutory requirements are met, and can be subsequently reviewed at trial by the court and the accused. The capabilities of sensitive investigative tools are classified. Releasing classified information is illegal under the *Security of Information Act* and would negatively and significantly impact public and officer safety and the integrity of the criminal justice system. As such, the RCMP safeguards classified information through stringent information security measures. At trial, police investigative tools and techniques may be further safeguarded through means such as Common Law or the *Canada Evidence Act*.

Media coverage on Mobile Device Identifiers (MDIs) and other investigative techniques

Issues concerning MDIs and other investigative techniques used by law enforcement (e.g., lawful assistance from BlackBerry) have garnered significant media and public attention. One specific focus of the media's attention has been in relation to a high profile criminal court case (Project Clemenza) involving organized crime and drug importation in Quebec, and the RCMP's investigative role. On June 10, 2016, the Quebec court for Project Clemenza lifted a publication ban. As a result, details of previously undisclosed specialized RCMP capabilities were made public, including in relation to MDIs. In a related murder case involving Project Clemenza suspects, (adjudicated prior to the Clemenza), Justice Stober ordered that additional information about MDIs be disclosed. Since then, the defence in the Project Clemenza organized crime case has applied for information about MDIs to also be disclosed. The RCMP has been in discussions with Crown prosecutors (Public Prosecution Service of Canada) about this request.

To protect the sensitivity of the MDI technology and other investigative techniques, the RCMP has publicly refused to either confirm or deny that it uses MDIs. It is critical that the RCMP protect the sensitivity of certain investigative techniques, so that they remain valuable tools for assisting investigations and maintaining public safety. Any disclosure that describes the technical capabilities of the MDI, for example, or the techniques used to operate the MDI, has the potential to impact investigations conducted by the RCMP, as well as the investigations of any other organization that uses MDI type devices.

The RCMP's position regarding media requests will be to: acknowledge that the RCMP employs specialized tools and techniques under lawful authority in the execution of criminal investigations in support of public safety and national security objectives; highlight that the RCMP does not speak about specific tools or capabilities to protect criminal investigations and national security objectives; note that the RCMP continues to readily cooperate with the Privacy Commissioner as part of its investigation of the RCMP's reported use of certain investigative tools (more below); and reinforce that the RCMP's investigative efforts are targeted, limited, specific, proportionate and lawfully authorized by an independent judiciary.

MDI technology has continued to garner noticeable media and public attention. For example, on September 13, 2016, the University of Toronto's Citizen Lab published a detailed report, "*Gone Opaque? An Analysis of Hypothetical IMSI [International Mobile Subscriber Identity] Catcher Overuse in Canada.*"

OPC investigation

On April 7, 2016, the RCMP received correspondence from the Office of the Privacy Commissioner (OPC) dated April 1, 2016, that indicated that the OPC had launched an investigation in response to a complaint the OPC had received that alleged that the RCMP "is contravening the collection provision of the *Privacy Act* by collecting personal information using 'StingRay' or similar devices known as IMSI catchers; and, has refused to either confirm or deny that it uses [IMSI] catchers as investigative tools." The investigation is ongoing and the RCMP continues to fully cooperate and respond to the OPC's questions, including information that was recently provided to the OPC on November 14, 2016.

CONTACTS:

PREPARED BY: JOE OLIVER,
ASSISTANT COMMISSIONER,
TECHNICAL OPERATIONS,
SPECIALIZED POLICING
SERVICES,
RCMP

Tel. no.
613-843-4494

Approved by
PETER HENSCHEL,
DEPUTY COMMISSIONER,
SPECIALIZED POLICING
SERVICES,
RCMP

Tel. no.
613-843-4494

Question Period Note / Note pour la Période des questions

RCMP INVESTIGATIVE TOOLS AND TECHNIQUES

ISSUE: RCMP technology in relation to lawfully obtaining evidence

PROPOSED RESPONSE:

- **Our government is committed to keeping Canadians safe while respecting rights and freedoms, and we welcome discussion about how best to achieve this dual objective.**
- **The Royal Canadian Mounted Police may use technical investigative methods to conduct priority criminal investigations and lawfully obtain digital evidence.**
- **The use of investigative tools by the RCMP is governed by the law, including the *Charter*, and is subject to appropriate judicial processes. Court orders are limited and specific to the criminality under investigation, and can only be obtained if the statutory requirements are met.**
- **The RCMP must inform judges of the potential impact of investigative tools when seeking authorization, and use them in accordance with the limits set out by the court.**
- **When considering whether to use particular technology, officers are expected to weigh the need to prevent imminent bodily harm, preserve life and investigate serious crimes against potential impacts on third parties.**
- **On April 7, 2016, the Privacy Commissioner indicated to the RCMP that, in response to a written complaint, he has launched an investigation in relation to certain investigative tools reportedly used by the Force. The RCMP continues to cooperate with the Privacy Commissioner in this important and ongoing matter.**

RCMP TECHNICAL INVESTIGATIVE TECHNIQUES

BACKGROUND:

The RCMP's Use and Safeguarding of Investigative Tools

The RCMP uses technical investigative tools under its mandate to safeguard Canadians and conduct priority criminal investigations. Use of any investigative tool is subject to lawful authority, which may refer to judicial authorization; common law; or, the presence of exigent circumstances, such as those in relation to recent child abductions or missing persons. Having lawful authority ensures that the important, specific and limited law enforcement purpose weighs both the public safety and privacy interests involved. Priority investigations include those linked to national security, organized crime, or financial crime. The oversight of any investigative technique used by the RCMP is governed by the appropriate judicial processes, as set out in criminal law, including the *Criminal Code of Canada*. By law, court orders must be limited and specific to the criminality under investigation, can only be obtained if the statutory requirements are met, and can be subsequently reviewed at trial by the court and the accused. The capabilities of sensitive investigative tools are classified. Releasing classified information is illegal under the *Security of Information Act* and would negatively and significantly impact public and officer safety and the integrity of the criminal justice system. As such, the RCMP safeguards classified information through stringent information security measures. At trial, police investigative tools and techniques may be further safeguarded through means such as Common Law or the *Canada Evidence Act*.

Media coverage on Mobile Device Identifiers (MDIs) and other investigative techniques

Issues concerning MDIs and other investigative techniques used by law enforcement (e.g. lawful assistance from BlackBerry) have garnered significant media and public attention. One specific focus of the media's attention has been in relation to a high profile criminal court case (Project Clemenza) involving organized crime and drug importation in Quebec, and the RCMP's investigative role. On June 10, 2016, the Quebec court for Project Clemenza lifted a publication ban in the case. As a result, details on hitherto undisclosed specialized RCMP capabilities were made public, including in relation to MDIs. In the related murder case involving Project Clemenza suspects that was adjudicated prior to the Clemenza organized crime case, Justice Stober ordered that additional information about MDIs be disclosed. Since then, the defence in the Project Clemenza organized crime case have applied for this type of information to also be disclosed. The RCMP is currently in discussions with Crown prosecutors (Public Prosecution Service of Canada) about this request.

To protect the sensitivity of the MDI technology and other investigative techniques, the RCMP has publicly refused to either confirm or deny that it uses MDIs. It is critical that the RCMP protect the sensitivity of certain investigative techniques, so that they remain valuable tools for assisting investigations and maintaining public safety. Any disclosure that describes the technical capabilities of the MDI, for example, or the techniques used to operate the MDI, has the potential to impact investigations conducted by the RCMP, as well as the investigations of any other organization that uses MDI type devices. The RCMP, in consultation with policing and security partners, is currently analyzing options with respect to its public position on MDIs, and the appropriate level of public disclosure regarding the RCMP's use of MDIs and possibly other sensitive, investigative techniques. In the meantime, the RCMP's position regarding media requests will be to: acknowledge that the RCMP employs specialized tools and techniques under lawful authority in the execution of criminal investigations in support of public safety and national security objectives; highlight that we do not speak about specific tools or capabilities, regardless of what might be available in the public domain; note that we continue to readily cooperate with the Privacy Commissioner as part of their examination of RCMP use of MDIs; and, reinforce that our investigative efforts are targeted, limited, specific, proportionate and lawfully authorized by an independent judiciary.

