Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Kimberley Pearce - [redacted]

From: Kimberley Pearce
To: Morris, Jeffrey
Date: 2016/05/05 10:11 AM
Subject: [redacted]

Hi Jeff,

s.23

The attachment didn't come through on the email.

Kim

>>> Jeffrey Morris <jeffrey.morris@rcmp-grc.gc.ca> 2016/05/05 7:11 AM >>>
Hello all,

[redacted]

Jeff

[redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

(Discussion Item)

[redacted]

(JUSTICE CANADA)

ISSUE/CONTEXT:

While the conference document that will guide the discussion is not out yet, [redacted] has proposed to discuss the issue of [redacted]

s.13(1)(c)
s.14(a)
s.21(1)(a)

STRATEGIC ADVICE:

It is recommended that you:

- [redacted]
- [redacted]
- [redacted]

BACKGROUND:

[redacted]

An extensive review of Canada's cryptography policy was undertaken in 1997-1998 under the leadership of Industry Canada in the context of Canada's e-commerce policy but extending to issues of law enforcement access and national security considerations. The government prepared and released a public consultation document, held meetings across the country and received more than 150 written submissions from banks, companies, industry organizations, law enforcement and concerned citizens. The government response, after careful study, affirmed the freedom of Canadians to develop, import and use whatever cryptography they wished. T~~;~~ the government

Author: Gareth Sansom Phone: 613-424-5300 Date: May 12, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

(Discussion Item)

affirmed support for private sector research and development and said that it~~; the Government~~ would not [redacted] and that~~;~~ export controls would continue to be consistent with Canada's international obligations. The ~~; and the~~ government also suggested that it would explore legislative and other options to protect consumer privacy and to assist law enforcement and national security agencies. The policy emphasized the importance of maintaining a balanced approach to a complex problem and this policy remains the Canadian policy on this issue.

The recent controversy in the United States with respect to FBI compelling access to encrypted stored data in Apple iPhones resulted in a strong backlash by the private sector, civil liberties organizations and the public.

PROVINCIAL/TERRITORIAL CONSIDERATIONS:

[redacted]

s.14(a)
s.21(1)(a)

JUSTICE CANADA POSITION:

E~~Justice Canada recognizes that the issues~~ [redacted] has found no simple solution in the past three decades and ~~that~~ any legislated solution to ~~encryption~~ this issue must be developed in a manner that is consistent with the *Canadian Charter of Rights and Freedoms*, with particular attention ~~paid~~ to the right against self-incrimination arising from compelled testimony; privacy and civil liberties as well as freedom of expression. As currently drafted, the Green Paper on National Security contains [redacted]

Formatted: Font: Italic

CURRENT STATUS:

Author: Gareth Sansom Phone: 613-424-5300 Date: May 12, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

(Discussion Item)

[redacted]

s.14(a)
s.21(1)(a)

DESIRED OUTCOME:

[redacted]

Author: Gareth Sansom Phone: 613-424-5300 Date: May 12, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

From: Kimberley.Pearce@rcmp-grc.gc.ca
To: Morris, Jeffrey <jeffrey.morris@rcmp-grc.gc.ca>
Subject: [redacted]
Date: 2016/05/13 3:01:00 PM

s.23

Hi Jeff,

[redacted]

Thanks,
Kim

>>> Jeffrey Morris 2016/05/13 11:02 AM >>>
Hi Kim,

[redacted]

Thanks,
Jeff

Pages 6 to / à 10

are withheld pursuant to section

sont retenues en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

None None None NoneNoneNoneNone

(/EN_US?TRK_SOURCE=HEADER-LOGO)

THE CHANNELS EN

Canada's Privacy Czar: 'Sometimes the Government Goes Too Far'

Written by **JORDAN PEARSON (/AUTHOR/JORDANPEARSON)**

Released under the Access to Information Act / Divulgué(s) en vertu de la Loi sur l'accès à l'information.

May 13, 2016 // 12:28 PM EST

(/EN_US?TRK_SOURCE=HEADER-LOGO)

On paper, the Office of the Privacy Commissioner (https://www.priv.gc.ca/) is Canada's top privacy watchdog, a mantle that exudes a "buck stops here" aura of authority.

The reality is pretty different.

When it comes to overseeing Canada's cops and security agencies, the privacy commissioner is uncomfortably toothless. Although government policy dictates that all agencies and departments consult the privacy commissioner regarding any new initiatives that have privacy implications, that doesn't always happen.

When the Royal Canadian Mounted Police, or RCMP, decided to start fishing around for facial recognition tech (http://motherboard.vice.com/read/the-rcmp--store-photos-of-strangers-they-cant-identify-surveillance-facial-recognition-database), they didn't bother to tell the OPC, as the office is known. When a prison in Warkworth, Ontario, decided to install a Stingray-like surveillance device (http://motherboard.vice.com/read/a-canadian-prison-was-spying-on-people-and-recording-their-calls-and-texts) in its facility, the OPC was similarly unaware, it told Motherboard at the time.

> "Encryption is one of the best tools to protect privacy, and it needs to be promoted, used, and protected"

With the passing of Bill C-51 (http://www.vice.com/en_ca/read/canadas-new-anti-terror-bill-is-everything-you-hoped-it-wasnt-723) last year, an anti-terror law that was widely criticized for giving police new and overreaching surveillance powers, and a recent Motherboard and VICE News investigation (http://motherboard.vice.com/read/rcmp-

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

blackberry-project-clemenza-global-encryption-key-canada) that revealed the RCMP hold the global decryption key for any and all consumer BlackBerry communications, it's clear that the privacy commissioner's role has become more important than ever.

(&EN_US;TRK_SOURCE=HEADER-LOGO)

In an uncommon one-on-one interview, I sat down with privacy commissioner Daniel Therrien at this week's International Association of Privacy Professionals conference (http://motherboard.vice.com/read/canadas-insurance-companies-want-all-your-genetic-information) in Toronto to talk about the role of privacy-protecting technologies like encryption in Canada, and why the OPC always seems to be playing catch-up with the cops.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

(/EN_US?TRK_SOURCE=HEADER-LOGO)

Image: Office of the Privacy Commissioner

Motherboard: Do you believe there needs to be a debate in Canada (http://motherboard.vice.com/read/canada-needs-to-revive-the-encryption-debate-it-had-in-the-1990s) **about balancing the use of encryption by citizens to protect their privacy, and the priorities of police? And what is your position on that issue?**

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Daniel Therrien: For sure, this needs to be discussed in Canada. The same issues, the same technology, the same need for the police or national security agencies to get access to information to do their job and identify criminals and terrorists, exist in Canada as they do in the US, Europe, and many other places.

(/EN_US?TRK_SOURCE=HEADER-LOGO)

It's a very tough nut to crack, this issue of the balance between encryption in this case and the need for the police to have access to some information. I don't think anybody has the exact answer to where to draw the line. I would say that there's no question that encryption is extremely important to protect the privacy of Canadians, including the vast majority of law-abiding citizens, obviously.

Encryption is one of the best tools to protect privacy, and it needs to be promoted, used, and protected. That's one side of the coin.

On the other side of the coin, the police and national security agencies also have a legitimate job to do, to get at information that will help them identify threats of criminality or national security. An important limitation to their powers is that they need to act according to the law. To me, there's a huge difference between police and national security agencies acting pursuant to a clear legal authority, or to a warrant. That is a situation where law enforcement agencies are able to implement the legal authorities that they have when they are clear and reasonable.

But when we get to issues like warrantless access (http://motherboard.vice.com/read/rcmp-warrantless-access-to-data-would-certainly-assist-new-cyber-crime-unit), when the legal authority is much less clear, that is a different matter.

Encryption absolutely needs to be there, and promoted. The police have a job to do, but they have to do it within the law. We've seen many examples of attempts by the state to get access to that information in a warrantless way, and that is of concern.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

"Often we see that the policy is not necessarily respected"

(/EN_US?TRK_SOURCE=HEADER-LOGO)

It seems like the Office of the Privacy Commissioner is sometimes the last to know about law enforcement initiatives that have clear privacy implications. For example, the RCMP soliciting facial recognition technology, or a prison using a Stingray-like device. Do you have a plan to change this?

On the RCMP device, we found out after the fact that the RCMP was sending out tenders for companies that might have this equipment without, they say, the intention in the short term to use facial recognition. So, that's a nuance on the facts.

On playing catch-up, we can only advise on issues that we're informed on. That's in part why I said in the recommendations to amend the Privacy Act (https://www.priv.gc.ca/media/nr-c/2016/nr-c_160310_e.asp) that federal institutions—departments and agencies—should have a legal obligation to inform the Privacy Commissioner's office of initiatives, programs, that involve privacy. Currently, it's under a policy that this is done, and often we see that the policy is not necessarily respected.

If this became a legal obligation, as it exists in certain jurisdictions—and some of them in Canada, provincially—we think it's more likely that we will be informed.

Returning to your point about warrantless access, we saw in a recent investigation by Motherboard and VICE News that the RCMP acquired the global decryption key for any and all consumer BlackBerry devices. We have no reason to believe that any of this was done without a warrant or legal consent. If the law allows this to take place, is the law too permissive?

That's certainly possible.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

When Bill C-13 (http://www.vice.com/en_ca/read/canadas-new-cyberbullying-bill-will-give-the-government-unnecessary-surveillance-superpowers) was before the house, I made comments along those lines. This was a bill that purported and did actually provide additional powers to law enforcement, which we said did not have the right threshold in terms of reasonable grounds to believe that a certain criminal act was committed before certain powers were used. It is absolutely possible.

(&EN_US?TRK_SOURCE=HEADER-LOGO)

But here, in these situations, we do know, because the introduction of legislation is a very public act. We can intervene and make comments. We would obviously prefer that our advice was heeded more often, but at least there we have the opportunity to make comments.

And yes, sometimes the government goes too far in the legislation that it puts forward.

--

TOPICS: state of surveillance (/tag/state+of+surveillance), Canada (/tag/Canada), Office of the Privacy Commissioner (/tag/Office+of+the+Privacy+Commissioner), OPC (/tag/OPC), Daniel Therrien (/tag/Daniel+Therrien), encryption (/tag/encryption), Encryption debate (/tag/Encryption+debate), rcmp (/tag/rcmp), Royal Canadian Mounted Police (/tag/Royal+Canadian+Mounted+Police), blackberry (/tag/blackberry), Spying (/tag/Spying), surveillance (/tag/surveillance), Spy (/tag/Spy), interview (/tag/interview), news (/tag/news)

Contact the author by email (mailto:jordan.pearson@vice.com) or Twitter (https://twitter.com/neuwaves).

You can reach us at letters@motherboard.tv (mailto:letters@motherboard.tv). Want to see other people talking about Motherboard? Check out our letters to the editor (http://motherboard.vice.com/tag/letters+to+the+editor).

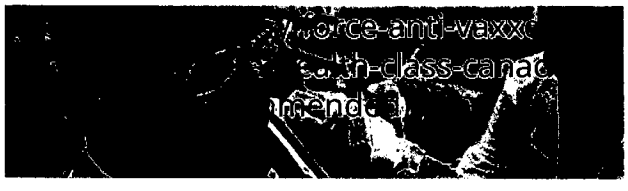
Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

(/EN_US?TRK_SOURCE=HEADER-LOGO)

RECOMMENDED

New MIT Tool Quickly Roots Out Hidden Web App Security Bugs (/read/new-mit-tool-quickly-roots-out-lurking-web-app-security-bugs?trk_source=recommended)

Should You Be Stoked Or Bummed About Hollywood's Snowden Movie? (/read/edward-snowden-trailer-movie-hollywood?trk_source=recommended)



Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Kimberley Pearce - THE HAGUE – May 20, 2016 – Europol and ENISA Joint Statement – On lawful criminal investigation that respects 21st century data protection

From: Tomasz Pacha
To: Aucoin, Marc; Cotton, Brian; Dhanoa, Gurinder; Flynn, Mark; Geber, D...
Date: 2016/05/24 4:04 PM
Subject: THE HAGUE – May 20, 2016 – Europol and ENISA Joint Statement – On lawful criminal investigation that respects 21st century data protection
CC: Gendre, Carol-Ann; Plomp, Jason; Price, Liam
Attachments: on-lawful-criminal-investigation-that-respects-21st-century-data-protection.pdf; nl-cabinet-encryption-position.pdf; The-European-Cybercrime-Centre-Bulletin.pdf; privacy-in-the-digital-age-of-encryption-and-anonymity-online.pdf; lawful-access-and-security-a-transatlantic-perspective-2013-eastwest-institute.pdf

Colleagues, (European Union Agency for Network and Information Security)

On May 20, 2016, Europol and ENISA released a Joint Statement entitled *On lawful criminal investigation that respects 21st century data protection*: attached and available from https://www.europol.europa.eu/content/lawful-criminal-investigation-respects-21st-century-data-protection-europol-and-enisa-joint.

In this joint statement, they "stress the importance of ***proportionality*** for the use of intrusive investigative tools" (emphasis in original), and then go on to conclude:

> "For the investigation and disruption of crimes, it is important to use all possible and lawfully permitted means to get access to any relevant information, even if the suspect encrypted it.
>
> To achieve this, it would be worthwhile to collect and share best practices to circumvent encryption already in use in some jurisdictions. Investigators would benefit from more explicit and ideally aligned regulation of the lawful online use of privacy-invasive investigative tools and the conditions under which they can be applied.
>
> Moreover, policy makers in consultation with the judiciary could further contribute by issuing clear policy guidance on the proportionality of the online use of such privacy-invasive investigative tools.
>
> When circumvention is not possible yet access to encrypted information is imperative for security and justice, then feasible solutions to decryption without weakening the protective mechanisms must be offered, both in legislation and through continuous technical evolution." (highlights mine)

Relatedly, you'll also find attached:

- The Government of the Netherlands' ***Cabinet's view on encryption*** (https://www.government.nl/documents/letters/2016/01/04/cabinet%E2%80%99s-view-

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

on-encryption)
- The October 2015 - February 2016 edition of the **EC3 bulletin**
- Statement made by the head of the European Union Agency for Network and Information Security (ENISA)
- Opening remarks by the head of ENISA

Carol-Ann Gendre

Thanks for sharing these final three, Carol-Ann – much appreciated.

The context here is the https://www.europol.europa.eu/content/europol-cooperation-eipa-hosts-conference-privacy-and-security-online conference; trip report from Carol-Ann and I in press.

FPSP and FPCO (the coordinators): please forward within FP as/if needed. Thank you.

Regards,
Tom

Tom Pacha
Senior Research Analyst
Strategic Policy and Integration
RCMP Specialized Policing Services
Office 613-843-6266
BB 613-793-5308

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

20 May 2016

On lawful criminal investigation that respects 21st Century data protection. Europol and ENISA Joint Statement.

1 The communication society

The desire to preserve the secrecy and integrity of a document is as old as written communication, and is deeply inscribed in our modern legislation, touching basic rights such as freedom of expression and the right to privacy. With the move to the information society and the automation of data processing, this need is becoming ever more important. Moreover, these issues go beyond individual's rights: in a society that is ever more depending on the correct functioning of electronic communication services, technical protection of these services is mandatory, since otherwise criminals will abuse vulnerable services. From a technical standpoint, both confidentiality and integrity may be fulfilled by the same cryptographic mechanisms. However, while secure communication services have many legitimate purposes, they may also be used to plan and conduct criminal activities. Hence, law enforcement services need tools to investigate cybercrimes as well as cyber-facilitated forms of crimes.

2 The limits of privacy

An individual's rights need to be evaluated carefully in relation to the individual rights of others to find a balance between the individual interests of the persons concerned. Thus, in the face of serious crimes, law enforcement may lawfully intrude privacy or break into security mechanisms of electronic communication systems. Legislation must explicitly stipulate the conditions under which law enforcement can operate. Here, we want to stress the importance of ***proportionality*** for the use of intrusive investigative tools. This requires that the intrusive effect of the investigative measure is proportionate to the crime that was committed. It also requires the selection of the least intrusive measure to achieve the investigative objective. The legislation should include the provision of appropriate supervision to ensure that intrusive measures are used in accordance with these principles.

Intercepting an encrypted communication or breaking into a digital service might be considered as proportional with respect to an individual suspect, but breaking the cryptographic mechanisms might cause collateral damage. The focus should be on getting access to the communication or information; not on breaking the protection mechanism. The good news is that the information needs to be unencrypted at some point to be useful to the criminals. This creates opportunities for alternatives such as undercover operations, infiltration into criminal groups, and getting access to the communication devices beyond the point of encryption, for instance by means of live forensics on seized devices or by lawful interception on those devices while still used by suspects. Moreover, forensic methods that make use of physical fingerprints of devices might not help to intercept the communication content itself, but might provide other important clues for the investigator. Even so, there are cases in which there are no such alternatives and access to the concealed content can only be gained by a form of decryption.

3 Considerations on decryption

While no practical encryption mechanism is perfect in its design and implementation, decryption appears to be less and less feasible for law enforcement purposes. This has led to proposals to introduce mandatory backdoors or key escrow to weaken encryption. While this would give investigators lawful access in the event of serious crimes or terrorist threats, it would also increase the attack surface for malicious abuse,

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

which, consequently, would have much wider implications for society. Moreover, criminals can easily circumvent such weakened mechanisms and make use of the existing knowledge on cryptography to develop (or buy) their own solutions without backdoors or key escrow.

The latest generation of encryption tools allow forward secrecy, meaning that the disclosure of a long-term private key does not allow the deciphering of messages from the past.

4 Resolving the encryption dilemma

Solutions that intentionally weaken technical protection mechanisms to support law enforcement will intrinsically weaken the protection against criminals as well, which makes an easy solution impossible. So far, we observe a continued arms race between cryptographers and crypto-analysts. In terms of practical breaks, cryptographers are currently miles ahead, which is good news for all the legitimate users who can benefit from the improving protection of their data. However, there is no doubt that malevolent parties use the same techniques to conceal their criminal activities and identities. For the investigation and disruption of crimes, it is important to use all possible and lawfully permitted means to get access to any relevant information, even if the suspect encrypted it.

To achieve this, it would be worthwhile to collect and share best practices to circumvent encryption already in use in some jurisdictions. Investigators would benefit from more explicit and ideally aligned regulation of the lawful online use of privacy-invasive investigative tools and the conditions under which they can be applied. Moreover, policy makers in consultation with the judiciary could further contribute by issuing clear policy guidance on the proportionality of the online use of such privacy-invasive investigative tools.

When circumvention is not possible yet access to encrypted information is imperative for security and justice, then feasible solutions to decryption without weakening the protective mechanisms must be offered, both in legislation and through continuous technical evolution. For the latter, the fostering of close cooperation with industry partners, as well as the research community with expertise in crypto-analyses for the breaking of encryption where lawfully indicated, is strongly advised. We are convinced that a solution that strikes a sensible and workable balance between individual rights and protection of EU citizen's security interests can be found. In this respect, the deployment of European R&D instruments may drive this collaboration while at the same time EU Agencies can work closely together in establishing best practices.

This Joint Statement is presented as a contribution from ENISA and Europol to the on-going debate on privacy and encryption. It is based on the practical experiences and perspectives of the two organisations and is neither intended as being the formal position of the EU Institutions on this subject, nor as having any prejudice to that.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

To the President of the House of Representatives
of the States General
Postbus 20018
2500 EA DEN HAAG

Ministry of Security and Justice

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Our reference
708641

Date 4 January 2016
Subject Cabinet's view on encryption

Cabinet's view on encryption
Please find below the cabinet's view on encryption. This is in line with promises made during the debate of the standing committee on Economic Affairs on the Telecommunications Council of10 June 2015 (TK 2014-2015, 21501-33, no. 552) and the debate of standing committee on Security and Justice on the JHA Council of 7 October 2015.

Introduction
Encryption is increasingly easy to obtain and use and is thus more often part of regular data transactions. Encryption is increasingly applied by the government, companies and citizens to protect the confidentiality and integrity of their communication and stored data. This is important for people's confidence in digital products and services and for the Dutch economy in the light of a fast developing digital society. At the same time, encryption inhibits the acquisition of information required for investigation, intelligence and security services when malicious actors (such as criminals and terrorists) use it. The recent attacks in Paris, where encrypted communication may have been used by the terrorists, lead to the justified question what investigation, intelligence and security services need to have and retain good insight into the planning of attacks.

The ambiguity described in the preceding paragraph was also heard in the public debate of the last few months about the dilemmas of the use of encryption. The topic was also discussed in your House. During the debate of the standing committee on Economic Affairs on the Telecommunications Council the question was asked what the cabinet is planning to do to encourage the use of strong encryption. Additionally, the House of Representatives requested the cabinet to adopt a view on encryption.

The importance of encryption for the system and information security of the government and companies and for the constitutional protection of privacy and the confidentiality of communication is discussed below. The importance of detection of serious crimes and protection of national security are also included. Finally, a conclusion is reached after all interests have been assessed.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Criminal Policy Department
(DSB)

Datum
4 January 2016

Ons kenmerk
708641

The situation in the Netherlands cannot be seen separately from its international context. Strong encryption software is increasingly available worldwide or an integral part of products or services. Considering the wide availability and application of advanced encryption techniques and the cross-border nature of data transaction, room for national action is limited.

The importance of encryption for the government, companies and citizens
Cryptography plays a key role in the technical security in the digital domain. Many cybersecurity measures in organisations are strongly based on the application of encryption. The secure storage of passwords, the protection of laptops against loss or theft and the secure storage of backups are more difficult without the use of encryption. The protection of data sent via the internet, for instance in internet banking, is only possible with the use of encryption. Due to the interconnectedness of networks, worldwide branching and the different routes communication can take, the risk of interception, infringement, perusal or modification of information and communication is always present.

The government increasingly communicates digitally with citizens and provides services whereby confidential information is exchanged, such as the use of a digital ID (DigiD) or filing a tax return. As formulated in the Coalition Agreement, citizens and companies must be able to arrange and settle their government affairs fully digitally from 2017 onwards. It is the duty of the government in that respect to make sure that this information is protected against third party examination; encryption is indispensable in that respect. The protection of the internal communication of the government also depends on encryption, for example with regard to the security of diplomatic and military communication.

Encryption is essential for companies to securely store and send company information. Being able to use encryption strengthens the international competitive position of the Netherlands and contributes to an attractive business and innovation climate for, for example, start-ups, data centres and cloud computing. Confidence in secure communication and data storage is essential for the (future) growth potential of the Dutch economy, which is mainly in the digital economy.

Encryption supports the respect of personal privacy and confidential communication of citizens because it offers them a means to protect the confidentiality and integrity of personal data and communication. This is also important for exercising the freedom of expression. It enables citizens, but also professions with an important democratic function such as journalists, to communicate confidentially.

Encryption therefore enables all parties involved to ensure the confidentiality and integrity of communication and to better defend themselves against espionage and cybercrime. Fundamental rights and freedoms, security and economic interests benefit from this.

Encryption and the investigation, intelligence and security services
The powers and resources available to the services must be suited for the current and future digital reality. The investigation, intelligence and security services support the security of the digital and physical world with effective, lawful access to information. Where encryption is applied by malicious actors, it hinders the access to that information for the investigation, intelligence and security services.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

They experience this for instance when they investigate the distribution and storage of child pornography, support military missions abroad, counter cyberattacks or when they want to gain and retain insight into the preparation of terrorist attacks. Criminals, terrorists and opponents in armed conflict are often aware that they might attract the attention of the services at some point in time and nowadays also have access to advanced encryption methods which are difficult to circumvent or break. The use of such methods requires little technical knowledge, as encryption is often an integral part of the internet services which they can use. That complicates, delays or renders it impossible to (timely) gain insight into the communication for the benefit of protecting national security and investigating criminal offences. Additionally, the investigative hearing at the trial and the case for a conviction can be seriously obstructed.

The right to respect for personal privacy and privacy of correspondence of citizens

As noted before, the use of encryption helps citizens secure their personal privacy and the confidentiality of their communication. The aforementioned lawful access to information and communication by the investigation, intelligence and security services however infringes on the confidential communication of citizens.

Privacy of communication relates to the constitutional respect for personal privacy and the right to protection of the privacy of correspondence, telephone and telegraph (hereinafter: 'privacy of correspondence'). These fundamental rights are rooted in Sections 10 and 13 respectively of the Constitution. These fundamental rights have also been laid down in Article 8 ECHR and Articles 7 and 8 of the EU Charter (to the extent it touches on EU Law).

The protection of fundamental rights applies to the digital world. The aforementioned constitutional and international law provisions together are the parameters for preventing illegal infringement. The rights mentioned are not absolute, which means that restrictions are allowed as long as they meet the requirements of the Constitution and the ECHR (and the EU Charter where EU law is concerned). An infringement is allowed if it serves a legitimate purpose, if it is regulated by law and if the restriction is foreseeable and known. The restriction must also be necessary in a democratic society. Finally, the infringement must be proportional, which means that the objective sought by the government must be proportionate to the infringement of the personal privacy and/or the privacy of communication.

These requirements are the parameters within which the balance can be decided between the interests at stake with encryption, such as the right to personal privacy and privacy of correspondence, public and national security and the prevention of criminal offences. To the extent it concerns the special powers of the intelligence and security services, the preceding assessment parameters have also been laid down in the Intelligence and Security Services Act 2002 (Sections 18 and 31). The obligations to cooperate regarding decryption that are included in the Intelligence and Security Services Act 2002 (Articles 24 (3) and 25 (7)) and in the Dutch Criminal Code (Article 126m (6)), may be invoked if associated special powers are exercised after an assessment as previously specified.

Assessment and conclusion

Nowadays the possibility to break encryption is decreasing. The possibility to obtain unencrypted information from a service provider is less often available.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Criminal Policy Department
(DSB)

Datum
4 January 2016

Ons kenmerk
708641

Service providers increasingly process information that has already been encrypted through modern applications of encryption when it reaches them. Considering the importance of the investigation and prosecution of criminal offences and the interests involved in national security, these developments require a search for new solutions.

There are currently no options in a general sense, e.g. via standards, to weaken encryption products without compromising the security of digital systems that use encryption. For instance, introducing technical access into an encryption product would make it possible for investigation services to inspect encrypted files, digital systems can become vulnerable to, for instance, criminals, terrorists and foreign intelligence services. This would have undesirable consequences for the security of communicated and stored information and the integrity of IT systems, which are increasingly important for the functioning of society.

For the performance of their statutory tasks, the investigation, intelligence and security services partly depend on cooperation with providers of IT products and services. Given this dependency, consultation with providers is needed about effectively providing information when their services are used by malicious actors, while taking into account to everyone's role and responsibilities and the statutory parameters.

Given the preceding assessment, the following conclusion is reached:

It is the responsibility of the cabinet to guarantee the security of the Netherlands and to investigate criminal offences. The cabinet underlines the necessity of lawful access to information and communication in this respect. Additionally, government authorities, companies, and citizens benefit from maximum security of digital systems. The cabinet endorses the importance of strong encryption for internet security to support the protection of personal privacy of citizens, for confidential communication of the government and companies and for the Dutch economy.

The cabinet is therefore of the opinion that at this point in time it is not desirable to take restrictive legal measures as regards the development, availability and use of encryption in the Netherlands. The Netherlands will disseminate this conclusion and the underlying assessment internationally. As regards the stimulation of strong encryption, the Minister of Economic Affairs will follow up on the purport of the amendment (TK 2015-2016, 34300 XIII, no.10) on the budget of the Ministry of Economic Affairs.

Minister of Security and Justice,

G.A. Van der Steur

Minister of Economic Affairs

H.G.J. Kamp

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

enisa

Privacy in the Digital Age of Encryption and Anonymity Online

Speech by ENISA Executive Director, Prof. Dr. Udo Helmbrecht

THE HAGUE
19TH- 20TH MAY, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Good morning Ladies and Gentlemen

It is a great pleasure to be able to welcome you to this conference. I am really impressed by the collection of different sector actors represented in this event today and I would like to thank Europol and the European Institute of Public Administrations for giving me the chance to address you.

The underlying point of today's event is that everything is becoming digital, from cars to cities to services to the whole economy. Network infrastructure, available anywhere and at any time, is transporting a huge volume of information. An obvious and immediate conclusion would thus be that the integrity of this information is crucial to the functioning of this economy.

So let's start with this point.

Continuous growth of e-commerce

It is often stated that we depend increasingly on trustworthy network services.

For example in 2014, about 13% of all retail trade in the UK was online; for 2016, retail researchers estimate that this share will grow by more than 30%. This will be good for 71 bn Euros. For Germany the numbers are slightly lower (10% in 2014 and 13.5 expected for 2016)[1].1 But in essence, for a market that depends on habits of people this growth rates are tremendous.

While it is harder to find numbers for B2B, my gut feeling says that an even bigger share of B2B transactions are carried out online or is at least supported by electronic communication – just try to remember when it was the last time that you selected a product from a paper catalogue and sent a letter to order it for your work. The younger among this audience might not even understand this question.

As a matter of fact **an increasing part of our everyday life is moving online**: e-Governance, e-health, and social networks. Most evident here is the change in the media sector. Most young people use the internet as news, communications and entertainment source - printed newspapers market share is constantly declining. For example, quite recently the newspaper *The Independent* announced its last printed issue on 26 March 2016. It is likely that this was only the first very prominent victim of the change.

Crime also goes online

So it is a fact.

We do depend increasingly on trustworthy network services for business and social life. Unfortunately also criminals "go digital". Already in 2012 12% of internet users reported that they experienced online fraud, and 8% have fallen victim to identity theft[2]. I am quite sure that our host can confirm that this issue did not disappear in the last 4 years.

And, vulnerable digital services are not only a risk for the individual users; **vulnerable services might also lead to a general decline of the overall trust in information technology and the services offered**. However, the European Digital Agenda points out that **trust in information technology** is of uttermost importance for our economy. This is echoed in the recently published NIS Directive that is aiming to *"allow[..] the public and private sector to trust digital networks' services at national and EU level. By setting incentives to foster*

[1] http://www.retailresearch.org/onlineretailing.php
[2] http://europa.eu/rapid/press-release_IP-12-751_en.htm?locale=en

000028

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

investments, transparency and user awareness, the strategy will boost competitiveness, growth and jobs in the EU."

In other words: **industry needs to be encouraged to provide trust trustworthy services**. They need to be asked to implement up to date technical protection measures. **It is our belief that in this, cryptography plays a key role.**

Is there a role for cryptography?

Cryptography is the essential tool to implement secrecy and integrity for electronic communication. It provides for electronic communication is the equivalent of the letter cover, seal and rubber stamp in the brick and mortar world. Hence, it is essential to protect IT services from criminal activities. However, the use of cryptography might also make law enforcement's investigations on crimes harder. For example, an investigator might have difficulties to intercept the communication of suspects. In such a scenario 'it is only natural' that under clear rules, law enforcement should be able to intercept suspicious communication. (As much as they can search a suspicious flat). However, it turns out that this is easier said than done.

Limited key size

Some legislators have proposed to limit the key size to facilitate law enforcement. This has been introduced under the assumption that these capabilities are used only for legitimate cause, and that criminal or terrorist organizations do not have access to the technology that would be necessary for abuse.

Now, this assumption might have been correct at the time, but technology moved much faster than expected and today, with computing power as a service and a tremendous drop in costs, they do not hold anymore.

Allow me here a short advertisement block: Later today there will be a panel on "Lawful Access and Security: A Transatlantic Perspective" organized by the EastWest Institute where I will comment on the issue of key sizes a bit more in detail.

Key escrow or recovery / back doors

Others proposed key escrow or recovery. Here, neither algorithms nor key sizes are limited. Instead, the investigator gets a (technical or organizational) mechanism provided to get the private key of the suspect. Here, key recovery means being able to reconstruct the key from the encrypted message itself, while key escrow means keeping a securely stored copy of that key. Back doors on the other hand, allow the investigator to intercept the communication without the knowledge of a key.

To my knowledge, ready to use implementations of these schemes do not exist. On the one hand, the deployment of such systems would imply fundamental changes of the telecommunication infrastructure. The design and development of such systems would require the involvement of several fields of expertise, namely cryptography, personal data protection and law enforcement.

My fear would be that such systems increase the complexity of protocols, which would in turn increase the attack surface, which than even might attract criminals; just imagine criminals or terrorist that got access to private keys or a law enforcement backdoor. Moreover, in the brick and mortar world, we do not deposit the key of our front door at the local police station; there is a process to require unlocking doors which only starts after crime investigations have started.

On the other hand, it will be an economic burden to software and service providers in our legislation. Creating an economic disadvantage for our industries, since providers outside of our legislative scope will be able to deliver more secure services at a lower cost.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

But the worst for law enforcement might be my last consideration: anyone who obtains a private key, can perfectly impersonate the legitimate key owner. This might be a risk to the quality of evidence that is gathered by these means.

Bypassing

But let us set aside the considerations above, in the end this all is still a matter of balance.

Society might accept the costs for industry, the risks of abuse, etc. There is a more fundamental problem with the limitation of the use of strong cryptographic tools, namely, criminals can and, by the very nature of criminals, will easily bypass all this rules, and it is hard to detect if they do so.

The research community in the field has a long tradition of creating open access and open source crypto tools; a vast amount of tools is readily free available. Furthermore, the algorithms are publically available and well documented; hence, an average skilled programmer could implement them (and it would be naïve to assume, that criminals are any less intelligent than honest people.)

This leads to the following challenge: without contextual information, such as the deployed algorithm, it is complicated to distinguish a cryptogram from a malformed message that contains only random noise. So a ban on end-to-end encryption would pose the following difficulty for the potential investigator: How to prove that a suspect has used such a forbidden technology?

Moreover, even if the use of cryptography could be easily detected, malicious users have access to a vast body of steganographic protocols, that is to say protocols that allow the user to put a hidden message in a cover media such as a picture. An investigator will usually not have enough information about the potential steganogram to discover its mere existence, let alone to decrypt the content.

To conclude

We need cryptography as the **electronic equivalent** of the **letter cover, the seal or rubber stamp**, and **signature**. These electronic tools are necessary **to protect our assets** in a **highly computerized world**. However, these are **dual-use technologies**. Any advance in cryptography, will cause new problems for crime investigation.

1) Key escrow and recovery is theoretically possible. But, it would need a fundamental change of our communication infrastructure and joint development efforts of many experts.

2) The resulting infrastructure would be more complex, making it more vulnerable to attacks and less resilient to failures. Future advances in cryptology and computing power might turn any law enforcement mechanism into a vulnerability that can be exploited by criminal and terroristic organizations.

3) The economic impact of such mechanisms might be undesirable.

4) For individuals, it would be rather simple to bypass these systems (unnoticeable for law enforcement).

One more thing, all the above mentioned issues are mere examples of currently widely used protection measures; emerging privacy enhancing technologies might introduce even more challenges. To overcome these issues, ENISA is inviting the European Commission as well as Member States and competent EU bodies to increase their efforts in performing further R&D.

Concerning all what was said above, my advice only can be: do not weaken encryption on purpose; do not inhibit the use of tools for data protection and privacy: promote secure IT.
Thank you for your attention.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Lawful Access and Security: A Transatlantic Perspective – EastWest Institute

Statement by Prof. Dr Udo Helmbrecht, ENISA Executive Director

THE HAGUE

19TH- 20TH MAY, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Einstein: "Insanity: doing the same thing over and over again and expecting different results." In this spirit, I would like to reflect on laws that limit the free use of cryptographic tools. Several attempts of such rules were made. The success was at most mixed, the negative impact on the other hand was sometimes huge.

Here, I would like to reflect on one prominent example: the US export regulation for crypto.

The United States Government classified cryptographic algorithms as Auxiliary Military Equipment in the US Munitions List. The use of strong encryption by software developed in the US was only allowed on US soil. Outside of the US, only weak variants of the encryption routines were allowed. As an immediate result, for example, Netscape developed two versions of its web browser. The "U.S. edition" supported full size RSA public keys in combination with full size symmetric keys. (At the time this was 1024bit RSA and 64bit symmetric, today that would be 4096bit and 256bit symmetric). While the "International Edition" had its effective key lengths reduced to 512 bits and 40 bits respectively. Interestingly, this even lowered the protection level in the U.S., since acquiring the 'U.S. domestic' version turned out to be sufficient hassle that most computer users ended up with the 'International' version. A similar situation occurred with Lotus Notes.

Now in a fast moving market like IT, one would expect the ruling has no impact anymore. But surprisingly, although the policy was changed (and mostly abolished) 15 years ago, today it has still an impact on security. Namely, the FREAK[1] and Logjam[2] attacks both have used legacy code that was only included in the systems because of the afore mentioned regulation.

Further, more subtle effects have been observed. In 1999 the U.S. Senate Committee on Commerce, Science, and Transportation collected information on the development of cryptographic products outside of the U.S. It was found that the foreign market was rapidly growing and that the quality of the offered products is at least at par with those from U.S. based companies. The testimony further suggests that U.S. export regulations did in fact damage IT industry.