Since the lifting of the publication ban in relation to Project Clemenza, the use of MDI technology has continued to garner noticeable media and public attention. For example, on September 13, 2016, the University of Toronto's Citizen Lab published a detailed report, "*Gone Opaque? An Analysis of Hypothetical IMSI [International Mobile Subscriber Identity] Catcher Overuse in Canada.*"

OPC investigation

On April 7, 2016, the RCMP received correspondence from the Office of the Privacy Commissioner (OPC) dated April 1, 2016, that indicated that the OPC had launched an investigation in response to a complaint the OPC had received that alleged that the RCMP "is contravening the collection provision of the *Privacy Act* by collecting personal information using 'StingRay' or similar devices known as IMSI catchers; and, has refused to either confirm or deny that it uses [IMSI] catchers as investigative tools." The RCMP has been and will continue to fully cooperate with the OPC in this matter. On June 23, 2016, the RCMP and OPC met to discuss the matter and subsequently the OPC sent the RCMP specific written questions. The RCMP is currently drafting its response to the OPC's specific written questions.

CONTACTS:

Submitted by
JOE OLIVER,
ASSISTANT COMMISSIONER,
TECHNICAL OPERATIONS,
SPECIALIZED POLICING
SERVICES,
RCMP

Tel. no.
613-993-1620

Approved by
PETER HENSCHEL,
DEPUTY COMMISSIONER,
SPECIALIZED POLICING
SERVICES,
RCMP

Tel. no.
613-843-4494

OUTILS ET TECHNIQUES D'ENQUÊTE DE LA GRC

SUJET : Technologie de la GRC et obtention légale d'éléments de preuve

RÉPONSE SUGGÉRÉE :

- **Le gouvernement s'est engagé à protéger les Canadiens tout en respectant les droits et les libertés, et nous encourageons une discussion sur la façon d'atteindre le mieux possible ce double objectif.**
- **La Gendarmerie royale du Canada peut utiliser des moyens d'enquête techniques pour effectuer des enquêtes criminelles prioritaires et obtenir légalement des éléments de preuve.**
- **L'utilisation d'outils d'enquête par la GRC est régie par la loi, y compris la *Charte*, et assujettie aux processus judiciaires applicables. Les ordonnances des tribunaux sont limitées et portent précisément sur le crime visé par l'enquête, et sont accordées uniquement si toutes les conditions prescrites par la loi sont remplies.**
- **La GRC doit informer les juges des incidences éventuelles des outils d'enquête au moment de demander l'autorisation de les utiliser et doit s'en servir conformément aux limites imposées par les tribunaux.**
- **Lorsqu'ils envisagent d'utiliser une technologie particulière, les agents doivent mettre en balance la nécessité de prévenir des préjudices corporels imminents, de préserver des vies et d'enquêter sur des crimes graves avec les incidences éventuelles de cette technologie sur des tierces parties.**
- **Le 7 avril 2016, le commissaire à la protection de la vie privée a fait savoir à la GRC qu'en réponse à une plainte écrite, il avait lancé une enquête concernant certains outils d'enquête qui seraient utilisés par la GRC. La GRC continue de collaborer avec le commissaire à la protection de la vie privée concernant cette question importante.**

OUTILS ET TECHNIQUES D'ENQUÊTE DE LA GRC

CONTEXTE :

Utilisation et protection d'outils d'enquête par la GRC

La GRC utilise divers outils d'enquête techniques pour remplir son mandat d'assurer la sécurité des Canadiens et d'effectuer des enquêtes criminelles prioritaires. L'utilisation de tout outil d'enquête est assujettie à l'existence d'une autorisation légale; il peut s'agir d'une autorisation judiciaire, de dispositions de la common law ou de l'existence d'une situation d'urgence, comme celle qui prévaut dans les cas récents d'enlèvement d'enfant ou de disparition d'une personne. Disposer d'une autorisation légale fait en sorte qu'au moment de fixer des objectifs d'application de la loi importants, spécifiques et limités, on tient compte à la fois de la sécurité publique et du droit à la vie privée des sujets concernés. Par enquêtes prioritaires, on entend celles qui ont trait à la sécurité nationale, au crime organisé ou à la criminalité financière. La surveillance de l'utilisation de toute technique d'enquête par la GRC est régie par les processus judiciaires applicables, tels que prévus en droit criminel, notamment dans le *Code criminel*. Selon la loi, les ordonnances des tribunaux doivent être limitées et porter précisément sur le crime visé par l'enquête, sont accordées uniquement si toutes les conditions prescrites sont remplies et peuvent faire l'objet d'un examen subséquent par le tribunal et l'accusé au moment du procès. Les données sur les capacités des outils d'enquête de nature délicate sont classifiées. En vertu de la *Loi sur la protection de l'information*, il est interdit de les divulguer, car on compromettrait alors de façon significative la sécurité du public et des policiers, ainsi que l'intégrité de l'appareil de justice pénale. C'est pourquoi la GRC protège cette information classifiée par des mesures rigoureuses. Dans un procès, les outils et techniques d'enquête de la police sont en outre protégés par des dispositions comme celles de la common law ou de la *Loi sur la preuve au Canada*.

Couverture médiatique sur les identificateurs d'appareils mobiles (Mobile Device Identifiers, MDI) et d'autres techniques d'enquête

L'utilisation de MDI et d'autres techniques d'enquête par les organismes d'application de la loi (p. ex. aide fournie par BlackBerry en conformité avec la loi) a suscité une vive attention de la part des médias et du public. Les médias se sont notamment intéressés à un important procès criminel (projet Clemenza) mettant en cause le crime organisé et l'importation de drogue au Québec, ainsi qu'au rôle de la GRC dans l'enquête. Le 10 juin 2016, le tribunal du Québec saisi du projet Clemenza a levé une interdiction de publication relativement à cette affaire. À la suite de cette levée, des détails sur les capacités spécialisées de la GRC ont été rendues publiques, y compris en ce qui concerne les MDI. De plus, dans une affaire de meurtre mettant en cause les suspects dans le projet Clemenza et l'utilisation de MDI, pour laquelle un jugement a été rendu avant l'affaire Clemenza, le juge Stober a ordonné la divulgation d'autres renseignements sur l'utilisation de ces appareils. Depuis, la défense dans le projet Clemenza a demandé à son tour la divulgation de ce type de renseignements. La GRC a entamé des discussions avec les procureurs de la Couronne (Service des poursuites pénales du Canada) concernant cette demande.

Pour assurer la confidentialité de la technologie MDI et d'autres techniques d'enquête, la GRC a refusé publiquement de confirmer ou d'infirmer qu'elle utilisait des MDI. Il est essentiel que la GRC préserve la confidentialité de certaines techniques d'enquête afin de pouvoir continuer à utiliser ces précieux outils pour appuyer des enquêtes et assurer la sécurité du public. La divulgation d'information sur les capacités techniques des MDI, par exemple, ou sur les techniques utilisées pour les exploiter pourrait nuire aux enquêtes menées par la GRC et par toute organisation qui emploie de tels appareils.

La GRC, en consultation avec ses partenaires policiers et du domaine de la sécurité, examine actuellement les options qui s'offrent à elle concernant sa position publique à l'égard des MDI et le niveau approprié d'informations à communiquer sur l'utilisation par la GRC de ces appareils et d'autres techniques d'enquête de nature délicate. Entre-temps, la position de la GRC concernant les demandes des médias sera la suivante : reconnaître que la GRC emploie des techniques et des outils spécialisés, en vertu d'autorisations légales, dans le cadre de ses enquêtes criminelles à l'appui d'objectifs liés à la sécurité publique et nationale; souligner que nous ne discutons pas de capacités ou d'outils particuliers, peu importe ce qui pourrait être disponible dans le domaine public; signaler que nous continuons de collaborer volontiers avec le commissaire à la protection de la vie privée dans le cadre de son examen sur l'utilisation de MDI par la GRC; réitérer que nos enquêtes sont ciblées, limitées, spécifiques, adaptées à la gravité du crime et menées en vertu d'autorisations légales accordées par une magistrature indépendante.

Après la levée de l'interdiction de publication relativement au projet Clemenza, l'utilisation de la technologie MDI a continué de retenir l'attention de médias et du public de façon notable. Par exemple, le 13 septembre 2016, le Citizen Lab de l'Université de Toronto a publié un rapport détaillé intitulé *Gone Opaque? An Analysis of Hypothetical IMSI [International Mobile Subscriber Identity] Catcher Overuse in Canada*.

Enquête du CPVP

Le 7 avril 2016, la GRC a reçu une lettre du Commissariat à la protection de la vie privée (CPVP), en date du 1^{er} avril 2016, dans laquelle celui-ci indiquait qu'il lançait une enquête en réponse à une plainte qu'il avait reçue selon laquelle la GRC contrevenait aux dispositions en matière de collecte d'information de la *Loi sur la protection des renseignements personnels* en recueillant des renseignements personnels au moyen d'appareils « StingRay » ou d'appareils semblables connus sous le nom de capteurs IMSI, et qu'elle refusait de confirmer ou d'infirmer qu'elle utilisait de tels

appareils comme outils d'enquête. La GRC a collaboré et continue de collaborer pleinement avec le CPVP concernant cette affaire. Le 23 juin 2016, des représentants de la GRC et du CPVP se sont réunis pour discuter de cette affaire, et après cette rencontre, le CPVP a fait parvenir à la GRC une série de questions écrites. La GRC s'emploie actuellement à rédiger des réponses à ces questions.

CONTACTS : Préparée par JOE OLIVER, COMMISSAIRE ADJOINT, OPÉRATIONS TECHNIQUES, GRC	N° de tél. 613-993-1620	Approuvée par PETER HENSCHEL, SOUS-COMMISSAIRE, SERVICES DE POLICE SPÉCIALISÉS, GRC	N° de tél. 613-843-4494
---	----------------------------	---	----------------------------

Question Period Note / Note pour la Période des questions

RCMP INVESTIGATIVE TOOLS AND TECHNIQUES

ISSUE: RCMP technology in relation to lawfully obtaining evidence

PROPOSED RESPONSE:

- **Our government is committed to keeping Canadians safe while respecting rights and freedoms, and we welcome discussion about how to ensure an appropriate balance.**
- **The Royal Canadian Mounted Police may use technical investigative methods to conduct priority criminal investigations and lawfully obtain digital evidence.**
- **The use of investigative tools by the RCMP is governed by the law, including the *Charter*, and is subject to appropriate judicial processes. Court orders are limited and specific to the criminality under investigation, and can only be obtained if the statutory requirements are met.**
- **The RCMP must inform judges of the potential impact of investigative tools when seeking authorization, and use them in accordance with the limits set out by the court.**
- **When considering whether to use particular technology, officers are expected to weigh the need to prevent imminent bodily harm, preserve life and investigate serious crimes against potential impacts on third parties.**
- **On April 7, 2016, the Privacy Commissioner indicated to the RCMP that, in response to a written complaint, he has launched an investigation in relation to certain investigative tools reportedly used by the Force. The RCMP assures me that it has and will continue to cooperate with the Privacy Commissioner in this important matter.**

RCMP TECHNICAL INVESTIGATIVE TECHNIQUES

BACKGROUND:

The RCMP's Use and Safeguarding of Investigative Tools

The RCMP uses technical investigative tools under its mandate to safeguard Canadians and conduct priority criminal investigations. Use of any investigative tool is subject to lawful authority, which may refer to judicial authorization; common law; or, the presence of exigent circumstances, such as those in relation to recent child abductions or missing persons. Having lawful authority ensures that the important, specific and limited law enforcement purpose weighs both the public safety and privacy interests involved. Priority investigations include those linked to national security, organized crime, or financial crime. The oversight of any investigative technique used by the RCMP is governed by the appropriate judicial processes, as set out in criminal law, including the *Criminal Code of Canada*. By law, court orders must be limited and specific to the criminality under investigation, can only be obtained if the statutory requirements are met, and can be subsequently reviewed at trial by the court and the accused. The capabilities of sensitive investigative tools are classified. Releasing classified information is illegal under the *Security of Information Act* and would negatively and significantly impact public and officer safety and the integrity of the criminal justice system. As such, the RCMP safeguards classified information through stringent information security measures. At trial, police investigative tools and techniques may be further safeguarded through means such as Common Law or the *Canada Evidence Act*.

Media coverage on Mobile Device Identifiers (MDIs) and other investigative techniques

Issues concerning MDIs and other investigative techniques used by law enforcement (e.g. lawful assistance from BlackBerry) have garnered significant media and other public attention for the past few months. The main focus of the media has been in relation to a high profile criminal court case (Project Clemenza) involving organized crime in Quebec, and the RCMP's investigative role. Most recently, on June 6, 2016, a reporter from Motherboard, VICE Media's technology news site contacted the RCMP and stated that it will be publishing a new feature on the RCMP's use of MDIs based on court documents from Project Clemenza (article has not been published at this time). On June 10, 2016, the CBC reported that the Quebec court for Project Clemenza could lift a publication ban in the case. The publication ban with respect to materials used in the 'Project Clemenza' case have remained in effect until June 10, 2016, at which time details on specialized RCMP capabilities that were not previously vetted from the record will be open for publication. That identified, the previously redacted versions of the Factum and companion documents from Project Clemenza already included information on the RCMP's use of MDIs and other investigative techniques, which have been the basis of previous media coverage.

To date, and to protect the sensitivity of the MDI technology and other investigative techniques, the RCMP has publicly refused to either confirm or deny that it uses MDIs. It is critical that the RCMP protect the sensitivity of certain investigative techniques, so that they remain valuable tools for assisting investigations and maintaining public safety. Any disclosure that describes the technical capabilities of the MDI, for example, or the techniques used to operate the MDI, has the potential to impact investigations conducted by the RCMP, as well as, the investigations of any other organization that uses MDI type devices. That identified, the RCMP recognizes that more information will be made public when the publication ban is lifted, and media and other inquiries will likely continue. The RCMP, in consultation with policing and security partners, is currently analyzing options with respect to its public position on MDIs, and the appropriate level of public disclosure regarding the RCMP's use of MDIs and possibly other sensitive, investigative techniques. In the meantime, the RCMP's position regarding media requests will be to: acknowledge that the RCMP employs specialized tools and techniques under lawful authority in the execution of criminal investigations in support of public safety and national security objectives; highlight that we do not speak about specific tools or capabilities, regardless of what might be available in the public domain; note that we continue to readily cooperate with the Privacy Commissioner as part of their examination of RCMP use of MDIs; and, reinforce that our investigative efforts are targeted, limited, specific, proportionate and lawfully authorized by an independent judiciary.