From these two observations I would conclude: It is the responsibility of the policy makers to pass laws that are just, equitable. The legal framework should have the least impact on peoples' and industries' freedom. Moreover, public policy tends to last for a long time. Computing costs are systematically decreasing, in ever shorter periods. Therefore, attacks that seem out of the reach of any one but a nation state will not remain so for the lifetime of the implementations. As such, policy makers

- Shall refrain from limiting in any way security features in computer software
- Shall refrain from limiting in any way the export of security features in computer software
- Shall consider lifting any and all existing limitations for security features in computer software

Otherwise, history will repeat itself: vulnerabilities that where left from legacy policy will be abused to attack systems. Further, policy that limits the use of cryptography in commercial products will again damage IT industry.

---

[1] "FREAK: Factoring RSA Export Keys," K. Bhargavan et al. [Online]. Available: https://www.smacktls.com/#freak last accessed in May 2016.

[2] "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice" David Adrian et al. [Online]. Available: https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf last accessed in May 2016.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Cookies

This site uses cookies to offer you a better browsing experience. Find out more on how we use cookies and how you can change your settings. (https://www.europol.europa.eu/cookies-policy)

I accept cookies | I refuse cookies

- About Europol (/content/about-europol)
- Media Corner (/content/megamenu/media-corner-1834)
- Partners (/content/megamenu/partners-1835)
- Europol Expertise (/content/megamenu/europol-expertise-1836)
- European Cybercrime Centre (EC3) (/content/megamenu/european-cybercrime-centre-ec3-1837)

Media Corner

- Europol Media Corner (/content/europol-media-corner)
- Press releases (/latest_press_releases)
- News (/latest_news)
- Events (/latest_events)
- Corporate Publications (/content/page/publications)
- Strategic Analysis Reports (/content/page/strategic_analysis_reports)
- Early Warning Notifications (/content/early-warning-notifications/early-warning-notifications)
- Public Access to Europol documents (/content/public-access-europol-documents)
- Crime Prevention Advice (/content/page/crime-prevention-advices-129)
- Image Galleries (/image)
- Europol Youtube Channel (/europol-youtube-channel)
- Corporate identity (/content/page/corporate-identity-191)
- TV, Films and Books (/content/page/tv-films-and-books-196)

Home (/) › Media Corner (/content/media-corner) › Press releases (/latest_press_releases) › Europol in cooperation with EIPA hosts conference on privacy and security online

Share:

(#) (#) (/content/page/rss-feeds-1157) (#) (#) (#)

Print friendly page (https://www.europol.europa.eu/print/content/europol-cooperation-eipa-hosts-conference-privacy-and-security-online)
Print as PDF (https://www.europol.europa.eu/printpdf/content/europol-cooperation-eipa-hosts-conference-privacy-and-security-online)

Europol in cooperation with EIPA hosts conference on privacy and security online

20 May 2016

(https://www.europol.europa.eu/sites/default/files/enisa_europol_2.jpg)

On 19-20 May, Europol in cooperation with the European Institute of Public Administration organised a conference on privacy in the digital age of encryption and anonymity online.

The conference saw participation from different organisations, public and private, such as the European Data Protection Supervisor, the Europol Joint Supervisory Body, the EU Agency for Network and Information Security -ENISA, Eurojust, Amnesty International, the EastWest Institute and many others from a broad range of professional backgrounds, representing private industry, academia, privacy advocates and law enforcement.

In several high-level discussion panels and workshops lively discussions took place on the polarizing challenges around privacy versus security online, and the need to protect citizens' privacy while giving law enforcement the means to investigate crime. There was general consensus that the availability and use of encryption and anonymity technologies is not only important and legitimate in many circumstances but essential to a secure and safe cyberspace.

One of the main themes at the conference was the dichotomy that encryption and anonymity online presents for law enforcement in terms of supporting strong encryption and opposing any technical solution that would weaken security in cyberspace for everyone, and the criminal abuse of these technologies, which seriously impedes on law enforcement's ability to protect citizens from criminal and extremist behaviour, and to bring those responsible to justice.

As highlighted by Europol's Director Mr Wainwright, the challenges for law enforcement are very real and lead to a loss of investigative opportunities as a result of the growing misuse of legitimate anonymity and encryption services and tools for illegal purposes. For law enforcement, therefore, the key aspect is to define the modalities of lawful access, within well-defined and regulated boundaries, while fully respecting fundamental rights.

Echoing the need for well-defined and regulated boundaries, ENISA's Executive Director Mr Helmbrecht advised: "Do not weaken encryption on purpose; do not inhibit the use of tools for data protection and privacy: promote secure IT. Rushed legislation is often inadequate legislation, we need to give time to discuss and invest into R&D"
The event provided a unique opportunity to have an open, inclusive and transparent debate among different viewholders towards finding a way to strike the right balance between freedom and security online.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

At the end of the conference, Mr Helmbrecht and Mr Wainwright issued a joint statement describing the challenges and proposing possible avenues of solutions for lawful criminal investigations that respect 21st century data protection. (https://www.europol.europa.eu/content/lawful-criminal-investigation-respects-21st-century-data-protection-europol-and-enisa-joint-)

Europol is the EU's law enforcement agency, assisting national authorities by exchanging information, intelligence analyses and threats assessments. The agency deals with terrorism and international crime such as cybercrime, drug smuggling and people trafficking. Europol, which has over 1 000 staff members, has its headquarters in The Hague in the Netherlands.

ENISA is a centre of expertise for cyber security in Europe. ENISA's mission is to contribute to securing Europe's information society by raising "awareness of network and information security and to develop and promote a culture, of network and information security in society for the benefit of citizens, consumers, enterprises and public sector organizations in the Union.

For interviews and further information regarding Europol's or ENISA's activities, please contact:
press@europol.europa.eu (mailto:press@europol.europa.eu)
press@enisa.europa.eu (mailto:press@enisa.europa.eu) , Tel. +30 2814409576

Tags: Conferences (/category/press-release-category/conferences) Europol (/category/press-release-category/europol)

© 2016 Europol. All Rights Reserved. | Disclaimer & Privacy (/content/page/glossary-disclaimers-163)

Popular Topics:
Press Releases (/latest_press_releases)
News (/latest_news)
Recruitment & Internships (/content/page/recruitment-internships-25)
Public Access to Europol documents (/content/public-access-europol-documents)
Procurement (/content/procurement)
Operations Overview (/operations_overview)
Joint Investigation Teams (JITs) (/content/page/joint-investigation-teams-989)
European Cybercrime Centre (/ec3)

Contact:
Telephone: + 31 70 302 5000
Fax: + 31 70 345 5896

For more information, general enquiries and details about visiting Europol please refer to our Contact us (/content/contact-us) section.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

(Discussion Item) (Item Sponsor -

Talking Points

[redacted]

(Justice Canada)

- **I wish to thank** [redacted] **for the conference document**
- [redacted]

s.14(a)
s.21(1)(b)
s.23

Author: Gareth Sansom Phone: 613-424-5300 Date: June 1, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

(Discussion Item) (Item Sponsor -

- [redacted]
- [redacted]
- [redacted]

s.14(a)
s.21(1)(a)

Author: Gareth Sansom Phone: 613-424-5300 Date: June 1, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

SERVING CANADIANS
AU SERVICE DES CANADIENS

MEETING OF FPT DEPUTY MINISTERS RESPONSIBLE FOR JUSTICE AND PUBLIC SAFETY
June 1-3, 2016

The Westin Wall Centre, Vancouver Airport
Richmond, British Columbia

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.14(a)

3:35 p.m. – 4:55 p.m.	[redacted] 13. [redacted] 14. Provide Legislative Solution to [redacted] (15 min) 15. [redacted] Supreme Court of Canada Decision in R.v.Spencer (Justice Canada & [redacted] (20 min)
4:55 p.m. – 5:20 p.m.	Deputy Ministers' Review of Decision Items
6:00 p.m. – 9:00 p.m.	Dinner for all Delegates *(Gulf of Georgia Cannery, 12138 Fourth Avenue)* Co-hosted by the British Columbia Ministry of Justice, Justice Canada and Public Safety Canada • Transportation will be provided

Friday, June 3, 2016

8:00 a.m. – 9:00 a.m.	Breakfast for all Delegates *(Steveston Room)* Co-hosted by Justice Canada and Public Safety Canada

B – Current and Emerging Issues

9:00 a.m. – 9:25 a.m.	16. [redacted] (Justice Canada & Public Safety) (25 min)
9:25 a.m. – 9:45 a.m.	17. [redacted] (20 min)
9:45 a.m. – 10:15 a.m.	18. [redacted] Budget 2016 [redacted] Justice Canada) (30 min)
10:15 a.m. – 10:30 a.m.	19. Private Members' Business – Report and Recommendations from the Working Group (British Columbia & Justice Canada) (15 min)
10:30 a.m. – 10:45 a.m.	Health Break *(Airport Ballroom Foyer)*

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

LEGISLATIVE SOLUTION TO [redacted]

Sponsoring Jurisdiction: [redacted]

[redacted]

Both Justice Canada and Public Safety Canada have an interest in this issue.

s.14(a)
s.21(1)(a)
s.21(1)(b)

EXPECTED DECISION OUTCOMES:

Federal/Provincial/Territorial (FPT) Deputy Ministers (DMs) acknowledged the challenges currently faced by law enforcement and national security agencies with regards to [redacted] They also acknowledged the tremendous benefit [redacted] brings to Canadians and Canada. DMs agreed that it would be beneficial to explore the issues and challenges together and [redacted]

STRATEGIC ADVICE

It is recommended that you:

- acknowledge the challenge that [redacted] poses for law enforcement and national security agencies while also acknowledging the tremendous benefit it brings to Canadians and their human rights, e-commerce, e-banking, cyber security;

[redacted]

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

BACKGROUND

Data encryption is the conversion of electronic data into another form, often called ciphertext, which can only be accessed and understood by authorized parties with the correct key (decryption key). Encryption can be applied to more specific items such as a message itself (i.e. email, text, or photo), the device (i.e. the cell phone, the computer, the tablet), or the transmission network and/or channel (i.e. the communication service provider network).

In recent years, encryption technologies have proliferated in both availability and use. This is mainly a result of the increased development of multiple commercially available software and hardware encryption technologies and a post-Snowden world, where Western society is wary of perceived state surveillance and is seeking to keep telecommunications opaque to outside observation. Many devices and communications services (e.g. webmail) are equipped with powerful default encryption settings. Encryption technologies play a vital role in protecting Canadians, e-commerce, e-banking and cybersecurity.

As with the proliferation of any technology, criminals now use data encryption methods on mobile devices which make it largely unreadable to a third-party who does not possess the "decryption keys" necessary to unlock the encryption and leave no trace or attribution. This is a challenge to law enforcement and national security agencies because, even when successful and lawful interception of communications on a network occurs, they often run into data encryption issues that are challenging or impossible to bypass. Encryption challenges also apply to the court-ordered production of historical data, such as e-mails, text messages, photos and videos from lawfully seized smartphones, computer hard drives and other digital devices. Data from these devices and modes of communication may have layers of encryption that make them unreadable.

Ultimately, the challenges relating to encryption are difficult to address and no other country is known to have succeeded in developing a complete solution given the necessity of encryption.

[redacted] s.21(1)

Although encryption can pose a significant challenge to law enforcement, this issue has not been directly addressed in Canadian law, except through export controls of designated technology to specified countries through the Wassenaar Agreement[1]. It is important to note that no other

[1] Canada is one of 33 signatories to the Wassenaar Arrangement which was established to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies (such as encryption software). Participating states seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities. The aim is also to prevent the acquisition of these items by terrorists.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.13(1)(c)
s.14(a)
s.21(1)(b)

country has fully addressed the challenge of encryption for a number of reasons, including but not limited to: human rights (freedom of expression and privacy); jurisdictional challenges (the borderless nature of the digital world); and the essential need for encryption to enable modern e-commerce, e-banking, and all types of cybersecurity.

In the past, legislative proposals have been introduced in the Parliament of Canada but have been unsuccessful. The aim of these proposals was to create requirements for telecommunications service providers to decrypt communications where it was readily possible for the service provider to do so, in the context of lawful interception. These proposals were valuable for law enforcement and national security agencies, but did not solve the problem posed by encryption in whole, nor did they purport to do so.

[redacted]

It should be noted that the Commissioner of the Royal Canadian Mounted Police (RCMP) has spoken publicly about encryption in the context of "going dark". [redacted]

PROVINCIAL/TERRITORIAL CONSIDERATIONS

[redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.14(a)
s.21(1)(a)

CURRENT STATUS/NEXT STEPS

[redacted]

Pages 45 to / à 62

are withheld pursuant to section

sont retenues en vertu de l'article

13(1)(c)

of the Access to Information Act

de la Loi sur l'accès à l'information

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

CBC Investigates

RCMP's BlackBerry-cracking methods could be revealed in Quebec court

Judge to decide if public gets to learn more about methods used to access Montreal mobsters' phones

By Dave Seglins, Matthew Braga and Jeremy McDonald, CBC News Posted: Jun 10, 2016 5:00 AM ET
Last Updated: Jun 10, 2016 5:00 AM ET

A Quebec court could today pull back the curtain on secretive police techniques, including how the RCMP intercepted BlackBerry text messages to prove a murder conspiracy plot, as a judge considers whether to lift a publication ban in a case involving the Montreal Mafia.

The case stems from Project Clemenza, a police operation that resulted in scores of organized crime arrests in 2014. At the time, police announced they had intercepted more than one million BlackBerry messages tied to allegations of drug trafficking, kidnapping, arson, weapons and other violent offences.

- **BlackBerry hands over user data to help police around the world 'kick ass'**
- **BlackBerry CEO tries to reassure users on encryption questions**

That information led to the arrests of seven accused mobsters in the shooting death of Salvatore (Sal the Ironworker) Montagna, a high-ranking member of a New York crime family killed outside Montreal in 2011. Six of the suspects pleaded guilty to conspiracy to murder last March, while the seventh pleaded guilty to a lesser charge of being an accessory after the fact.

But the prosecution asked for — and was granted — a publication ban on many details around how the RCMP intercepted the mobile phones and descrambled the BlackBerry messages.

Chief Supt. Jeff Adam, who oversees the RCMP's Technical Investigations Services, declined to discuss with CBC News the specific methods used.

But given rapid changes in technology and public concern in the post-Snowden era, as mobile developers move toward more secure "end-to-end" encryption, he says investigators are finding their jobs increasingly difficult.

"What we're seeing now is ... the best evidence of people conspiring to commit a crime is lost to us. And that's what we call 'going dark,'" Adam said.

Busting BlackBerry encryption

The RCMP's technical investigations lab in Ottawa has developed a reputation for its ability to crack BlackBerry devices — a company that has built its brand on the strength of its security.

There have been questions whether the RCMP has obtained Blackberry's global encryption key to enable easy access to encoded communications.

In April 2016, authorities in England credited the Mounties with recovering encrypted emails and texts from BlackBerry phones to help convict two men of smuggling dozens of high-powered machine guns into the U.K.

How they did it is unclear. But court records from another case suggest one possibility.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

For years, police forensic experts have been able to physically open devices, accessing their internal memory chips. The highly specialized procedure, dubbed "chip-off," involves using heat guns to remove sealed components inside a phone in a bid to thwart passwords and encryption.

The RCMP used this chip-off technique to retrieve BBM messages — even ones that had been deleted — to help convict two men in the 2011 murder of a popular Toronto-area real estate agent.

The Mounties also relied on software made by Cellebrite, a leader in digital forensics that specializes in retrieving hard-to-access data from a wide range of devices and apps, including BlackBerrys and iPhones.

Additionally, the RCMP has found ways around BlackBerrys customized to use PGP — a form of encryption known as "Pretty Good Privacy" — giving investigators access to emails and texts in a number of Canadian cases, including a Vancouver kidnapping plot and a cocaine and pot trafficking case in Thunder Bay, Ont.

"This encryption was previously thought to be undefeatable. The RCMP technological laboratory destroyed this illusion," a Thunder Bay judge remarked in that case.

It is unlikely that the RCMP cracked PGP itself, generally considered secure by cryptographers. Rather, they may have exploited a weakness in either the software or device to get around PGP.

'It's a battle'

Daniel Tobok, of Cytelligence, is a cybersecurity and data forensics specialist who used to work with Telus. He says techniques such as chip-off only work on older phones and law enforcement agencies are constantly in a "cat-and-mouse" race with tech-savvy criminals.

"Technology is advancing very quickly and new encryption methods are coming out. And the bad guys are starting to use them," Tobok said. "[Police] don't have budgets, they don't always have the right people ... We are seeing a trend where law enforcement and the government sector are being shut out in the new evolution in encryption world, absolutely. It's a battle."

- **Apple's privacy fight with the FBI explained**
- **Tim Bosma case shows Apple doesn't always say no to police**

Despite talk of investigations "going dark," criminal defence lawyer Alan Gold believes police are better equipped to fight crime than they'll publicly admit.

"I think we see the tip of the iceberg because police, by nature, are secretive about their capabilities," Gold said.

What has changed, he said, is despite the rise of encrypted communications and devices, our reliance on technology has created a motherlode of potential evidence for police to target.

"What people don't appreciate [is] that they are essentially living in this giant visible sphere of digital information. And it's there forever."

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Kimberley Pearce - [redacted]

s.23

From: Kimberley Pearce
To: Morris, Jeffrey
Date: 2016/06/14 4:44 PM
Subject: [redacted]
CC: Lynam, Chris

Hi Jeff,

[redacted]

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Hope this helps,
Kim s.23

>>> Jeffrey Morris 2016/06/14 3:30 PM >>>
Kim,

[redacted]

With thanks,
Jeff

Chris, please see attached for your review too (in advance of tomorrow's meeting if possible).

>>> Kimberley Pearce 2016/06/13 3:24 PM >>>
Hi Jeff,

[redacted]

Kim

>>> Jeffrey Morris 2016/06/13 2:56 PM >>>
Thanks Kim, very helpful.

[redacted]

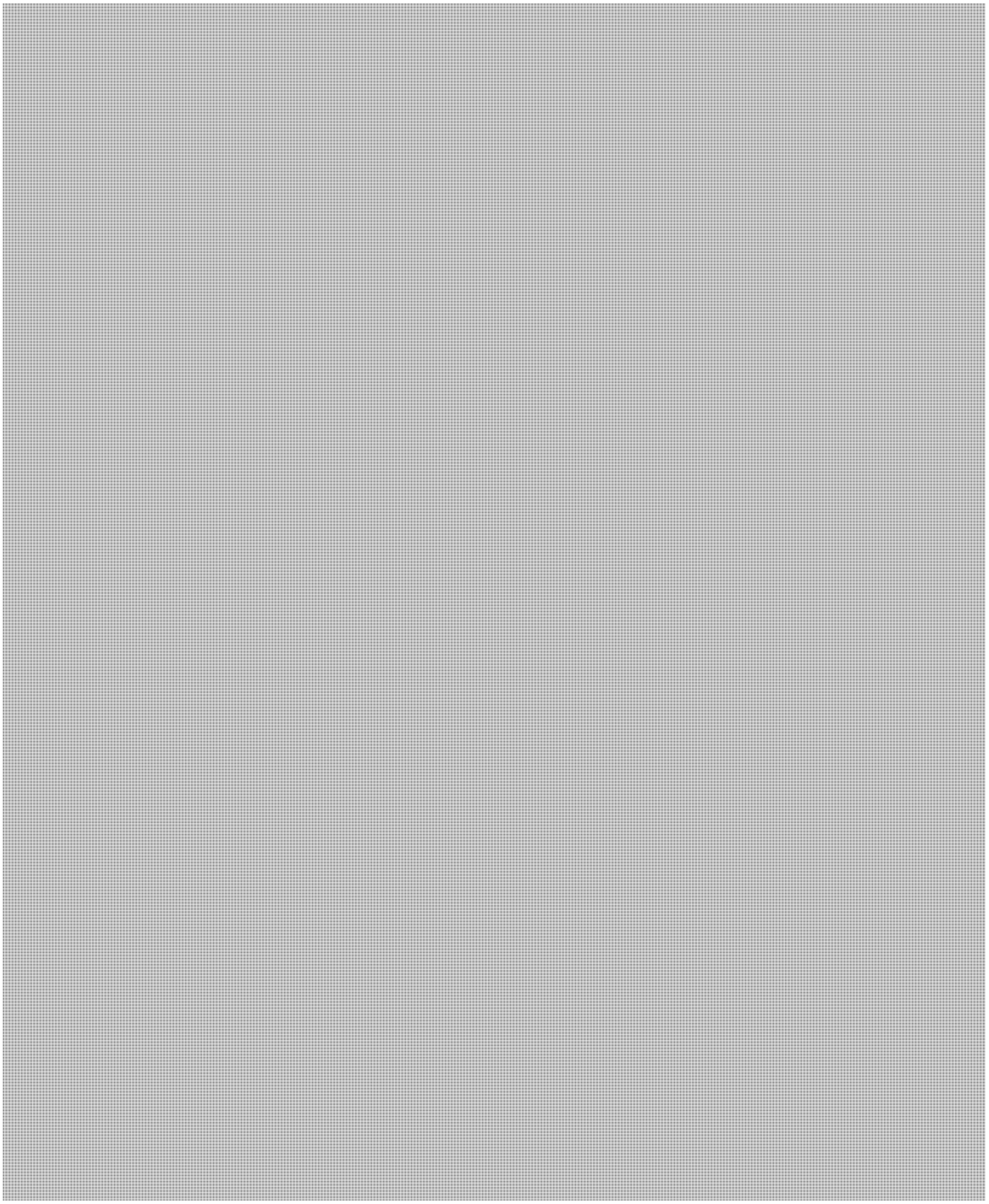
Jeff

>>> Kimberley Pearce 2016/06/13 1:20 PM >>>
Hi Jeff,

[redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.23



Please let me know if you have any questions,

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Kim Pearce
Counsel / Avocate
Legal Services - RCMP / Services Juridiques - GRC
73 Leikin Drive, Mail Stop #69
Building M8, 2nd Floor, Room 831
Ottawa, ON K1A 0R2
Tel: 613-843-4478
Fax: 613-825-1241
Kimberley.Pearce@rcmp-grc.gc.ca

s.23

>>> Jeffrey Morris 2016/06/10 1:07 PM >>>
Hello all,

[redacted]

With thanks,
Jeff

Jeffrey Morris,
Policy Analyst / Analyste des politiques
Directorate of Strategic Policy and Integration, Specialized Policing Services /
Direction des politiques stratégiques et d'intégration, Services de police spécialisés
Tel / Tél: 613-843-6621
Email / Courriel: jeffrey.morris@rcmp-grc.gc.ca
73 Leikin Drive / 73, promenade Leikin
M8-3-821-55, Ottawa, Ontario, K1A 0R2

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Kimberley Pearce - Fw: CACP 2016 Resolution: Reasonable Law to Address the Impact ofEncrypted and Password-Protected Electronic Devices

From: Jeffrey Morris <jeffrey.morris@rcmp-grc.gc.ca>
To: Mark.Scrivens@rcmp-grc.gc.ca, Cheryl.Tremblay@rcmp-grc.gc.ca, tomasz.pac...
Date: 2016/07/21 6:33 PM
Subject: Fw: CACP 2016 Resolution: Reasonable Law to Address the Impact ofEncrypted and Password-Protected Electronic Devices
Attachments: CACP - 2016 Annual Conference - Position NoteTemplate R.docx; Resolution Law to address the impact ofencrypted and pa.docx; CACP Resolution Encryption and PasswordProtection Law .docx

FYI at this time. SPS SPI will coordinate next week.

Jeff

Sent from my BlackBerry 10 smartphone on the Rogers network.

From: Joe Oliver <Joe.Oliver@rcmp-grc.gc.ca>
Sent: Thursday, July 21, 2016 4:39 PM
To: Jeffrey Morris
Cc: Kevin Brosseau; Chris Lynam; Jeff Adam; Maury Medjuck
Subject: Fwd: CACP 2016 Resolution: Reasonable Law to Address the Impact of Encrypted and Password-Protected Electronic Devices

Hi Jeff - Could you please work with FP & TIS to prepare a draft RCMP position note on this encryption resolution. I am attaching the full resolution which includes background, action plan and media lines. Thanks in advance, Joe

>>> ES&ML-EBS 2016/07/21 1:29 PM >>>
Good afternoon,

As you may be aware, at the 2016 CACP Annual Conference, the Law Amendments Committee will put forward a resolution for a Reasonable Law to Address the Impact of Encrypted and Password Protected Electronic Devices (please see proposed resolution attached).

Could you please fill out the attached template, indicating strategic considerations from the RCMP's perspective (i.e., implications for the RCMP), as well as RCMP's position on the proposed resolution)

Please send the completed template by **COB Friday, July 29, 2016**.

If you have any questions, please contact Philip McLinton at 613-843-3853.

-Executive Briefing Services

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Canadian Association of Chiefs of Police – 2016 Annual Conference
Proposed Resolution

Proposal

- The Law Amendments Committee will put forward a resolution for a Reasonable Law to Address the Impact of Encrypted and Password-Protected Electronic Devices.

Current Status

- ...
- ...
- ...

Strategic Considerations

- *[State considerations from RCMP's perspective]*

Recommended Approach

- *[State RCMP's position on this resolution]*

Key Messages

- ...
- ...
- ...

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Resolution # - 2016

REASONABLE LAW TO ADDRESS THE IMPACT OF ENCRYPTED AND PASSWORD-PROTECTED ELECTRONIC DEVICES

Submitted by the Law Amendments Committee

WHEREAS electronic devices are ubiquitous in both the licit and illicit facets of modern society, and;

WHEREAS electronic devices can be and are used to facilitate the commission of serious and multi-jurisdictional crime, such as organized crime, violent crime, fraud and other financially-motivated crime, and Internet and computer-related crime, and;

WHEREAS Internet and computer-related crime is a growing area of criminal activity that threatens Canadians' privacy and security interests, and Canada's financial systems, and;

WHEREAS the contents of electronic devices can yield critical evidence of such crimes, and;

WHEREAS users of electronic devices have ready access to encryption and password-protection that renders the contents inaccessible to public safety agencies and, not withstanding a valid judicial authorization to search those contents, and;

WHEREAS the inability to execute judicially authorized searches of electronic devices has and will bring serious criminal, and national security investigations to abrupt and unsuccessful ends, and;

WHEREAS there is no legislative power specifically designed to compel an individual to provide either law enforcement or public safety agencies with the password or encryption key for an electronic device, the search of which has been judicially authorized;

WHEREAS other jurisdictions have afforded law enforcement agencies with such legislative powers, and have achieved success in defending that legislation and in furthering legitimate law enforcement interests, and;

WHEREAS this is a possible solution being requested, and;

WHEREAS the Canadian Association of Chiefs of Police, as the national voice of Canadian police leadership, is committed to raising issues where the Criminal Code should be amended.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police urges the Government of Canada, for the purpose of community safety, to identify a legislative means for public safety agencies inclusive of law enforcement, through

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

judicial authorization, to compel the holder of an encryption key or password to reveal it to law enforcement.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

REASONABLE LAW TO ADDRESS THE IMPACT OF ENCRYPTED AND PASSWORD-PROTECTED ELECTRONIC DEVICES

Submitted by the Law Amendments Committee

WHEREAS electronic devices are ubiquitous in both the licit and illicit facets of modern society, and;

WHEREAS electronic devices can be and are used to facilitate the commission of serious and multi-jurisdictional crime, such as organized crime, violent crime, fraud and other financially-motivated crime, and Internet and computer-related crime, and;

WHEREAS Internet and computer-related crime is a growing area of criminal activity that threatens Canadians' privacy and security interests, and Canada's financial systems, and;

WHEREAS the contents of electronic devices can yield critical evidence of such crimes, and;

WHEREAS users of electronic devices have ready access to encryption and password-protection that renders the contents inaccessible to public safety agencies and, not withstanding a valid judicial authorization to search those contents, and;

WHEREAS the inability to execute judicially authorized searches of electronic devices has and will bring serious criminal, and national security investigations to abrupt and unsuccessful ends, and;

WHEREAS there is no legislative power specifically designed to compel an individual to provide either law enforcement or public safety agencies with the password or encryption key for an electronic device, the search of which has been judicially authorized;

WHEREAS other jurisdictions have afforded law enforcement agencies with such legislative powers, and have achieved success in defending that legislation and in furthering legitimate law enforcement interests, and;

WHEREAS this is a possible solution being requested, and;

WHEREAS the Canadian Association of Chiefs of Police, as the national voice of Canadian police leadership, is committed to raising issues where the Criminal Code should be amended.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police urges the Government of Canada, for the purpose of community safety, to identify a legislative means for public safety agencies inclusive of law enforcement, through judicial authorization, to compel the holder of an encryption key or password to reveal it to law enforcement.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

REASONABLE LAW TO ADDRESS THE IMPACT OF ENCRYPTED AND PASS-WORD PROTECTED ELECTRONIC DEVICES

Background

James B. Comey, Director of the Federal Bureau of Investigation, described the U.S. experience with encrypted and password-protected electronic devices as follows: "Armed with lawful authority, we increasingly find ourselves simply unable to do that which the courts have authorized us to do, and that is to collect information being transmitted by terrorists, by criminals, by pedophiles, by bad people of all sorts." In response, the National District Attorneys Association and the International Association of Chiefs of Police are supporting legislation, a discussion draft of which was released on April 13, 2016, that would compel companies to provide "technical assistance" to law enforcement in respect of encrypted and password-protected data.

Canadian law enforcement faces the same investigative challenges and requires an analogous legislative response. However, legislation directed at companies, many of which will be located outside of Canada, may not suffice. Law enforcement requires reasonable, constitutionally-compliant legislation crafted to suit the Canadian context.

Digital security technology has now advanced to the point that impenetrable password protection and encryption are readily – and in many cases *freely* – available on all electronic devices. This technology immunizes legally seized electronic devices from the execution of a judicially-authorized search, and often compels the abrupt and unsuccessful end of a serious criminal investigation. Recent law enforcement experience provides specific examples of criminal investigations that have been derailed in this manner.

While the issue potentially bears on a wide range of investigations, it will have particular ramifications for the investigation of online child sexual exploitation and abuse, fraud and other financially-motivated crimes, organized crime, requests for international law enforcement assistance, and national security matters involving suspected extremism and other threats to Canada.

Furthermore, technical advancements in techniques to crack password-protected devices alone will not suffice in the case of newer devices with operating systems that erase data (wiping clean) after a limited number of unsuccessful password attempts.

While there are numerous benefits that encryption provides to assure privacy and to cyber security such as e-commerce, it is contrary to the public interest to permit criminals or those that threaten the security of Canadians to create a zone of immunity by encrypting and password-protecting their data, and to thereby limit the reach of validly-issued judicial authorizations. In contrast, a reasonable and proportional law that would permit law enforcement to access encrypted and password-protected data, in appropriate cases, through the application for and granting of a judicial authorization, would promote the safety of

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Canadian children on the Internet, enhance the integrity of Canadian financial system, improve national security, and assist in the investigation and prosecution of organized and violent criminals. It must be emphasized that Canadian law enforcement agencies have identified this public safety gap and are seeking a legislated process where a judicially authorized format may compel the production of a password or encryption key. It is recognized the use of this privacy-intrusive legislated framework would need to be balanced on a concept of proportionality.

In January 2015, in his address to the Annual Symposium of the Canadian Association for Security and Intelligence Studies, when describing challenges of the basic problem for law enforcement to acquire information, RCMP Commissioner Paulson stated: "We also, and perhaps more urgently, need new tools, to be able to enforce the criminal law quickly and efficiently, in a way consistent with Canadian values and the Charter of Rights and Freedoms".

Recent Law Enforcement Experiences

Several recent examples from the United States and Canada highlight the gravity of this problem:

- In 2010-2011, the Ontario Provincial Police investigated a male for setting up hidden cameras in his house to spy on a young woman who worked for his wife. Police obtained a warrant to search the house and found an encrypted hard drive hidden in the rafters of the basement. E-Crimes could not break the encryption. Police ultimately discovered documents and books containing the suspect's computer information, and entered a series of possible passwords until one of them opened the hard drive. Thousands of voyeuristic images were obtained from the device. The investigating officer explained that the investigation would have failed if the suspect not written down the password in those documents.

- In 2012, police lawfully seized computers from Justin Gryba in Saskatoon in relation to a child pornography investigation. Some of the computers had been locked and encrypted. Mr. Gryba refused to provide the passwords. Forensic technicians from Saskatoon and Ottawa were not able to break the encryption on one device until two-and-a-half years later. That device contained child pornography depicting many different victims. Mr. Gryba was charged with making and possessing child pornography and, on April 15, 2016, sentenced to serve a further two years less a day in custody (on top of 29 months' credit).

- In May 2013, the Ontario Provincial Police received information that an individual had child pornography on his Apple iPad and potentially on his Apple Macbook Pro laptop. A warrant was executed at the individual's residence and the devices were seized. The items were submitted to OPP E-Crimes for examination and retrieval of any images. Both items were password-protected. E-Crimes did not have the capabilities to gain access without the password. The investigating officer was unable to obtain Production and Assistance Orders for Apple in California, and would have been unwilling to send

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

the devices to California given their probable illegal content. The officer also could not obtain a destruction order, and was forced to make arrangements to return the devices to the suspect. Conditions of return were negotiated: the suspect would provide the password for the purpose of wiping the devices before their return, and no charges would be laid.

- Between October 2014 and June 2015, law enforcement in Manhattan, New York, seized 74 Apple iPhones related to investigations into offences such as the attempted murder of three individuals, the repeated sexual abuse of a child, an ongoing sex trafficking ring, and numerous assaults and robberies. Warrants to search the devices were obtained, but could not be executed.

- In Fort Frances, Ontario, there was a recent case of theft of narcotics from a hospital. A phone was seized and forwarded to the Ontario Provincial Police Technological Crime Unit ("E-Crimes"), which was unable to unlock it. The investigation has stalled, though OPP E-Crimes suggested they "might" be able to use a software new program to unlock the phone in 8-12 months.

- In June 2015, a father of six was shot dead in Evanston, Illinois, 10 miles north of Chicago. There were neither witnesses nor surveillance footage. Investigators found an Apple iPhone and a Samsung phone running on Google's Android operating system next to the body of the deceased. Both devices were password-protected. An Illinois state judge issued a warrant ordering Apple and Google to unlock the phones and share with authorities any data that could potentially solve the murder. Apple and Google replied that they could not do so without knowing the user's passcode. The murder remains unsolved.

Potential solutions: other jurisdictions' experiences

Canadian law enforcement may have the ability to compel the production of biometrics through an impression warrant (s. 487.092) or a general warrant (s. 487.01), but not the production of passwords or encryption keys. Several other jurisdictions have explored or implemented legislation to the permit the latter:

- The United Kingdom's *Regulation of Investigatory Powers Act 2000* empowers the court to order a person to supply decrypted information and/or encryption keys. The legislation has been unsuccessfully challenged on self-incrimination grounds.

- Australia's *Cybercrime Act 2001* provides authorization for a magistrate to order a specified person, including a suspect or an accused person, to provide any information or assistance that is reasonable and necessary to allow law enforcement to access, copy, and convert electronic data, with a penalty for non-compliance.

- Key production legislation is in force in South Africa (*Regulation of Interception of Communications and Provision of Communication-Related Information Act*), France (*Loi sur la sécurité quotidienne*), and Finland (*The Coercive Measures Act (Pakkokeinolaki)).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Sweden has recently proposed encryption key production legislation.

- New Zealand Customs released a Discussion Paper in 2015 proposing new powers in the *Customs and Excise Act* to demand passwords from persons crossing the border.

- The United States has yet to fully embrace key production, but there have been instances of judges subpoenaing accused individuals to provide their passwords to law enforcement. U.S. Courts have yet to fully resolve whether compelled key production or compelled production of an unencrypted copy of encrypted data violates the privilege against self-incrimination protected by the Constitution's Fifth Amendment.

  However, on April 13, 2016, U.S. Senate Intelligence Committee Chairman Richard Burr and Senator Dianne Feinstein, released a discussion draft of proposed legislation ("Compliance with Court Orders Act of 2016") that would address encrypted and password-protected electronic devices by directing the relevant company to decrypt data or provide other technical assistance to law enforcement. Their proposal is supported by the National District Attorneys Association and the International Association of Chiefs of Police.

Further review of the legislation in the United Kingdom:

The legislation in the United Kingdom was further examined because of its well-established encryption key/password production legislation and our shared legal and constitutional principles. A summary of data from the Office of Surveillance Commissioners ("OSC") Annual Reports provided further insight about the efficacy of that legislation. The OSC is a public body sponsored by the Home Office that oversees the conduct of covert surveillance and covert human intelligence sources by public authorities in accordance with the Regulation of Investigatory Powers Act 2000 ("RIPA").

Section 49 of the RIPA, activated by ministerial order in October 2007, requires persons to supply decrypted information and/or encryption keys to state representatives upon receipt of a court order. In practice, an application involves the following steps:

- The Home Office National Technical Assistance Centre ("NTAC") must approve the application for the service of an s. 49 notice.
- Once NTAC approval is in place, permission may be sought from a Judge.
- Once judicial permission is given, the s. 49 notice should be served.
- If a person fails to comply with the s. 49 notice, a criminal charge may be laid.