OPC investigation

On April 7, 2016, the RCMP's Access to Information and Privacy (ATIP) Branch received correspondence from the Office of the Privacy Commissioner (OPC) dated April 1, 2016, that indicated that the OPC was launching an investigation in response to a complaint the OPC had received that alleged that the RCMP "is contravening the collection provision of the *Privacy Act* by collecting personal information using 'StingRay' or similar devices known as IMSI catchers; and, has refused to either confirm or deny that it uses International Mobile Subscriber Identity catchers as investigative tools." The RCMP has been and will continue to fully cooperate with the OPC in this matter. The RCMP is scheduled to meet with the lead OPC investigator during the week of June, 20, 2016, to further discuss the investigation and move it forward.

CONTACTS:

Submitted by
JOE OLIVER,
ASSISTANT COMMISSIONER,
TECHNICAL OPERATIONS,
RCMP

Tel. no.
613-843-4494

Approved by
PETER HENSCHEL,
DEPUTY COMMISSIONER
SPECIALIZED POLICING
SERVICES, RCMP

Tel. no.
613-843-4494

OUTILS ET TECHNIQUES D'ENQUÊTE DE LA GRC

SUJET : Technologie de la GRC et obtention légale d'éléments de preuve

RÉPONSE SUGGÉRÉE :

- **La Gendarmerie royale du Canada peut utiliser des moyens d'enquête techniques pour effectuer des enquêtes criminelles prioritaires et obtenir légalement des éléments de preuve.**
- **L'utilisation d'outils d'enquête par la GRC est régie par la loi et par la Charte et assujettie aux processus judiciaires applicables. Les ordonnances des tribunaux doivent être limitées, spécifiques et proportionnées à la gravité du crime visé par l'enquête.**
- **La GRC doit informer les juges des incidences éventuelles des outils d'enquête au moment de demander l'autorisation de les utiliser et doit s'en servir conformément aux limites imposées par les tribunaux.**
- **Lorsqu'ils envisagent d'utiliser une technologie particulière, les agents doivent mettre en balance la nécessité de prévenir des préjudices corporels imminents, de préserver des vies et d'enquêter sur des crimes graves avec les incidences éventuelles de cette technologie sur des tierces parties.**
- **Le gouvernement s'est engagé à protéger les Canadiens tout en respectant les droits et les libertés, et nous encourageons une discussion de la façon d'assurer un juste équilibre à ces égards.**
- **Le 7 avril 2016, le commissaire à la protection de la vie privée a fait savoir à la GRC qu'en réponse à une plainte écrite, il avait lancé une enquête concernant certains outils d'enquête qui seraient utilisés par la GRC. La GRC m'assure qu'elle a collaboré et continue de collaborer avec le commissaire à la protection de la vie privée concernant cette question importante.**

OUTILS ET TECHNIQUES D'ENQUÊTE DE LA GRC

CONTEXTE :

Utilisation et protection d'outils d'enquête par la GRC

La GRC utilise divers outils d'enquête techniques pour remplir son mandat d'assurer la sécurité des Canadiens et d'effectuer des enquêtes criminelles prioritaires. L'utilisation de tout outil d'enquête est assujettie à l'existence d'une autorisation légale; il peut s'agir d'une autorisation judiciaire, de dispositions de la common law ou de l'existence d'une situation d'urgence, comme celle qui prévaut dans les cas récents d'enlèvement d'enfant ou de disparition d'une personne. Disposer d'une autorisation légale fait en sorte qu'au moment de fixer des objectifs d'application de la loi importants, spécifiques et limités, on tient compte à la fois de la sécurité publique et du droit à la vie privée des sujets concernés. Par enquêtes prioritaires, on entend celles qui ont trait à la sécurité nationale, au crime organisé ou à la criminalité financière.

La surveillance de l'utilisation de toute technique d'enquête par la GRC est régie par les processus judiciaires applicables, tels que prévus en droit criminel, notamment dans le *Code criminel*. Conformément à la loi, les ordonnances des tribunaux sont limitées, spécifiques et proportionnées à la gravité du crime visé par l'enquête, et elles peuvent faire l'objet d'un examen par le tribunal et l'accusé lors d'une instance judiciaire.

Les données sur les capacités des outils d'enquête de nature délicate sont classifiées. En vertu de la *Loi sur la protection de l'information*, il est interdit de les divulguer, car on compromettrait alors de façon significative la sécurité du public et des policiers, ainsi que l'intégrité de l'appareil de justice pénale. C'est pourquoi la GRC protège cette information classifiée par des mesures rigoureuses. Dans un procès, les outils et techniques d'enquête de la police sont en outre protégés par des dispositions comme celles de la common law ou de la *Loi sur la preuve au Canada*.

Article du *Globe and Mail* sur l'utilisation par la GRC de capteurs IMSI (identité internationale d'abonné mobile) (18 avril 2016)

Cet article du *Globe and Mail* porte sur une note de service de la GRC datant de 2011 dans laquelle il est indiqué que la GRC utilisait des capteurs IMSI pour imiter des tours de téléphonie cellulaire et recueillir des numéros de téléphone à l'intérieur d'une portée cible. L'article souligne aussi les risques associés aux capteurs IMSI, à savoir le fait que cette technologie peut perturber les appels de tierces parties innocentes, y compris les appels au 911, dans le secteur visé. L'article précise que des essais effectués par la GRC sur l'utilisation de capteurs IMSI avaient démontré que les nouveaux appels dans la portée d'un capteur IMSI pouvaient être perturbés, y compris les appels au 911. Ces essais ont révélé que pour plus de 50 % des téléphones mobiles testés à l'époque de la note de service de 2011, les appels au 911 avaient été perturbés et l'appelant avait dû composer de nouveau.

La GRC réduit les risques liés au déploiement opérationnel et à l'utilisation de tout outil d'enquête en informant pleinement le juge des incidences éventuelles ou connues de cet outil au moment de demander une autorisation judiciaire et en utilisant des outils approuvés par un juge de manière à en réduire les interférences inutiles.

Concernant une question connexe, le 7 avril 2016, la Sous-direction de l'accès à l'information et de la protection des renseignements personnels de la GRC a reçu une lettre du Commissariat à la protection de la vie privée (CPVP), en date du 1^{er} avril 2016, dans laquelle il indiquait que le CPVP lançait une enquête en réponse à une plainte qu'il avait reçue selon laquelle la GRC contrevenait aux dispositions en matière de collecte d'information de la *Loi sur la protection des renseignements personnels* en recueillant des renseignements personnels au moyen d'appareils « StingRay » ou d'appareils semblables connus sous le nom de capteurs IMSI et qu'elle refusait de confirmer ou d'infirmer qu'elle utilisait de tels appareils comme outils d'enquête. La GRC a collaboré et continue de collaborer pleinement avec le CPVP concernant cette affaire.

De plus, pour ce qui est du « projet Clemenza » (procès tenu à Montréal et mettant en cause la GRC, dont on a parlé récemment dans les médias), le tribunal avait imposé une interdiction de publication concernant le matériel utilisé dans cette affaire, en lien avec des techniques d'enquête de nature délicate. La GRC croit comprendre que cette interdiction devait rester en vigueur jusqu'au 10 juin 2016 sous réserve du dépôt d'autres arguments par la Couronne.

La GRC collabore avec le Service des poursuites pénales du Canada afin de déterminer les circonstances entourant la diffusion apparente d'information visée par l'interdiction de publication. Comme ces questions sont en cours d'examen et que l'interdiction est, selon nous, toujours en vigueur, le gouvernement doit s'abstenir de commenter en détail l'affaire Clemenza ou toute technique d'enquête de nature délicate.

CONTACTS :

Préparée par
JOË OLIVER,
COMMISSAIRE ADJOINT,
OPÉRATIONS TECHNIQUES,
GRC

N° de tél.
613-843-4494

Approuvée par
PETER HENSCHEL,
SOUS-COMMISSAIRE,
SERVICES DE POLICE
SPÉCIALISÉS, GRC

N° de tél.
613-843-4494

2016-2017 Supplementary Estimates (A)

RCMP INVESTIGATIVE TOOLS AND TECHNIQUES

PROPOSED RESPONSE:

- **The RCMP may use technical investigative methods to conduct priority criminal investigations and lawfully obtain digital evidence.**
- **The use of investigative tools by the RCMP is governed by the Charter and subject to appropriate judicial processes. Court orders are limited, specific and proportionate to the seriousness of the criminality under investigation.**
- **The RCMP must inform judges of the potential impact of investigative tools when seeking authorization, and use them in accordance with the limits set out by the court.**
- **When considering whether to use particular technology, officers are expected to weigh the need to prevent imminent bodily harm, preserve life and investigate serious crimes against potential impacts on third parties.**
- **Our government is committed to keeping Canadians safe while respecting rights and freedoms, and we welcome discussion about how to ensure an appropriate balance. Our government is also committed to establishing a parliamentary committee to oversee all national security activities, including those involving investigative tools and techniques by law enforcement.**
- **On April 7, 2016, the Privacy Commissioner indicated to the RCMP that, in response to a written complaint, he has launched an investigation in relation to certain investigative tools reportedly used by the force. The RCMP assures me that it has and will continue to cooperate with the Privacy Commissioner in this important matter.**

Backgrounder:

The RCMP uses technical investigative tools under its mandate to safeguard Canadians and conduct priority criminal investigations. Priority criminal investigations include those linked to national security, organized crime, or financial crime.

The use of any investigative tool is subject to lawful authority, which may refer to judicial authorization; common law; or, the presence of exigent circumstances, such as those in relation to recent child abductions or missing persons. Having lawful authority ensures that the important, specific and limited law enforcement purpose weighs both the public safety and privacy interests involved. Investigative techniques are governed by judicial processes where applicable, as set out in criminal law, including the Criminal Code. By law, court orders are limited, specific and proportionate to the seriousness of the criminality under investigation, and can be subsequently reviewed at trial by the court and the accused.

The capabilities of sensitive investigative tools are classified. Depending on the circumstances, releasing classified information may be illegal under the *Security of Information Act* and could negatively and significantly impact public and officer safety and the integrity of the criminal justice system. As such, the RCMP safeguards classified information through stringent information security measures. At trial, police investigative tools and techniques may be further safeguarded through means such as common law or the *Canada Evidence Act*.

Office of the Privacy Commissioner

In April 2016, the RCMP received notification from the Office of the Privacy Commissioner that an investigation was being launched in response to a complaint that the RCMP “is contravening the collection provision of the *Privacy Act* by collecting personal information using ‘StingRay’ or similar devices known as International Mobile Subscriber Identity (IMSI) catchers; and, has refused to either confirm or deny that it uses IMSI catchers as investigative tools.” The RCMP continues to fully cooperate with the Office of the Privacy Commissioner in this matter.

It is recommended that the Government refrains from publicly speaking in detail about sensitive investigative techniques. The release of sensitive and classified technical tools could permit criminals to modify their behaviour and employ countermeasures to evade law enforcement. The RCMP safeguards sensitive investigative techniques pursuant to Canadian laws and non-disclosure agreements with applicable vendors, which ensures that vendors continue to provide technical and lawful support to priority criminal investigations.

CONTACTS: Prepared by JOE OLIVER, ASSISTANT COMMISSIONER, TECHNICAL OPERATIONS, RCMP	Tel. no. 613-843-4944	Approved by PETER HENSCHEL, DEPUTY COMMISSIONER SPECIALIZED POLICING SERVICES, RCMP	Tel. no. 613-843-4944
--	------------------------------	---	------------------------------

Question Period Note / Note pour la Période des questions

RCMP INVESTIGATIVE TOOLS AND TECHNIQUES

ISSUE: RCMP technology in relation to lawfully obtaining evidence

PROPOSED RESPONSE:

- **The Royal Canadian Mounted Police may use technical investigative methods to conduct priority criminal investigations and lawfully obtain digital evidence.**
- **The use of investigative tools by the RCMP is governed by the law and the *Charter* and is subject to appropriate judicial processes. Court orders must be limited, specific and proportionate to the seriousness of the criminality under investigation.**
- **The RCMP must inform judges of the potential impact of investigative tools when seeking authorization, and use them in accordance with the limits set out by the court.**
- **When considering whether to use particular technology, officers are expected to weigh the need to prevent imminent bodily harm, preserve life and investigate serious crimes against potential impacts on third parties.**
- **Our government is committed to keeping Canadians safe while respecting rights and freedoms, and we welcome discussion about how to ensure an appropriate balance.**
- **On April 7, 2016, the Privacy Commissioner indicated to the RCMP that, in response to a written complaint, he has launched an investigation in relation to certain investigative tools reportedly used by the force. The RCMP assures me that it has and will continue to cooperate with the Privacy Commissioner in this important matter.**

RCMP TECHNICAL INVESTIGATIVE TECHNIQUES

BACKGROUND:

The RCMP's Use and Safeguarding of Investigative Tools

The RCMP uses technical investigative tools under its mandate to safeguard Canadians and conduct priority criminal investigations. Use of any investigative tool is subject to lawful authority, which may refer to judicial authorization; common law; or, the presence of exigent circumstances, such as those in relation to recent child abductions or missing persons. Having lawful authority ensures that the important, specific and limited law enforcement purpose weighs both the public safety and privacy interests involved. Priority investigations include those linked to national security, organized crime, or financial crime.

The oversight of any investigative technique used by the RCMP is governed by the appropriate judicial processes, as set out in criminal law, including the *Criminal Code of Canada*. By law, court orders are limited, specific and proportionate to the seriousness of the criminality under investigation, and can be subsequently reviewed at trial by the court and the accused.

The capabilities of sensitive investigative tools are classified. Releasing classified information is illegal under the *Security of Information Act* and would negatively and significantly impact public and officer safety and the integrity of the criminal justice system. As such, the RCMP safeguards classified information through stringent information security measures. At trial, police investigative tools and techniques may be further safeguarded through means such as Common Law or the *Canada Evidence Act*.

Globe and Mail article in relation to RCMP use of international mobile subscriber identity (IMSI) catchers (April 18, 2016).

The above-mentioned Globe and Mail article focuses on an 2011 RCMP memo, which states that the RCMP has used IMSI catchers to mimic cellphone towers and collect phone numbers within a specific, targeted range. The article also highlights risks associated with IMSI catchers, namely that the respective technology may disrupt phone calls from innocent third parties, including 911 calls within the targeted range. Specifically, the article reports that previous RCMP testing on the use of IMSI catchers has identified that new phone calls within the range of an IMSI catcher may be disrupted, including 911 calls. The testing identified that more than 50% of the mobile telephones tested at the time of the 2011 memo had experienced disrupted 911 calls, which would require the caller to redial.

The RCMP mitigates risks concerning the operational deployment and use of investigative tools by fully informing a judge of the potential or known impacts of investigative tools when seeking judicial authorization, and by using judicially-approved tools in such a manner to mitigate against unnecessary interferences.

On a related issue, on April 7, 2016, the RCMP's Access to Information and Privacy (ATIP) Branch received correspondence from the Office of the Privacy Commissioner (OPC) dated April 1, 2016, that indicated that the OPC was launching an investigation in response to a complaint the OPC had received that alleged that the RCMP "is contravening the collection provision of the *Privacy Act* by collecting personal information using 'StingRay' or similar devices known as IMSI catchers; and, has refused to either confirm or deny that it uses International Mobile Subscriber Identity catchers as investigative tools." The RCMP has been and will continue to fully cooperate with the OPC in this matter.

Also, as per "Project Clemenza" (noted in recent media coverage, i.e. Montreal court case involving the RCMP), the court imposed a publication ban with respect to materials used in the case, which related to sensitive investigative techniques. It is the RCMP's understanding that the publication ban was to remain effect until June 10, 2016 pending further arguments by the Crown.