The OSC has reported annually on the use of s. 49 since its 2008-2009 Annual Report. The most recent Report is for 2014-2015. The available data from 2008 – 2015 suggests the following:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- 160 notices were issued under s. 49 of *Regulation of Investigatory Powers Act:*
    - The investigations consistently involve terrorism, domestic extremism, indecent images of children, insider dealing, fraud, evasion of excise duty and drugs.
    - Investigations into human trafficking and kidnapping of children seem to be an emerging issue.
- Between 38 and 42 individuals (~24% to ~26%) complied with the notice;[1]
- 93 individuals (~58%) did not to comply with the notice;[2]
- 68 of those individuals were charged;
- 46 of those individuals were prosecuted; and
- 14 prosecutions resulted in convictions.

[1] The 2008-2009 Report does not set out the number of notices complied with or still pending. Since the Report provides that 15 notices were issued and that 11 notices were not complied with, this estimate was generated using the minimum (0) and maximum (4) number of individuals who could have complied.

[2] This percentage does not account for notices that are still pending. Year-to-year percentages for non-compliance have questionable explanatory value, given the overlap in data across reporting years. To the extent that they are useful as a benchmark, they are as follows:

- 2008-2009 (~73%);
- 2009-2010 (~41%);
- 2010-2011 (~17%);
- 2011-2012 (~75%);
- 2012-2013 (~73%);
- 2013-2014 (~52%);
- 2014-2015 (~59%).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Action Plan

1. That the Law Amendments Committee of the Canadian Association of Chiefs of Police consult with Justice Canada and other stakeholders regarding this public safety issue.

2. That the Law Amendments Committee of the Canadian Association of Chiefs of Police continue ongoing consultation with the Federal/Provincial/Territorial Criminal Procedure Committee.

3. That the Law Amendments Committee of the Canadian Association of Chiefs of Police continue ongoing consultation with CACP Cybercrime Committee.

4. That the Executive Director of the Canadian Association of Chiefs of Police forward correspondence to the Public Safety Minister of Canada; the Minister of Justice and Attorney General of Canada; and the Minister of Transportation of Canada, petitioning for legislation requiring persons to be judicially ordered to supply passwords or encryption keys or face legal sanctions.

5. That the Law Amendments Committee of the Canadian Association of Chiefs of Police accompany the President of the CACP to meetings with the Minister of Public Safety and with the Minister of Justice and Attorney General to further discuss this technological and legal challenge in keeping Canadians safe.

6. That the Canadian Association of Chiefs of Police develop a comprehensive media plan to further educate Canadians to the public safety need for this encryption legislation to help reduce the risk to Canadians from those that use encryption for criminal or extremist activities.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Media Lines

Canadian law enforcement recognizes the importance of cyber security for all Canadians. Encryption is obviously a complex issue with various considerations and legitimate uses such as e-commerce, protection of privacy, transmission of data, etc. Police services are also users of data encryption for secure communications and data storage.

Electronic devices can be and are used to facilitate the commission of serious and multi-jurisdictional crime, electronic devices can be and are used to facilitate the commission of serious and multi-jurisdictional crime, such as organized crime, violent crime, fraud and other financially-motivated crime, and Internet and computer-related crime, and;

Internet and computer-related crime is a growing area of criminal activity that threatens Canadians' privacy and security interests, and Canada's financial systems. The contents of electronic devices can yield critical evidence of such crimes, and users of electronic devices have ready access to encryption and password-protection that renders the contents inaccessible to law enforcement, not withstanding a valid judicial authorization to search those contents.

The inability of law enforcement personnel to execute judicially authorized searches of electronic devices has and will bring serious criminal investigations to abrupt and unsuccessful ends.

There is no legislative power in Canada specifically designed to compel an individual to provide law enforcement with the password or encryption key for an electronic device, the search of which has been judicially authorized.

Other jurisdictions in the world have afforded law enforcement agencies with such legislative powers, with judicial oversight, and have achieved success in defending that legislation and in furthering legitimate law enforcement interests.

Canadian law enforcement is seeking a legislated process whereby a court could grant an order to compel the production of a password or encryption key for an electronic device where, on reasonable and probable grounds, a crime has been or is being committed.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Kimberley Pearce - [redacted]

From: Jeffrey Morris
To: Alter, Susan
Date: 2016/07/28 11:45 AM
Subject: [redacted]
CC: Pearce, Kimberley
Attachments: EBinder - FPT Justice & Public Safety - June 2016_2_3.pdf

s.23

Hello Susan,

[redacted]

Jeff

Jeffrey Morris,
Policy Analyst / Analyste des politiques
Directorate of Strategic Policy and Integration, Specialized Policing Services /
Direction des politiques stratégiques et d'intégration, Services de police spécialisés
Tel / Tél: 613-843-6621
Email / Courriel: jeffrey.morris@rcmp-grc.gc.ca
73 Leikin Drive / 73, promenade Leikin
M8-3-821-55, Ottawa, Ontario, K1A 0R2
>>> Susan Alter 2016/07/28 11:35 AM >>>
Hello Jeff,

[redacted]

Susan

Susan Alter, Senior Counsel /

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Avocate-conseil
RCMP Legal Services /
Services juridiques GRC
Department of Justice /
Ministère de la Justice
Ottawa, Canada K1A 0R2
susan.alter@rcmp-grc.gc.ca
Telephone /Téléphone 613-843-4490
Facsimile /Télécopieur 613-825-1241
Government of Canada / Gouvernement du Canada

s.23

>>> On 2016/07/27 at 9:49 AM, in message <5798BBE5.FE0 : 187 : 49978>, Jeffrey Morris wrote:

> Hello Susan,
>
> [redacted]
>
> Any questions, please let me know.
>
> Best regards,
> Jeff
>
> Jeffrey Morris,
> Policy Analyst / Analyste des politiques
> Directorate of Strategic Policy and Integration, Specialized Policing Services /
> Direction des politiques stratégiques et d'intégration, Services de police spécialisés
> Tel / Tél: 613-843-6621
> Email / Courriel: jeffrey.morris@rcmp-grc.gc.ca
> 73 Leikin Drive / 73, promenade Leikin
> M8-3-821-55, Ottawa, Ontario, K1A 0R2

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.23

Kimberley Pearce ·

From: Susan Alter
To: Morris, Jeffrey
Date: 2016/07/28 11:35 AM
Subject:
CC: Pearce, Kimberley
Attachments:

Hello Jeff,

Susan

Susan Alter, Senior Counsel /
Avocate-conseil
RCMP Legal Services /
Services juridiques GRC
Department of Justice /
Ministère de la Justice
Ottawa, Canada K1A 0R2
susan.alter@rcmp-grc.gc.ca
Telephone /Téléphone 613-843-4490
Facsimile /Télécopieur 613-825-1241
Government of Canada / Gouvernement du Canada

>>> On 2016/07/27 at 9:49 AM, in message <5798BBE5.FE0 : 187 : 49978>, Jeffrey Morris wrote:

> Hello Susan,
>
> Any questions, please let me know.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Best regards,
Jeff

Jeffrey Morris,
Policy Analyst / Analyste des politiques
Directorate of Strategic Policy and Integration, Specialized Policing Services /
Direction des politiques stratégiques et d'intégration, Services de police spécialisés
Tel / Tél: 613-843-6621
Email / Courriel: jeffrey.morris@rcmp-grc.gc.ca
73 Leikin Drive / 73, promenade Leikin
M8-3-821-55, Ottawa, Ontario, K1A 0R2

Page 85

is withheld pursuant to section

est retenue en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Kimberley Pearce [redacted]

[redacted]

From: Jeffrey Morris s.23
To: Alter, Susan
Date: 2016/07/28 12:42 PM
Subject: [redacted]
CC: Pearce, Kimberley

Thanks Susan [redacted]

[redacted]

Aug. 15.

[redacted]

Jeff

>>> Susan Alter 2016/07/28 12:35 PM >>>
Hi Jeff,

[redacted]

Susan

Susan Alter, Senior Counsel /
Avocate-conseil
RCMP Legal Services /
Services juridiques GRC
Department of Justice /
Ministère de la Justice
Ottawa, Canada K1A 0R2
susan.alter@rcmp-grc.gc.ca
Telephone /Téléphone 613-843-4490
Facsimile /Télécopieur 613-825-1241
Government of Canada / Gouvernement du Canada

>>> On 2016/07/28 at 11:45 AM, in message <579A28A9.42F : 187 : 49978>, Jeffrey Morris wrote:

> Hello Susan,
>
> [redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

[redacted]

Jeff

s.23

Jeffrey Morris,
Policy Analyst / Analyste des politiques
Directorate of Strategic Policy and Integration, Specialized Policing Services /
Direction des politiques stratégiques et d'intégration, Services de police spécialisés
Tel / Tél: 613-843-6621
Email / Courriel: jeffrey.morris@rcmp-grc.gc.ca
73 Leikin Drive / 73, promenade Leikin
M8-3-821-55, Ottawa, Ontario, K1A 0R2
>>> Susan Alter 2016/07/28 11:35 AM >>>
Hello Jeff,

[redacted]

Susan

Susan Alter, Senior Counsel /
Avocate-conseil
RCMP Legal Services /
Services juridiques GRC
Department of Justice /
Ministère de la Justice
Ottawa, Canada K1A 0R2
susan.alter@rcmp-grc.gc.ca
Telephone /Téléphone 613-843-4490
Facsimile /Télécopieur 613-825-1241
Government of Canada / Gouvernement du Canada
>>> On 2016/07/27 at 9:49 AM, in message <5798BBE5.FE0 : 187 : 49978>, Jeffrey Morris wrote:

> Hello Susan,
>
> [redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

[redacted]

Any questions, please let me know.

Best regards,
Jeff

Jeffrey Morris,
Policy Analyst / Analyste des politiques
Directorate of Strategic Policy and Integration, Specialized Policing Services /
Direction des politiques stratégiques et d'intégration, Services de police spécialisés
Tel / Tél: 613-843-6621
Email / Courriel: jeffrey.morris@rcmp-grc.gc.ca
73 Leikin Drive / 73, promenade Leikin
M8-3-821-55, Ottawa, Ontario, K1A 0R2

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Kimberley Pearce - Important - Media scrutiny - encrypted passwords resolution

From:
To:
Date: 2016/08/19 10:27 AM
Subject: Important - Media scrutiny - encrypted passwords resolution
CC:
Attachments: Resolution3.doc; Résolution3.doc

s.19(1)

Following the release of our resolutions, we have received many media requests, particularly on the issue of encrypted passwords. Directeur Harel, Chief Chaffin, Chief Blais, Supt Truax and others have been responding, Mario receiving many calls from Quebec media.

There has often been, perpetuated by the usual privacy and civil libertarian opponents, false statements made or a lack of understanding of what is being requested.

It would be welcomed if each of you, within your own communities, speak to this issue as you see fit. I am providing the simple media lines, the resolution (English and French with background and further media lines) and excellent articles in which CPS and Chief Blais have responded.

A few key messages for consideration:

- Respecting our valued rights as Cdns, we also need to address that there are real people being victimized
- Recognize **this is all based on judicial authorization and predicated on criminal use of encryption technologies.**
- Finally, this is not about creating divisions between us all. We have a real problem. Lets find solutions, together! It's real crime with real victims

- given the cybercrime threat, police encourage the public to protect their on-line activities and data from cybercriminals including the use of encrytpion
- however, in light of the criminal use of encryption technologies, police require a mechanism that respects Canadian values when critical evidence of a serious crime is inaccessible due to encryption
- to be clear, police are not looking for a backdoor to encryption
- police are seeking a proportionate and targeted authority to seek a **court order** from a judge to obtain a password to access encrypted evidence
- the CACP recognizes the importance of judicial oversight in balancing public safety with privacy interests

Note - the resolution is publicly available on our website at the following link: https://cacp.ca/news/resolutions-adopted-at-the-cacp-agm.html

5 things Halifax police chief took away from annual conference of colleagues
http://www.news957.com/2016/08/17/5-things-halifaxs-police-chief-took-from-annual-conference-of-colleagues/

This is not mass surveillance says Calgary police of password resolution
http://www.cbc.ca/beta/news/canada/calgary/police-smartphone-computer-password-1.3726590

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Resolution #03 - 2016

REASONABLE LAW TO ADDRESS THE IMPACT OF ENCRYPTED AND PASSWORD-PROTECTED ELECTRONIC DEVICES

Submitted by the Law Amendments Committee

WHEREAS electronic devices are ubiquitous in both the licit and illicit facets of modern society, and;

WHEREAS electronic devices can be and are used to facilitate the commission of serious and multi-jurisdictional crime, such as organized crime, violent crime, fraud and other financially-motivated crime, and Internet and computer-related crime, and;

WHEREAS Internet and computer-related crime is a growing area of criminal activity that threatens Canadians' privacy and security interests, and Canada's financial systems, and;

WHEREAS the contents of electronic devices can yield critical evidence of such crimes, and;

WHEREAS users of electronic devices have ready access to encryption and password-protection that renders the contents inaccessible to public safety agencies and, not withstanding a valid judicial authorization to search those contents, and;

WHEREAS the inability to execute judicially authorized searches of electronic devices has and will bring serious criminal, and national security investigations to abrupt and unsuccessful ends, and;

WHEREAS there is no legislative power specifically designed to compel an individual to provide either law enforcement or public safety agencies with the password or encryption key for an electronic device, the search of which has been judicially authorized;

WHEREAS other jurisdictions have afforded law enforcement agencies with such legislative powers, and have achieved success in defending that legislation and in furthering legitimate law enforcement interests, and;

WHEREAS this is a possible solution being requested, and;

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

WHEREAS the Canadian Association of Chiefs of Police, as the national voice of Canadian police leadership, is committed to raising issues where the Criminal Code should be amended.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police urges the Government of Canada, for the purpose of community safety, to identify a legislative means for public safety agencies inclusive of law enforcement, through judicial authorization, to compel the holder of an encryption key or password to reveal it to law enforcement.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Resolution #03 - 2016

REASONABLE LAW TO ADDRESS THE IMPACT OF ENCRYPTED AND PASS-WORD PROTECTED ELECTRONIC DEVICES

Background

James B. Comey, Director of the Federal Bureau of Investigation, described the U.S. experience with encrypted and password-protected electronic devices as follows: "Armed with lawful authority, we increasingly find ourselves simply unable to do that which the courts have authorized us to do, and that is to collect information being transmitted by terrorists, by criminals, by pedophiles, by bad people of all sorts." In response, the National District Attorneys Association and the International Association of Chiefs of Police are supporting legislation, a discussion draft of which was released on April 13, 2016, that would compel companies to provide "technical assistance" to law enforcement in respect of encrypted and password-protected data.

Canadian law enforcement faces the same investigative challenges and requires an analogous legislative response. However, legislation directed at companies, many of which will be located outside of Canada, may not suffice. Law enforcement requires reasonable, constitutionally-compliant legislation crafted to suit the Canadian context.

Digital security technology has now advanced to the point that impenetrable password protection and encryption are readily – and in many cases *freely* – available on all electronic devices. This technology immunizes legally seized electronic devices from the execution of a judicially-authorized search, and often compels the abrupt and unsuccessful end of a serious criminal investigation. Recent law enforcement experience provides specific examples of criminal investigations that have been derailed in this manner.

While the issue potentially bears on a wide range of investigations, it will have particular ramifications for the investigation of online child sexual exploitation and abuse, fraud and other financially-motivated crimes, organized crime, requests for international law enforcement assistance, and national security matters involving suspected extremism and other threats to Canada.

Furthermore, technical advancements in techniques to crack password-protected devices alone will not suffice in the case of newer devices with operating systems that erase data (wiping clean) after a limited number of unsuccessful password attempts.

While there are numerous benefits that encryption provides to assure privacy and to cyber security such as e-commerce, it is contrary to the public interest to permit criminals or those that threaten the security of Canadians to create a zone of immunity by encrypting and password-protecting their data, and to thereby limit the reach of validly-issued judicial authorizations. In contrast, a reasonable and proportional law that would permit law enforcement to access encrypted and password-protected data, in appropriate cases, through the application for and granting of a judicial authorization, would promote the safety of Canadian children on the Internet, enhance the integrity of Canadian financial system, improve national security, and assist

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

in the investigation and prosecution of organized and violent criminals. It must be emphasized that Canadian law enforcement agencies have identified this public safety gap and are seeking a legislated process where a judicially authorized format may compel the production of a password or encryption key. It is recognized the use of this privacy-intrusive legislated framework would need to be balanced on a concept of proportionality.

In January 2015, in his address to the Annual Symposium of the Canadian Association for Security and Intelligence Studies, when describing challenges of the basic problem for law enforcement to acquire information, RCMP Commissioner Paulson stated: "We also, and perhaps more urgently, need new tools, to be able to enforce the criminal law quickly and efficiently, in a way consistent with Canadian values and the Charter of Rights and Freedoms".

Recent Law Enforcement Experiences

Several recent examples from the United States and Canada highlight the gravity of this problem:

- In 2010-2011, the Ontario Provincial Police investigated a male for setting up hidden cameras in his house to spy on a young woman who worked for his wife. Police obtained a warrant to search the house and found an encrypted hard drive hidden in the rafters of the basement. E-Crimes could not break the encryption. Police ultimately discovered documents and books containing the suspect's computer information, and entered a series of possible passwords until one of them opened the hard drive. Thousands of voyeuristic images were obtained from the device. The investigating officer explained that the investigation would have failed if the suspect had not written down the password in those documents.

- In 2012, police lawfully seized computers from Justin Gryba in Saskatoon in relation to a child pornography investigation. Some of the computers had been locked and encrypted. Mr. Gryba refused to provide the passwords. Forensic technicians from Saskatoon and Ottawa were not able to break the encryption on one device until two-and-a-half years later. That device contained child pornography depicting many different victims. Mr. Gryba was charged with making and possessing child pornography and, on April 15, 2016, sentenced to serve a further two years less a day in custody (on top of 29 months' credit).

- In May 2013, the Ontario Provincial Police received information that an individual had child pornography on his Apple iPad and potentially on his Apple Macbook Pro laptop. A warrant was executed at the individual's residence and the devices were seized. The items were submitted to OPP E-Crimes for examination and retrieval of any images. Both items were password-protected. E-Crimes did not have the capabilities to gain access without the password. The investigating officer was unable to obtain Production and Assistance Orders for Apple in California, and would have been unwilling to send the devices to California given their probable illegal content. The officer also could not obtain a destruction order, and was forced to make arrangements to return the devices to the suspect. Conditions of return were negotiated: the suspect would provide the password for the purpose of wiping the devices before their return, and no charges would be laid.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Between October 2014 and June 2015, law enforcement in Manhattan, New York, seized 74 Apple iPhones related to investigations into offences such as the attempted murder of three individuals, the repeated sexual abuse of a child, an ongoing sex trafficking ring, and numerous assaults and robberies. Warrants to search the devices were obtained, but could not be executed.

- In Fort Frances, Ontario, there was a recent case of theft of narcotics from a hospital. A phone was seized and forwarded to the Ontario Provincial Police Technological Crime Unit ("E-Crimes"), which was unable to unlock it. The investigation has stalled, though OPP E-Crimes suggested they "might" be able to use a new software program to unlock the phone in 8-12 months.

- In June 2015, a father of six was shot dead in Evanston, Illinois, 10 miles north of Chicago. There were neither witnesses nor surveillance footage. Investigators found an Apple iPhone and a Samsung phone running on Google's Android operating system next to the body of the deceased. Both devices were password-protected. An Illinois state judge issued a warrant ordering Apple and Google to unlock the phones and share with authorities any data that could potentially solve the murder. Apple and Google replied that they could not do so without knowing the user's passcode. The murder remains unsolved.

Potential solutions: other jurisdictions' experiences

Canadian law enforcement may have the ability to compel the production of biometrics through an impression warrant (s. 487.092) or a general warrant (s. 487.01), but not the production of passwords or encryption keys. Several other jurisdictions have explored or implemented legislation to the permit the latter:

- The United Kingdom's *Regulation of Investigatory Powers Act 2000* empowers the court to order a person to supply decrypted information and/or encryption keys. The legislation has been unsuccessfully challenged on self-incrimination grounds.

- Australia's *Cybercrime Act 2001* provides authorization for a magistrate to order a specified person, including a suspect or an accused person, to provide any information or assistance that is reasonable and necessary to allow law enforcement to access, copy, and convert electronic data, with a penalty for non-compliance.

- Key production legislation is in force in South Africa (*Regulation of Interception of Communications and Provision of Communication-Related Information Act*), France (*Loi sur la sécurité quotidienne*), and Finland (*The Coercive Measures Act (Pakkokeinolaki)).*

- Sweden has recently proposed encryption key production legislation.

- New Zealand Customs released a Discussion Paper in 2015 proposing new powers in the *Customs and Excise Act* to demand passwords from persons crossing the border.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- The United States has yet to fully embrace key production, but there have been instances of judges subpoenaing accused individuals to provide their passwords to law enforcement. U.S. Courts have yet to fully resolve whether compelled key production or compelled production of an unencrypted copy of encrypted data violates the privilege against self-incrimination protected by the Constitution's Fifth Amendment.

  However, on April 13, 2016, U.S. Senate Intelligence Committee Chairman Richard Burr and Senator Dianne Feinstein, released a discussion draft of proposed legislation ("Compliance with Court Orders Act of 2016") that would address encrypted and password-protected electronic devices by directing the relevant company to decrypt data or provide other technical assistance to law enforcement. Their proposal is supported by the National District Attorneys Association and the International Association of Chiefs of Police.

Further review of the legislation in the United Kingdom:

The legislation in the United Kingdom was further examined because of its well-established encryption key/password production legislation and our shared legal and constitutional principles. A summary of data from the Office of Surveillance Commissioners ("OSC") Annual Reports provided further insight about the efficacy of that legislation. The OSC is a public body sponsored by the Home Office that oversees the conduct of covert surveillance and covert human intelligence sources by public authorities in accordance with the Regulation of Investigatory Powers Act 2000 ("RIPA").

Section 49 of the RIPA, activated by ministerial order in October 2007, requires persons to supply decrypted information and/or encryption keys to state representatives upon receipt of a court order. In practice, an application involves the following steps:

- The Home Office National Technical Assistance Centre ("NTAC") must approve the application for the service of an s. 49 notice.
- Once NTAC approval is in place, permission may be sought from a Judge.
- Once judicial permission is given, the s. 49 notice should be served.
- If a person fails to comply with the s. 49 notice, a criminal charge may be laid.

The OSC has reported annually on the use of s. 49 since its 2008-2009 Annual Report. The most recent Report is for 2014-2015. The available data from 2008 – 2015 suggests the following:

- 160 notices were issued under s. 49 of *Regulation of Investigatory Powers Act:*
  - The investigations consistently involve terrorism, domestic extremism, indecent images of children, insider dealing, fraud, evasion of excise duty and drugs.
  - Investigations into human trafficking and kidnapping of children seem to be an emerging issue.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Between 38 and 42 individuals (~24% to ~26%) complied with the notice;[1]
- 93 individuals (~58%) did not to comply with the notice;[2]
- 68 of those individuals were charged;
- 46 of those individuals were prosecuted; and
- 14 prosecutions resulted in convictions.

[1] The 2008-2009 Report does not set out the number of notices complied with or still pending. Since the Report provides that 15 notices were issued and that 11 notices were not complied with, this estimate was generated using the minimum (0) and maximum (4) number of individuals who could have complied.

[2] This percentage does not account for notices that are still pending. Year-to-year percentages for non-compliance have questionable explanatory value, given the overlap in data across reporting years. To the extent that they are useful as a benchmark, they are as follows:

- 2008-2009 (~73%);
- 2009-2010 (~41%);
- 2010-2011 (~17%);
- 2011-2012 (~75%);
- 2012-2013 (~73%);
- 2013-2014 (~52%);
- 2014-2015 (~59%).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Resolution #03 - 2016

REASONABLE LAW TO ADDRESS THE IMPACT OF ENCRYPTED AND PASS-WORD PROTECTED ELECTRONIC DEVICES

Media Lines

Canadian law enforcement recognizes the importance of cyber security for all Canadians. Encryption is obviously a complex issue with various considerations and legitimate uses such as e-commerce, protection of privacy, transmission of data, etc. Police services are also users of data encryption for secure communications and data storage.

Electronic devices can be and are used to facilitate the commission of serious and multi-jurisdictional crime, such as organized crime, violent crime, fraud and other financially-motivated crime, and Internet and computer-related crime.

Internet and computer-related crime is a growing area of criminal activity that threatens Canadians' privacy and security interests, and Canada's financial systems. The contents of electronic devices can yield critical evidence of such crimes, and users of electronic devices have ready access to encryption and password-protection that renders the contents inaccessible to law enforcement, notwithstanding a valid judicial authorization to search those contents.

The inability of law enforcement personnel to execute judicially authorized searches of electronic devices has and will bring serious criminal investigations to abrupt and unsuccessful ends.

There is no legislative power in Canada specifically designed to compel an individual to provide law enforcement with the password or encryption key for an electronic device, the search of which has been judicially authorized.

Other jurisdictions in the world have afforded law enforcement agencies with such legislative powers, with judicial oversight, and have achieved success in defending that legislation and in furthering legitimate law enforcement interests.

Canadian law enforcement is seeking a legislated process whereby a court could grant an order to compel the production of a password or encryption key for an electronic device where, on reasonable and probable grounds, a crime has been or is being committed.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Resolution #03 - 2016

REASONABLE LAW TO ADDRESS THE IMPACT OF ENCRYPTED AND PASS-WORD PROTECTED ELECTRONIC DEVICES

Action Plan

1. That the Law Amendments Committee of the Canadian Association of Chiefs of Police consult with Justice Canada and other stakeholders regarding this public safety issue.

2. That the Law Amendments Committee of the Canadian Association of Chiefs of Police continue ongoing consultation with the Federal/Provincial/Territorial Criminal Procedure Committee.

3. That the Law Amendments Committee of the Canadian Association of Chiefs of Police continue ongoing consultation with CACP Cybercrime Committee.

4. That the Executive Director of the Canadian Association of Chiefs of Police forward correspondence to the Public Safety Minister of Canada; the Minister of Justice and Attorney General of Canada; and the Minister of Transportation of Canada, petitioning for legislation requiring persons to be judicially ordered to supply passwords or encryption keys or face legal sanctions.

5. That the Law Amendments Committee of the Canadian Association of Chiefs of Police accompany the President of the CACP to meetings with the Minister of Public Safety and with the Minister of Justice and Attorney General to further discuss this technological and legal challenge in keeping Canadians safe.

6. That the Canadian Association of Chiefs of Police develop a comprehensive media plan to further educate Canadians to the public safety need for this encryption legislation to help reduce the risk to Canadians from those that use encryption for criminal or extremist activities.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Kimberley Pearce - Fwd: Important - Media scrutiny - encrypted passwords resolution

From: Joe Oliver
To: Adam, Jeff; Cefaloni, Derek; Goguen, Taunya; Hiegel, Shannon; Higgs,...
Date: 2016/08/19 10:37 AM
Subject: Fwd: Important - Media scrutiny - encrypted passwords resolution
Attachments: Important - Media scrutiny - encrypted passwords resolution

---

FYI

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Kimberley Pearce - Fwd: Important - Media scrutiny - encrypted passwords resolution

From: Jeffrey Morris
To: Pacha, Tomasz; Pearce, Kimberley; Tremblay, Cheryl
Date: 2016/08/19 10:39 AM
Subject: Fwd: Important - Media scrutiny - encrypted passwords resolution
Attachments: Fwd: Important - Media scrutiny - encrypted passwords resolution

FYI

Pages 101 to / à 116

are withheld pursuant to section

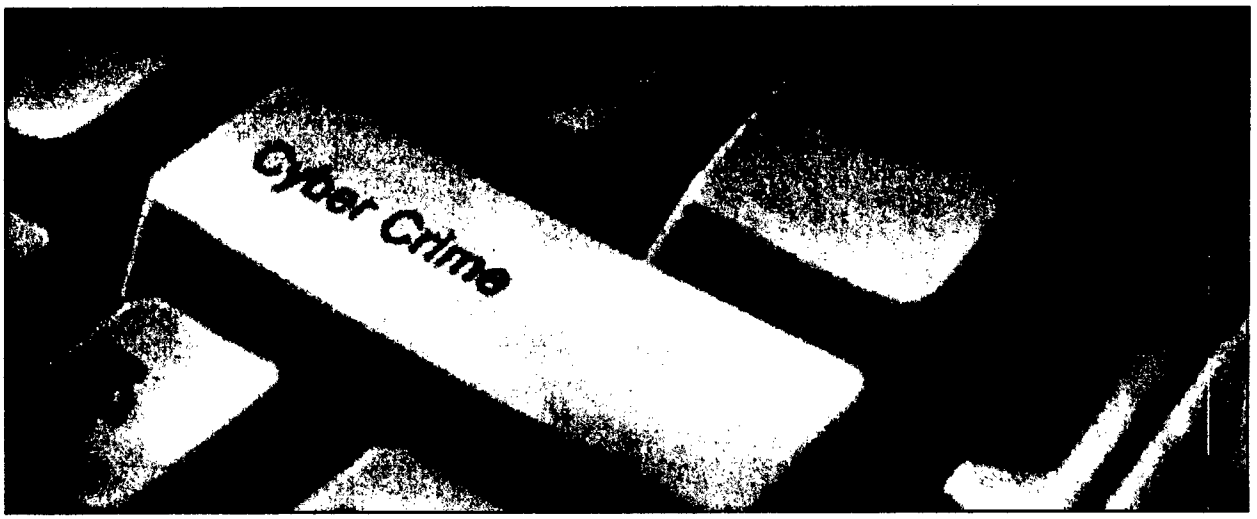
sont retenues en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.



Canada's police chiefs: "We need laws that force cybercriminals to reveal their passwords"

Ryan Patrick - August 18, 2016

The news that Canada's police chiefs are advocating for federal laws that would compel individuals to provide electronic passwords with a judge's consent isn't sitting well with some members of Canada's IT community.

Earlier this week at its annual conference in Ottawa, the Canadian Association of Chiefs of Police (CACP) passed a resolution that formally requests legal measures to lawfully unlock digital evidence, citing the rise of cybercriminals who are using encryption tools to hide illicit activities as the impetus.

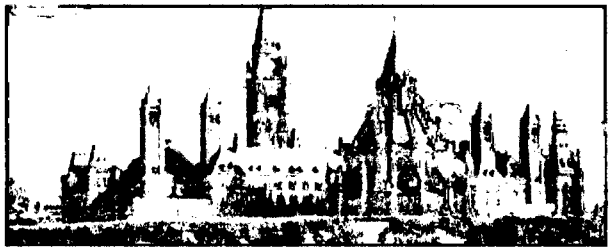
During a news conference on Tuesday, RCMP Assistant Commissioner Joe Oliver noted that at present under Canadian law, police cannot compel individuals to comply with a request to provide a password during an investigation. Law enforcement needs to keep pace with modern criminals who are effectively "going dark" by operating in cyberspace with tools that mask their identities, said Oliver.

"The victims in the digital space are real," said Oliver, adding that Canada's law and policing capabilities aren't keeping pace with the evolution of technology.

But according to Jacob Ginsberg, senior director for Toronto-based email encryption software firm Echoworx, such as move would be an "unconscionable" one.

Related Articles

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.



Ottawa announces public consultation on cyber security strategy

The federal government has started a three-month public consultation on updating its cyber security strategy, asking security pros and

August 16th, 2016 Howard Solomon @itworldca

"While we don't blame CACP for wanting tools to make their jobs easier, a law of this kind would criminalize privacy, and it would be unconscionable for a democratic society to draft a law whereby denying a request from police to go through your things, digital or otherwise, would be illegal," he said in an email.

The association represents in excess of 90 per cent of the police community in Canada which include federal (RCMP), First Nations, provincial, regional and municipal, transportation and military police leaders. The CACP theme for its 111th conference was "public safety in a digital age" and police chiefs such as Ottawa Police Chief Charles Bordeleau noted in a statement the event was intended as an "opportunity to share, learn and work together on a way forward that helps us fuse traditional policing with modern day cyber activity."

"Police services across the world are facing new challenges and threats related to technological developments and the criminal innovation that has ensued," Bordeleau said.

In 2014, the rights of online users were upheld in a Supreme Court of Canada ruling that Internet service providers cannot deliver user names and addresses to law enforcement without a warrant. At the time, The Supreme Court didn't agree with the concept of users having "no reasonable expectation of privacy" for the data obtained by police.

According to police, service-oriented enterprises such as financial firms and telecommunication companies currently require court approval for nearly all types of requests from authorities for basic identifying information.

The CACP also cited a recent Osterman Research report that revealed that 44 of 125 Canadian companies interviewed suffered a ransomware attack in the past 12 months — of which 33 of the victims paid a ransom that was between $1,000 and $50,000 in order to regain stolen data.

But the issue of handing over passwords —even with a court order — will be controversial, predicts Ray Boisvert, CEO of I-Sec Integrated Strategies and former deputy director of intelligence at the Canadian Security Intelligence Service (CSIS).

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

In an interview with IT World Canada, he said he understands the view of those worried about privacy. However, he also understands the position of police, who have legitimate obligations to investigate crime.

In the non-digital world, he noted, search warrants already allow police to seize and go through paper documents looking for specific information spelled out in the warrant. Sometimes, he added, the warrant can be quite broad.

"On the face of it, this seems like it's clearly unconstitutional," David Christopher of Internet advocacy group OpenMedia told CBC News, adding the CACP request represents a "wildly disproportionate" response considering the individual privacy risks involved.

Added Echoworx's Ginberg: "Policy makers and courts across the globe are still adjusting to crime in the digital age, but having the power to access a person's whole digital life, especially during the course of an investigation where it's not established that wrongdoing has taken place, should not make you a criminal."

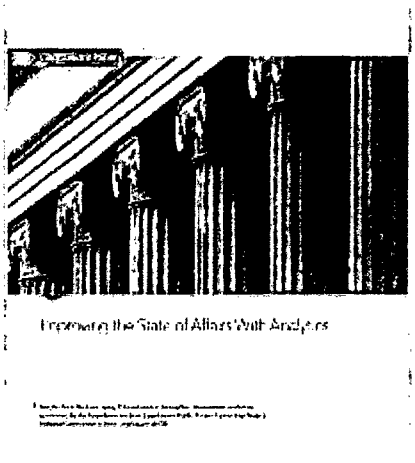
— with files from Howard Solomon

RELATED

Canada should be prepared for "unprecedented" levels of cyber risk, warns ex-CSIS official

Appeal court agrees CSIS lawyers weren't candid on spy warrant

Related Download



Sponsor: **SAS**

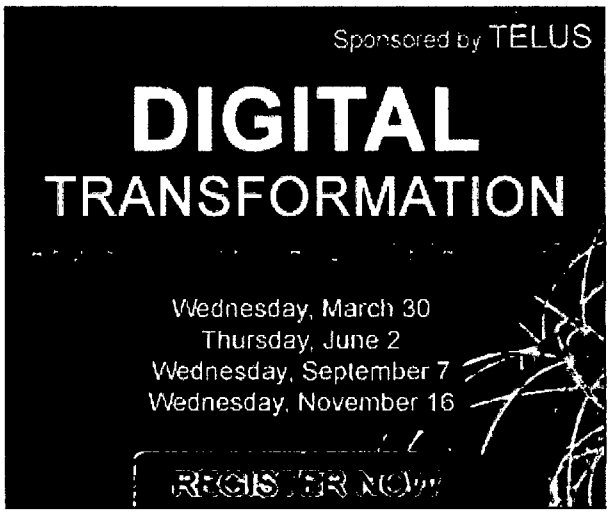
Improving the State of Affairs With Analytics

Download this case study-rich white paper to learn why data management and analytics are so crucial in the public sector, and how to put it to work in your organization.

Register Now

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Government, Privacy, Security **crime, cybersecurity, passwords**



About Ryan Patrick

Seasoned technology reporter, editor and senior content producer.

Follow

WEBSITES

ITWC.ca
ITBusiness.ca
ComputerDealerNews.com
DirectionInformatique.com

PUBLICATIONS

CSO Digital

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Provided by NewsDesk http://www.infomedia.gc.ca/ps-sp/ Fourni par InfoMédia

Published | Publié: 2016-08-22
Received | Reçu: 2016-08-22 3:29 AM

THE RECORD

WATERLOO REGION RECORD (FIRST)
EDITORIAL, Page: A6

Help police but preserve rights

It is no wonder that **police** agencies across the country want easier access to the contents of smartphones, computers and other electronic devices to help solve crimes ranging from online financial rip-offs to possession of vile **child pornography**.

Personal digital data in our wired world is a deep, powerful source of evidence, a virtual treasure trove of communications, images, documents, search histories and, in the case of GPS-enabled mobile devices, travel records.

Experts say our devices often know more about us than we know, or can remember, about ourselves.

Information found on them has been used to catch and convict countless murderers, drug dealers, pedophiles and other miscreants - and their potential value to investigators is only growing as electronic gadgets become ever more integral parts of our lives.

Increasingly, however, **police** are stymied by passwords and encryption keys designed to keep prying eyes in the dark. Even after obtaining legal authorization to seize and search devices, those barriers mean officers can't get at the data stored inside them.

Their understandable frustration provided the context when the **Canadian Association of Chiefs of Police** of Canada recently passed a resolution calling for a new law that would, with the approval of a judge, compel suspects to divulge their passwords.

Such a provision would, to be sure, represent a huge intrusion in a country that properly prizes the right to privacy. The question is whether it could be justified, and collectively tolerated, for the sake of law, order and security.

In that regard, it is useful to remember that **police** have long had the power, after obtaining search warrants from judges, to forcefully break down doors and enter homes to look for damning evidence.

They can also tap into telephone systems to secretly listen to, and record, private conversations provided they can similarly satisfy requirements including the demonstration of reasonable and probable grounds.

Those crucial checks and safeguards already apply as well to the seizure and search of electronic devices that aren't password-protected or can be accessed using forensic tools.

Critics will say that forcing suspects to give up passwords as well as their devices would take the intrusion to a higher, unacceptable level by actively involving them in their own incrimination, a point certainly worth careful consideration.

But there is at least one existing provision in Canada - the law making it a crime to refuse to provide a breath sample in impaired driving investigations - that does much the same thing and has nevertheless been deemed warranted.

Given the challenge **police** face keeping up with criminals who are armed with the latest technology and know how to use it to their advantage, could this be another area where the benefits of greater **police** power outweigh the loss of some liberty?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

At the very least, that question should get a full airing as the federal government embarks on three months of public consultation on cybersecurity. Now is the time for Canadians to make their feelings known on this important and challenging issue.

© 2016 Torstar Corporation

Media contents in NewsDesk are copyright protected.
Please refer to **Important Notices** page for the details.

Le contenu médiatique d'InfoMédia est protégé par les droits d'auteur.
Veuillez vous reporter à la page des **avis importants** pour les détails.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Provided by **NewsDesk** http://www.infomedia.gc.ca/ps-sp/ Fourni par **InfoMédia**

Published | Publié: 2016-08-22
Received | Reçu: 2016-08-22 2:31 AM

THE GLOBE AND MAIL

Globe and Mail
Editorial, Page: A8

The key to the key

Last week, the **Canadian Association of Chiefs of Police** urged the **Canadian** government to provide a way "for public agencies, inclusive of law enforcement, through judicial authorization, to compel the holder of an encryption key or password to reveal it to **law enforcement**."

That was quite a mouthful. Translation: The **police** want the ability to get a legal order that would force someone to hand over their computer or smartphone passwords.

The really important phrase in the police chiefs' statement is "judicial authorization." The phrase that should be used, and that has been around for a very long time, is "search warrant." Judges have a long history of rules and precedents for deciding when **police** are allowed to demand entry to a home or place of business, to take away ostensible evidence of various kinds. Under some circumstances, the **police** can even force their entry.

If and when **police** want to obtain evidence hidden inside an electronic device, the principles and rules for how they get authorization from a court, and when a court will give such authorization, shouldn't be much different from the situation in which **police** officers are knocking audibly at any other, more ordinary door.

For a potentially major new type of invasion of privacy, there should indeed be serious scrutiny about what ought to be examined or what should be treated delicately.

Some conversations at the **police** chiefs' convention reportedly turned on the case of R. v. Spencer, which ended up at the Supreme Court two years ago. In that instance, the **police** were able to locate one consumer of **child pornography** in Saskatchewan after some legal demands on the Internet service provider.

Police are not allowed to enter your locked home and go on a fishing expedition through your papers, looking for evidence of wrongdoing. They need to convince a judge that they should be granted a warrant, which will limit where they can search, and for what. If **police** want to enter your locked computer, the rules should be no different.

Media contents in NewsDesk are copyright protected.
Please refer to **Important Notices** page for the details.

Le contenu médiatique d'InfoMédia est protégé par les droits d'auteur.
Veuillez vous reporter à la page des **avis importants** pour les détails.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Provided by **NewsDesk** http://www.infomedia.gc.ca/ps-sp/ Fourni par **InfoMédia**

Published | Publié: 2016-08-23
Received | Reçu: 2016-08-23 3:30 AM

THE HAMILTON SPECTATOR

THE HAMILTON SPECTATOR (FIRST)
EDITORIAL, Page: A12

Police chiefs' request goes one step too far

Howard Elliott

Time for another discussion about balancing our individual rights with the need for reasonable security measures. This time, though, there's no middle ground from our perspective. The national association of **police** chiefs wants the ability to compel citizens to hand over online passwords provided a court order is obtained.

This is a bad idea.

A step too far. Beyond the pale.

Why?

Here are two arguments against this idea. One, admittedly tongue-in-cheek, goes like this. Who remembers all their passwords? So the **police** get a court order and want them all. So you end up giving them three old ones before you stumble across the new one. We can just hear it now: "Honest officer, I never log off so I don't need my password ..."

Two, more seriously: This is idea is just too broad and duplicates tools the **police** should be able to use now. As it stands, if the **police** have adequate evidence justifying a search of your property, they can get it by obtaining a court-sanctioned search warrant. Typically, warrants include appropriate conditions and restraints. How is searching your car or house any different than searching your phone or hard drive?

Why invent a whole new system of rules and regulations when we have a tried and true one already in place? If **police** have evidence justifying seeing what's in and on your phone, they should use existing tools, even if some procedural modifications are needed.

The justification for this echoes sentiments expressed by U.S. **law enforcement** officials who say bad guys of all sorts are running amok and getting away with it because crucial evidence is concealed in encrypted (password protected) devices. Maybe, but the argument is pretty flimsy for the U.S., lacking many specifics. And that's even more true for **Canada**. Supporters of this idea cite one case of a Saskatchewan **child porn** consumer who was apprehended thanks to information from his Internet service provider (ISP). One case does not a justification make.

Federal **Public Safety Minister Ralph Goodale** hasn't said what he thinks of this specific measure. But he's likely to hear from his advisers that it will be tested through a constitutional challenge if enacted, and it will probably lose. It goes too far and is too broad.

Goodale is right about one thing. He says these issues are getting a lot more scrutiny in the U.S. than they are here. **Canadians**, Goodale says, need to have more discussion about how far **police** and security agencies should be willing to go. He's right. Certain reasonable curtailments to privacy and freedom may be justifiable, others may not be - like this one.

But we may not know one from the other without a robust national discussion.

© 2016 Torstar Corporation

Media contents in NewsDesk are copyright protected.
Please refer to **Important Notices** page for the details.

Le contenu médiatique d'InfoMédia est protégé par les droits d'auteur.
Veuillez vous reporter à la page des **avis importants** pour les détails.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Provided by NewsDesk http://www.infomedia.gc.ca/ps-sp/ Fourni par InfoMédia

Published | Publié: 2016-08-23
Received | Reçu: 2016-08-23 3:42 AM

TIMES COLONIST

TIMES COLONIST (VICTORIA) (FINAL)
COMMENT, Page: A8

Police and passwords

Toronto Star

Handing over the electronic password to your computer or cellphone to police could give them more access to your personal information than turning over the key to your house.

That's why **Canadians** must carefully guard their privacy rights when considering any proposal to make it easier for **law-enforcement** officials to rummage through their digital data.

Public Safety Minister Ralph Goodale is calling for a public discussion on how to strike the right balance between the need for privacy and the need to give police adequate tools to fight all sorts of Internet-and computerrelated crime.

It's a debate that's long overdue. And it's one that cannot be delayed much longer in light of a high-profile call from the country's police chiefs for a new **law** that would force people to hand over electronic passwords, albeit with the permission of a judge.

The **Canadian Association of Chiefs of Police** argues quite rightly that electronic devices are being used in the commission of all sorts of crime - from fraud to child abuse - and **law enforcement** is struggling to keep up. It notes that **Canada** has no **law** to compel someone to provide a password or encryption key during an investigation.

The trick is to find a way to give police the powers they really need while safeguarding the right to privacy, as well as constitutional guarantees against self-incrimination and unreasonable search and seizure. Reasonable and probable grounds of a potential crime must be shown in a warrant. It can't be a fishing expedition. The warrant would have to describe exactly what police are looking for.

Police should look at all the other leads available to them before requesting a warrant for a password. They are right to want the tools they need to protect citizens from online criminal threats. But **Canadians** should not have to toss away personal freedoms to achieve that goal.

Media contents in NewsDesk are copyright protected.
Please refer to **Important Notices** page for the details.

Le contenu médiatique d'InfoMédia est protégé par les droits d'auteur.
Veuillez vous reporter à la page des **avis importants** pour les détails.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Provided by NewsDesk http://www.infomedia.gc.ca/ps-sp/ Fourni par InfoMédia

Published | Publié: 2016-08-23
Received | Reçu: 2016-08-23 3:30 AM

TORONTO STAR

TORONTO STAR (ONT)
OPINION, Page: A11

Password protection a crucial charter right

Nader R. Hasan and Stephen Aylward

You have the right to remain silent - for now. If certain **law enforcement** officials have their way, we may soon be required to divulge our Facebook and iPhone passwords to the police.

Last week, the **Canadian Association of Chiefs of Police** adopted a startling resolution calling for legislation that, on judicial authorization, would "compel the holder of an encryption key or password to reveal it to **law enforcement**." **Public Safety Minister Ralph Goodale** invited public debate on the proposal.

Police are responding to new challenges wrought by modern technology. Encryption renders data unintelligible without the user's password. Even with a warrant to seize and search a cellphone or computer, police cannot gain access to the valuable information stored on those devices unless they can guess the password (or hack into the device, as the FBI recently did with a locked iPhone in the San Bernardino case).

Police worry criminals are "going dark" — i.e., using encryption to evade detection and prosecution. Compelling suspects to surrender their cellphone and computer passwords is an enticing solution to this problem. But it is one that ought to be unacceptable in a free and democratic society.

The police chiefs' proposal would lead to a radical erosion of our constitutional rights protected under the **Canadian** Charter of Rights and Freedoms. When the state accuses us of a crime, we are entitled to say, "prove it." The Supreme Court of **Canada** has said this right - the right against self-incrimination - is the organizing principle of our criminal justice system. An accused person is under no obligation to assist the state in her or his own prosecution, whether by answering questions about where she was the previous night or by revealing passcodes.

Canadian law jealously protects the right against self-incrimination for reasons that are both historical and principled. The right against self-incrimination has its historical roots in the revulsion toward the 17th century courts of the Star Chamber, which would detain supposed enemies of the state on mere suspicion, compel them to swear an oath and then require them on pain of punishment to answer questions.

Our constitutional law protects the right against self-incrimination because we recognize there is a power imbalance in criminal prosecutions, which frequently pit a single (often marginalized) individual against the overwhelming power of the state. The right against self-incrimination is the great equalizer. It ensures an individual is put through the criminal process only once police have built a case. It also protects the dignity of the accused and limits the risk that state officials will abuse their power.

Supporters of the police chiefs' proposal may point out that there are already certain contexts under our laws where the right against self-incrimination has been abridged and individuals are required by law to provide information to the state. But these exceptions are narrow and in highly regulated contexts.

Drivers are required to report car accidents. Travellers must answer questions posed by customs officials about the contents of their bags. The difference is that the state treats driving and international travel as privileges bestowed only on those who agree to relinquish some liberty in order to participate in the highly regulated activity. And even in these highly regulated contexts, as soon as the state's purpose shifts from compliance with the regulatory regime to a criminal investigation, the individual's full panoply of charter rights - including the right against self-incrimination - are engaged.

s.23

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Any response to the challenge of encryption must also take into account the heightened expectation of privacy that individuals have in their digital devices. Our cellphones and computers can hold a massive amount of highly private and personal information about ourselves. As the Supreme Court has repeatedly recognized, searches of these devices are profoundly invasive.

Expediency of criminal investigations has not been and cannot be the only goal of the criminal justice system. Encryption is new but the need for law enforcement to adapt to changing technologies is not. With every technological advancement, criminals become more sophisticated and law enforcement must meet the challenge. The police should invest in training the next generation of tech-savvy **law enforcement** officers. But sacrificing the right against self-incrimination should be off the table.

Nader R. Hasan is a lawyer practising criminal, constitutional and regulatory law at Stockwoods LLP in Toronto, and is an adjunct professor at the University of Toronto, Faculty of Law.

Stephen Aylward is a lawyer practising criminal, regulatory, and civil litigation at Stockwoods LLP.

© 2016 Torstar Corporation

Media contents in NewsDesk are copyright protected. Please refer to **Important Notices** page for the details.

Le contenu médiatique d'InfoMédia est protégé par les droits d'auteur. Veuillez vous reporter à la page des **avis importants** pour les détails.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Canadian Law Enforcement Want Government To Force People To Turn Over Their Passwords

from the *the-legislative-$5-wrench* dept

Legal Issues
by **Tim Cushing**
Thu, Aug 25th 2016
3:33am

Filed Under: **canada, encryption, going dark, law enforcement, passwords**

Permalink.

Legislators and law enforcement (for the most part...) have been hesitant to demand companies build backdoors into their encryption schemes. The unwillingness to cross this government overreach line hasn't really tempered cursing of the impending darkness, however. That remains, largely propelled by a few of law enforcement's loudest mouths, who haven't seen a problem nerds can't solve, even after the nerds have told them repeatedly the problem (safely backdoored encryption) is unsolvable.

A lobbying group for Canadian law enforcement thinks it has the answer. Why mandate encryption backdoors when you can just utilize the "backdoor" built into every electronic device?

> *Canada's police chiefs want a new law that would force people to hand over their electronic passwords with a judge's consent.*
>
> *The Canadian Association of Chiefs of Police has passed a resolution calling for the legal measure to unlock digital evidence, saying criminals increasingly use encryption to hide illicit activities.*

The legislated human backdoor. Obviously, such a demand raises constitutional questions, even on that side of the border.

> *The chiefs' proposed password scheme is "wildly disproportionate," because in the case of a laptop computer it would mean handing over the "key to your whole personal life," said David Christopher, a spokesman for OpenMedia, a group that works to keep the Internet surveillance-free.*
>
> *"On the face of it, this seems like it's clearly unconstitutional."*

On this side of the border, such a mandate would also seem clearly unconstitutional, even though some courts have ruled that providing a passcode to unlock a device isn't testimonial -- even if what's on the unlocked device may prove to be incriminating.

The head of Royal Canadian Mounted Police echoes FBI Director James Comey's lament about (potential) evidence remaining out of reach of investigators. In fact, he pretty much quotes him directly.

> *There is nothing currently in Canadian law that would compel someone to provide a password to police during an investigation, RCMP Assistant Commissioner Joe Oliver told a news conference Tuesday.*
>
> *Oliver said criminals -- from child abusers to mobsters -- are operating online in almost complete anonymity with the help of tools that mask identities and messages, a phenomenon police call "going dark."*

Mandating the divulging of passwords relies on some very dubious assumptions. One, it assumes that any information still unseen by prosecutors or investigators is of evidentiary value -- hence the perceived need to *force* suspects to unlock devices. As was seen in the San Bernardino case, a lengthy court battle and a million-dollar payout to Israeli hackers recovered nothing of interest from the shooter's iPhone.

Second, it assumes law enforcement will use this power wisely and with restraint -- something that has historically been a problem for it. When an agency uses repurposed military technology (Stingrays) to (almost) hunt down fast food thieves, it's safe to assume forcing someone to expose their "whole personal life" by turning over a password is likely to result in the same sort of misuse... and abuse. It won't be reserved for the "worst of the worst" criminal suspects and will likely be legislated into existence without enough statutory restrictions to prevent device seizures incident to even the most innocuous of arrests to be viewed as evidentiary fishing expeditions.

Insider Shop - Show Your Support!

READ POSTS EARLY. JOIN THE INSIDER CHAT & MORE
INSIDER SHOP

Advertisement

Report this ad | Hide Techdirt ads

Essential Reading

Hot Topics

5.9 Nice Officials Say They'll Sue Internet Users Who Share Photos Of French Fashion Police Fining Women In Burkinis

5.3 Engineers Say If Automated Cars Experience 'The Trolley Problem,' They've Already Screwed Up

5.1 Baltimore PD Can Keep Tabs On The Entire City, Thanks To Privately-Donated Aerial Surveillance System

New To Techdirt?

Explore some core concepts:

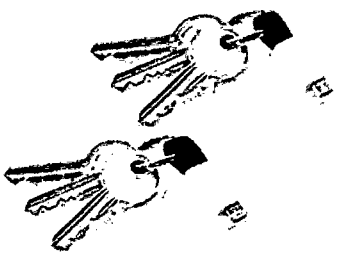
The Future Of Music Business Models (And Those Who Are Already There)

An Economic Explanation For Why DRM Cannot Open Up New Business Model Opportunities

The Grand Unified Theory On The Economics Of Free

read all »

Techdirt Deals



KEYRING CHARGERS \\ 30% OFF >

Report this ad | Hide Techdirt ads

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The only standing between this law (if it becomes law) will be Canada's judges. While some judges may be unwilling to expose a person's entire life just because law enforcement swears it's necessary, others will be more amenable. Bring on the forum shopping!

5 Comments | Leave a Comment

ADVERTISEMENT

Report ad | Hide ads

If you liked this post, you may also be interested in...

- Canadian Law Enforcement Admit -- And Then Deny -- They Own A Stingray Device
- Canadian Court Says No Expectation Of Privacy In SMS Messages Residing On Someone Else's Phone
- French Government Wants A 'Global Initiative' To Undermine Encryption And Put Everyone At Risk
- Terrorist-Fighting License Plate Readers Just Mobile Revenue Generators Cruising Poor Neighborhoods
- Volkswagen Created A 'Backdoor' To Basically All Its Cars... And Now Hackers Can Open All Of Them

ADVERTISEMENT

How the Panama Papers Document Leak Could've Been Prevented

11.5 million documents; 2 terabytes of sensitive files. That's how much data was compromised during the Panama Papers leak. And the files could all have been easily protected - here's how.

Post sponsored by BLACKBERRY

Techdirt Insider Chat

Machin Shin: But was something along those lines, I have been really tempted to go and try to find it to get a picture of it. I suspect if I asked the guy he would happily tell me where it was, he didn't seem to see the problem with it at all.

audiomagi: I've never served in the military, but I've been taught the above listed "four rules," and I (naively) assumed law enforcement officers would be, also. I was obviously mistaken, which is a disheartening realization.

TheResidentSkeptic: A bigger issue is having a rifle with a scope and hitting the wrong target from less than 100 ft. SWAT should get 10 out of 10 in the 10 ring.

Groaker: While I agree with your that the accuracy and precision of too many police in SWAT is a disaster, many lives have been lost

Join the Insider Chat

Advertisement

Reader Comments (rss)

(Flattened / Threaded)

1.  **That One Guy** (profile), *Aug 25th, 2016 @ 1:54am* + | + | FW | LW |

'You first'

Prior to any vote each and every person pushing for this should be required to make public the log-in credentials to their personal computers, email accounts, and any other personal password protected systems/devices they have access to.

After all it's entirely possible that one or more of those devices/accounts *might* contain evidence of illegal actions, and if a 'maybe' is good enough *for* them, it should be good enough to be used *against* them to demonstrate what it's like to have their privacy stripped from them on nothing more than the whim of another.

They're welcome to refuse of course, in which case they get to enjoy being known from then on as the hypocrites that they are, demanding that their privacy be respected while the privacy of others is blatantly violated.

[reply to this | link to this | view in thread]

2.  **Anonymous Coward**, *Aug 25th, 2016 @ 4:03am* + | + | FW | LW |

yet another thing that the USA has started and snowballing to other nations! why the hell cant the USA just stop with all these anti-privacy and anti-freedom laws? does it not realise that it is fucking up the planet more than even terrorism is? it just never seems to stop! and those at the top of the USA tree who are so paranoid as to want to bring in the very things it fought against Germany to stop need to get the fuck off the planet!!

[reply to this | link to this | view in thread]

3.  **Anonymous Coward**, *Aug 25th, 2016 @ 4:07am* + | + | FW | LW |

The limpending darkness is in reality the world stepping back to towards a pre-electronic era, where there was just not the records available for the governments and law enforcement to gather up and use or abuse. It is not so much the world going dark, as the world realizing leaving readable information lying around is much too tempting for governments and law enforcement to resist.
Even with encryption, the meta-data is giving law enforcement and governments much more information than they had pre-internet.

[reply to this | link to this | view in thread]

4.  **Anonymous Coward**, *Aug 25th, 2016 @ 4:20am* + | + | FW | LW |

Remember, in the U.S., a lot of the argument against this practice is based on your Fifth Amendment right to not incriminate yourself.

No such right exists in Canada: you can be compelled to testify against yourself here.

[reply to this | link to this | view in thread]

5.  **Paul Renault** (profile), *Aug 25th, 2016 @ 4:46am* + | + | FW | LW |

Report this ad | *Hide Techdirt ads*

Recent Stories

Thursday

03:33 Canadian Law Enforcement Want Government To Force People To Turn Over Their Passwords (5)

Wednesday

22:36 Engineers Say If Automated Cars Experience 'The Trolley Problem,' They've Already Screwed Up (16)

16:07 FISA Court: Government Can Collect Content Along With Dialing Data Using Pen Register Orders (13)

14:32 Arrest Warrant Issued For District Attorney Involved In DEA's California Wiretap Warrant Mill (20)

13:05 Baltimore PD Can Keep Tabs On The Entire City, Thanks To Privately-Donated Aerial Surveillance System (30)

11:45 Nice Officials Say They'll Sue Internet Users Who Share Photos Of French Fashion Police Fining Women In Burkinis (79)

10:39 Bogus Defamation Lawsuit With Fake Defendant Results In Negative Reviews Of Dentist Being Taken Down (28)

10:34 Daily Deal: Ultimate PC Data Security Suite Bundle (0)

09:30 Copyright Group, In Arguing Against FCC's Set Top Box Proposal, Appears To Argue That VCRs & DVRs Are Also Illegal (44)

08:31 Tempting Fate: Pittsburgh Election Officials Insist Their E-Voting Machines Can't Be Hacked (36)

More

Advertisement

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Kimberley Pearce -

From: Ian Bradley
To: Chan, Judy; Dale, Michael; Dawson, Donald; Johnson, Douglas; Kilfoil... s.23
Date: 2016/08/29 1:34 PM
Subject:
CC: Scrivens, Mark; Walter, Sharon
Attachments:

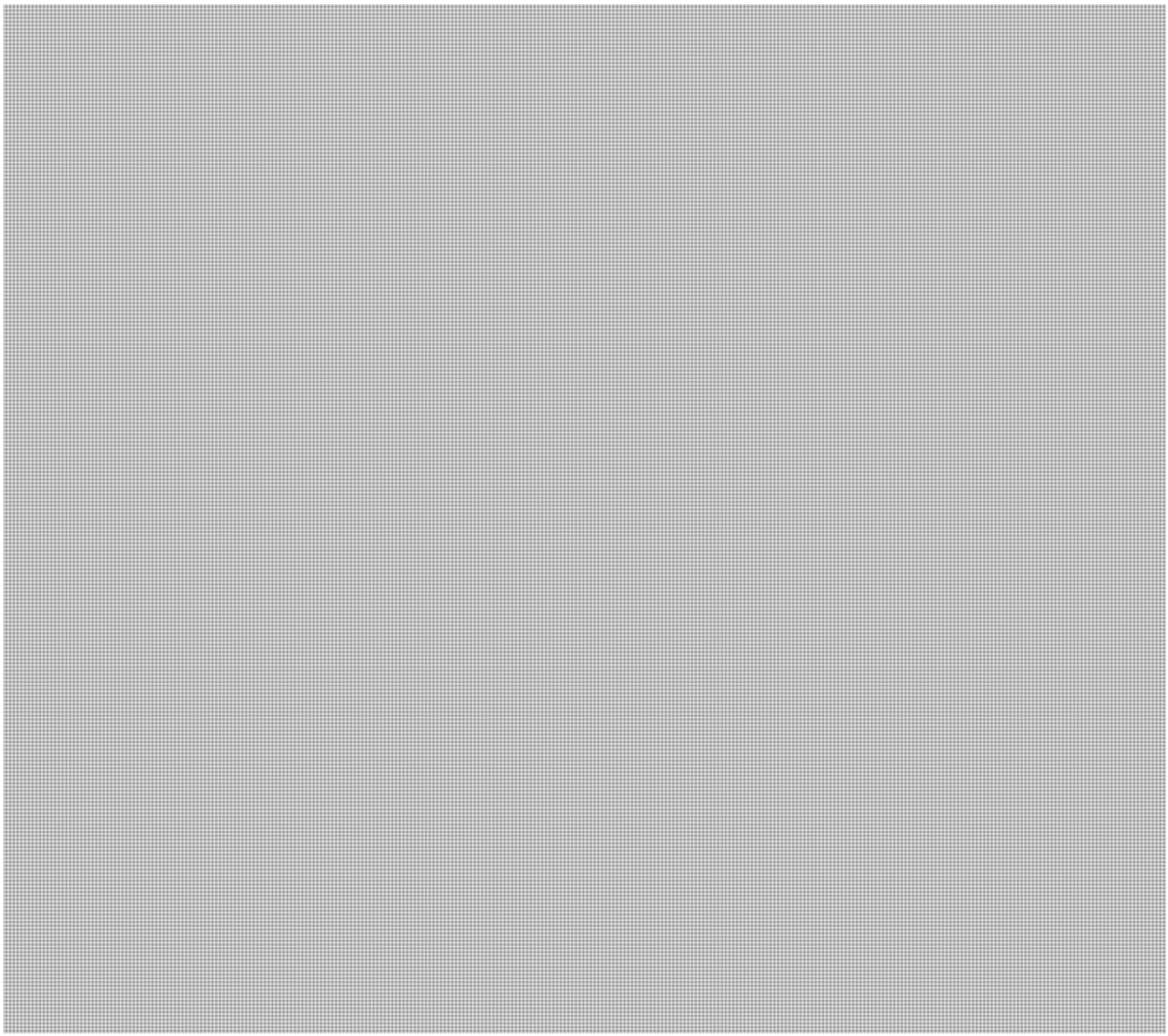
Judy, Christine, Kim, Doug, Don and Mike,

Cheers,

>>> "Duffy, Michael" <Michael.Duffy@justice.gc.ca> 2016/08/29 1:06 PM >>>

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.23



Michael

Michael W. Duffy
Senior General Counsel / Avocat général principal

Office of the Assistant Deputy Minister / Bureau du sous-ministre adjoint
Public Safety, Defence and Immigration Portfolio / Portefeuille de la Securité publique, de la Défence et de l'Immigration

Department of Justice Canada / Ministère de la justice Canada
284 Wellington Street / 284, rue Wellington
Ottawa, Ontario K1A 0H8

Telephone / Téléphone: 613-960-0880 Email / courrier électronique: michael.duffy@justice.gc.ca

Pages 133 to / à 229

are withheld pursuant to section

sont retenues en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Kimberley Pearce - RE: URGENT ACTION REQUEST 2016-019524 Meeting with FBI Director Comey, US Ambassador to Canada & Minister Goodale

From: Mark Scrivens
To: Angers, Lucie; Audcent, Karen; Matte, Daniel
Date: 2016/09/16 4:08 PM
Subject: RE: URGENT ACTION REQUEST 2016-019524 Meeting with FBI Director Comey, US Ambassador to Canada & Minister Goodale
CC: 'Sugunasiri, Shalin (PS/SP)'; Baker, Christine; Douglas, Michelle; Du... s.23
Attachments: [redacted]

Thanks for this Lucie,

[redacted]

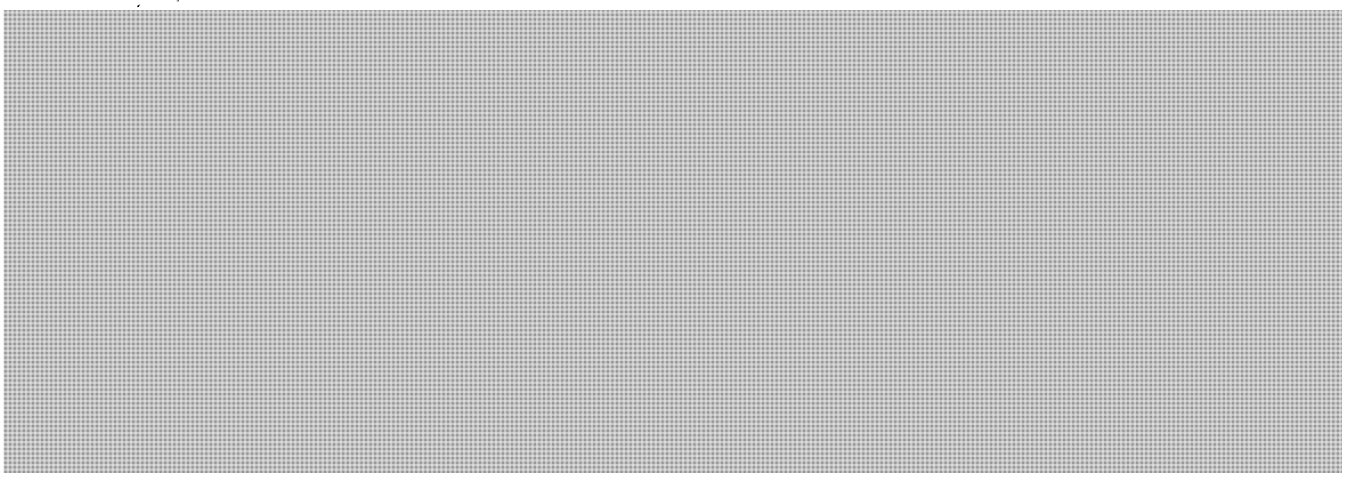
Mark Scrivens, Senior Counsel /
Avocat-conseil
RCMP Legal Services /
Services juridiques GRC
Department of Justice /
Ministère de la Justice
Ottawa, Canada K1A 0R2
mark.scrivens@rcmp-grc.gc.ca
Telephone /Téléphone 613-843-4782
Facsimile /Télécopieur 613-825-1241
Government of Canada / Gouvernement du Canada
RCMP Legal Services/Services juridiques de la GRC
Tél: (613) 843-4782
Fax/télé: (613) 825-1241
Government of Canada / Gouvernement du Canada
>>> "Angers, Lucie" <Lucie.Angers@justice.gc.ca> 2016/09/16 10:35 AM >>>
Bonjour Daniel, In Karen's absence, [redacted] I will be unavailable to read my e-mails until 13:00. Thanks, Lucie

From: Matte, Daniel
Sent: Friday, September 16, 2016 10:12 AM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Duffy, Michael <Michael.Duffy@justice.gc.ca>; Scrivens, Mark (RCMP) <Mark.Scrivens@rcmp-grc.gc.ca>; Pearce, Kimberley (RCMP) <kimberley.pearce@rcmp-grc.gc.ca>; 'Sugunasiri, Shalin (PS/SP)' <shalin.sugunasiri@canada.ca>; Douglas, Michelle <Michelle.Douglas@justice.gc.ca>; Baker, Christine <Christine.Baker@justice.gc.ca>
Subject: FW: URGENT ACTION REQUEST 2016-019524 Meeting with FBI Director Comey, US Ambassador to Canada & Minister Goodale

Karen [redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.23



Cheers,

Daniel

From: Audcent, Karen
Sent: 2016-Sep-15 11:51 AM
To: Duffy, Michael <Michael.Duffy@justice.gc.ca<mailto:Michael.Duffy@justice.gc.ca>>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca<mailto:Lucie.Angers@justice.gc.ca>>
Subject: FW: URGENT ACTION REQUEST 2016-019524 Meeting with FBI Director Comey, US Ambassador to Canada & Minister Goodale

Hi Michael, thanks! Karen

From: Melanson, Janice
Sent: 2016-Sep-15 11:22 AM
To: * CLP SGC/Office <CLPSGC_Office@justice.gc.ca<mailto:CLPSGC_Office@justice.gc.ca>>; Angers, Lucie <Lucie.Angers@justice.gc.ca<mailto:Lucie.Angers@justice.gc.ca>>; Audcent, Karen <Karen.Audcent@justice.gc.ca<mailto:Karen.Audcent@justice.gc.ca>>
Cc: Millette, Pierre <Pierre.Millette@justice.gc.ca<mailto:Pierre.Millette@justice.gc.ca>>
Subject: FW: URGENT ACTION REQUEST 2016-019524 Meeting with FBI Director Comey, US Ambassador to Canada & Minister Goodale

Please note the correction in the CCM # on this request.

Janice Melanson
Senior Assistant Deputy Minister's Office |
Bureau du Sous-ministre adjoint principal
Policy Sector | Secteur des politiques
janice.melanson@justice.gc.ca<mailto:janice.melanson@justice.gc.ca>
Telephone | Téléphone 613-941-4120
Facsimile | Télécopieur 613-957-9949

From: Ministerial Liaison Unit
Sent: September-15-16 11:17 AM
To: Ministerial Liaison Unit <MLU@justice.gc.ca<mailto:MLU@justice.gc.ca>>; * SADMO/Admin

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

<SADMO_Admin@justice.gc.ca<mailto:SADMO_Admin@justice.gc.ca>>
Cc: * MLU Group <MLUGroup@justice.gc.ca<mailto:MLUGroup@justice.gc.ca>>; Leclerc, Caroline <Caroline.Leclerc@justice.gc.ca<mailto:Caroline.Leclerc@justice.gc.ca>>; Patry, Claudine <Claudine.Patry@justice.gc.ca<mailto:Claudine.Patry@justice.gc.ca>>; Garskey, Adam <Adam.Garskey@justice.gc.ca<mailto:Adam.Garskey@justice.gc.ca>>; Taschereau, Alexia <Alexia.Taschereau@justice.gc.ca<mailto:Alexia.Taschereau@justice.gc.ca>>; Douglas, Michelle <Michelle.Douglas@justice.gc.ca<mailto:Michelle.Douglas@justice.gc.ca>>; Nesrallah, Tania <Tania.Nesrallah@justice.gc.ca<mailto:Tania.Nesrallah@justice.gc.ca>>; Matte, Daniel <Daniel.Matte@justice.gc.ca<mailto:Daniel.Matte@justice.gc.ca>>; Budgell, Alexandra <Alexandra.Budgell@justice.gc.ca<mailto:Alexandra.Budgell@justice.gc.ca>>; Baker, Christine <Christine.Baker@justice.gc.ca<mailto:Christine.Baker@justice.gc.ca>>
Subject: RE: URGENT ACTION REQUEST 2016-019524 Meeting with FBI Director Comey, US Ambassador to Canada & Minister Goodale

Please note that the correct CCM # for this request is 2016-019524.

SB

From: Ministerial Liaison Unit
Sent: September-13-16 11:06 AM
To: * SADMO/Admin <SADMO_Admin@justice.gc.ca<mailto:SADMO_Admin@justice.gc.ca>>
Cc: Ministerial Liaison Unit <MLU@justice.gc.ca<mailto:MLU@justice.gc.ca>>; * MLU Group <MLUGroup@justice.gc.ca<mailto:MLUGroup@justice.gc.ca>>; Leclerc, Caroline <Caroline.Leclerc@justice.gc.ca<mailto:Caroline.Leclerc@justice.gc.ca>>; Patry, Claudine <Claudine.Patry@justice.gc.ca<mailto:Claudine.Patry@justice.gc.ca>>; Garskey, Adam <Adam.Garskey@justice.gc.ca<mailto:Adam.Garskey@justice.gc.ca>>; Taschereau, Alexia <Alexia.Taschereau@justice.gc.ca<mailto:Alexia.Taschereau@justice.gc.ca>>; Douglas, Michelle <Michelle.Douglas@justice.gc.ca<mailto:Michelle.Douglas@justice.gc.ca>>; Nesrallah, Tania <Tania.Nesrallah@justice.gc.ca<mailto:Tania.Nesrallah@justice.gc.ca>>; Matte, Daniel <Daniel.Matte@justice.gc.ca<mailto:Daniel.Matte@justice.gc.ca>>; Budgell, Alexandra <Alexandra.Budgell@justice.gc.ca<mailto:Alexandra.Budgell@justice.gc.ca>>; Baker, Christine <Christine.Baker@justice.gc.ca<mailto:Christine.Baker@justice.gc.ca>>
Subject: URGENT ACTION REQUEST Meeting with FBI Director Comey, US Ambassador to Canada & Minister Goodale
Importance: High

Please use the attached approval slip / Veuillez svp utiliser la fiche d'approbation ci-jointe

MLU # / # ULM
2016-019524

Due in MLU / Date limite
September 16, 2016

At / À
1 pm

Lead Sector / Secteur Responsable
Policy

Consultation

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

PSDI

Topic / Sujet
Meeting with FBI Director Comey, US Ambassador to Canada & Minister Goodale

Request / Demande
Please prepare briefing materials for the Minister's courtesy meeting with FBI Director Comey, US Ambassador to Canada & Minister Goodale to be held on September 19 at 3:15 pm.