The RCMP is working with Public Prosecution Service of Canada to determine the circumstances around the apparent release of information that was subject to a publication ban. Given that these matters are still under review and that to our understanding the publication ban remains in effect, the Government should refrain from speaking in detail about the Clemenza case or sensitive investigative techniques.

CONTACTS:

Submitted by
JOE OLIVER,
ASSISTANT COMMISSIONER,
TECHNICAL OPERATIONS,
RCMP

Tel. no.
613-843-4494

Approved by
PETER HENSCHEL,
DEPUTY COMMISSIONER
SPECIALIZED POLICING
SERVICES, RCMP

Tel. no.
613-843-4494

OUTILS ET TECHNIQUES D'ENQUÊTE DE LA GRC

SUJET : Technologie de la GRC et obtention légale d'éléments de preuve

RÉPONSE SUGGÉRÉE :

- **La Gendarmerie royale du Canada peut utiliser des moyens d'enquête techniques pour effectuer des enquêtes criminelles prioritaires et obtenir légalement des éléments de preuve.**
- **L'utilisation d'outils d'enquête par la GRC est régie par la loi et par la Charte et assujettie aux processus judiciaires applicables. Les ordonnances des tribunaux doivent être limitées, spécifiques et proportionnées à la gravité du crime visé par l'enquête.**
- **La GRC doit informer les juges des incidences éventuelles des outils d'enquête au moment de demander l'autorisation de les utiliser et doit s'en servir conformément aux limites imposées par les tribunaux.**
- **Lorsqu'ils envisagent d'utiliser une technologie particulière, les agents doivent mettre en balance la nécessité de prévenir des préjudices corporels imminents, de préserver des vies et d'enquêter sur des crimes graves avec les incidences éventuelles de cette technologie sur des tierces parties.**
- **Le gouvernement s'est engagé à protéger les Canadiens tout en respectant les droits et les libertés, et nous encourageons une discussion de la façon d'assurer un juste équilibre à ces égards.**
- **Le 7 avril 2016, le commissaire à la protection de la vie privée a fait savoir à la GRC qu'en réponse à une plainte écrite, il avait lancé une enquête concernant certains outils d'enquête qui seraient utilisés par la GRC. La GRC m'assure qu'elle a collaboré et continue de collaborer avec le commissaire à la protection de la vie privée concernant cette question importante.**

OUTILS ET TECHNIQUES D'ENQUÊTE DE LA GRC

CONTEXTE :

Utilisation et protection d'outils d'enquête par la GRC

La GRC utilise divers outils d'enquête techniques pour remplir son mandat d'assurer la sécurité des Canadiens et d'effectuer des enquêtes criminelles prioritaires. L'utilisation de tout outil d'enquête est assujettie à l'existence d'une autorisation légale; il peut s'agir d'une autorisation judiciaire, de dispositions de la common law ou de l'existence d'une situation d'urgence, comme celle qui prévaut dans les cas récents d'enlèvement d'enfant ou de disparition d'une personne. Disposer d'une autorisation légale fait en sorte qu'au moment de fixer des objectifs d'application de la loi importants, spécifiques et limités, on tient compte à la fois de la sécurité publique et du droit à la vie privée des sujets concernés. Par enquêtes prioritaires, on entend celles qui ont trait à la sécurité nationale, au crime organisé ou à la criminalité financière.

La surveillance de l'utilisation de toute technique d'enquête par la GRC est régie par les processus judiciaires applicables, tels que prévus en droit criminel, notamment dans le *Code criminel*. Conformément à la loi, les ordonnances des tribunaux sont limitées, spécifiques et proportionnées à la gravité du crime visé par l'enquête, et elles peuvent faire l'objet d'un examen par le tribunal et l'accusé lors d'une instance judiciaire.

Les données sur les capacités des outils d'enquête de nature délicate sont classifiées. En vertu de la *Loi sur la protection de l'information*, il est interdit de les divulguer, car on compromettrait alors de façon significative la sécurité du public et des policiers, ainsi que l'intégrité de l'appareil de justice pénale. C'est pourquoi la GRC protège cette information classifiée par des mesures rigoureuses. Dans un procès, les outils et techniques d'enquête de la police sont en outre protégés par des dispositions comme celles de la common law ou de la *Loi sur la preuve au Canada*.

Article du *Globe and Mail* sur l'utilisation par la GRC de capteurs IMSI (identité internationale d'abonné mobile) (18 avril 2016)

Cet article du *Globe and Mail* porte sur une note de service de la GRC datant de 2011 dans laquelle il est indiqué que la GRC utilisait des capteurs IMSI pour imiter des tours de téléphonie cellulaire et recueillir des numéros de téléphone à l'intérieur d'une portée cible. L'article souligne aussi les risques associés aux capteurs IMSI, à savoir le fait que cette technologie peut perturber les appels de tierces parties innocentes, y compris les appels au 911, dans le secteur visé. L'article précise que des essais effectués par la GRC sur l'utilisation de capteurs IMSI avaient démontré que les nouveaux appels dans la portée d'un capteur IMSI pouvaient être perturbés, y compris les appels au 911. Ces essais ont révélé que pour plus de 50 % des téléphones mobiles testés à l'époque de la note de service de 2011, les appels au 911 avaient été perturbés et l'appelant avait dû composer de nouveau.

La GRC réduit les risques liés au déploiement opérationnel et à l'utilisation de tout outil d'enquête en informant pleinement le juge des incidences éventuelles ou connues de cet outil au moment de demander une autorisation judiciaire et en utilisant des outils approuvés par un juge de manière à en réduire les interférences inutiles.

Concernant une question connexe, le 7 avril 2016, la Sous-direction de l'accès à l'information et de la protection des renseignements personnels de la GRC a reçu une lettre du Commissariat à la protection de la vie privée (CPVP), en date du 1^{er} avril 2016, dans laquelle il indiquait que le CPVP lançait une enquête en réponse à une plainte qu'il avait reçue selon laquelle la GRC contrevenait aux dispositions en matière de collecte d'information de la *Loi sur la protection des renseignements personnels* en recueillant des renseignements personnels au moyen d'appareils « StingRay » ou d'appareils semblables connus sous le nom de capteurs IMSI et qu'elle refusait de confirmer ou d'infirmer qu'elle utilisait de tels appareils comme outils d'enquête. La GRC a collaboré et continue de collaborer pleinement avec le CPVP concernant cette affaire.

De plus, pour ce qui est du « projet Clemenza » (procès tenu à Montréal et mettant en cause la GRC, dont on a parlé récemment dans les médias), le tribunal avait imposé une interdiction de publication concernant le matériel utilisé dans cette affaire, en lien avec des techniques d'enquête de nature délicate. La GRC croit comprendre que cette interdiction devait rester en vigueur jusqu'au 10 juin 2016 sous réserve du dépôt d'autres arguments par la Couronne.

La GRC collabore avec le Service des poursuites pénales du Canada afin de déterminer les circonstances entourant la diffusion apparente d'information visée par l'interdiction de publication. Comme ces questions sont en cours d'examen et que l'interdiction est, selon nous, toujours en vigueur, le gouvernement doit s'abstenir de commenter en détail l'affaire Clemenza ou toute technique d'enquête de nature délicate.