Please note that briefing notes should be limited to one to two pages, when possible, with additional information annexed to the note. The general templates posted on JUSnet should be used. Please use the MLU # mentioned above, and make sure that the CCM fields are accurate and are filled accordingly.

Please forward the electronic version (up to Protected B) of the briefing note to MLU-ULM@justice.gc.ca<mailto:MLU-ULM@justice.gc.ca>, or "Ministerial Liaison Unit" in the Global Address List. For material containing secret or cabinet confidence information, please bring the documents on a secure USB key to EMB 4262 or 4228. If you have any questions concerning this request, please do not hesitate to contact the MLU.

If this request should have been sent to a different sector, please reply to this email.

Veuillez noter que les notes d'information devraient se limiter à une ou deux pages, et toute information additionnelle devrait être jointe à la note en annexe. Les gabarits à utiliser se retrouvent sur le site intranet JUSnet. Veuillez utiliser le # ULM mentionné ci-dessus, et s'assurer que tous les champs de CCM sont adéquats et complétés en conséquence.

Veuillez transmettre la version électronique (jusqu'à Protégé B) de la note d'information à l'adresse MLU-ULM@justice.gc.ca<mailto:MLU-ULM@justice.gc.ca>, or "Ministerial Liaison Unit" dans la liste d'adresses globales. Si le matériel contient de l'information secrète ou confidence du cabinet, veuillez apporter les documents par clef USB au EMB 4262 ou 4228. N'hésitez pas à contacter l'ULM pour tout complément d'information à ce sujet.

Si cette demande aurait dû être envoyée à un différent secteur, s'il vous plaît répondez à ce courriel.

Merci,

Sophie Bonenfant
Coordination Officer | Agente de coordination
Ministerial Liaison Unit | Unité de liaison ministérielle
Department of Justice Canada | Ministère de la Justice Canada
284 Wellington Street, Room 4260| 284, rue Wellington, pièce 4260
Ottawa, Ontario K1A 0H8
Telephone | Téléphone 613-952-1509
B.B. 613-415-8204
sophie.bonenfant@justice.gc.ca<mailto:jennifer.hall@justice.gc.ca>

Page 234

is withheld pursuant to section

est retenue en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

Pages 235 to / à 236

are withheld pursuant to sections

sont retenues en vertu des articles

15(1), 21(1)(a), 23

of the Access to Information Act

de la Loi sur l'accès à l'information

Pages 237 to / à 239

are withheld pursuant to sections

sont retenues en vertu des articles

15(1), 21(1)(a)

of the Access to Information Act

de la Loi sur l'accès à l'information

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Piekarzewski, Anna (PS/SP)

From: Adamowski, Andrew (PS/SP)
Sent: Friday, June 10, 2016 11:59 AM
To: Oakes, Lindsey (PS/SP); Audcent, Karen; 'terence.stechysin@cb.gc.ca'; [redacted]@smtp.gc.ca); Benoit, Nathalie (Nathalie.Benoit@justice.gc.ca); Pitcairn, Laura (Laura.Pitcairn@ppsc-sppc.gc.ca); 'Janelle.Vincent@international.gc.ca'; [redacted] (CSE) [redacted]@cse-cst.gc.ca); Nelligan, Christopher (CRA) (Christopher.Nelligan@cbsa-asfc.gc.ca); Hattlmann, Kevin; Wong, Normand (Normand.Wong@justice.gc.ca); Angers, Lucie (Lucie.Angers@justice.gc.ca); Sansom, Gareth (Gareth.Sansom@justice.gc.ca); Taschereau, Rodrigue (PS/SP); '[redacted]@smtp.gc.ca'; '[redacted]@smtp.gc.ca'; Piekarzewski, Anna (PS/SP); Jeffrey Morris (jeffrey.morris@rcmp-grc.gc.ca)
Subject: [redacted]

s.15(1)

Good Afternoon,

s.23

[redacted]

Thanks,

Andrew

Andrew Adamowski

Senior Policy Advisor, National Security Operations
Public Safety Canada, Government of Canada
andrew.adamowski@canada.ca, Tel: 613-991-2930

Analyste principale des politiques
Sécurité publique Canada, Gouvernement du Canada
andrew.adamowski@canada.ca, Tél: 613-991-2930

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.




s.23

Pages 242 to / à 247

are withheld pursuant to section

sont retenues en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Piekarzewski, Anna (PS/SP)

From: Oakes, Lindsey (PS/SP)
Sent: Monday, June 27, 2016 11:30 AM
To: Audcent, Karen; Stechysin, Terence (IC); Chris LYNAM; Jeffrey Morris; Benoit, Nathalie; Pitcairn, Laura; 'Janelle.Vincent@international.gc.ca'; [redacted](CSE); [redacted]@cse-cst.gc.ca; Nelligan, Christopher (CRA); Hattlmann, Kevin; Wong, Normand; Sansom, Gareth; Angers, Lucie; Adamowski, Andrew (PS/SP); Taschereau, Rodrigue (PS/SP); [redacted]@smtp.gc.ca; [redacted]@smtp.gc.ca; Cyndy.Nelson@international.gc.ca; Palumbo, Jacqueline; Piekarzewski, Anna (PS/SP); Foley, Lisa (IC); Leduc, Andre (IC); De Santis, Michael (IC) s.15(1)
Cc: Carole SMITH
Subject: RE: NS Consultations

Importance: High

Good Morning all,

[redacted] s.23

Thank you for your on-going support throughout this process. Please do not hesitate to contact myself or Andrew Adamowski should you have any questions or concerns.

Regards,

Lindsey Oakes
Telephone: 613-990-8020
Blackberry: 613-410-6057
E-mail | Courriel: lindsey.oakes@canada.ca

Public Safety Canada | Sécurité publique Canada

From: Oakes, Lindsey (PS/SP)
Sent: Monday, June 20, 2016 3:16 PM
To: Audcent, Karen; Stechysin, Terence (IC); [redacted]@smtp.gc.ca); Jeffrey Morris; Benoit, Nathalie (Nathalie.Benoit@justice.gc.ca); Pitcairn, Laura (Laura.Pitcairn@ppsc-sppc.gc.ca); 'Janelle.Vincent@international.gc.ca' (Janelle.Vincent@international.gc.ca); [redacted]@cse-cst.gc.ca); [redacted]@cse- s.15(1)

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

cst.gc.ca; Nelligan, Christopher (CRA) (Christopher.Nelligan@cbsa-asfc.gc.ca); Hattlmann, Kevin; Wong, Normand (Normand.Wong@justice.gc.ca); Sansom, Gareth (Gareth.Sansom@justice.gc.ca); Angers, Lucie (Lucie.Angers@justice.gc.ca); Adamowski, Andrew (PS/SP); Taschereau, Rodrigue; [redacted]smtp.gc.ca; [redacted]@smtp.gc.ca; 'Cyndy.Nelson@international.gc.ca'; Palumbo, Jacqueline (Jacqueline.Palumbo@justice.gc.ca); Piekarzewski, Anna (PS/SP); Foley, Lisa (IC); Leduc, Andre (IC); De Santis, Michael (IC); Williams, Matthew (Matthew.Williams@justice.gc.ca); Robert.Young2@international.gc.ca
Cc: Carole SMITH
Subject: RE: NS Consultations

s.15(1)

Good Afternoon,

[redacted]

s.23

Please do not hesitate to contact myself or Andrew Adamowski if you have any further questions or concerns.

Thanks,

Lindsey Oakes
Telephone: 613-990-8020
Blackberry: 613-410-6057
E-mail | Courriel: lindsey.oakes@canada.ca

<< OLE Object: Picture (Device Independent Bitmap) >>

-----Original Appointment-----
From: Oakes, Lindsey (PS/SP)
Sent: Monday, June 13, 2016 2:50 PM
To: Oakes, Lindsey (PS/SP); Audcent, Karen; Stechysin, Terence (IC); [redacted]@smtp.gc.ca); Jeffrey Morris; Benoit, Nathalie (Nathalie.Benoit@justice.gc.ca); Pitcairn, Laura (Laura.Pitcairn@ppsc-sppc.gc.ca); 'Janelle.Vincent@international.gc.ca' (Janelle.Vincent@international.gc.ca); [redacted]@cse-cst.gc.ca); [redacted]@cse-cst.gc.ca; Nelligan, Christopher (CRA) (Christopher.Nelligan@cbsa-asfc.gc.ca); Hattlmann, Kevin; Wong, Normand (Normand.Wong@justice.gc.ca); Sansom, Gareth (Gareth.Sansom@justice.gc.ca); Angers, Lucie (Lucie.Angers@justice.gc.ca); Adamowski, Andrew (PS/SP); Taschereau, Rodrigue; [redacted]@smtp.gc.ca; [redacted]@smtp.gc.ca; Cyndy.Nelson@international.gc.ca; Palumbo, Jacqueline (Jacqueline.Palumbo@justice.gc.ca); Piekarzewski, Anna (PS/SP); Foley, Lisa (IC); Leduc, Andre (IC); De Santis, Michael (IC); Williams, Matthew (Matthew.Williams@justice.gc.ca); Robert.Young2@international.gc.ca
Cc: Carole SMITH
Subject: [redacted]
When: Wednesday, June 15, 2016 1:30 PM-3:00 PM (UTC-05:00) Eastern Time (US & Canada).
Where: 340 Laurier Ave - 13th Floor

s.15(1)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Hi All,

It looks like we had some technical difficulties in sending out this original meeting invitations, so it seem like it didn't make it to everyone.

s.23

That said, we would like to reschedule the meeting to this Wednesday afternoon from 1:30-3:00. [redacted] if you haven't received them, please let me know.

The meeting will now take place at 340 Laurier Ave. Please note that we will be in a secure board room and you will be asked to lock up all electronic devices.

If you could please confirm your attendance ASAP it would be greatly appreciated.

Thanks,
Lindsey

Pages 251 to / à 256

are withheld pursuant to section

sont retenues en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Piekarzewski, Anna (PS/SP)

From: Adamowski, Andrew (PS/SP)
Sent: Thursday, June 30, 2016 12:41 PM
To: Oakes, Lindsey (PS/SP); Audcent, Karen; 'terence.stechysin@cb.gc.ca'; [redacted]@smtp.gc.ca); Benoit, Nathalie (Nathalie.Benoit@justice.gc.ca); Pitcairn, Laura (Laura.Pitcairn@ppsc-sppc.gc.ca); 'Janelle.Vincent@international.gc.ca'; [redacted](CSE) [redacted]@cse-cst.gc.ca); Nelligan, Christopher (CRA) (Christopher.Nelligan@cbsa-asfc.gc.ca); Hattlmann, Kevin; Wong, Normand (Normand.Wong@justice.gc.ca); Angers, Lucie (Lucie.Angers@justice.gc.ca); Sansom, Gareth (Gareth.Sansom@justice.gc.ca); Belanger, Pierre-Gilles (Pierre-Gilles.Belanger@justice.gc.ca); Garson, Amy (CRA) (amy.garson@cra-arc.gc.ca); Thérien, Michelle (Michelle.Therien@justice.gc.ca); Cyndy.Nelson@international.gc.ca; [redacted]@smtp.gc.ca'; [redacted]@smtp.gc.ca'; De Santis, Michael (IC); 'michael.walma@international.gc.ca'; Palumbo, Jacqueline (Jacqueline.Palumbo@justice.gc.ca); Piekarzewski, Anna (PS/SP); Jeffrey Morris; Leduc, Andre (IC); Foley, Lisa (IC); De Santis, Michael (IC); David.Janzen@rcmp-grc.gc.ca; Kimberley Pearce (Kimberley.Pearce@rcmp-grc.gc.ca) s.15(1)
Cc: Taschereau, Rodrigue (PS/SP)
Subject: [redacted]
Attachments: [redacted]

s.23

Good Afternoon,

[redacted]

Thanks again,

Andrew

Andrew Adamowski

Senior Policy Advisor, National Security Operations
Public Safety Canada, Government of Canada
andrew.adamowski@canada.ca, Tel: 613-991-2930

Analyste principale des politiques
Sécurité publique Canada, Gouvernement du Canada
andrew.adamowski@canada.ca, Tél: 613-991-2930

Pages 258 to / à 264

are withheld pursuant to section

sont retenues en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Piekarzewski, Anna (PS/SP)

From: Oakes, Lindsey (PS/SP)
Sent: Tuesday, July 12, 2016 1:30 PM
To: Audcent, Karen; Stechysin, Terence (IC); Chris LYNAM; Jeffrey Morris; Benoit, Nathalie; Pitcairn, Laura; 'Janelle.Vincent@international.gc.ca'; [redacted]CSE); [redacted]@cse-cst.gc.ca; Nelligan, Christopher (CRA); Hattlmann, Kevin; Wong, Normand; Sansom, Gareth; Angers, Lucie; Adamowski, Andrew (PS/SP); Taschereau, Rodrigue (PS/SP); [redacted]@smtp.gc.ca; [redacted]@smtp.gc.ca; Cyndy.Nelson@international.gc.ca; Palumbo, Jacqueline; Piekarzewski, Anna (PS/SP); Foley, Lisa (IC); Leduc, Andre (IC); De Santis, Michael (IC) s.15(1)
Subject: [redacted]
Attachments:

Importance: High

s.23

Good Afternoon all,

[redacted]

Thanks in advance,

Lindsey Oakes
Telephone: 613-990-8020
Blackberry: 613-410-6057
E-mail | Courriel: lindsey.oakes@canada.ca

Public Safety Canada | Sécurité publique Canada

Pages 266 to / à 333

are withheld pursuant to section

sont retenues en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Piekarzewski, Anna (PS/SP)

From: Oakes, Lindsey (PS/SP)
Sent: Tuesday, July 12, 2016 8:17 AM
To: [redacted] (PS/SP) s.15(1)
Cc: Taschereau, Rodrigue (PS/SP); Adamowski, Andrew (PS/SP)
Subject: RE: Discussion paper
Attachments: PS-SP-#1902430-v1-NS_Consultations_-_Discussion_Paper_-_Input_from_NSOD_....docx

Tracking:

Recipient	Read
[redacted]	Read: 7/12/2016 8:25 AM
Taschereau, Rodrigue (PS/SP)	Read: 7/12/2016 8:57 AM
Adamowski, Andrew (PS/SP)	

Good Morning [redacted]

[redacted]

Generally speaking, we have a couple of comments / concerns that we would like to add in addition to what is included in the document:

[redacted]

Thanks for your on-going work and for allowing us to provide comments.

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

Lindsey Oakes
Telephone: 613-990-8020
Blackberry: 613-410-6057
E-mail | Courriel: lindsey.oakes@canada.ca

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Public Safety Canada | Sécurité publique Canada

From: Taschereau, Rodrigue (PS/SP)
Sent: Monday, July 11, 2016 8:42 AM
To: Adamowski, Andrew (PS/SP); Oakes, Lindsey (PS/SP)
Subject: s.23

Please note deadline

Rodrigue Taschereau
Director, National Security Operations
Public Safety
613-998-4826

From: Banerjee, Ritu (PS/SP)
Sent: Friday, July 08, 2016 11:43 AM
To: Rogers, Daniel; Wong, Suki (PS/SP); Edward Drodge; Alison Whelan; Davies, John (PS/SP); Soper, Lesley L; Breithaupt, Doug; Greg Koster; Duffy, Michael; Audcent, Karen s.15(1)
Cc: Michael Lister; MacIntyre, David (PS/SP); Renaud, Élise (PS/SP); Cintrat, Jean (PS/SP); (PS/SP); Taschereau, Rodrigue (PS/SP); Ho, Fenton (PS/SP); Beecher, Sophie (PS/SP)
Subject:

Hi,

Thanks for your help and cooperation. s.23

Ritu

Sent from my BlackBerry 10 smartphone on the Rogers network.

>

Pages 336 to / à 338

are withheld pursuant to section

sont retenues en vertu de l'article

23

of the Access to Information Act

de la Loi sur l'accès à l'information

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Piekarzewski, Anna (PS/SP)

From: Oakes, Lindsey (PS/SP)
Sent: Tuesday, July 12, 2016 1:43 PM
To: Audcent, Karen; Stechysin, Terence (IC); Chris LYNAM; Jeffrey Morris; Benoit, Nathalie; Pitcairn, Laura; 'Janelle.Vincent@international.gc.ca'; [redacted](CSE); [redacted]@cse-cst.gc.ca; Nelligan, Christopher (CRA); Hattlmann, Kevin; Wong, Normand; Sansom, Gareth; Angers, Lucie; Adamowski, Andrew (PS/SP); Taschereau, Rodrigue (PS/SP); [redacted]@smtp.gc.ca; [redacted]@smtp.gc.ca; Cyndy.Nelson@international.gc.ca; Palumbo, Jacqueline; Piekarzewski, Anna (PS/SP); Foley, Lisa (IC); Leduc, Andre (IC); De Santis, Michael (IC)
Subject: [redacted]
Attachments:

s.15(1)

s.23

Good Afternoon all,

[redacted]

Many thanks,

Lindsey Oakes

Senior Policy Analyst | Analyste principale en politiques
National and Cyber Security Branch | Secteur de la Sécurité et de la Cybersécurité Nationale
Public Safety Canada | Sécurité publique Canada
340 Laurier Ave West, Ottawa, Canada K1A 0P8 | 340, av. Laurier Ouest, Ottawa, Canada K1A 0P8
E-mail | Courriel: lindsey.oakes@canada.ca / **Telephone:** 613-990-8020 / **Blackberry:** 613-410-6057

Public Safety Canada | Sécurité publique Canada

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Diagnostic Concerning the Challenges in Relation to Cybercrime
- Outline -

Introduction

- Cyberspace is broader than the Internet – it refers to all interconnected digital technologies, such as cellular networks and cloud infrastructure. It is a community of communities similar to the real world; a place where innovation and new ideas flourish and where individuals, businesses, governments and diverse organizations increasingly operate on a daily basis. However, it is also a place where criminals can steal, extort, launder, traffic, conspire and commit serious offenses with very little risk of being detected or apprehended, in comparison to the same criminal activity in a non-digital environment. In short, the Internet and new technologies are vehicles used to facilitate the perpetration of cybercrime, for they enable actors to operate with impunity due to their virtual and often anonymous nature.

- Cybercrime within the context of cybersecurity:
  - Definition of Cybercrime:
    - *Technology-as-target*
    - *Technology-as-instrument (level of sophistication)*

- The current and rapidly evolving state of cyberspace presents unprecedented growing challenges for the RCMP and law enforcement partners.
  - 'Old Crimes in New Ways' and 'New Crimes in New Ways'
  - Pressing public safety issues for the Canadian law enforcement community because of overall lack of capability, capacity and authority
    - Communications technology: the ability of police to access and gather necessary information to apprehend targets has not advanced in parallel

- Cybercrime is a global problem that significantly impacts the safety and economic well-being of Canadians, and regularly victimizes:
  - vulnerable members of our society (e.g., children, the elderly); and,
  - private businesses and individuals given Canada's relative wealth and internet-dependent economy.

  Accordingly, various private sectors are calling for action, especially the financial sector.

Threat Environment

- The cyber threat environment is constantly shifting, as emerging criminal actors increasingly developing their cyber capabilities, in order to communicate their ideology, gain political and competitive advantage or for illicit gain.

- Criminal and terrorist networks are fully embracing the cyber environment. This is to their advantage given the cyber challenges police currently face. Their activities range from hacking government systems to illegally obtain Social Insurance Numbers; to selling illicit goods and their cyber services online; to using the Internet and secure online fora to recruit and plan a variety of criminal and terrorist activities.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- There has also been a significant increase in the proliferation of cyber tools and capabilities that are low in cost and readily available for a variety of criminal activities, including espionage, extortion and obtaining illegal goods.

- There is a noticeable increase in the scale and impact of cyber-related criminality linked to national security, serious and organized crime and financial crimes. Domestically, the volume and severity of cybercrime impacting Canadians and businesses are increasing, but is still felt to be considerably under-reported.
  - Domestic data
  - International data
  - Nearly all cyber incidents are crimes

- Given the borderless environment of cyberspace, threats to Canadians and domestic businesses are known to come from foreign jurisdictions hosting cybercriminals or criminal market platforms. One of these ways is through the use of malicious software, such as ransomware, and "botnets" for illicit purposes and profit.

- Response to the threat environment by Five Eyes Partners.

- RCMP to collaborate with OGDs to develop threat environment more fully.

Roles of Federal Departments and Agencies and Private Sector in Addressing Cybercrime

- Build off bubble chart language - RCMP, CSEC, GAC, FINTRAC, CRTC, ISED, DoJ, PS

- Private Sector

Government of Canada Efforts to Tackle Cybercrime from a Criminal Justice Approach

Canada's Cyber Security Strategy (2010)

- Phase I ($1.4M new and ongoing funding):
  - Creation of a dedicated cybercrime intelligence team at RCMP; and,
  - *Cybercrime: An Overview of Incidents and Issues in Canada* (2014).
- Phase II ($7.1M new and ongoing funding):
  - RCMP to create first cybercrime investigative team;
  - Expand existing cybercrime intelligence team;
  - Improve digital evidence capabilities in support of cybercrime investigations; and,
  - Expand basic cybercrime training opportunities for Canadian policing community
- Less than 10% of funding, to date, has been invested in Pillar III, entitled *Helping Canadians to be secure online*, which is the pillar that includes law enforcement efforts to combat cybercrime.

Council of Europe Convention on Cybercrime

- The Budapest Convention sets out that "Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force" (e.g. a bilateral mutual

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

legal assistance treaty) between two Convention countries, then these countries may use the Convention as a bilateral mutual assistance mechanism within the scope of the treaty.
- Resourcing highlights

Legislative Amendments (input from DOJ)
- ***Protecting Canadians from Online Crime Act***
  - The *Act* created new preservation demand and preservation order powers in relation to electronic information

RCMP Cybercrime Strategy (2015)
- Reduce the threat, impact and victimization of cybercrime in Canada through law enforcement action by:
  - Identifying and prioritizing cybercrime threats through intelligence collection and analysis;
  - Pursuing cybercrime through targeted enforcement and investigative action; and
  - Supporting cybercrime investigations with specialized skills, tools and training.

Operational Framework and a supporting Action Plan, objectives, strategic enablers and 15 action items, which the RCMP will implement over the next five years funding provided from *Canada's Cyber Security Strategy*. Collectively, these initiatives will enable Canada's national police force to better combat cybercrime in concert with its domestic and international law enforcement partners and other stakeholders.

Study of the Technological Barriers to Obtaining Judicially Authorized Digital Evidence in Major Federal Projects (2016)
- The RCMP is studying the operational impacts on the Federal Policing Program's project-based investigations given the technological barriers to obtaining judicially authorized evidence.

<u>Operationalizing the Current Approach to Tackle Cybercrime</u>
- The following components follow the cycle of how the Government of Canada pursues cybercriminals.

Prevention / Awareness
- Cybertip - As a registered charitable organization, the Canadian Centre for Child Protection operates Cybertip.ca for the public to report suspected cases of online child sexual exploitation, through which it examines and triages reports to appropriate law enforcement officials, and provides public awareness and education programming.

- Get Cyber Safe - Government's multimedia, multi-platform public awareness campaign on cyber security.

Criminal Intelligence
- The RCMP takes an intelligence-led approach to policing. Given the borderless nature of cybercrime and the inherent need to identify patterns and relationships between cybercrime data and other relevant data sources from multiple jurisdictions, criminal intelligence is an integral component in identifying criminal targets.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Cybercrime intelligence – originating from investigations, police information databases, open source research and analysis, or public/private partner collaboration – can identify prolific and serious offenders in cyberspace and may objectively direct police resource to major cybercrime targets.

- CAFC - The CAFC, along with private sector partners, work to disrupt illicit activity utilizing various initiatives. For example, subsequent to receiving a referral from CAFC, service providers can terminate email accounts and telephone numbers used to facilitate fraud. In addition, the CAFC has developed an informal partnership with VISA and MasterCard to share descriptor information from fraud complaints, in order to assess the suspect account for unusual or suspicious transaction activity, ultimately to mitigate future fraud losses. In a cybercrime environment, an Internet Service Provider can disrupt IP addresses to take down fraudulent websites.

- The RCMP's NCECC is the central point of contact for investigations related to online sexual exploitation of children in Canada and those international investigations involving Canadian victims or offenders. The NCECC also provides a number of services to domestic and international law enforcement, including immediately responding to a child at risk, coordinating investigative files, conducting operational research, and providing specialized training specific to online child sexual exploitation investigations. The NCECC maintains ongoing collaborative partnerships with Canadian and international police agencies across the globe; working with international agencies to develop new practices, investigational tools, and evidence based approaches to keep pace with the changing scope of online child sexual exploitation.

Criminal Investigations

- At the federal level, the RCMP investigates serious and organized crime, economic crime, a range of national security threats, and enforces Federal statutes. These investigations may extend to federal offences involving suspected cybercrime activities, such as money laundering and terrorist financing, market fraud, threats to Canada's critical infrastructure, intellectual property infringements or drug trafficking.

- Through contract policing services, the RCMP plays a role in addressing cybercrime in contracted provinces, territories and municipalities. Policing activities in these jurisdictions extend to a range of criminal offences where the Internet and related technologies play an integral role; however, the capabilities of contract policing with regard to investigating cybercrime are nascent.

- Support to investigations from other federal and policing partners.

- As cybercrime is largely transnational, international policing plays a pivotal role in the RCMP's response to cybercrime. Therefore, the RCMP must work with multilateral partners to obtain and analyze evidence, which is enabled by police-to-police information sharing and formal legal mechanisms.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Specialized Policing Services

- The RCMP's specialized and technological services play a critical role in cybercrime investigations.
  - The Technical Investigations Services provides technical domain expertise and digital forensic services to cybercrime investigations to all levels of policing in Canada, in addition to those involving international policing.
  - The Integrated Technological Crime Units also provide specialized services, by responding to cybercrime incidents in collaboration with other domestic and international police services, and often lead cybercrime investigations on behalf of Canada that are national or international in scope.
- The Canadian Police College provides training and educational opportunities on cybercrime investigations and intelligence gathering.

- Technical Expertise collaboration with other federal and policing partners.

Prosecutions

- ;...

Disruption

- Ability to disrupt domestically
- Ability to develop intelligence to provide international partners with the ability to disrupt

Canadian Policing Community

- Calls for action by key police stakeholders, include:
  - **2015:** The Canadian Association of Chiefs of Police (CACP) and National Police Services (NPS) National Advisory Committee (NAC) called for the creation of the National Cybercrime Coordination Centre (NC3)
  - **2016:** The CACP passed a resolution calling for a new law that would, with judicial authorization, compel an individual to provide either law enforcement or public safety agencies with the password or encryption key for an electronic device.

Impediments

Criminal Intelligence and Investigations

Policy Impediments:

- Cybercrimes are underreported and as such, police lack the data to comprehensively understand the extent and impact of the problem, which significantly impedes the development of policing strategies to combat these crimes. Conversely, if police direct the public and Canadian business to contact them when a cybercrime has been committed and they are not resourced or capability to take on the investigation, they will lose the trust of the victim and discourage future reporting.
- Insufficient information from victims to understand the true scope of the problem in Canada.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- The ability of the RCMP and policing partners to tackle cybercrime varies from jurisdiction to jurisdiction, but is generally at the nascent stage and thus unable to respond to the level and complexity of the cyber incidents affecting Canadians.

Operational Impediments - Capabilities:

- While the RCMP does have a recognized technical capacity in some areas of combating cybercrime, federal investigative teams do not have dedicated cyber expertise needed to bridge the gap between investigative experts across the country and technical expertise, which are largely centralized (e.g., investigators left to decipher encrypted and coded data).
- Reactive requests for technological support (e.g. no capability to intercept a communication or to decrypt data on a specific device at this time) that are unable to consider the intricacies of the investigation and to propose alternative solutions to original request, present missed opportunities to advance the investigation.
- Despite having judicial authority do so, law enforcement increasingly cannot access the digital evidence needed to support all types of criminal investigations. Where the tools and capabilities of law enforcement have not kept pace with the barriers presented by new and emerging technologies, there has been a sharp decrease in the technical capabilities of police to intercept private communications. In cases where communications can be collected, criminals are taking full advantage of new and robust encryption and anonymizing technologies to defeat police efforts to collect evidence pursuant to court orders.
- Increased use of traditional investigative techniques (e.g. covert entries and undercover operators) to supplement technical solutions are costly, resource intensive, pose significant safety concerns for the undercover operators and agents, and present increased risks of detection by criminals.
- Lack of ability to conduct meta-data analysis.

Operation Impediments – Coordination:

- The lack of central reporting of cybercrime incidents perpetuates the lack of knowledge regarding the prevalence of these incidents in Canada.
- Multi-jurisdictional nature of cybercrime requires a significant level of police-to-police coordination and deconfliction, nationally. Gap leads to an inability to link perpetrators, offences and victims (which are almost always in different jurisdictions), and results in inefficient, duplicative or no effort to solve these complex crimes.

Operational Impediments – Collaboration:

- Communications service providers are increasingly reluctant to provide the information requested by authorities.
- In line with the transnational nature of cybercrime, law enforcement digital evidence may remain outside of reach due to jurisdictional obstacles.
- Lack of international policing presence.

Specialized Policing Services

- There is a marked lack of police technical expertise and capacity at the federal, provincial/ territorial and municipal levels.

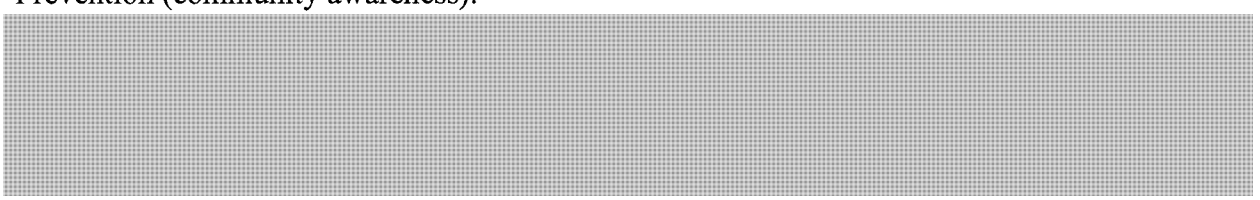
Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Overarching Enablers

The Expectation for Policing in Cyberspace:

- A key gap for all Canadian police agencies exist with regards to the expectation of the level of response and assistance to Canadians and private sector businesses on cybercrime-related incidents (e.g. a bitcoin wallet was stolen).

Prevention (community awareness):



Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Training and Capacity Building:

- Criminal investigators at the federal level, as well as local investigators and intelligence analysts require basic and advanced training in new and emerging technologies and the types of information that can be gleaned to keep pace with cybercrime.
- Shortage of highly specialized and technical skills, such as advanced proficiencies in computer science and network engineering, and other technical domain areas, to conduct or assist in complex federal investigations.

Partnerships with industry, academia and other levels of government:

- Find and/or maintain the most effective partnerships in other fields to leverage expertise and bolster Canada's ability to prevent, develop investigative and technical expertise.
- Given the global nature of cybercrime, Canada's footprint abroad to support international collaboration with close allies needs to be established in order to better understand and combat cybercrimes that are victimizing Canadians by foreign perpetrators.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

MESSAGE FROM THE MINISTERS

When it comes to national security, the dual responsibilities of government are clear:

- We must keep Canadians safe, at home and abroad.

- In so doing, we must preserve our rights and freedoms, which help to shape the character of our open, generous and inclusive country.

We cannot enjoy our individual freedoms without effective collective security. But we must achieve that security in manner that does not undermine the essence of that which we seek to protect – in short, the very qualities that define the country we love.

The former Bill C-51 – the *Anti-Terrorism Act, 2015* – was an important piece of legislation. It addressed certain gaps in Canada's counter-terrorism framework. But the legislation contained a number of problematic elements. Many Canadians were concerned, and remain so.

Now is the opportunity to get it right – to bring forward new initiatives and introduce new legislation that strengthens accountability, bolsters our security and further protects the rights of Canadians.

As a government, we have already pledged to deliver legislative changes and new initiatives that will:

- protect the right of Canadians to protest, demonstrate and advocate;
- ensure that security and intelligence efforts comply with the *Charter of Canadian Rights and Freedoms*;
- more precisely define "terrorist propaganda" to make certain we focus on genuine threats to Canadians;
- draw a clear distinction between security services and police forces;
- create a new national security committee of parliamentarians to review and scrutinize security and intelligence activities;
- launch a new national office and center of excellence for community outreach and engagement – to better understand and prevent radicalization to violence;
- correct shortcomings in our No Fly List, while continuing to ensure air

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

travel is safe and would-be terrorists are kept from travelling to become foreign fighters.

This is only a beginning. More can be done to keep Canadians safe and to protect our democratic way of life.

This discussion paper serves as an invitation to Canadians to participate in, and contribute to, the next stage of our counter-terrorism efforts.

We want your opinions and your ideas as we work to ensure that the appropriate tools are available to our law enforcement and security officials – tools that are in keeping with Canadian values and respectful of the *Charter*.

Please read this discussion paper and the other relevant documents available online. Let us know what you think. Working together, we can better protect both our national security and the fundamental rights of all Canadians.

Hon. Ralph Goodale, P.C., M.P.
Minister of Public Safety and Emergency Preparedness

Hon. Jody Wilson-Raybould, P.C., M.P
Minister of Justice and Attorney General of Canada

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

INTRODUCTION

In Canada, we are not isolated from the terrorist threat. We are not immune to menace and tragedy. Since 2001, when Canada passed into law the *Anti-terrorism Act*, threats to our domestic and international security have continued to evolve.

New terrorist groups – including the Islamic State of Iraq and the Levant (ISIL) – have emerged and engineered chaos and destruction in many parts of the world. Increasing numbers of Canadians have traveled to the Middle East to join ISIL. And extremist narratives have inspired a number of Canadians to plot and pursue attacks against domestic targets.

Indeed, the principal terrorist threat to Canada remains the possibility of violent extremists carrying out attacks within our borders.

Our national security institutions share a duty to keep Canadians safe – and they do so daily. At the same time, these agencies are themselves subject to measures that keep them accountable to Canadians and ensure the rule of law is respected.

In a world of uncertainty, risk and rapid change, do we have the tools necessary to keep people safe – and are we using all our tools in ways that also safeguard our values?

The government urges Canadians to use this consultation process to be active partners in revamping our counter-terrorism framework. We want policies that are more informed and that better reflect the nature of the country we share.

Counter-terrorism efforts represent a complex and deeply charged area of public policy. People have strong perspectives and clear opinions, as they should on matters of such importance.

Each of the following chapters briefly outlines the issues at hand and gives a sense of the relevant challenges. Other documents available online – including an expanded version of this discussion paper – provide more detailed, technical information on issues.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

As a Canadian, you are invited and encouraged to respond online and share your views on this discussion paper and the associated documents. Your input will be welcomed until [Xxxxx, xx] – at which point the government will begin the process of crafting new legislation relating to counter-terrorism measures.

We have before us the opportunity to build the security and intelligence framework we want for our country – a framework that reflects Canadian values and priorities, and the nature and character of who we are and how we want to live in the world. Let's begin.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

ACCOUNTABILTY

To protect our national security, a number of government agencies are given the power to collect intelligence and enforce laws. Much of this work must be done in secret. That's just common sense.

But even as we preserve this secrecy, we must make certain that a system is in place to ensure the accountability of these agencies. That's how Canadians will know that our intelligence and enforcement powers are being exercised with great care, in a way that respects the *Canadian Charter of Rights and Freedoms.*

Ministerial Oversight

Two ministers in particular have important responsibilities related to national security and intelligence gathering:

- The Minister of Public Safety and Emergency Preparedness is responsible for the Canadian Border Services Agency (CBSA), the Canadian Security Intelligence Service (CSIS), the Royal Canadian Mounted Police (RCMP) and Public Safety Canada.

- The Minister of National Defence is responsible for the Communications Security Establishment (CSE), the Department of National Defence and the Canadian Armed Forces.

The Ministers are directly accountable to Parliament for the activities of their agencies.

The Judiciary

Courts play an important role in our national security.

For example, they rule on whether a warrant will be issued to allow the use of intrusive powers to investigate a threat. That's one way of ensuring that our security efforts respect the *Charter.*

The courts also examine and judge whether the methods used to secure arrests and prosecutions were justifiable and proper. And they have the

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

authority to provide remedies to any citizen who complains of law enforcement misconduct.

Independent Review

There are independent, non-partisan review bodies that scrutinize the activities of certain government agencies. Their task is straightforward: to ensure that our national security and intelligence agencies operate:

- within the law; and
- respecting the directions set out by their Ministers.

There are three such review bodies:

- The Civilian Review and Complaints Commission (CRCC), which is responsible for reviewing the RCMP;

- The Security Intelligence Review Committee (SIRC), which reviews CSIS;

- The Office of the Communications Security Establishment Commissioner (OCSEC), which reviews the CSE.

All three review bodies have a mandate to review activities and hear complaints. Each produces an annual public report that summarizes its activities.

Parliament

Parliament holds Ministers to account for the actions of the agencies they oversee. It also considers and debates legislation on national security matters.

House of Commons and Senate committees can also examine policy issues related to national security, and conduct studies of government activities and existing legislation.

Currently, most Parliamentarians do not have access to classified information, which limits their ability to fully examine national security issues. The government has therefore committed to creating a new national security and

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

intelligence committee made up of Parliamentarians who will be given broad access to classified material.

Agents of Parliament

Certain so-called "agents of Parliament" have the authority to scrutinize national security activities.

The Privacy Commissioner, for instance, can examine how personal information is handled. The Information Commissioner can investigate complaints regarding access to information requests. And the Auditor General can conduct "value-for-money" audits on national security programs.

Commissions of Inquiry

Commissions can be established to impartially investigate issues of national importance. Over the past decade, three separate Commissions of Inquiry have examined certain national security agencies and offered recommendations in the public interest.

What Do You Think?

Should review bodies have even greater powers?

Should agencies such as the CBSA be subjected to this kind of independent review?

Does the establishment of a committee of Parliamentarians – with access to classified material – mean there is no need to create an independent review body to examine national security activities across government (an idea currently under consideration)?

These questions are a starting point. We want to know your thoughts on how best to ensure our national security agencies remain accountable.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

PREVENTION

In recent years, we have all become familiar with the concept of "radicalization to violence." It's a process whereby a person or group of people adopt a belief or ideological position that moves them toward extremism and, ultimately, to terrorist activity.

It is not a crime to be a radical, nor to have radical thoughts or ideas. But as a society, our goal must be to prevent violence committed in the name of radical ideologies or beliefs.

To do this, we must better understand how and why the terrorist impulse takes root. And we must ask ourselves: What more can we do to prevent people from becoming radicalized to violence?

What plays a role?

Here's what we know:

- Radicalization to violence is often driven by "narratives" that reduce global events to a few simplistic ideas.
- It frequently takes place within networks and communities, both physical and virtual (the Internet often plays an critical role).
- Radicalization can be incited by friends, mentors or other influential individuals.
- Association with radicalized people can influence others to adopt a similar perspective.

What are we currently doing?

There is a role to be played by a number of people and agencies in identifying and steering at-risk individuals off the path to radicalization:

- The RCMP trains officers on how to recognize early warning signs of radicalization. It also leads interventions in an effort to divert those on the path to violence.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Correctional Services Canada conducts tailored interventions for individuals in prison who have radicalized to violence, or are at risk of doing so.

- Family members and friends of at-risk individuals are often the first ones aware of radicalization to violence – and may be in the best position to steer these individuals off the path of potential terrorist activity.

What more can we do?

The Government is dedicating $35 million over five years to create an office for community outreach and countering radicalization to violence.

Activities to be supported by this office could include:

- *Working with Communities.* Early intervention programs run by local leaders can be an effective way of preventing radicalization to violence.

- *Youth Engagement.* Given that radicalization to violence is disproportionately common among young people, it is important to provide tailored outreach that can steer at-risk youth off the path that could lead to terrorist activity.

- *Alternative Narratives.* Promoting positive narratives through credible voices is one way to counter the influence of violent, radical messages.

- *Emerging Research.* By engaging academics, think tanks and other Canadians, we can collect best practices and ensure the most effective tactics are being used to counter radicalization to violence. Knowing what works will help inform future policy in this area.

What do you think?

What role should the government play in actively countering radicalization to violence?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

How should the government engage with communities as we work to protect security and improve prevention efforts?

How should we prioritize funding for efforts to counter radicalization to violence?

What are the most effective ways to counteract the negative ideologies?

These questions are a starting point. We want to know your thoughts on how best to prevent the radicalization to violence in Canada – and which programs the new office should pursue.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

THREAT REDUCTION

Here's how our system has worked for the past 30 years:

- The Canadian Security Intelligence Service collects intelligence on potential threats to the security of Canada and Canadians, at home and abroad.

- CSIS advises other agencies of government – law enforcement, for example – about the threats.

- These agencies act on the information.

When Bill C-51 (the *Anti-terrorism Act, 2015*) was passed, CSIS was given a new mandate to reduce threats to the security of Canada.

CSIS can now do more than simply share information about a threat – it can take direct action to reduce the danger. This is known as "threat reduction," or "disruption."

CSIS can't arrest people. But it now has the authority to take timely action to reduce a threat – disrupting financial transactions, for instance, or interfering with terrorist communications.

Depending on the actions it plans to take, CSIS may require a warrant to proceed, especially if the measures would potentially affect the rights of Canadians as enshrined in the *Charter*.

It is important to recognize that the *Charter* itself declares that our rights and freedoms may at times be justifiably limited. For example, traditional wiretap and search warrants justifiably infringe on a person's privacy rights.

That said, threat reduction warrants can limit the full range of *Charter* rights, not just privacy rights.

What do you think?

What scope should CSIS have to limit or reduce the threats it identifies through intelligence gathering?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Should additional safeguards be put in place to ensure that CSIS makes responsible use of its threat reduction powers?

These questions are a starting point. We want to know your thoughts on CSIS's new mandate for threat reduction.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

DOMESTIC NATIONAL SECURITY INFORMATION SHARING

National security threats can emerge and evolve quickly. Intelligence must be gathered and shared among government agencies to ensure a full understanding of a potential threat.

There are rules in place that affect government's ability to share information, especially information about individuals. This is to ensure that privacy rights are protected.

However, these rules are complex. It is sometimes difficult for one agency to know whether it can share information with another agency. This can affect our awareness of, and response to, an emerging national security threat.

Here's some important background: Under the *Privacy Act*, the personal information of Canadians is protected. Government must follow rules on how to collect, retain and disclose this information. But there are some exceptions that allow government to share information in certain instances, especially as it relates to national security.

For example, the Department of Immigration, Refugees and Citizenship Canada will share with CSIS some personal information of applicants for permanent resident status in our country. This allows for a more efficient and effective method of security screening.

The Security of Canada Information Sharing Act

When Bill C-51(the *Anti-terrorism Act, 2015*) was passed, a new process was established for national security information sharing. It provides greater clarity about when information can be disclosed.

The Security of Canada Information Sharing Act (SCISA) gives all federal institutions the power to disclose information related to "activities that undermine the security of Canada." Importantly, this does not include activities such as lawful protest, advocacy or dissent. Information about these activities cannot be disclosed under the SCISA.

Another important fact: Information sharing practices under the SCISA can be reviewed. For instance, the Privacy Commissioner can examine the handling

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

of personal information to hold institutions accountable and ensure *Charter* rights have been respected.

What do you think?

Is there more the government can do to reinforce the fact that lawful protest and advocacy is permitted and do not fall with the definition of "activity that undermines the security of Canada?"

Should the Privacy Commissioner be mandated to deliver an annual public report on information disclosed under the SCISA?

These questions are a starting point. We want to know your thoughts on how information is shared under the Security of Canada Information Sharing Act.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

THE PASSENGER PROTECT PROGRAM

Protecting air travelers is a key responsibility of government. We must also confront the threat posed by individuals who travel abroad – to countries such as Syria and Iraq – to engage in acts of terrorism.

These individuals can be involved in training, fundraising and other activities on behalf of terrorist groups such as the Islamic State in Iraq and the Levant (ISIL). There is also the risk that, upon returning to Canada, these people may launch or inspire attacks here.

Under the new Secure Air Travel Act (SATA), which came into being with the passage of Bill C-51, government can use the Passenger Protect Program (PPP) – an air passenger identity screening program – to identify individuals who pose a threat to transportation security or are seeking to travel to commit terrorism offences.

These people are placed on what's known with government as "the SATA list" – but is perhaps better understood as a "No Fly List."

Individuals on this list are denied the right to board an aircraft – or forced to undergo additional screening. The listing process is conducted confidentially and is based on intelligence and other information from investigations. The list is reviewed every 90 days to ensure there are still reasonable grounds to suspect an individual.

Anyone who is denied the right to board an aircraft has the right to apply to be removed from the No Fly List and, if unsuccessful, to appeal the decision to the Federal Court.

False positive matches sometimes occur. This can result in air travel delays. The government has made a commitment to enhance the current redress process and make it more reliable and efficient.

What do you think?

We want to know your thoughts on how the No Fly List list is managed, and what more can be done to mitigate the impact of false matches.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

CRIMINAL CODE TERRORISM MEASURES

Since 2001, a number of people have been convicted of terrorism offences in Canada. Some have received life sentences. Our *Criminal Code* sets out a range of anti-terrorism powers for law enforcement and lists a range of terrorism-related offences.

With the *Anti-terrorism Act, 2015*, the *Criminal Code* was amended to:

- make it easier to temporarily detain an individual to prevent the carrying out of terrorist activity;
- make it a crime to advocate or promote a terrorist act;
- give courts the power to order the seizure and forfeiture of terrorist propaganda;
- give additional protection to witnesses and other participants in national security proceedings.

Let's look at each of these amendments, one by one.

Temporary Detention

Generally, Canadian criminal law focuses on the prosecution of offences that have already taken place. But courts can also impose what are known as "preventative conditions" on an individual, so long as there is evidence that the person is likely to commit an offence.

When it comes to potential terrorism, courts have two tools at their disposal:

- **Recognizance with conditions**, which allows police to intervene when an individual is suspected of being connected in some way to terrorist activity.
- A **terrorism peace bond**, which is used to prevent an individual from committing a specific terrorism offence, such as leaving Canada to commit an offence for a terrorist group.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

With the passage of Bill C-51, it became easier for police to apply for, and use, these two tools.

For example, the threshold to obtain a **recognizance with conditions** was lowered to apply to instances in which law enforcement officials believe terrorist activity "may be carried out" – rather than the previous "will be carried out."

And a **terrorism peace bond** can now be issued where law enforcement believes an individual "may commit" a terrorism offence – rather than "will commit."

People who are subject to **recognizance with conditions** or a **terrorism peace bond** face the possibility of detention and other restrictions on their liberty, without having been charged with, or convicted of, an offence.

Promotion of Terrorism

It is now a criminal offence for a person to knowingly advocate the commission of terrorist acts in general. The individual *must know* that an offence will be committed or *be reckless* as to whether an offence may be committed as a result of what they say or write.

The maximum penalty is five years' imprisonment.

It is important to note that this offence is directed exclusively at prohibiting the *active encouragement* of the *commission of terrorism offences.* It's not about mere expressions of opinion regarding the acceptability of terrorism.

Seizure and forfeiture of terrorist propaganda

There are two new warrants in the *Criminal Code* that allow police to seize terrorist propaganda. This is material that encourages the commission of a specific terrorist act, or terrorist offences in general. This material can be in printed or audio form, or it can be in electronic form on the Internet.

Protection of witnesses and other participants in the justice system

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Under the *Anti-terrorism Act, 2015*, enhanced measures are now available to protect witnesses and other participants in terrorism-related proceedings.

For example, judges can now order that witnesses testify behind a screen to conceal their identity, or use a pseudonym, or wear a disguise. And there are broader instances under which charges can be laid against those who attempt to intimidate justice system participants.

What do you think?

Should it be harder or easier to obtain **recognizance with conditions** or a **terrorism peace bond**?

Should those who use propaganda to promote terrorism offences in general be charged with a crime?

These questions are a starting point. We want to know your thoughts on anti-terrorism measures as included in the *Criminal Code*.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

TERRORIST ENTITY LISTING PROCEDURES

Formally listing an individual or group as a "terrorist entity" is a way of curtailing their support and publicizing their involvement with terrorism.

Right now, there are three ways a terrorist entry may be listed in Canada. The most common method is available through the *Criminal Code.* A group listed as a terrorist entity under the *Criminal Code* has its funds immediately frozen, and potentially seized and forfeited.

There are currently more than 50 terrorist entities who have been listed in this way. They include al-Qaida, the Taliban, ISIL, Boko Haram and more.

How does a group get listed?

It begins with an investigation by RCMP or CSIS. The Minister of Public Safety and Emergency Preparedness may then recommend to Cabinet that the entity be listed, so long as there are reasonable grounds to believe that the group:

- knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity; or

- is knowingly acting on behalf of, at the direction of, or in association with an entity that has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity.

Many of Canada's closest allies keep similar lists of terrorist entities.

What do you think?

How does the current process of listing terrorist entities help Canada meet its domestic needs and international obligations?

Most listed entities are groups that originated overseas. How should Canada focus its listing activities in the future?

These questions are a starting point. We want to know your thoughts on the formal listing of terrorist groups and individuals.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

TERRORIST FINANCING

Terrorist entities raise, collect and transfer funds all over the world to finance their attacks and support their day-to-day operations. They make use of everything from the formal banking system to money service outlets to the physical transfer of gold.

Individuals also finance terrorist activities by raising money on their own behalf to travel abroad for terrorist purposes, or to purchase materials for an attack.

Funds are vital to these organizations. It is therefore important that we deprive them of the money they need to plan and conduct their activities.

This is a goal shared by countries around the world. For example, one of the five priorities of the Global Coalition against ISIL is to diminish the group's capabilities by cutting off its funding.

Canada's approach to cutting off funds to terrorist groups involves 11 departments and agencies. Additionally, financial service providers – such as banks – have an obligation to know their customers and report transactions over $10,000 to help identify money laundering and terrorist financing.

Law enforcement and intelligence agencies can use this information to assist in their efforts to identify and disrupt terrorist activities.

Looking beyond our borders, Canada is an active member of the Financial Action Task Force, an international organization that sets standards in the fight against money laundering and terrorist financing. We also support developing regions that are at a high risk for terrorist financing, helping countries in the Middle East and North Africa maintain the integrity of their financial system.

A challenge faced by Canada and other advanced nations is the pace of evolution within the financial sector. It can be difficult to keep up to date as financial technology advances and new platforms for terrorist financing emerge.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Another challenge: Terrorist supporters often transfer funds below the $10,000 threshold, which means the financing goes unreported.

This is one of the ways in which terrorists exploit gaps to avoid detection.

What do you think?

What changes could be made to ensure counter-terrorist financing measures are more effective?

What additional measures could the government undertake to improve its ability to cut off terrorist financing?

These questions are a starting point. We want to know your thoughts on how terrorist financing should be further curtailed.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

INVESTIGATIVE CAPABILITIES IN A DIGITAL WORLD

We live in a highly networked world where technological innovation is always forging ahead, bringing great advancements to our quality of life but also evolving threats to our security.

The same technologies we enjoy and rely on everyday – smartphones, laptop computers and the like – can be exploited by terrorists to coordinate, finance and conduct their attacks.

Digital devices allow terrorists to buy equipment, send encrypted messages and radicalize individuals to violence.

Our national intelligence investigators must therefore be able to work as effectively in the digital world as they do in the physical world.

To make that possible, we need to ensure that our laws for the collection of intelligence and evidence keep up with the pace of technology. For instance, our current investigative capability can be impeded by:

- lack of consistent and timely access to basic subscriber information, to help identify the subscriber to a communications service;
- lack of reliable technical intercept capability on domestic telecommunications networks;
- diminished ability to investigate due to the use of advanced encryption;
- lack of consistent retention of communication data.

Let's look more closely at each of these four challenges:

Basic subscriber information. This is a way for law enforcement officials to use a communications subscription (to an Internet provider, for instance) to identify an otherwise anonymous individual. But court rulings have made it difficult to access this information in a timely and effective manner. Many countries allow police and intelligence agencies to access basic subscriber information without going to court.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Intercept capability. Investigations into national security threats can be strengthened by the interception of private communications (with court approval). However, some communications providers are unable to comply with these court orders because they lack the technical ability to intercept communications. Investigators can therefore miss out on key evidence.

Encryption. Encryption technology gives terrorists an additional way to avoid discovery, investigation and prosecution. Often, even when law enforcement is able to intercept communications, the messages are protected and unreadable. Currently, there is no way to force a person or organization to decrypt their communications.

Data retention. This term refers to the storage of telecommunication information – keeping track of which telephone numbers a person dialed, for instance, or how long the calls lasted. Phone and Internet data of this kind can be useful in intelligence and evidence gathering.

However, there is currently no widespread requirement for communications providers to retain this information. Some delete it very quickly.

The government recently enacted what's known as "preservation" powers in the *Criminal Code*. This gives law enforcement the power to seek a court order to preserve specific computer data belonging to a specific person, for a brief period of time to help with an investigation.

These and other challenges can be amplified by the fact that cyberspace is not easily bound by national borders. Communications service providers may offer services in Canada – but may have no business presence here, and therefore may fall beyond the reach of Canadian law.

What do you think?

How can Canada address the challenges posed by the rapidly evolving technological landscape in a manner that respects privacy rights and is consistent with Canadian values?

Should our expectation of privacy be different in the digital world?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Should Canada compel communications providers to have interception capability on their networks, as is the case in the United States, United Kingdom, Australia and other countries?

Should investigators have the power to compel individuals or companies to assist in decrypting messages?

Should service providers be required by law to keep phone and Internet data for a fixed period of time to potentially aid in criminal and terrorism investigations?

These questions are a starting point. We want to know your thoughts on how best to enhance our digital investigative capabilities.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

INTELLIGENCE AND EVIDENCE

We all want to ensure that Canada's national security information is protected. Indeed, the government has an obligation to protect sensitive sources, capabilities and techniques. At the same time, there are instances in which this information may be required for a legal proceeding.

There is an existing framework that governs the use of national security information in a range of legal proceedings. In essence, a federal judge must decide whether disclosure of the information would hurt our international relations, national security or national defence. If so, the judge must then consider whether the public interest in disclosing the information outweighs the public interest in keeping it protected.

Sometimes, this means that a criminal court may be unable to hear the national security information – and may need to rely on an unclassified summary instead. Or it could be the case that, in a civil proceeding, a plaintiff may not have full access to the information required to make its case – or a defendant may be unable to fully defend itself. This raises the question of whether justice can truly be served in these examples.

There are also implications relating to immigration decisions, which are sometimes made based on classified information. A good example is the so-called "security certificate proceeding," in which government makes the case that a person is inadmissible to Canada for reasons of security, violation of human or international rights, serious criminality or organized criminality.

In this case, a federal judge rules on whether the certificate is reasonable.

What do you think?

How can the government ensure an appropriate balance between protecting national security and respecting the principles of justice?

How do we properly balance the accused's right to know the source of the case against him?

Are we currently assuring both fairness and security in legal proceedings that involve classified material?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Are there any non-legislative measures that could improve both the use and protection of national security information in legal proceedings?

These questions are simply a starting point. We want to know your thoughts on how to navigate the challenging terrain of intelligence and evidence.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

CONCLUSION

We invite all Canadians to consider the questions raised in this discussion paper – and to read the longer and more comprehensive version of the Counter-Terrorism Green Paper, which includes greater detail and a number of scenarios that help to illustrate what's at stake as we work to improve our security and intelligence framework.

Most of all, we encourage Canadians to let their opinions, ideas and potential solutions be heard.

Invariably, views will differ. Not all of us will share the same perspective on what is justified and what is reasonable. There will be strong opinions on which tools should be made available to government and its security and intelligence agencies.

But that's what we want. We want to hear your views, and the views of your fellow Canadians.

We want to carefully consider the impact of each potential measure as we work to make meaningful and long-lasting improvements to Canada's counter-terrorism efforts.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Dunne, Thomas (IC) <thomas.dunne@canada.ca>
Sent: 2016-May-02 3:25 PM
To: Audcent, Karen; Oakes, Lindsey (PS/SP)
Cc: Wong, Normand; Angers, Lucie; Sansom, Gareth; Adamowski, Andrew (PS/SP); Taschereau, Rodrigue (PS/SP); Wallace, Bruce (IC); Foley, Lisa (IC); De Santis, Michael (IC); Dunne, Thomas (IC)
Subject: RE: Encryption Annex
Attachments: SITT-STIT-#674274-v2-ENC_Annex.DOCX

Some comments and notes on the encryption annex, attached.

Thanks,
Thomas

Thomas Dunne

Manager, Digital Policy Branch
Innovation, Science and Economic Development Canada / Government of Canada
Thomas.Dunne@canada.ca / Tel: 613-608-6067 / TTY: 1-866-694-8389

Gestionairre, Direction générale des politiques numériques
Innovation, Sciences et Développement économique Canada / Gouvernement du Canada
Thomas.Dunne@canada.ca / Tél: 613-608-6067 / ATS: 1-866-694-8389

From: Audcent, Karen [mailto:Karen.Audcent@justice.gc.ca]
Sent: April-25-16 4:41 PM
To: Oakes, Lindsey (PS/SP); Dunne, Thomas (IC)
Cc: Wong, Normand; Angers, Lucie; Sansom, Gareth; Adamowski, Andrew (PS/SP); Taschereau, Rodrigue (PS/SP); Wallace, Bruce (IC); Foley, Lisa (IC); De Santis, Michael (IC)
Subject: Encryption Annex

Thanks for this Lindsey, looks good, as discussed I have made some suggestions in the attached in track changes. Karen

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

ANNEX 3

Encryption

INTRODUCTION

Cryptography is the practice and study of techniques for communication. One of the main fields in cryptography is encryption which converts a readable message into an unreadable encrypted message. Encryption is central to electronic commerce, banking, cybersecurity, data and intellectual property protection. However, this same technology that brings many benefits is also used to conceal criminal activities. The use of encryption technologies has grown tremendously in both availability and use with the growth of the internet. Encryption plays an important role as it allows users to authenticate and safeguard sensitive data, and other information stored on computers or transmitted over closed or public networks.

Law enforcement and national security agencies' concern relative to encryption is primarily that investigative techniques employed, under judicial authority, to obtain information, including interception of private communications (wiretap), production orders, and search warrants, can be made ineffective by the use of encryption. Encryption can be used by criminals or terrorists to prevent an investigation from being able to make heads or tails of the information obtained, which is needed to solve a crime.

Although encryption can pose a significant challenge to law enforcement, this issue hast not been directly addressed in law in Canada, In trying to address the challenges faced by law enforcement and national security agencies, some of the issues ~~are~~ raised are relative to: human rights, jurisdiction, and the essential need for encryption to enable modern e-commerce, e-banking and all types of cybersecurity and critical infrastructure. These issues, along with others will be discussed further in this annex.

The *Canadian Charter of Rights and Freedoms*, under sections 1, 8 and 24, ~~which allows~~ sets out the basic constitutional principles in Canada that lawful access must be "reasonable" and "justifiable" in a free and democratic society.

s.21(1)(a)

TYPES OF ENCRYPTION

Encryption is technology that can be applied to data-in-use, data-in-motion and data-at-rest. Any of these could have various layers of encryption applied to it by any or all of the following: the end user, third party applications, and telecommunication service providers.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Data-in-use, otherwise known as active data, is data that is live and under constant change and manipulation by an application. Data-in-use is physically stored in databases, data warehouses, spreadsheets, etc. Data-in-motion is data that is currently in transit over some type of network or temporarily residing in computer memory. Data-at-rest is inactive data stored physically in databases, data warehouses, spreadsheets, archives, hard drives, tapes, off-site backups, mobile devices, etc.

In addition, encryption can be applied to more specific items such as the message itself (i.e. email, text message, or photo), the device (i.e. the cell phone, the computer, the tablet), or the transmission network and/or channel (i.e. the communication service provider network).

[redacted]

POLICY AND LEGISLATION

THE GOVERNMENT OF CANADA'S ELECTRONIC COMMERCE STRATEGY & THE POLICY ON ~~1998~~ CRYPTOGRAPHY ~~POLICY~~)

An extensive review of Canada's Cryptography policy was undertaken in 1997-1998 under the leadership of Industry Canada (now Innovation, Science, and Economic Development Canada) in the context of Canada's e-commerce policy but extended to the issues of law enforcement access and national security considerations. In 1998, Canada announced its Cryptography policy which remains in place today.

A number of key considerations played a role in helping shape Canada's Cryptography policy. The following were some significant developments that helped guide the policy development process:

- The increasing use of strong encryption software and computers powerful enough to encrypt and decrypt data easily are commonly available;
- The rapidly increasing use of telecommunications media suitable for encryption (e.g. email and other data conveyed via the Internet and other computer-based media) for both personal and commercial communications;
- The increasing use of wireless cellular telephones, which has created pressure for the development of digital equipment and lead to the encryption of their signals in some cases; and
- The increasing reliance on computers and computer networks for commercial activities and the need to protect privacy and security, which has led companies to store business records in secure computer facilities and in encrypted forms.

s.21(1)(a)

Notably ~~Interestingly~~, many of these developments are still relevant today given the proliferation of and reliance on the use of technology, encryption and digital communications. Both then, and now, encryption forms part of the core framework that allows electronic commerce to flourish.

In an effort to develop a cryptography framework [redacted] To date, these remain ~~to be~~ some of the key considerations [redacted]

[redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Electronic Commerce

In 1998, more and more transactions were shifting from closed networks to open networks and cryptography became essential for the conduct of electronic commerce. Open networks allowed for more global trading, but came with a variety of security challenges including concerns over the authentication of communicating parties, the integrity of the data being communicated, the confidentiality of the proprietary or personal data, and the assurance that transactions have been authorized by legitimate users. Without cryptography, these challenges may not have been addressed. Also, cryptography increased the competitiveness of businesses and provided opportunities for job creation and industrial growth.

The aims of law enforcement and business align when cryptography protects proprietary information, trade secrets, and in general, helps defend industry and consumers against fraud and other unlawful activities. In addition, cryptography meets national objectives to the extent that it helps protect sovereignty, national infrastructures, and their valuable information.

The policy challenge was, and continues to be, the need to find solutions that will limit [redacted] with legitimate business, institutional or individual interests. [redacted]

s.21(1)(a)

[redacted] personal and commercial communications and the overall increase in the use of technology, [redacted] ~~generated~~ new forms of criminal activity, new methods of committing old crimes, and new ways of concealing evidence. The widespread use of cryptography can raise~~d~~ concerns in this context because it can create~~d~~ ~~significant~~ obstacles to the detection and investigation of criminal activities and security threats, as well as the inspection of computer records [redacted] Agencies that play ~~a~~ key role~~s~~ in law enforcement, national security, and regulatory compliance investigations include the RCMP, provincial and local police forces, the Canadian Security Intelligence Service, the Canadian Revenue Agency (taxation, customs and excise), the federal Competition Bureau, as well as federal and provincial environmental enforcement agencies. These agencies are responsible for identifying threats and detecting, investigating and prosecuting matters ~~ranging from~~ related to terrorism, crimes of violence and related to property, ~~crimes to~~ and abuses of domestic and international commercial and financial systems.

The effectiveness of these agencies in monitoring criminal activities, and in investigating and prosecuting offenders has depended on their ability to conduct electronic surveillance of

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

communications and to search and inspect places, including computers, where relevant information may be kept. [redacted]

Formatted: Font: Italic

[redacted]

Formatted: Font: Italic

The increase in the use of strong cryptography [redacted] technical protection for confidential information, [redacted] it can also impede [redacted] lawful and authorized electronic surveillance. Notwithstanding the receipt of [redacted] judicial authorizations [redacted] for the interception of communications, intercepted [redacted] data in an encrypted form may [redacted] be unreadable and undecipherable for authorities. This creates two challenges: (1) it becomes difficult or impossible to determine whether the information being intercepted fallsell within the scope of the legal authorization to intercept it; and (2) it becomes difficult for authorities to decipher the information, or to do so in time to be able to effectively use it or take action to prevent harm from occurring.

s.21(1)(a)

[redacted]

Commented [DTD7]: These read to me like the same challenge.

LThe law enforcement, regulatory and national security agencies [redacted] are challenged to [redacted] effectively respond and adhere to their individual mandates in the face of undecipherable encrypted communications, and ; the agencies involved require some means whereby encrypted data can be decrypted and read within a reasonable time and at a reasonable expenditure of resources.

[redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.21(1)(a)

Human rights and civil liberties

[redacted]

Formatted: Heading 3

~~t~~The rights of Canadians to ~~some degree of~~ privacy and to express themselves freely are constitutionally protected. Section 8 of the *Charter* guarantees Canadians the right to be free from "unreasonable search or seizure" which has been interpreted through jurisprudence as

Formatted: Font: Italic

[redacted]

Formatted: Font: Italic

Formatted: Font: Italic

freedom of expression may extend to both the production of cryptographic products and their use to protect the messages being expressed or data being stored. [redacted] ~~absolute~~. Invasions of privacy, including the seizure of data or interception of communications, must be justified, [redacted]

[redacted]

[redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

[redacted]trong cryptography products are difficult to "break", and success with a ~~A short of a~~ "brute force" attack by powerful computers is only feasible in some cases, as the computing time required may be prohibitive, depending on the strength of the encryption, and the strength of the computer attempting the brute force attack. [redacted]

s.21(1)(a)

[redacted]

[redacted]

The 1998 Policy

After careful study, the 1998 Cryptography policy was announced by the Canadian Minister of Industry in the context of e-commerce. In this policy, the Government affirmed the following principles:

1) The freedom of Canadians to develop, import and use whatever cryptography they wished;
2) Support for private sector research and development
3) It was decided that the Government would not implement mandatory key recovery requirements or licensing regimes for certification authorities or trusted third parties;
4) Export controls would continue to be consistent with Canada's international obligations; and
5) The Government would explore legislative and other options to protect consumer privacy and to assist law enforcement and national security agencies.

The policy emphasized the importance of maintaining a balanced approach to a complex problem.

WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Canada is one of 33 signatories to the Wassenaar Arrangement which was established to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies (such as encryption software). Participating states seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities. The aim is also to prevent the acquisition of these items by terrorists.

Participating States control all items set forth in the List of Dual-Use Goods and Technologies and Munitions list, with the objective of preventing unauthorized transfers or re-transfers of those items. Items included on the lists focus on items designed for military use, and general technology and software notes (i.e. encryption software).

The participating states have an agreement to maintain national export controls on listed items, which are implemented via national legislation; are guided by agreed upon best practices, guidelines or elements; have agreed to report on transfers and denials of specific controlled items to destinations outside of the arrangement; and exchange information on sensitive dual-use goods and technologies.

s.23

[redacted]

BILL C-30 – PROTECTING CHILDREN FROM INTERNET PREDATORS ACT, 2012

In the past, in the context of work on lawful access issues, and most recently in former Bill C-30 (*Protecting Children from Internet Predators Act*, 2012, 41st Parliament, 1st session), legislative proposals were introduced to create requirements for telecommunications service providers to decrypt communications where it was readily possible for the service provide to do so, in the context of lawful interception. However, telecommunications service providers were not required to develop specific decryption techniques themselves.

For example, if interception was successful but the data retrieved was encrypted by a tool that was implemented directly by the service provider, rather than the user, then the service provider would be asked to decrypt the data.

These proposals were supported by law enforcement. However, in the larger picture, these proposals would not have solved the problem posed by encryption in whole. This is particularly true given that many major IT companies have built mobile and other digital devices that enable individuals to encrypt and decrypt data at the user level.

Jurisdictional and International Challenges

[redacted] Law enforcement and national security agencies can face other challenges when attempting to ~~making attempts to~~ compel communication service providers to [redacted] communications, as ~~are~~ the international nature of the software market and the borderless nature of cyberspace, in addition to the locations (jurisdiction) of the communications service provider [redacted] In addition, m~~M~~any communication service providers, particularly software and application service providers, do not

s.21(1)(a)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

have physical premises in Canada, and may not be subject to Canadian jurisdiction. In order to be able to obtain information held by these companies, currently the process available is through the use of Mutual Legal Assistance Treaties (MLATs). Currently MLAT processes are not always timely enough for the exigencies of investigations involving electronic evidence, nor were they designed for a high volume of requests that could ensue given the trend toward global inter-connectivity and challenges in relation to jurisdiction in the context of modern communications.

s.21(1)(a)

There is also some concern about setting a precedent in accessing encrypted data. If western Governments (such as the US and Canada) demand companies create backdoors into products and services, there is a concern that more authoritarian regimes or governments will insist on having access to these same capabilities. This may mean that the more authoritarian regimes may use these capabilities to monitor and censor the legitimate activities of their citizens in a manner inconsistent with Canadian values, such as free expression and privacy, rather than focusing on ~~just~~ accessing information believed to be related to criminal activity and threats to national security in a specific and targeted way, with court oversight, as is done in Canada and in other countries with similar values and systems.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Audcent, Karen
Sent: 2016-May-02 4:36 PM
To: 'Dunne, Thomas (IC)'; Oakes, Lindsey (PS/SP)
Cc: Wong, Normand; Angers, Lucie; Sansom, Gareth; Adamowski, Andrew (PS/SP); Taschereau, Rodrigue (PS/SP); Wallace, Bruce (IC); Foley, Lisa (IC); De Santis, Michael (IC)
Subject: RE: Encryption Annex
Attachments: Encryption v3.DOCX

Attached version includes my annotations to Thomas' changes, and some replies to some of his comments and questions. Hope this is helpful. Karen

---

From: Dunne, Thomas (IC) [mailto:thomas.dunne@canada.ca]
Sent: 2016-May-02 3:25 PM
To: Audcent, Karen; Oakes, Lindsey (PS/SP)
Cc: Wong, Normand; Angers, Lucie; Sansom, Gareth; Adamowski, Andrew (PS/SP); Taschereau, Rodrigue (PS/SP); Wallace, Bruce (IC); Foley, Lisa (IC); De Santis, Michael (IC); Dunne, Thomas (IC)
Subject: RE: Encryption Annex

Some comments and notes on the encryption annex, attached.

Thanks,
Thomas

Thomas Dunne

Manager, Digital Policy Branch
Innovation, Science and Economic Development Canada / Government of Canada
Thomas.Dunne@canada.ca / Tel: 613-608-6067 / TTY: 1-866-694-8389

Gestionairre, Direction générale des politiques numériques
Innovation, Sciences et Développement économique Canada / Gouvernement du Canada
Thomas.Dunne@canada.ca / Tél: 613-608-6067 / ATS: 1-866-694-8389

From: Audcent, Karen [mailto:Karen.Audcent@justice.gc.ca]
Sent: April-25-16 4:41 PM
To: Oakes, Lindsey (PS/SP); Dunne, Thomas (IC)
Cc: Wong, Normand; Angers, Lucie; Sansom, Gareth; Adamowski, Andrew (PS/SP); Taschereau, Rodrigue (PS/SP); Wallace, Bruce (IC); Foley, Lisa (IC); De Santis, Michael (IC)
Subject: Encryption Annex

Thanks for this Lindsey, looks good, as discussed I have made some suggestions in the attached in track changes. Karen

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

DRAFT

ANNEX 3

Encryption

INTRODUCTION

Cryptography is the practice and study of techniques for communication. One of the main fields in cryptography is encryption which converts a readable message into an unreadable encrypted message. Encryption is central to electronic commerce, banking, cybersecurity, data and intellectual property protection. However, this same technology that brings many benefits is also used to conceal criminal activities. The use of encryption technologies has grown tremendously in both availability and use with the growth of the internet. Encryption plays an important role as it allows users to authenticate and safeguard sensitive data, and other information stored on computers or transmitted over closed or public networks.

Law enforcement and national security agencies' concern relative to encryption is primarily that investigative techniques employed, under judicial authority, to obtain information, including interception of private communications (wiretap), production orders, and search warrants, can be made ineffective by the use of encryption. Encryption can be used by criminals or terrorists to prevent an investigation from being able to make heads or tails of the information obtained, which is needed to solve a crime.

Although encryption can pose a significant challenge to law enforcement, this issue hast not been directly addressed in law in Canada, [redacted] In trying to address the challenges faced by law enforcement and national security agencies, some of the issues ~~are~~ raised are relative to: human rights, jurisdiction, and the essential need for encryption to enable modern e-commerce, e-banking and all types of cybersecurity and critical infrastructure. These issues, along with others will be discussed further in this annex.

s.21(1)(a)

[redacted] The *Canadian Charter of Rights and Freedoms*, under sections 1, 8 and 24, ~~which allows~~ sets out the basic constitutional principles in Canada that lawful access must be [redacted] reasonable" and "justifiable" in a free and democratic society. [redacted]

TYPES OF ENCRYPTION

Encryption is technology that can be applied to data-in-use, data-in-motion and data-at-rest. Any of these could have various layers of encryption applied to it by any ~~either~~ or all of the following: the end user, third party applications, and telecommunication service providers.

[redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Data-in-use, otherwise known as active data, is data that is live and under constant change and manipulation by an application. Data-in-use is physically stored in databases, data warehouses, spreadsheets, etc. Data-in-motion is data that is currently in transit over some type of network or temporarily residing in computer memory. Data-at-rest is inactive data stored physically in databases, data warehouses, spreadsheets, archives, hard drives, tapes, off-site backups, mobile devices, etc.

In addition, encryption can be applied to more specific items such as the message itself (i.e. email, text message, or photo), the device (i.e. the cell phone, the computer, the tablet), or the transmission network and/or channel (i.e. the communication service provider network).