CONTACTS :

Préparée par
JOE OLIVER,
COMMISSAIRE ADJOINT,
OPÉRATIONS TECHNIQUES,
GRC

N° de tél.
613-843-4494

Approuvée par
PETER HENSCHERL,
SOUS-COMMISSAIRE,
SERVICES DE POLICE
SPÉCIALISÉS, GRC

N° de tél.
613-843-4494

Question Period Note – Senate Appearance

RCMP INVESTIGATIVE TOOLS AND TECHNIQUES

PROPOSED RESPONSE:

- **Our government is committed to keeping Canadians safe while respecting rights and freedoms, and we welcome discussion about how best to achieve this dual objective.**
- **The Royal Canadian Mounted Police may use technical investigative methods to conduct priority criminal investigations and lawfully obtain digital evidence.**
- **The use of investigative tools by the RCMP is governed by the law, including the *Charter*, and is subject to appropriate judicial processes. Court orders are limited and specific to the criminality under investigation, and can only be obtained if the statutory requirements are met.**
- **The RCMP must inform judges of the potential impact of investigative tools when seeking authorization, and use them in accordance with the limits set out by the court.**
- **When considering whether to use particular technology, officers are expected to weigh the need to prevent imminent bodily harm, preserve life and investigate serious crimes against potential impacts on third parties.**
- **On April 7, 2016, the Privacy Commissioner indicated to the RCMP that, in response to a written complaint, he has launched an investigation in relation to certain investigative tools reportedly used by the Force. The RCMP continues to cooperate with the Privacy Commissioner in this important and ongoing matter.**

RCMP INVESTIGATIVE TOOLS AND TECHNIQUES

BACKGROUND:

The RCMP's Use and Safeguarding of Investigative Tools

The RCMP uses technical investigative tools under its mandate to safeguard Canadians and conduct priority criminal investigations. Use of any investigative tool is subject to lawful authority, which may refer to judicial authorization; common law; or, the presence of exigent circumstances, such as those in relation to recent child abductions or missing persons. Having lawful authority ensures that the important, specific and limited law enforcement purpose weighs both the public safety and privacy interests involved. Priority investigations include those linked to national security, organized crime, or financial crime. The oversight of any investigative technique used by the RCMP is governed by the appropriate judicial processes, as set out in criminal law, including the *Criminal Code of Canada*. By law, court orders must be limited and specific to the criminality under investigation, can only be obtained if the statutory requirements are met, and can be subsequently reviewed at trial by the court and the accused. The capabilities of sensitive investigative tools are classified. Releasing classified information is illegal under the *Security of Information Act* and would negatively and significantly impact public and officer safety and the integrity of the criminal justice system. As such, the RCMP safeguards classified information through stringent information security measures. At trial, police investigative tools and techniques may be further safeguarded through means such as Common Law or the *Canada Evidence Act*.

Media coverage on Mobile Device Identifiers (MDIs) and other investigative techniques

Issues concerning MDIs and other investigative techniques used by law enforcement (e.g., lawful assistance from BlackBerry) have garnered significant media and public attention. One specific focus of the media's attention has been in relation to a high profile criminal court case (Project Clemenza) involving organized crime and drug importation in Quebec, and the RCMP's investigative role. On June 10, 2016, the Quebec court for Project Clemenza lifted a publication ban. As a result, details of previously undisclosed specialized RCMP capabilities were made public, including in relation to MDIs. In a related murder case involving Project Clemenza suspects, (adjudicated prior to the Clemenza), Justice Stober ordered that additional information about MDIs be disclosed. Since then, the defence in the Project Clemenza organized crime case has applied for information about MDIs to also be disclosed. The RCMP is currently in discussions with Crown prosecutors (Public Prosecution Service of Canada) about this request.

To protect the sensitivity of the MDI technology and other investigative techniques, the RCMP has publicly refused to either confirm or deny that it uses MDIs. It is critical that the RCMP protect the sensitivity of certain investigative techniques, so that they remain valuable tools for assisting investigations and maintaining public safety. Any disclosure that describes the technical capabilities of the MDI, for example, or the techniques used to operate the MDI, has the potential to impact investigations conducted by the RCMP, as well as the investigations of any other organization that uses MDI type devices. The RCMP, in consultation with policing and security partners, is currently analyzing options with respect to its public position on MDIs, and the appropriate level of public disclosure regarding the RCMP's use of MDIs and possibly other sensitive, investigative techniques. In the meantime, the RCMP's position regarding media requests will be to: acknowledge that the RCMP employs specialized tools and techniques under lawful authority in the execution of criminal investigations in support of public safety and national security objectives; highlight that we do not speak about specific tools or capabilities, regardless of what might be available in the public domain; note that we continue to readily cooperate with the Privacy Commissioner as part of their examination of RCMP use of MDIs; and, reinforce that our investigative efforts are targeted, limited, specific, proportionate and lawfully authorized by an independent judiciary.

Since the lifting of the publication ban in relation to Project Clemenza, the use of MDI technology has continued to garner noticeable media and public attention. For example, on September 13, 2016, the University of Toronto's Citizen Lab published a detailed report, "*Gone Opaque? An Analysis of Hypothetical IMSI [International Mobile Subscriber Identity] Catcher Overuse in Canada.*"

OPC investigation

On April 7, 2016, the RCMP received correspondence from the Office of the Privacy Commissioner (OPC) dated April 1, 2016, that indicated that the OPC had launched an investigation in response to a complaint the OPC had received that alleged that the RCMP "is contravening the collection provision of the *Privacy Act* by collecting personal information using 'StingRay' or similar devices known as IMSI catchers; and, has refused to either confirm or deny that it uses [IMSI] catchers as investigative tools." The RCMP has been and will continue to fully cooperate with the OPC in this matter. On June 23, 2016, the RCMP and OPC met to discuss the matter and subsequently the OPC sent the RCMP specific written questions. The RCMP is currently drafting its response to the OPC's specific written questions.

CONTACTS: Prepared By: Joe Oliver, Assistant Commissioner, Technical Operations, Specialized Policing Services, RCMP	Tel. no. 613-843-4944	Approved by: Peter Henschel, Deputy Commissioner, Specialized Policing Services, RCMP	Tel. no. 613-843-4944
--	--------------------------	---	--------------------------



Gendarmerie royale du Canada

ES&ML No:
No. des SE&LM:
Pages: 3
CCM#: 16-001526

16-04-070
Sec. Ser. PS/Serv. Sec. SP
Received / Reçu
MAY 16 2016

Security Classification:
Classification sécuritaire

PROTECTED B (Not for further distribution)

**BRIEFING NOTE
TO THE MINISTER OF
PUBLIC SAFETY AND
EMERGENCY PREPAREDNESS**

**NOTE D'INFORMATION
AU MINISTRE DE LA
SÉCURITÉ PUBLIQUE ET DE
LA PROTECTION CIVILE**

ISSUE:

To brief on the Royal Canadian Mounted Police (RCMP) use of Mobile Device Identifiers (MDIs) and recent media and public attention concerning RCMP investigations and MDIs.

BACKGROUND:

MDIs (also referred to as international mobile subscriber identity (IMSI) catchers) may be used by Canadian police services to capture unique serial numbers associated with cell phones within a specific, targeted range. By mimicking a cell phone tower, an MDI attracts mobile devices within its range and collects unique alphanumeric identifiers transmitted by the mobile devices. In turn, an MDI may be used at different locations to identify common numerical identifiers and eventually link a cellular phone to a target of police investigation. MDIs provide a vital, modern investigative technique for identifying mobile devices used by suspects, which in turn, provides police with critical information to pursue the lawful and targeted acquisition of digital evidence.