[redacted]

POLICY AND LEGISLATION

THE GOVERNMENT OF CANADA'S ELECTRONIC COMMERCE STRATEGY -& THE POLICY ON ~~1998~~ CRYPTOGRAPHY ~~POLICY~~)

An extensive review of Canada's Cryptography policy was undertaken in 1997-1998 under the leadership of Industry Canada (now Innovation, Science, and Economic Development Canada) in the context of Canada's e-commerce policy but extended to the issues of law enforcement access and national security considerations. In 1998, Canada announced its Cryptography policy which remains in place today.

A number of key considerations played a role in helping shape Canada's Cryptography policy. The following were some significant developments that helped guide the policy development process:

s.21(1)(a)

- The increasing use of strong encryption software and computers powerful enough to encrypt and decrypt data easily are commonly available;
- The rapidly increasing use of telecommunications media suitable for encryption (e.g. email and other data conveyed via the Internet and other computer-based media) for both personal and commercial communications;
- The increasing use of wireless cellular telephones, which has created pressure for the development of digital equipment and lead to the encryption of their signals in some cases; and
- The increasing reliance on computers and computer networks for commercial activities and the need to protect privacy and security, which has led companies to store business records in secure computer facilities and in encrypted forms.

Notably ~~Interestingly~~, many of these developments are still relevant today given the proliferation of and reliance on the use of technology, encryption and digital communications. Both then, and now, encryption forms part of the core framework that allows electronic commerce to flourish.

In an effort to develop a cryptography framework, [redacted] To date, these remain ~~to be~~ some of the key considerations [redacted]

[redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Electronic Commerce

In 1998, more and more transactions were shifting from closed networks to open networks and cryptography became essential for the conduct of electronic commerce. Open networks allowed for more global trading, but came with a variety of security challenges including concerns over the authentication of communicating parties, the integrity of the data being communicated, the confidentiality of the proprietary or personal data, and the assurance that transactions have been authorized by legitimate users. Without cryptography, these challenges may not have been addressed. Also, cryptography increased the competitiveness of businesses and provided opportunities for job creation and industrial growth.

The aims of law enforcement and business align when cryptography protects proprietary information, trade secrets, and in general, helps defend industry and consumers against fraud and other unlawful activities. In addition, cryptography meets national objectives to the extent that it helps protect sovereignty, national infrastructures, and their valuable information.

The policy challenge was, and continues to be, the need to find solutions that will limit [redacted] with legitimate business, institutional or individual interests. [redacted]

s.21(1)(a)

[redacted] personal and commercial communications and the overall increase in the use of technology [redacted] ~~generated~~ new forms of criminal activity, new methods of committing old crimes, and new ways of concealing evidence. The widespread use of cryptography can raise~~d~~ concerns in this context because it can create~~d~~ ~~significant~~ obstacles to the detection and investigation of criminal activities and security threats, as well as the inspection of computer records [redacted] Agencies that play ~~a~~ key role~~s~~ in law enforcement, national security, and regulatory compliance investigations ~~-~~include the RCMP, provincial and local police forces, the Canadian Security Intelligence Service, the Canadian Revenue Agency (taxation, customs and excise), the federal Competition Bureau, as well as federal and provincial environmental enforcement agencies. These agencies are responsible for, among other things, identifying threats and detecting, investigating and prosecuting matters ~~ranging from~~related to terrorism, crimes of violence and related to property, ~~crimes to~~ and abuses of domestic and international commercial and financial systems.

The effectiveness of these agencies in monitoring criminal activities, and in investigating and prosecuting offenders has depended on their ability to conduct electronic surveillance of

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

communications and to search and inspect places, including computers, where relevant information may be kept. [redacted]

Formatted: Font: Italic

[redacted]

Formatted: Font: Italic

The increase in the use of strong cryptography [redacted] technical protection for confidential information, it can also impede [redacted] the ability to conduct lawful and authorized electronic surveillance. Notwithstanding the receipt of ~~While~~ judicial authorizations [redacted] for the interception of communications, intercepted [redacted] data in an encrypted form may [redacted] be unreadable and undecipherable for authorities. This creates two challenges: (1) it becomes difficult or impossible to determine whether the information being intercepted fallsell within the scope of the legal authorization to intercept it; and (2) it becomes difficult for authorities to decipher the information, or to do so in time to be able to effectively use it or take action to prevent harm from occurring.

s.21(1)(a)

[redacted]

L~~The~~ law enforcement, regulatory and national security agencies [redacted] are challenged to [redacted] effectively respond and adhere to their individual mandates in the face of undecipherable encrypted communications, and ~~the agencies involved~~ require some means whereby encrypted data can be decrypted and read within a reasonable time and at a reasonable expenditure of resources.

[redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Human rights and civil liberties

[redacted]

Formatted: Heading 3

[redacted] The rights of Canadians to ~~some degree of~~ privacy and to express themselves freely are constitutionally protected. Section 8 of the *Charter* guarantees Canadians the right to be free from "unreasonable search or seizure" which has been interpreted through jurisprudence as

Formatted: Font: Italic

[redacted]

Formatted: Font: Italic

Formatted: Font: Italic

freedom of expression may extend to both the production of cryptographic products and their use to protect the messages being expressed or data being stored. [redacted] Invasions of privacy, including the seizure of data or interception of communications, must be justified. [redacted]

[redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

[redacted] ~~speaking,~~ strong cryptography products are difficult to "break~~.~~", and success with a ~~A short of a~~ "brute force" attack by powerful computers is only feasible in some cases, as the computing time required may be prohibitive, depending on the strength of the encryption, and the strength of the computer attempting the brute force attack.

s.21(1)(a)

[redacted]

The 1998 Policy

After careful study, the 1998 Cryptography policy was announced by the Canadian Minister of Industry in the context of e-commerce. In this policy, the Government affirmed the following principles:

1) The freedom of Canadians to develop, import and use whatever cryptography they wished;
2) Support for private sector research and development
3) It was decided that the Government would not implement mandatory key recovery requirements or licensing regimes for certification authorities or trusted third parties;
4) Export controls would continue to be consistent with Canada's international obligations; and
5) The Government would explore legislative and other options to protect consumer privacy and to assist law enforcement and national security agencies.

The policy emphasized the importance of maintaining a balanced approach to a complex problem.

WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Canada is one of 33 signatories to the Wassenaar Arrangement which was established to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies (such as encryption software). Participating states seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities. The aim is also to prevent the acquisition of these items by terrorists.

Participating States control all items set forth in the List of Dual-Use Goods and Technologies and Munitions list, with the objective of preventing unauthorized transfers or re-transfers of those items. Items included on the lists focus on items designed for military use, and general technology and software notes (i.e. encryption software).

The participating states have an agreement to maintain national export controls on listed items, which are implemented via national legislation; are guided by agreed upon best practices, guidelines or elements; have agreed to report on transfers and denials of specific controlled items to destinations outside of the arrangement; and exchange information on sensitive dual-use goods and technologies.

s.23

[redacted]

BILL C-30 – PROTECTING CHILDREN FROM INTERNET PREDATORS ACT, 2012

In the past, in the context of work on lawful access issues, and most recently in former Bill C-30 (*Protecting Children from Internet Predators Act*, 2012, 41st Parliament, 1st session), legislative proposals were introduced to create requirements for telecommunications service providers to decrypt communications where it was readily possible for the service provide to do so, in the context of lawful interception. However, telecommunications service providers were not required to develop specific decryption techniques themselves.

For example, if interception was successful but the data retrieved was encrypted by a tool that was implemented directly by the service provider, rather than the user, then the service provider would be asked to decrypt the data.

These proposals were supported by law enforcement. However, in the larger picture, these proposals would not have solved the problem posed by encryption in whole. This is particularly true given that many major IT companies have built mobile and other digital devices that enable individuals to encrypt and decrypt data at the user level.

Jurisdictional and International Challenges

[redacted] ~~L~~Law enforcement and national security agencies can face other challenges when attempting to [redacted] compel communication service providers to [redacted] communications, as ~~are~~ the international nature of the software market and the borderless nature of cyberspace, in addition to the locations (jurisdiction) of the communications service provider [redacted] communication service providers, particularly software and application service providers, do not

s.21(1)(a)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

have physical premises in Canada, and may not be subject to Canadian jurisdiction. In order to be able to obtain information held by these companies, currently the process available is through the use of Mutual Legal Assistance Treaties (MLATs). Currently MLAT processes are not always timely enough for the exigencies of investigations involving electronic evidence, nor were they designed for a high volume of requests that could ensue given the trend toward global inter-connectivity and challenges in relation to jurisdiction in the context of modern communications.

s.21(1)(a)

There is also some concern about setting a precedent in accessing encrypted data. If western Governments (such as the US and Canada) demand companies create backdoors into products and services, there is a concern that more authoritarian regimes or governments will insist on having access to these~~the~~ same capabilities. This may mean that the more authoritarian regimes may use these capabilities to monitor and censor the legitimate activities of their citizens in a manner inconsistent with Canadian values, such as free expression and privacy, rather than focusing on~~just~~ accessing information believed to be related to criminal activity and threats to national security in a specific and targeted way, with court oversight, as is done in Canada and in other countries with similar values and systems.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Oakes, Lindsey (PS/SP) <lindsey.oakes@canada.ca>
Sent: 2016-May-03 8:47 AM
To: Audcent, Karen; Dunne, Thomas (IC)
Cc: Wong, Normand; Angers, Lucie; Sansom, Gareth; Adamowski, Andrew (PS/SP); Taschereau, Rodrigue (PS/SP); Wallace, Bruce (IC); Foley, Lisa (IC); De Santis, Michael (IC)
Subject: Re: Encryption Annex

Thanks karen and thomas. Much appreciated

Sent from my BlackBerry 10 smartphone on the Rogers network.

From: Audcent, Karen
Sent: Monday, May 2, 2016 4:36 PM
To: Dunne, Thomas (IC); Oakes, Lindsey (PS/SP)
Cc: Wong, Normand; Angers, Lucie; Sansom, Gareth; Adamowski, Andrew (PS/SP); Taschereau, Rodrigue (PS/SP); Wallace, Bruce (IC); Foley, Lisa (IC); De Santis, Michael (IC)
Subject: RE: Encryption Annex

Attached version includes my annotations to Thomas' changes, and some replies to some of his comments and questions. Hope this is helpful. Karen

From: Dunne, Thomas (IC) [mailto:thomas.dunne@canada.ca]
Sent: 2016-May-02 3:25 PM
To: Audcent, Karen; Oakes, Lindsey (PS/SP)
Cc: Wong, Normand; Angers, Lucie; Sansom, Gareth; Adamowski, Andrew (PS/SP); Taschereau, Rodrigue (PS/SP); Wallace, Bruce (IC); Foley, Lisa (IC); De Santis, Michael (IC); Dunne, Thomas (IC)
Subject: RE: Encryption Annex

Some comments and notes on the encryption annex, attached.

Thanks,
Thomas

Thomas Dunne

Manager, Digital Policy Branch
Innovation, Science and Economic Development Canada / Government of Canada
Thomas.Dunne@canada.ca / Tel: 613-608-6067 / TTY: 1-866-694-8389

Gestionairre, Direction générale des politiques numériques
Innovation, Sciences et Développement économique Canada / Gouvernement du Canada
Thomas.Dunne@canada.ca / Tél: 613-608-6067 / ATS: 1-866-694-8389

From: Audcent, Karen [mailto:Karen.Audcent@justice.gc.ca]
Sent: April-25-16 4:41 PM
To: Oakes, Lindsey (PS/SP); Dunne, Thomas (IC)
Cc: Wong, Normand; Angers, Lucie; Sansom, Gareth; Adamowski, Andrew (PS/SP); Taschereau, Rodrigue (PS/SP);

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Wallace, Bruce (IC); Foley, Lisa (IC); De Santis, Michael (IC)
Subject: Encryption Annex

Thanks for this Lindsey, looks good, as discussed I have made some suggestions in the attached in track changes. Karen

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

[redacted]

From: Angers, Lucie [mailto:Lucie.Angers@justice.gc.ca]
Sent: May-05-16 5:06 PM
To: [redacted]; Mileto, Joe; McIntyre, Janet
Cc: Audcent, Karen
Subject: RE: Encryption

s.13(1)(c)
s.19(1)

Hi [redacted] No problem. As I said I was asked to check with you, so thanks for the follow-up. Joe and Janet are on the e-mail so they will keep the issue on the agenda. Two small points then. Will it be [redacted] who makes the presentation? Do you have a preference as to whether the discussion on encryption takes place before or after Spencer? Thanks, Lucie

[redacted]

Page 398

is withheld pursuant to sections

est retenue en vertu des articles

13(1)(c), 19(1)

of the Access to Information Act

de la Loi sur l'accès à l'information

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Sansom, Gareth
Sent: 2016-May-12 3:43 PM
To: Audcent, Karen; Angers, Lucie; Millette, Pierre
Subject:
Attachments:

Fixed footer. **s.14(a)**

- Gareth

From: Audcent, Karen
Sent: Thursday, May 12, 2016 3:38 PM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Angers, Lucie <Lucie.Angers@justice.gc.ca>; Millette, Pierre <Pierre.Millette@justice.gc.ca>
Subject:

Hi Gareth, I read the TPs, looks good, no substantive changes to suggest, however you forgot to include your name and other info in the footer, maybe Pierre can add that in when he reviews the formatting. Karen

---

From: Sansom, Gareth
Sent: 2016-May-12 3:35 PM
To: Angers, Lucie; Audcent, Karen; Millette, Pierre
Subject:

Attached please find the revised Briefing Note (including Karen's changes) and the Talking Points for the Deputy Miniser.

Pierre, could you please make a routing slip?

Thank-you,
Gareth

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

(Discussion Item) (Item Sponsor -

Talking Points

(Justice Canada)

- [redacted]

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

CAUTION: The Government has proposed to release a Green Paper and one of the issues to be raised is [redacted]

Author: Gareth Sansom Phone: 623-424-5300 Date: May 12, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

(Discussion Item)

[redacted]

[redacted]

(JUSTICE CANADA)

ISSUE/CONTEXT:

While the conference document that will guide the discussion is not out yet, [redacted] has proposed to discuss the issue of [redacted]

STRATEGIC ADVICE:

It is recommended that you:

- [redacted]
-
-

s.14(a)
s.21(1)(a)

BACKGROUND:

[redacted]

An extensive review of Canada's cryptography policy was undertaken in 1997-1998 under the leadership of Industry Canada in the context of Canada's e-commerce policy but extending to issues of law enforcement access and national security considerations. The government prepared and released a public consultation document, held meetings across the country and received more than 150 written submissions from banks, companies, industry organizations, law enforcement and concerned citizens. The government response, after careful study, affirmed the freedom of Canadians to develop, import and use whatever cryptography they wished. T~~:~~he government

Author: Gareth Sansom Phone: 613-424-5300 Date: May 12, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

(Discussion Item)

affirmed support for private sector research and development and said that it~~; the Government~~ would not [redacted] and that~~:~~ export controls would continue to be consistent with Canada's international obligations. The ~~; and the~~ government also suggested that it would explore legislative and other options to protect consumer privacy and to assist law enforcement and national security agencies. The policy emphasized the importance of maintaining a balanced approach to a complex problem and this policy remains the Canadian policy on this issue.

The recent controversy in the United States with respect to FBI compelling access to encrypted stored data in Apple iPhones resulted in a strong backlash by the private sector, civil liberties organizations and the public.

PROVINCIAL/TERRITORIAL CONSIDERATIONS:

[redacted]

s.14(a)
s.21(1)(a)

JUSTICE CANADA POSITION:

E~~Justice Canada recognizes that the issues~~ [redacted] has found no simple solution in the past three decades and ~~that~~ any legislated solution to ~~encryption~~ this issue must be developed in a manner that is consistent with the *Canadian Charter of Rights and Freedoms*, with particular attention ~~paid~~ to the right against self-incrimination arising from compelled testimony; privacy and civil liberties as well as freedom of expression. ~~As currently drafted, the Green Paper on National Security contains a~~ [redacted]

Formatted: Font: Italic

CURRENT STATUS:

Author: Gareth Sansom Phone: 613-424-5300 Date: May 12, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

(Discussion Item)

[redacted]

DESIRED OUTCOME:

[redacted]

s.14(a)
s.21(1)(a)

Author: Gareth Sansom Phone: 613-424-5300 Date: May 12, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Audcent, Karen
Sent: 2016-May-12 3:45 PM
To: Sansom, Gareth
Subject: [redacted]

Thanks for the BN and TPs.

From: Sansom, Gareth
Sent: 2016-May-12 3:43 PM
To: Audcent, Karen; Angers, Lucie; Millette, Pierre
Subject: [redacted]

Fixed footer.

- Gareth

From: Audcent, Karen
Sent: Thursday, May 12, 2016 3:38 PM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Angers, Lucie <Lucie.Angers@justice.gc.ca>; Millette, Pierre <Pierre.Millette@justice.gc.ca>
Subject: [redacted] s.14(a)

Hi Gareth, I read the TPs, looks good, no substantive changes to suggest, however you forgot to include your name and other info in the footer, maybe Pierre can add that in when he reviews the formatting. Karen

---

From: Sansom, Gareth
Sent: 2016-May-12 3:35 PM
To: Angers, Lucie; Audcent, Karen; Millette, Pierre
Subject [redacted]

Attached please find the revised Briefing Note (including Karen's changes) and the Talking Points for the Deputy Miniser.

Pierre, could you please make a routing slip?

Thank-you,
Gareth

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Cyndy.Nelson@international.gc.ca
Sent: 2016-May-18 10:11 AM
To: Audcent, Karen; lindsey.oakes@canada.ca
Cc: Robert.Young2@international.gc.ca; Johanna.Kruger@international.gc.ca
Subject: IT World Canada - Twitter Chat on Encryption - Tuesday May 31

FYI – In case you haven't seen already, this looks interesting. The questions reminded me of some of the issues we are looking at in the green paper and may provide insight into the directions the public consultations may take.

Best,
Cyndy

Join us on **Tues. May 31, from 1 to 2 p.m. ET.** We'll be using the hashtag **#ITWCchats.**

If this is your first time participating, check out this video on how to take part in a Twitter chat. The questions are listed below, so feel free to join in with your own answers. See you there.

Q1. What is your reaction to revelations of BlackBerry giving the RCMP the encryption key to its consumer devices? #ITWCchats

Q2. Is there something Canadian about how BlackBerry & Rogers complied with RCMP vs how Apple publicly refused FBI backdoor? #ITWCchats

Q3. Are we, in 2016, at a tipping point where public/businesses/regulators must directly address boundaries of security vs privacy? #ITWCchats

Q4. What, to you, is reasonable access to data by government or law enforcement? What checks & balances are needed? #ITWCchats

Q5. How could law enforcement minimize harm? I.e. target individual users of devices/servers/data centres vs. manufacturers? #ITWCchats

Q6. Should there be a distinction made between handling consumer data and corporate data, as BlackBerry has done? #ITWCchats

Q7. Are governments sending the wrong message by sanctioning hacks? I.e. that encryption is becoming irrelevant? #ITWCchats

Q8. Should our or other governments raise data sovereignty concerns over US Supreme Court enabling FBI cross-border hacking? #ITWCchats

Q9. How should businesses act in the absence of clear legal boundaries in terms of client encryption, compliance, or advocacy? #ITWCchats

Read more: http://www.itworldcanada.com/article/will-state-sanctioned-hacks-make-encryption-irrelevant-join-our-discussion-on-the-future-of-privacy/383357#ixzz4913YPjNa
or visit http://www.itworldcanada.com for more Canadian IT News

Cyndy Nelson
Senior Policy Officer | Agente principale des politiques

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Policy Planning Division | Direction de la Planification des politiques
cyndy.nelson@international.gc.ca
343-203-2078
125 Sussex Drive, Ottawa, Ontario K1A 0G2
Global Affairs Canada | Affaires mondiales Canada
Government of Canada | Gouvernement du Canada

Global Affairs Canada | Affaires mondiales Canada

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Oakes, Lindsey (PS/SP) <lindsey.oakes@canada.ca>
Sent: 2016-May-18 10:29 AM
To: Cyndy.Nelson@international.gc.ca; Audcent, Karen
Cc: Robert.Young2@international.gc.ca; Johanna.Kruger@international.gc.ca; Taschereau, Rodrigue (PS/SP)
Subject: RE: IT World Canada - Twitter Chat on Encryption - Tuesday May 31

Thanks Cyndy

Lindsey Oakes
Telephone: 613-990-8020
Blackberry: 613-410-6057
E-mail | Courriel: lindsey.oakes@canada.ca

Public Safety Canada | Sécurité publique Canada

From: Cyndy.Nelson@international.gc.ca [mailto:Cyndy.Nelson@international.gc.ca]
Sent: Wednesday, May 18, 2016 10:11 AM
To: karen.audcent@JUSTICE.GC.CA; Oakes, Lindsey (PS/SP)
Cc: Robert.Young2@international.gc.ca; Johanna.Kruger@international.gc.ca
Subject: IT World Canada - Twitter Chat on Encryption - Tuesday May 31

FYI – In case you haven't seen already, this looks interesting. The questions reminded me of some of the issues we are looking at in the green paper and may provide insight into the directions the public consultations may take.

Best,
Cyndy

Join us on **Tues. May 31, from 1 to 2 p.m. ET**. We'll be using the hashtag **#ITWCchats.**

If this is your first time participating, check out this video on how to take part in a Twitter chat. The questions are listed below, so feel free to join in with your own answers. See you there.

Q1. What is your reaction to revelations of BlackBerry giving the RCMP the encryption key to its consumer devices? #ITWCchats

Q2. Is there something Canadian about how BlackBerry & Rogers complied with RCMP vs how Apple publicly refused FBI backdoor? #ITWCchats

Q3. Are we, in 2016, at a tipping point where public/businesses/regulators must directly address boundaries of security vs privacy? #ITWCchats

Q4. What, to you, is reasonable access to data by government or law enforcement? What checks & balances are needed? #ITWCchats

Q5. How could law enforcement minimize harm? I.e. target individual users of devices/servers/data centres vs. manufacturers? #ITWCchats

Q6. Should there be a distinction made between handling consumer data and corporate data, as BlackBerry has done? #ITWCchats

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Q7. Are governments sending the wrong message by sanctioning hacks? I.e. that encryption is becoming irrelevant? #ITWCchats

Q8. Should our or other governments raise data sovereignty concerns over US Supreme Court enabling FBI cross-border hacking? #ITWCchats

Q9. How should businesses act in the absence of clear legal boundaries in terms of client encryption, compliance, or advocacy? #ITWCchats

Read more: http://www.itworldcanada.com/article/will-state-sanctioned-hacks-make-encryption-irrelevant-join-our-discussion-on-the-future-of-privacy/383357#ixzz4913YPjNa
or visit http://www.itworldcanada.com for more Canadian IT News

Cyndy Nelson
Senior Policy Officer | Agente principale des politiques
Policy Planning Division | Direction de la Planification des politiques
cyndy.nelson@international.gc.ca
343-203-2078
125 Sussex Drive, Ottawa, Ontario K1A 0G2
Global Affairs Canada | Affaires mondiales Canada
Government of Canada | Gouvernement du Canada

Global Affairs Canada | Affaires mondiales Canada

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Angers, Lucie
Sent: 2016-May-30 4:15 PM
To: Sansom, Gareth; Audcent, Karen; Wong, Normand
Subject: [redacted]
Attachments: [redacted]

s.14(a)
s.21(1)(a)

Hi Gareth, I hope that your meeting at the CoE went well. I think we should all talk when I'm back next week from FPT DMs about the discussions we had at the UN. On another note, [redacted] As discussed with Karen, I don't think that we should send an updated version of your BN and TPs given that everybody in DoJ (including myself) is leaving Wednesday. However, I think that it would be useful if you could please review the three documents and let us know if you have thoughts additional to those you included in the BN and TPs. [redacted] Thanks, Lucie

Pages 410 to / à 428
are withheld pursuant to section
sont retenues en vertu de l'article

13(1)(c)

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

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Angers, Lucie
Sent: 2016-May-31 6:35 PM
To: Sansom, Gareth; Audcent, Karen; Wong, Normand
Subject: [redacted] s.14(a) s.21(1)(a) s.21(1)(b)

This is very useful, thanks!!

From: Sansom, Gareth
Sent: Tuesday, May 31, 2016 4:04 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Subject: [redacted]

[redacted]

From: Angers, Lucie
Sent: Monday, May 30, 2016 4:15 PM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Subject: FPT DMs - Encryption

Hi Gareth, I hope that your meeting at the CoE went well. I think we should all talk when I'm back next week from FPT DMs about the discussions we had at the UN. On another note, [redacted] As discussed with

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Karen, I don't think that we should send an updated version of your BN and TPs given that everybody in DoJ (including myself) is leaving Wednesday. However, I think that it would be useful if you could please review the three documents and let us know if you have thoughts additional to those you included in the BN and TPs. [redacted] Thanks, Lucie

s.21(1)(a)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Oakes, Lindsey (PS/SP) <lindsey.oakes@canada.ca>
Sent: 2016-Jun-01 10:58 AM
To: Audcent, Karen
Subject: FYI - Encryption / future of privacy

http://www.computerdealernews.com/news/will-state-sanctioned-hacks-make-encryption-irrelevant-join-our-discussion-on-the-future-of-privacy/48092?utm_source=4596920&utm_medium=CDN&utm_campaign=cdnnews','&scid=b4d43ed9-af4c-4fd5-da01-570e4b41c791

Lindsey Oakes

Senior Policy Analyst | Analyste principale en politiques
National and Cyber Security Branch | Secteur de la Sécurité et de la Cybersécurité Nationale
Public Safety Canada | Sécurité publique Canada
340 Laurier Ave West, Ottawa, Canada K1A 0P8 | 340, av. Laurier Ouest, Ottawa, Canada K1A 0P8
E-mail | Courriel: lindsey.oakes@canada.ca / **Telephone**: 613-990-8020 / **Blackberry**: 613-410-6057

Public Safety Canada | Sécurité publique Canada

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

ANNEX 3Z

ENCRYPTION

INTRODUCTION

As our society and economy becomes ever more interwoven with the internet, encryption has become a critically important tool for safety, security and privacy online. Widely regarded as a best practice, encryption enhances security and protects privacy online and is commonly used to protect individual messages, personal devices and transmission channels. Encryption is central to electronic commerce, banking, cybersecurity, data and intellectual property protection. The use of encryption technologies has grown tremendously in both availability and use with the growth of the internet.

Cryptography is the practice and study of communications and the procedures, processes, and methods of making and using secret communications, such as codes or ciphers. One of the main fields in cryptography is encryption. To encrypt, means to make hidden or secret. Encryption uses a process or algorithm (sometimes known as a cipher) and converts a readable message into an unreadable encrypted message. In order to access the hidden or secret message, the user must have the key (which can be an algorithm or another type of code) to unlock it. Encryption plays an important role as it allows users to authenticate and safeguard sensitive data, and other information stored on computers or transmitted over closed or public networks.

While this technology provides tremendous benefits, it also gives criminals and terrorists additional means to avoid discovery, investigation, and prosecution by concealing their activities. Law enforcement and national security agencies' concern relative to encryption is primarily that investigative techniques employed, under judicial authority, to obtain information, including interception of private communications (wiretap), production orders, and search warrants, can be made ineffective by the use of encryption. Encryption can be used by criminals or terrorists to prevent an investigation from being able to make heads or tails of the information obtained, which is needed to solve a crime or address a threat to Canada or Canada's interests.

[redacted] s.21(1)(a)

Although encryption can pose a challenge to law enforcement, this issue has not been directly addressed in law in Canada, and the question of it, or how, to address this challenge continues to make headlines in many jurisdictions around the world. In trying to address the challenges faced by law enforcement and national security agencies, some of the issues raised relate to:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- human rights, including privacy rights, freedom of expression, and the right against self-incrimination,
- commercial interests, such as competitiveness and the protection of intellectual property;
- jurisdictional implications; and
- the need for encryption to enable modern e-commerce, e-banking and all types of cybersecurity and critical infrastructure.

s.21(1)(a)

These issues, along with others, will be discussed further in this annex.

TYPES OF ENCRYPTION

Encryption is technology that can be applied to data-in-use, data-in-motion and data-at-rest. Any of these could have various layers of encryption applied to it by any or all of the following: the end user, third party applications, and telecommunication service providers.

Data-in-use, otherwise known as active data, is data that is live and under constant change and manipulation by an application. Data-in-use is physically stored in databases, data warehouses, spreadsheets, etc. Data-in-motion is data that is currently in transit over some type of network or temporarily residing in computer memory. Data-at-rest is inactive data stored physically in databases, data warehouses, spreadsheets, archives, hard drives, tapes, off-site backups, mobile devices, etc.

In addition, encryption can be applied to more specific items such as the message itself (i.e. email, text message, or photo), the device (i.e. the cell phone, the computer, the tablet), or the transmission network and/or channel (i.e. a VPN network, an enterprise server, or even the communication service provider's network).

POLICY AND LEGISLATION

THE GOVERNMENT OF CANADA'S ELECTRONIC COMMERCE STRATEGY & THE POLICY ON CRYPTOGRAPHY)

An extensive review of Canada's Cryptography policy was undertaken in 1997-1998 under the leadership of Industry Canada (now Innovation, Science, and Economic Development Canada) in the context of Canada's e-commerce policy but extended to the issues of law enforcement access and national security considerations. In 1998, Canada's Minister of Industry announced its Cryptography policy and, this policy remains in place today.
In this policy, the Government affirmed the following principles:

1) The freedom of Canadians to develop, import and use whatever cryptography they wished;
2) Support for private sector research and development
3) It was decided that the Government would not implement mandatory key recovery requirements or licensing regimes for certification authorities or trusted third parties;
4) Export controls would continue to be consistent with Canada's international obligations; and

Commented [LO1]:

Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Times New Roman, No underline
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Times New Roman, 12 pt

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

5) The Government would explore legislative and other options to protect consumer privacy and to assist law enforcement and national security agencies.

The policy emphasized the importance of maintaining a balanced approach to a complex problem.

A number of key considerations played a role in helping shape Canada's Cryptography policy. The following were some significant developments that helped guide the policy development process:

- The increasing use of strong encryption software and computers powerful enough to encrypt and decrypt data easily are commonly available;
- The rapidly increasing use of telecommunications media suitable for encryption (e.g. email and other data conveyed via the Internet and other computer-based media) for both personal and commercial communications;
- The increasing use of wireless cellular telephones, which has created pressure for the development of digital equipment and lead to the encryption of their signals in some cases; and
- The increasing reliance on computers and computer networks for commercial activities and the need to protect privacy and security, which has led companies to store business records in secure computer facilities and in encrypted forms.

Notably, many of these developments are still relevant today given the proliferation of and reliance on the use of technology, encryption and digital communications. Both then, and now, encryption forms part of the core framework that allows electronic commerce to flourish.
In an effort to develop a cryptography framework, specific considerations were given to the areas of electronic commerce, [redacted] considerations. [redacted] involved in any discussion of encryption.

s.21(1)(a)

Electronic Commerce

In 1998, more and more transactions were shifting from closed networks to open networks and cryptography became essential for the conduct of electronic commerce. Open networks allowed for more global trading, but came with a variety of security challenges including concerns over the authentication of communicating parties, the integrity of the data being communicated, the confidentiality of the proprietary or personal data, and the assurance that transactions have been authorized by legitimate users. Without cryptography, these challenges may not have been addressed. Also, cryptography increased the competitiveness of businesses and provided opportunities for job creation and industrial growth.

The aims of law enforcement and business align when cryptography protects proprietary information, trade secrets, and in general, helps defend industry and consumers against fraud and other unlawful activities. In addition, cryptography meets national security objectives to the

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.21(1)(a)

extent that it helps protect Canada, and its national critical infrastructure and valuable information.

The policy challenge was, and continues to be, the need to find solutions that will manage the [redacted] without interfering with legitimate business, institutional or individual interests and national security and law enforcement interests.

Lawful Access

With the development of new means of personal and commercial communications and the overall increase in the use of technology, we have also seen new forms of criminal activity, new methods of committing old crimes, and new ways of concealing evidence. The widespread use of cryptography can raise concerns in this context because it can create obstacles to the detection and investigation of criminal activities and security threats, as well as the inspection of computer records subject to investigation.

Agencies that play key roles in law enforcement, national security, and regulatory compliance investigations include, but are not limited to: the RCMP, provincial and local police forces, the Canadian Security Intelligence Service (CSIS), Canadian Border Service Agency (CBSA), the Canada Revenue Agency (taxation, customs and excise), the federal Competition Bureau, as well as federal and provincial environmental enforcement agencies. The respective responsibilities of these agencies are diverse but include aspects such as: identifying threats and detecting, investigating and prosecuting matters related to terrorism, crimes of violence and related to property, and abuses of domestic and international commercial and financial systems, as they relate to the actions of Canadians or persons in Canada.

The effectiveness of these agencies in monitoring criminal activities, and in investigating and prosecuting offenders in Canada has depended on their ability to conduct electronic surveillance of communications and to search and inspect places and materials, including computers, where relevant information may be kept.

The increase in the use of cryptography can provide concurrent, yet competing, outcomes; while it can provide enhanced technical protection for confidential information, it can also impede the ability to conduct lawful and authorized electronic surveillance. Notwithstanding the receipt of judicial authorizations for the interception of communications, intercepted data in an encrypted form may be unreadable and undecipherable for authorities. This makes it difficult for authorities to decipher the information, or to do so in time to be able to effectively use it or take action to prevent harm from occurring.

Law enforcement, regulatory and national security agencies are challenged to effectively respond and adhere to their individual mandates in the face of undecipherable encrypted communications, and would benefit from some means whereby encrypted data can be decrypted and read within a reasonable time and at a reasonable expenditure of resources.

Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Space Before: 0 pt, Line spacing: single
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Space After: 0 pt, Line spacing: single
Formatted: Font: (Default) Times New Roman, 12 pt, Not Bold
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Times New Roman, 12 pt

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Human rights and civil liberties

The rights of Canadians to privacy and to express themselves freely are constitutionally protected. Section 8 of the *Charter* guarantees Canadians the right to be free from "unreasonable search or seizure" which has been interpreted through jurisprudence [redacted] and the right to freedom of expression may extend to both the production of cryptographic products and their use to protect the messages being expressed or data being stored. The protection of a reasonable expectation of privacy, and invasions of that privacy must be justified, must be authorized in law and generally require specific pre-authorization by the courts.

s.21(1)(a)

WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES

It is important to note that Canada is one of 33 signatories to the Wassenaar Arrangement which was established to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies (such as encryption software). Participating states seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities. The aim is also to prevent the acquisition of these items by terrorists. Participating States control all items set forth in the List of Dual-Use Goods and Technologies and Munitions list, with the objective of preventing unauthorized transfers or re-transfers of those items. Items included on the lists focus on items designed for military use, and general technology and software notes (i.e. encryption software).

The participating states have an agreement to maintain national export controls on listed items, which are implemented via national legislation; are guided by agreed upon best practices, guidelines or elements; have agreed to report on transfers and denials of specific controlled items to destinations outside of the arrangement; and exchange information on sensitive dual-use goods and technologies.

BILL C-30 – *PROTECTING CHILDREN FROM INTERNET PREDATORS ACT*, 2012

In the past, in the context of work on lawful access issues, and most recently in former Bill C-30 (*Protecting Children from Internet Predators Act*, 2012, 41st Parliament, 1st session), legislative proposals were introduced, but did not come into force, to create requirements for telecommunications service providers to decrypt communications where it was readily possible for the service provide to do so, in the context of lawful interception. However, telecommunications service providers were not required to develop specific decryption techniques themselves.

Formatted: Space Before: 0 pt, Line spacing: single

Formatted: Font: (Default) Times New Roman, 12 pt, No underline, Font color: Auto, Not Small caps

Formatted: Space After: 0 pt, Line spacing: single

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, Not Bold

Formatted: Space After: 0 pt, Line spacing: single, Border: Bottom: (No border)

Formatted: Font: (Default) Times New Roman, Not Italic

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt, Not Italic

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt, Not Italic

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

For example, if interception was successful but the data retrieved was encrypted by a tool that was implemented directly by the service provider, rather than the user, then the service provider would be asked to decrypt the data.

These proposals were supported by law enforcement. However, in the larger picture, these proposals would not have solved the problem posed by encryption in whole, nor did they purport to do so. This is particularly true given that many major IT companies have built mobile and other digital devices that enable individuals to encrypt and decrypt data at the user level.

JURISDICTIONAL AND INTERNATIONAL CHALLENGES

Law enforcement and national security agencies can face other challenges when attempting to compel communication service providers to decrypt communications, as the international nature of the software market and the borderless nature of cyberspace, in addition to the locations (jurisdiction) of the communications service provider [redacted] In addition, many communication service providers, particularly software and application service providers, do not have physical premises in Canada, and may not be subject to Canadian jurisdiction. In order to be able to obtain information held by these companies, currently the principal process available is through the use of Mutual Legal Assistance Treaties (MLATs). Currently, MLAT processes are not always timely enough for the exigencies of investigations involving electronic evidence, nor were they designed for a high volume of requests that could ensue given the trend toward global inter-connectivity and challenges in relation to jurisdiction in the context of modern communications.

s.21(1)(a)

It is important to note that encryption and challenges being faced by law enforcement and national security agencies are the topic of on-going discussion and work in various international fora. Canada is not the only country exploring options that address the on-going need for capacity to address law enforcement and national security challenges arising from use of encryption, in a way that supports the many beneficial uses of encryption, including its value for cybersecurity but also takes into consideration the investigative needs of law enforcement, national security and regulatory agencies.