In addition to technical and operational factors that limit the impact of MDIs on third parties and mitigate against unnecessary cellular interference, the RCMP has further restricted its use through operational policies. The RCMP obtains prior judicial authorization for its operational deployment and use of an MDI. Pursuant to section 492.2 of the *Criminal Code*, the RCMP seeks a Transmission Data Recorder Warrant to use an MDI, based on a "reasonable grounds to suspect" threshold. A subsequent judicial authorization is required to advance the investigation by seeking access to information with a higher privacy threshold, such as the actual content of private communications. Each court order is limited, specific and proportionate to the seriousness of the criminality under police investigation. The data collected through an MDI is specific and limited. In particular, the data collected through an MDI only includes unique alphanumeric identifiers associated with mobile devices within a targeted range. The collected data does not include the actual content of cellular communications, cell phone numbers or other personal identifiers. Moreover, any data collected through an MDI is properly sealed as an exhibit, pursuant to policy and is treated in accordance with the judicial authorization. The RCMP also uses MDIs in a way that mitigates against unnecessary interference. Specifically, MDIs used by the RCMP do not have the capability to monitor large groups of people, record calls, intercept the content of voice calls or text messages, or extract encryption keys used to conceal private communications.

The use of MDIs by police may involve certain risks to third parties. Specifically, third party cellular devices may be attracted to an MDI signal, depending on distance, the environment, the carrier, and the technical power of the MDI. Phone calls that are in progress when a MDI is activated are not normally disrupted, however, attempts to initiate or receive a phone call, or transmit or receive data, may be temporarily disrupted. Generally, a disrupted phone call means that an impacted cellular device cannot initiate a call while the MDI is activated. The RCMP mitigates this risk by deploying an MDI for a maximum of two to three minutes at a time. Notably, third party phones will typically be impacted for only 10-15 seconds during this activation period. With respect to 911 calls, an MDI will

T.D. No.
No. T.D. L-02003904
File No.
No. Dossier 7194-1
C.C. on ASDN P.A.C.S. 2015-0118



Royal
Canadian
Mounted
Police

Gendarmerie
royale
du
Canada

ES&ML No
No. des SE&LM.
Pages : 3
CCM# : 16-001526

Security Classification
Classification sécuritaire

PROTECTED B (Not for further distribution)

typically allow a cellular device to proceed with the call or to perform an auto-redial function, especially with newer cellular technology. Previous testing in 2011, however, when older cellular technology was used, identified that 50% of the phones tested required the user to redial 911 to complete the call. Given the potential risks associated with the use of an MDI, the RCMP weighs the need to prevent imminent harm, preserve life and investigate serious crimes against potential impacts on third parties. When seeking judicial authorization, the RCMP also informs the judge of the potential or known impacts of the use of the MDI. In situations where exigent circumstances exist, such as in the case of a kidnapping, imminent murder or terrorist activities, an MDI may be used without prior judicial authorization. In these situations, however, judicial authorization would be sought shortly after the deployment of the MDI. The RCMP applies further controls through its internal policy. Specifically, all judicial requests for the deployment of an MDI must first be authorized by the RCMP Divisional Criminal Operations Officer, and an MDI must only be deployed and operated by specially trained RCMP members. In 2015, the RCMP used an MDI in connection with 24 operational files, and only for priority criminal investigations including those linked to national security, serious and organized crime, and financial crime.

CURRENT STATUS:

The RCMP use of MDIs has recently garnered media and other public attention. The main focus of the media has been in relation to a high profile criminal court case (Project Clemenza) involving organized crime in Quebec, and inquiries involving Innovation, Science, and Economic Development Canada (ISED). The RCMP has also been notified that the Office of the Privacy Commissioner is conducting an investigation into its use of MDIs. A summary and update on pertinent issues is provided below.

Project Clemenza and the Publication Ban

From March to April 2016, the media reported that the RCMP used an MDI during Project Clemenza. A publication ban with respect to materials used in this case remains in effect until June 10, 2016 pending further arguments by the Crown. The publication ban means that while the media and public can access redacted court material, they are prohibited from publishing the details. Some media outlets have referenced court documents from Project Clemenza (i.e., redacted versions of the Factum and companion documents) pertaining to the RCMP's use of MDIs. Notwithstanding the publication ban and its parameters, the RCMP is concerned that certain information within the redacted court material could potentially aid criminals in determining how to detect and defeat or minimize the effectiveness of MDI techniques. Consultation between the RCMP and the Public Prosecution Service of Canada in this matter is ongoing.

MDI Impact on 911 Calls

In April 2016, the Globe and Mail reported on the RCMP's use of MDIs and the impact of MDIs on cellular devices to initiate 911 calls. As identified above, new phone calls within the range of an MDI may be disrupted, including 911 calls. Cell phones with newer technology, however, are experiencing less interference and are automatically redialing 911 when an initial call fails. The RCMP is currently testing cellular technologies vis-à-vis MDIs to further examine the potential impact. Testing is ongoing at this time.

Links to the Radiocommunication Act

In March 2016, the Globe and Mail reported that federal agencies did not receive federal authorization for certain technical investigative devices under the *Radiocommunication Act*. The media coverage involved the RCMP, ISED and the boundaries of an RCMP exemption order under the



Royal Canadian Mounted Police

Gendarmerie royale du Canada

ES&ML No.
No des SE&LM
Pages : 3
CCM# : 16-001526

Security Classification .
Classification sécuritaire .

PROTECTED B (Not for further distribution)

Radiocommunication Act. Specifically, in February 2015, the former Minister of Industry signed an exemption order, which exempts the RCMP from prohibitions under the *Radiocommunication Act* against the use of jammers. A "jammer" is defined in legislation as any device or combination of devices that transmits, emits or radiates electromagnetic energy and that is designed to cause interference or obstruction to radiocommunication. To date, the RCMP has been seeking judicial authorization for the use of MDIs during approved operations under what it reasonably considers to be lawful means to pursue priority criminal investigations in the interests of public safety. There is a lack of clarity, however, between the RCMP and ISED with respect to the definition and scope of jammers (i.e. whether it includes an MDI or not) and the parameters of the RCMP's current exemption under the *Radiocommunication Act*. The RCMP and ISED, through their Legal Services Units, are currently working together to come to a common understanding of the legal framework for the RCMP's exemption under the Act. The framework will assist in determining if the use of an MDI falls within the RCMP's current exemption order, or if the RCMP must seek separate authorization from the Minister of Innovation, Science, and Economic Development.

Office of the Privacy Commissioner

In April 2016, the RCMP received notification from the Office of the Privacy Commissioner that an investigation was being launched in response to a complaint that the RCMP "is contravening the collection provision of the *Privacy Act* by collecting personal information using 'StingRay' or similar devices known as IMSI catchers; and, has refused to either confirm or deny that it uses International Mobile Subscriber Identity catchers as investigative tools." The RCMP continues to fully cooperate with the Office of the Privacy Commissioner in this matter.

NEXT STEPS:

The Government should limit speaking in detail about the Project Clemenza case or sensitive investigative techniques. The release of sensitive and classified technical tools could permit criminals to modify their behaviour and employ countermeasures to evade law enforcement. The RCMP safeguards sensitive investigative techniques pursuant to Canadian laws and non-disclosure agreements with applicable vendors, which ensures that vendors may continue to provide technical and lawful support to priority criminal investigations. In relation to Project Clemenza, there are active discussions between the RCMP and the Crown to determine options, if any, to further redact the public record for sensitive information before the current publication ban is lifted. The RCMP is currently reviewing the Factum and accompanying documents in detail to determine if additional sensitive information should be vetted. Notably, the redacted Factum, as it stands, reveals RCMP use of sensitive techniques, such as the RCMP's use of the MDI as an investigative tool, or possession of an encryption key for a well-known cellular manufacturer.

Given the complexity and high profile nature of this issue, the RCMP welcomes representatives from the Minister's office to visit the RCMP's Technical Operations facilities in Ottawa for an in-person briefing on how it develops and deploys specialized technical services in criminal investigations.

Approved by : Approuvée par :	Date
 Bob Paulson Commissioner	MAY 3 '15

**Pages 123 to / à 132
are withheld pursuant to sections
sont retenues en vertu des articles**

15(1) - Subv, 16(1)(b), 16(1)(c)

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