Formatted: Space After: 0 pt, Line spacing: single
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Times New Roman, 12 pt, All caps
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Times New Roman, 12 pt

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

ANNEX 3

Encryption

INTRODUCTION

Cryptography is the practice and study of techniques for communication. One of the main fields in cryptography is encryption which converts a readable message into an unreadable encrypted message. Encryption is central to electronic commerce, banking, cybersecurity, data and intellectual property protection. However, this same technology that brings many benefits is also used to conceal criminal activities. The use of encryption technologies has grown tremendously in both availability and use with the growth of the internet. Encryption plays an important role as it allows users to authenticate and safeguard sensitive data, and other information stored on computers or transmitted over closed or public networks.

Law enforcement and national security agencies' concern relative to encryption is primarily that investigative techniques employed, under judicial authority, to obtain information, including interception of private communications (wiretap), production orders, and search warrants, can be made ineffective by the use of encryption. Encryption can be used by criminals or terrorists to prevent an investigation from being able to make heads or tails of the information obtained, which is needed to solve a crime.

Although encryption can pose a significant challenge to law enforcement, this issue hast not been directly addressed in law in Canada, [redacted] the question of if, or how, to address this challenge continues to make headlines in many jurisidictions around the world. ~~, nor has this issue been fully addressed in any jurisdiction~~. In trying to address the challenges faced by law enforcement and national security agencies, some of the issues ~~are~~ raised are relative to: human rights, jurisdiction, and the essential need for encryption to enable modern e-commerce, e-banking and all types of cybersecurity and critical infrastructure. These issues, along with others will be discussed further in this annex.

s.21(1)(a)

[redacted] The *Canadian Charter of Rights and Freedoms*, under sections 1, 8 and 24, sets out the basic constitutional principles in Canada that lawful access must be "reasonable" and "justifiable" in a free and democratic society. [redacted]

TYPES OF ENCRYPTION

Encryption is technology that can be applied to data-in-use, data-in-motion and data-at-rest. Any of these could have various layers of encryption applied to it by any ~~either~~ or all of the following: the end user, third party applications, and telecommunication service providers.

[redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Data-in-use, otherwise known as active data, is data that is live and under constant change and manipulation by an application. Data-in-use is physically stored in databases, data warehouses, spreadsheets, etc. Data-in-motion is data that is currently in transit over some type of network or temporarily residing in computer memory. Data-at-rest is inactive data stored physically in databases, data warehouses, spreadsheets, archives, hard drives, tapes, off-site backups, mobile devices, etc.

In addition, encryption can be applied to more specific items such as the message itself (i.e. email, text message, or photo), the device (i.e. the cell phone, the computer, the tablet), or the transmission network and/or channel (i.e. the communication service provider network).

[redacted]

POLICY AND LEGISLATION

THE GOVERNMENT OF CANADA'S ELECTRONIC COMMERCE STRATEGY -& THE POLICY ON ~~1998~~ CRYPTOGRAPHY ~~POLICY~~)

An extensive review of Canada's Cryptography policy was undertaken in 1997-1998 under the leadership of Industry Canada (now Innovation, Science, and Economic Development Canada) in the context of Canada's e-commerce policy but extended to the issues of law enforcement access and national security considerations. In 1998, Canada announced its Cryptography policy which remains in place today.

A number of key considerations played a role in helping shape Canada's Cryptography policy. The following were some significant developments that helped guide the policy development process:

- The increasing use of strong encryption software and computers powerful enough to encrypt and decrypt data easily are commonly available;
- The rapidly increasing use of telecommunications media suitable for encryption (e.g. email and other data conveyed via the Internet and other computer-based media) for both personal and commercial communications;
- The increasing use of wireless cellular telephones, which has created pressure for the development of digital equipment and lead to the encryption of their signals in some cases; and
- The increasing reliance on computers and computer networks for commercial activities and the need to protect privacy and security, which has led companies to store business records in secure computer facilities and in encrypted forms.

s.21(1)(a)

Notably ~~Interestingly~~, many of these developments are still relevant today given the proliferation of and reliance on the use of technology, encryption and digital communications. Both then, and now, encryption forms part of the core framework that allows electronic commerce to flourish.

In an effort to develop a cryptography framework, ~~more~~ specific considerations were given to the areas of: electronic commerce, lawful [redacted] To date, these remain ~~to be~~ some of the key considerations [redacted]

[redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Electronic Commerce

In 1998, more and more transactions were shifting from closed networks to open networks and cryptography became essential for the conduct of electronic commerce. Open networks allowed for more global trading, but came with a variety of security challenges including concerns over the authentication of communicating parties, the integrity of the data being communicated, the confidentiality of the proprietary or personal data, and the assurance that transactions have been authorized by legitimate users. Without cryptography, these challenges may not have been addressed. Also, cryptography increased the competitiveness of businesses and provided opportunities for job creation and industrial growth.

The aims of law enforcement and business align when cryptography protects proprietary information, trade secrets, and in general, helps defend industry and consumers against fraud and other unlawful activities. In addition, cryptography meets national objectives to the extent that it helps protect sovereignty, national infrastructures, and their valuable information.

The policy challenge was, and continues to be, the need to find solutions that will limit [redacted] without interfering with legitimate business, institutional or individual interests. [redacted]

[redacted] personal and commercial communications and the overall increase in the use of technology, [redacted] new forms of criminal activity, new methods of committing old crimes, and new ways of concealing evidence. The widespread use of cryptography can raise~~d~~ concerns in this context because it can create~~d~~ [redacted] obstacles to the detection and investigation of criminal activities and security threats, as well as the inspection of computer records [redacted] Agencies that play ~~a~~ key roles in law enforcement, national security, and regulatory compliance investigations include the RCMP, provincial and local police forces, the Canadian Security Intelligence Service, the Canadian Revenue Agency (taxation, customs and excise), the federal Competition Bureau, as well as federal and provincial environmental enforcement agencies. These agencies are responsible for, among other things, identifying threats and detecting, investigating and prosecuting matters ~~ranging from~~related to terrorism, crimes of violence and related to property, ~~crimes to~~ and abuses of domestic and international commercial and financial systems.

s.21(1)(a)

The effectiveness of these agencies in monitoring criminal activities, and in investigating and prosecuting offenders has depended on their ability to conduct electronic surveillance of

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

communications and to search and inspect places, including computers, where relevant information may be kept. [redacted]

Formatted: Font: Italic

[redacted]

Formatted: Font: Italic

s.21(1)(a)

The increase in the use of strong cryptography can provide concurrent, yet competing, outcomes; while it can provide enhanced [redacted] technical protection for confidential information, ~~but~~ it can also impede~~represents a significant threat to~~ the ability to conduct lawful and authorized electronic surveillance. Notwithstanding the receipt of [redacted] judicial authorizations [redacted] for the interception of communications, intercepted [redacted] data in an encrypted form may [redacted] be unreadable and undecipherable for authorities. This creates two challenges: (1) it becomes difficult or impossible to determine whether the information being intercepted fallsell within the scope of the legal authorization to intercept it; and (2) it becomes difficult for authorities to decipher the information, or to do so in time to be able to effectively use it or take action to prevent harm from occurring.

Commented [KA8]: Is this really a key point that we would want to flag? I understand that it may be an issue, but it seems to me to be much less of an issue than issue #2. I'd be inclined to delete it.

Commented [DTD9]: These read to me like the same challenge.

L~~The~~ law enforcement, regulatory and national security agencies ~~communities clearly recognized, and~~ [redacted] are challenged to [redacted] effectively respond and adhere to their individual mandates in the face of undecipherable encrypted communications, and [redacted] require some means whereby encrypted data can be decrypted and read within a reasonable time and at a reasonable expenditure of resources.

[redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Human rights and civil liberties

[redacted]

s.21(1)(a)

Formatted: Heading 3

[redacted]tThe rights of Canadians to ~~some degree of~~ privacy and to express themselves freely are constitutionally protected. Section 8 of the *Charter* guarantees Canadians the right to be free from "unreasonable search or seizure" which has been interpreted through jurisprudence as [redacted] freedom of expression may extend to both the production of cryptographic products and their use to protect the messages being expressed or data being stored. [redacted] Invasions of privacy, including the seizure of data or interception of communications, must be justified. [redacted]

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: Italic

[redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

[redacted] strong cryptography products are difficult to "break", and success with a "brute force" attack by powerful computers is only feasible in some cases, as the computing time required may be prohibitive, depending on the strength of the encryption, and the strength of the computer attempting the brute force attack. [redacted]

s.21(1)(a)

[redacted]

The 1998 Policy

After careful study, the 1998 Cryptography policy was announced by the Canadian Minister of Industry in the context of e-commerce. In this policy, the Government affirmed the following principles:

1) The freedom of Canadians to develop, import and use whatever cryptography they wished;
2) Support for private sector research and development
3) It was decided that the Government would not implement mandatory key recovery requirements or licensing regimes for certification authorities or trusted third parties;
4) Export controls would continue to be consistent with Canada's international obligations; and
5) The Government would explore legislative and other options to protect consumer privacy and to assist law enforcement and national security agencies.

The policy emphasized the importance of maintaining a balanced approach to a complex problem.

WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Canada is one of 33 signatories to the Wassenaar Arrangement which was established to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies (such as encryption software). Participating states seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities. The aim is also to prevent the acquisition of these items by terrorists.

Participating States control all items set forth in the List of Dual-Use Goods and Technologies and Munitions list, with the objective of preventing unauthorized transfers or re-transfers of those items. Items included on the lists focus on items designed for military use, and general technology and software notes (i.e. encryption software).

The participating states have an agreement to maintain national export controls on listed items, which are implemented via national legislation; are guided by agreed upon best practices, guidelines or elements; have agreed to report on transfers and denials of specific controlled items to destinations outside of the arrangement; and exchange information on sensitive dual-use goods and technologies.

s.21(1)(a)

[redacted]

BILL C-30 – PROTECTING CHILDREN FROM INTERNET PREDATORS ACT, 2012

In the past, in the context of work on lawful access issues, and most recently in former Bill C-30 (*Protecting Children from Internet Predators Act*, 2012, 41st Parliament, 1st session), legislative proposals were introduced to create requirements for telecommunications service providers to decrypt communications where it was readily possible for the service provide to do so, in the context of lawful interception. However, telecommunications service providers were not required to develop specific decryption techniques themselves.

For example, if interception was successful but the data retrieved was encrypted by a tool that was implemented directly by the service provider, rather than the user, then the service provider would be asked to decrypt the data.

These proposals were supported by law enforcement. However, in the larger picture, these proposals would not have solved the problem posed by encryption in whole. This is particularly true given that many major IT companies have built mobile and other digital devices that enable individuals to encrypt and decrypt data at the user level.

Jurisdictional and International Challenges

[redacted] Law enforcement and national security agencies can face other challenges when attempting to [redacted] compel communication service providers to [redacted] decrypt communications, as ~~are~~ the international nature of the software market and the borderless nature of cyberspace, in addition to the locations (jurisdiction) of the communications service provider [redacted] In addition, m~~M~~any communication service providers, particularly software and application service providers, do not

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

have physical premises in Canada, and may not be subject to Canadian jurisdiction. In order to be able to obtain information held by these companies, currently the [redacted] process available is through the use of Mutual Legal Assistance Treaties (MLATs). [redacted] Currently [redacted] MLAT processes are not always timely enough for the exigencies of investigations involving electronic evidence, nor were they designed for a high volume of requests that could ensue given the trend toward global inter-connectivity and challenges in relation to jurisdiction in the context of modern communications.

s.21(1)(a)

There is also some concern about setting a precedent in accessing encrypted data. If western Governments (such as the US and Canada) demand companies create backdoors into products and services, there is a concern that more authoritarian regimes or governments will insist on having access to these~~the~~ same capabilities. This may mean that the more authoritarian regimes may use these capabilities to monitor and censor the legitimate activities of their citizens in a manner inconsistent with Canadian values, such as free expression and privacy, rather than focusing on~~just~~ accessing information believed to be related to criminal activity and threats to national security in a specific and targeted way, with court oversight, as is done in Canada and in other countries with similar values and systems.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

DRAFT

ANNEX 3

Encryption

INTRODUCTION

As our society and economy becomes ever more interwoven with the internet, encryption has become a critically important tool for safety, security and privacy online. Widely regarded as a best practice, encryption enhances security and protects privacy online and is commonly used to protect individual messages, personal devices and transmission channels. Encryption is central to electronic commerce, banking, cybersecurity, data and intellectual property protection. The use of encryption technologies has grown tremendously in both availability and use with the growth of the internet.

Cryptography is the practice and study of [redacted] communications and the procedures, processes, and methods of making and using secret communications, such as codes or ciphers. One of the main fields in cryptography is encryption. To encrypt, means to make hidden or secret. Encryption uses a process or algorithm (sometimes known as a cipher) and converts a readable message into an unreadable encrypted message. In order to access the hidden or secret message, the user must have the key (which can be an algorithm or another type of code) to unlock it. Encryption plays an important role as it allows users to authenticate and safeguard sensitive data, and other information stored on computers or transmitted over closed or public networks.

While this technology provides tremendous benefits, it also gives criminals and terrorists additional means to avoid discovery, investigation, and prosecution by concealing their activities. Law enforcement and national security agencies' concern relative to encryption is primarily that investigative techniques employed, under judicial authority, to obtain information, including interception of private communications (wiretap), production orders, and search warrants, can be made ineffective by the use of encryption. Encryption can be used by criminals or terrorists to prevent an investigation from being able to make heads or tails of the information obtained, which is needed to solve a crime or address a threat to Canada or Canada's interests.

s.21(1)(a)

[redacted]

[redacted]

Although encryption can pose a challenge to law enforcement, this issue hast not been directly addressed in law in Canada, and the question of it, or how, to address this challenge continues to make headlines in many jurisdictions around the world. In trying to address the challenges faced by law enforcement and national security agencies, some of the issues raised relate to:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- human rights, including privacy rights, freedom of expression, and the right against self-incrimination,
- commercial interests, such as competitiveness and the protection of intellectual property;
- jurisdictional implications; and
- the need for encryption to enable modern e-commerce, e-banking and all types of cybersecurity and critical infrastructure.

These issues, along with others, will be discussed further in this annex.

TYPES OF ENCRYPTION

Encryption is technology that can be applied to data-in-use, data-in-motion and data-at-rest. Any of these could have various layers of encryption applied to it by any or all of the following: the end user, third party applications, and telecommunication service providers.

Data-in-use, otherwise known as active data, is data that is live and under constant change and manipulation by an application. Data-in-use is physically stored in databases, data warehouses, spreadsheets, etc. Data-in-motion is data that is currently in transit over some type of network or temporarily residing in computer memory. Data-at-rest is inactive data stored physically in databases, data warehouses, spreadsheets, archives, hard drives, tapes, off-site backups, mobile devices, etc.

In addition, encryption can be applied to more specific items such as the message itself (i.e. email, text message, or photo), the device (i.e. the cell phone, the computer, the tablet), or the transmission network and/or channel (i.e. a VPN network, an enterprise server, or even the communication service provider's network).

POLICY AND LEGISLATION

s.21(1)(a)

THE GOVERNMENT OF CANADA'S ELECTRONIC COMMERCE STRATEGY & THE POLICY ON CRYPTOGRAPHY)

An extensive review of Canada's Cryptography policy was undertaken in 1997-1998 under the leadership of Industry Canada (now Innovation, Science, and Economic Development Canada) in the context of Canada's e-commerce policy but extended to the issues of law enforcement access and national security considerations. In 1998, Canada's Minister of Industry announced its Cryptography policy and this policy remains in place today.

In this policy, the Government affirmed the following principles:

1) The freedom of Canadians to develop, import and use whatever cryptography they wished;
2) Support for private sector research and development
3) It was decided that the Government would not implement mandatory key recovery requirements or licensing regimes for certification authorities or trusted third parties;
4) Export controls would continue to be consistent with Canada's international obligations; and

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

5) The Government would explore legislative and other options to protect consumer privacy and to assist law enforcement and national security agencies.

The policy emphasized the importance of maintaining a balanced approach to a complex problem.

A number of key considerations played a role in helping shape Canada's Cryptography policy. The following were some significant developments that helped guide the policy development process:

- The increasing use of strong encryption software and computers powerful enough to encrypt and decrypt data easily are commonly available;
- The rapidly increasing use of telecommunications media suitable for encryption (e.g. email and other data conveyed via the Internet and other computer-based media) for both personal and commercial communications;
- The increasing use of wireless cellular telephones, which has created pressure for the development of digital equipment and lead to the encryption of their signals in some cases; and
- The increasing reliance on computers and computer networks for commercial activities and the need to protect privacy and security, which has led companies to store business records in secure computer facilities and in encrypted forms.

Notably, many of these developments are still relevant today given the proliferation of and reliance on the use of technology, encryption and digital communications. Both then, and now, encryption forms part of the core framework that allows electronic commerce to flourish.

In an effort to develop a cryptography framework, specific considerations were given to the areas of electronic commerce, [redacted] s.21(1)(a)
[redacted] To date, these remain some of the key considerations [redacted]

Electronic Commerce

In 1998, more and more transactions were shifting from closed networks to open networks and cryptography became essential for the conduct of electronic commerce. Open networks allowed for more global trading, but came with a variety of security challenges including concerns over the authentication of communicating parties, the integrity of the data being communicated, the confidentiality of the proprietary or personal data, and the assurance that transactions have been authorized by legitimate users. Without cryptography, these challenges may not have been addressed. Also, cryptography increased the competitiveness of businesses and provided opportunities for job creation and industrial growth.

The aims of law enforcement and business align when cryptography protects proprietary information, trade secrets, and in general, helps defend industry and consumers against fraud and other unlawful activities. In addition, cryptography meets national security objectives to the extent that it helps protect Canada, and its national critical infrastructure and valuable information.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The policy challenge was, and continues to be, the need to find solutions that will manage the [redacted] without interfering with legitimate business, institutional or individual interests and national security and law enforcement interests.

Lawful Access

With the development of new means of personal and commercial communications and the overall increase in the use of technology, we have also seen new forms of criminal activity, new methods of committing old crimes, and new ways of concealing evidence. The widespread use of cryptography can raise concerns in this context because it can create obstacles to the detection and investigation of criminal activities and security threats, as well as the inspection of computer records subject to investigation.

s.21(1)(a)

Agencies that play key roles in law enforcement, national security, and regulatory compliance investigations include, but are not limited to: the RCMP, provincial and local police forces, the Canadian Security Intelligence Service (CSIS), Canadian Border Service Agency (CBSA), the Canada Revenue Agency (taxation, customs and excise), the federal Competition Bureau, as well as federal and provincial environmental enforcement agencies. The respective responsibilities of these agencies are diverse but include aspects such as: ~~These agencies are responsible for, among other things,~~ identifying threats and detecting, investigating and prosecuting matters related to terrorism, crimes of violence and related to property, and abuses of domestic and international commercial and financial systems, as they relate to the actions of Canadians or persons in Canada.

The effectiveness of these agencies in monitoring criminal activities, and in investigating and prosecuting offenders in Canada has depended on their ability to conduct electronic surveillance of communications and to search and inspect places and materials, including computers, where relevant information may be kept. [redacted]

The increase in the use of cryptography can provide concurrent, yet competing, outcomes; while it can provide enhanced technical protection for confidential information, it can also impede the ability to conduct lawful and authorized electronic surveillance. Notwithstanding the receipt of judicial authorizations for the interception of communications, intercepted data in an encrypted form may be unreadable and undecipherable for authorities. This makes it difficult for authorities to decipher the information, or to do so in time to be able to effectively use it or take action to prevent harm from occurring.

Law enforcement, regulatory and national security agencies are challenged to effectively respond and adhere to their individual mandates in the face of undecipherable encrypted communications, and ~~require~~ would benefit from some means whereby encrypted data can be decrypted and read within a reasonable time and at a reasonable expenditure of resources.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Human rights and civil liberties

The rights of Canadians to privacy and to express themselves freely are constitutionally protected. Section 8 of the *Charter* guarantees Canadians the right to be free from "unreasonable search or seizure" which has been interpreted through jurisprudence [redacted] and [redacted] the right to freedom of expression may extend to both the production of cryptographic products and their use to protect the messages being expressed or data being stored. The protection of a reasonable expectation of privacy, and invasions of that privacy, [redacted] must be justified, must be authorized in law (and generally require [redacted] pre-authorization by the courts).

s.21(1)(a)

Formatted: Border: Bottom: (No border), Pattern: Clear

WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES

[redacted]

It is important to note that Canada is one of 33 signatories to the Wassenaar Arrangement which was established to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies (such as encryption software). Participating states seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities. The aim is also to prevent the acquisition of these items by terrorists.

Participating States control all items set forth in the List of Dual-Use Goods and Technologies and Munitions list, with the objective of preventing unauthorized transfers or re-transfers of those items. Items included on the lists focus on items designed for military use, and general technology and software notes (i.e. encryption software).

The participating states have an agreement to maintain national export controls on listed items, which are implemented via national legislation; are guided by agreed upon best practices, guidelines or elements; have agreed to report on transfers and denials of specific controlled items to destinations outside of the arrangement; and exchange information on sensitive dual-use goods and technologies.

BILL C-30 – PROTECTING CHILDREN FROM INTERNET PREDATORS ACT, 2012

In the past, in the context of work on lawful access issues, and most recently in former Bill C-30 (*Protecting Children from Internet Predators Act*, 2012, 41st Parliament, 1st session), legislative proposals were introduced, but did not come into force, to create requirements for telecommunications service

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

providers to decrypt communications where it was readily possible for the service provide to do so, in the context of lawful interception. However, telecommunications service providers were not required to develop specific decryption techniques themselves.

For example, if interception was successful but the data retrieved was encrypted by a tool that was implemented directly by the service provider, rather than the user, then the service provider would be asked to decrypt the data.

These proposals were supported by law enforcement. However, in the larger picture, these proposals would not have solved the problem posed by encryption in whole, nor did they purport to do so. This is particularly true given that many major IT companies have built mobile and other digital devices that enable individuals to encrypt and decrypt data at the user level.

Jurisdictional and International Challenges

Law enforcement and national security agencies can face other challenges when attempting to compel communication service providers to decrypt communications, as the international nature of the software market and the borderless nature of cyberspace, in addition to the locations (jurisdiction) of the communications service provider [redacted] In addition, many communication service providers, particularly software and application service providers, do not have physical premises in Canada, and may not be subject to Canadian jurisdiction. In order to be able to obtain information held by these companies, currently the principal process available is through the use of Mutual Legal Assistance Treaties (MLATs). Currently, MLAT processes are not always timely enough for the exigencies of investigations involving electronic evidence, nor were they designed for a high volume of requests that could ensue given the trend toward global inter-connectivity and challenges in relation to jurisdiction in the context of modern communications.

s.21(1)(a)

It is important to note that encryption and challenges being faced by law enforcement and national security agencies are the topic of on-going discussion and work in various international fora. Canada is not the only country exploring options that address the on-going need for capacity to address law enforcement and national security challenges arising from use of encryption, in a way that supports the many beneficial uses of encryption, including its value for cybersecurity but also takes into consideration the investigative needs of law enforcement, national security and regulatory agencies.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Audcent, Karen
Sent: 2016-Jun-17 12:29 PM
To: Sansom, Gareth; Wong, Normand
Cc: Angers, Lucie
Subject: [redacted]

Here is a quick TP mash up of Gareth's TPs and Norm's TPs, does this work? You'll note that I am now the author, which I did for convenience only and am happy to revise to either or both of you if you wish to see your name on this.
Karen

Talking Points [redacted]

s.15(1)

From: Sansom, Gareth
Sent: 2016-Jun-17 12:14 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: [redacted]

Although the request has now changed to be simply Talking Points, attached is the draft briefing note I prepared this morning to answer the two questions. It incorporates Norm's input on [redacted]

So, this may not be needed any longer but here it is anyway.
[redacted]
Regards,
Gareth

From: Audcent, Karen
Sent: Friday, June 17, 2016 10:42 AM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: The questions to be answered in the BN

s.13(1)(a)
s.15(1)

[redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

[redacted]

Karen

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

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Wong, Normand
Sent: 2016-Jun-17 1:04 PM
To: Thérien, Michelle
Cc: Angers, Lucie; Audcent, Karen; Sansom, Gareth
Subject:

Am forwarding this to Michelle to get approved. Martine came looking for it. Michelle you can send Martine the e-version too. I reviewed the version Gareth just sent and am fine with it.

Normand Wong
613.941.2341 o
613.791.4669 m

s.15(1)

From: Sansom, Gareth
Sent: 2016-Jun-17 12:49 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject:

Made a minor tweak to first bullet.
-Gareth

Talking Points

From: Audcent, Karen
Sent: Friday, June 17, 2016 12:29 PM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject:

Here is a quick TP mash up of Gareth's TPs and Norm's TPs, does this work? You'll note that I am now the author, which I did for convenience only and am happy to revise to either or both of you if you wish to see your name on this.
Karen

<< File: Talking Points Meeting France Encryption Keylogging.docx >>

From: Sansom, Gareth
Sent: 2016-Jun-17 12:14 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Although the request has now changed to be simply Talking Points, attached is the draft briefing note I prepared this morning to answer the two questions. It incorporates Norm's input on [redacted] s.15(1)

So, this may not be needed any longer but here it is anyway.
[redacted]

Regards,
Gareth

From: Audcent, Karen
Sent: Friday, June 17, 2016 10:42 AM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: The questions to be answered in the BN s.13(1)(a) s.15(1)

[redacted]

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

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Unclassified
2016-001959

Talking Points

[redacted]

s.15(1)
s.21(1)(a)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

[redacted]

s.15(1)
s.21(1)(a)

PREPARED BY
Karen Audcent
Senior Counsel
Criminal Law Policy Section
613-957-4733
Date

Formatted: Normal

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Thérien, Michelle
Sent: 2016-Jun-17 1:29 PM
To: Audcent, Karen; Wong, Normand; Sansom, Gareth
Cc: Angers, Lucie
Subject: [redacted]

Attachments:

Karen/Lucie

For your approval pls.. Martine is waiting for it. Thank you!

s.15(1)

Michelle L. Therien
Administrative Assistant | Adjointe administrative
Policy Sector/Secteur des politiques |
Criminal Law Policy Section | Politique en matière de droit pénal
284 Wellington Street | 284, rue Wellington
EMB-5053 | ECE-5053 Ottawa, ON K1A 0H8
michelle.therien@justice.gc.ca
Tel | : 613 946-2215
Fax | : 613 941-9310
Government of Canada | Gouvernement du Canada
Pensez vert avant d'imprimer / Before printing, think green

From: Thérien, Michelle
Sent: 2016-Jun-17 11:25 AM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>
Cc: Wong, Normand <Normand.Wong@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: [redacted]

Karen,

I have attached the approval slip for your review. Could Norm and Gareth send me the BN and TP once completed for formatting and I will print and bring you the hard copies for approval.

NOTE: pls. attach the documents to this e-mail.

Michelle L. Therien
Administrative Assistant | Adjointe administrative
Policy Sector/Secteur des politiques |
Criminal Law Policy Section | Politique en matière de droit pénal
284 Wellington Street | 284, rue Wellington
EMB-5053 | ECE-5053 Ottawa, ON K1A 0H8
michelle.therien@justice.gc.ca
Tel | : 613 946-2215
Fax | : 613 941-9310
Government of Canada | Gouvernement du Canada
Pensez vert avant d'imprimer / Before printing, think green

From: Valin, Martine
Sent: 2016-Jun-17 10:45 AM

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

To: Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Subject: [redacted]

Looks like they are combining both into one BN and one set of TPs

s.15(1)
s.21(1)(a)
s.21(1)(b)

Martine

From: Audcent, Karen
Sent: June 17, 2016 10:33 AM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Douglas, Michelle <Michelle.Douglas@justice.gc.ca>; Breithaupt, Doug <Doug.Breithaupt@justice.gc.ca>
Cc: Nesrallah, Tania <Tania.Nesrallah@justice.gc.ca>; Valin, Martine <Martine.Valin@justice.gc.ca>; Morency, Carole <Carole.Morency@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Subject: [redacted]

I've discussed with Gareth and with Norm, Gareth will draft a BN and TPs, Norm will draft some text and TPs on [redacted] and provide the text and TPs to Gareth to include in his note. Norm thought it would be difficult to give the Minister TPs [redacted] o us the easiest approach. We think we can have the BN and TPs drafted by end of day.

Karen

From: Angers, Lucie
Sent: 2016-Jun-17 8:27 AM
To: Douglas, Michelle <Michelle.Douglas@justice.gc.ca>; Breithaupt, Doug <Doug.Breithaupt@justice.gc.ca>
Cc: Nesrallah, Tania <Tania.Nesrallah@justice.gc.ca>; Valin, Martine <Martine.Valin@justice.gc.ca>; Morency, Carole <Carole.Morency@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Subject [redacted]

Given the earlier material, Gareth should be able to do it first thing this morning by updating the BN and TP to reflect the question asked. Norm and Karen, what about the other request? If we could do only TPs on this one it could probably also be done today. Michelle, would that work? Thanks, Lucie

Sent from my BlackBerry 10 smartphone on the Rogers network.

From: Douglas, Michelle
Sent: Friday, June 17, 2016 8:21 AM
To: Angers, Lucie; Breithaupt, Doug
Cc: Nesrallah, Tania; Valin, Martine; Morency, Carole; Audcent, Karen; Sansom, Gareth; Wong, Normand
Subject: [redacted]

Thanks, Lucie.

The package is going to the Minister's Office at noon today. In light of the timing, I suspect that this is information best put in the hands of the DM as he will be attending the meeting with the Minister. Do you think we could get something by end of day or early Monday?

Something quite brief or even some TPS (Q&A type thing) might be a good way to approach this.

The TPs should be prepared in English, please. The meeting will be fully interpreted.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Thanks very much!
Michelle

Sent from my BlackBerry

From: Angers, Lucie
Sent: Friday, June 17, 2016 7:56 AM
To: Douglas, Michelle; Breithaupt, Doug
Cc: Nesrallah, Tania; Valin, Martine; Morency, Carole; Audcent, Karen; Sansom, Gareth; Wong, Normand
Subject: [redacted]

s.15(1)
s.21(1)(b)

Hi Michelle, Gareth could prepare a BN. He prepared an excellent one for FPT DMS and could use part of it for for the first issue. [redacted] would it be you Norm? I vaguely remember one of you doing a BN on this year's ago?? Thanks, Lucie

Sent from my BlackBerry 10 smartphone on the Rogers network.

From: Douglas, Michelle
Sent: Thursday, June 16, 2016 12:18 PM
To: Angers, Lucie; Breithaupt, Doug
Cc: Nesrallah, Tania
Subject: [redacted]

Hi Doug and Lucie,

s.15(1)

[redacted]

Kindly advise.

Thanks,
Michelle

s.13(1)(a)

[redacted]

Pages 461 to / à 462

are withheld pursuant to section

sont retenues en vertu de l'article

13(1)(a)

of the Access to Information Act

de la Loi sur l'accès à l'information

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Department of Justice Canada | Ministère de la Justice Canada

Fiche d'approbation
Approval Slip

À remplir par le secteur / To be completed by sector **DOSSIER/FILE #2016-001959**

Objet / Subject: TPs [redacted] s.15(1)

Préparée par /
Prepared by: Norm Wong / Gareth Sansom

Cote de sécurité /
Security level: Protected

Personnel de soutien /
Administrative personnel: Michelle Therien

Numéro de téléphone /
Telephone number: 946-2212

Nombre de pièces jointes /
# of attachments:

Date limite à l'ULM /
Due at MLU: _____

Soumise pour approbation à **Sector approvals as required**	**Initiales** **Initials**	**Année** **Year**	**Mois** **Month**	**Journée** **Day**
KAREN AUDCENT, Senior Counsel, CLPS				
LUCIE ANGERS, Directrice et AG, SPMDP – Director and GC, CLPS, External Relations				
CAROLE MORENCY, DG et AGP, SPMDP - DG and SGC, CLPS				
DONALD K. PIRAGOFF, SADM				
WILLIAM F. PENTNEY, Deputy Minister				
Équipe du SM / DM-Team				

Approbation/signature/examen/du ministre demandé pour le :
Minister's signature/approval/review requested by: _____

Remarques / remarks: _____

À remplir par l'ULM / To be completed by MLU

À la demande de /Requested by:/ Veuillez faire parvenir à :/Please forward to:

_____

Reçue / received: _____

Revue interne / Seen by: _____

Rédaction par/ Edited by: _____

Received in MLU: _____

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Department of Justice Canada | Ministère de la Justice Canada

PROTECTED
2016-001959

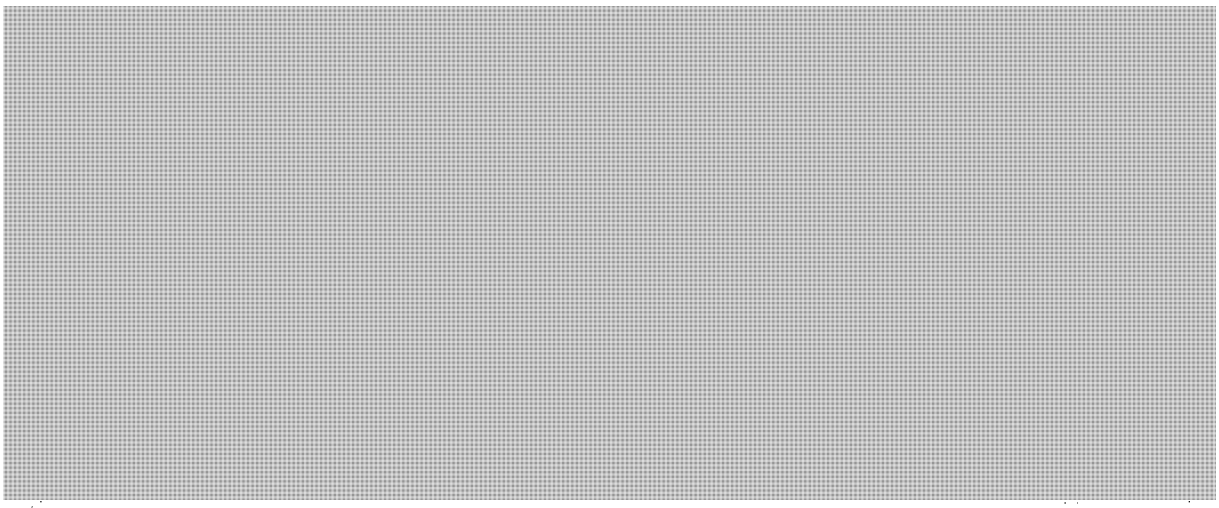
Talking Points

[redacted]

s.15(1)
s.21(1)(a)

000464

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.



PREPARED BY
Norm Wong / Gareth Sansom, Counsels
Criminal Law Policy Section
613-941-2341

s.15(1)
s.21(1)(a)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Audcent, Karen
Sent: 2016-Jun-17 1:34 PM
To: Angers, Lucie; Wong, Normand; Thérien, Michelle
Cc: Sansom, Gareth
Subject:

Ok I will revise and re-send

From: Angers, Lucie
Sent: 2016-Jun-17 1:33 PM
To: Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

s.15(1)
s.23

Thanks!

Could we clarify in the TPs? Thanks, Lucie

From: Wong, Normand
Sent: Friday, June 17, 2016 1:04 PM
To: Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

Am forwarding this to Michelle to get approved. Martine came looking for it. Michelle you can send Martine the e-version too. I reviewed the version Gareth just sent and am fine with it.

Normand Wong
613.941.2341 o
613.791.4669 m

From: Sansom, Gareth
Sent: 2016-Jun-17 12:49 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject:

Made a minor tweak to first bullet.
-Gareth

<< File: Talking Points v2.docx >>

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

From: Audcent, Karen
Sent: Friday, June 17, 2016 12:29 PM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: [redacted] s.15(1)

Here is a quick TP mash up of Gareth's TPs and Norm's TPs, does this work? You'll note that I am now the author, which I did for convenience only and am happy to revise to either or both of you if you wish to see your name on this.
Karen

<< File: Talking Points [redacted] docx >>

From: Sansom, Gareth
Sent: 2016-Jun-17 12:14 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: [redacted]

Although the request has now changed to be simply Talking Points, attached is the draft briefing note I prepared this morning to answer the two questions. It incorporates Norm's input on [redacted]

So, this may not be needed any longer but here it is anyway.
[redacted]
Regards,
Gareth

From: Audcent, Karen
Sent: Friday, June 17, 2016 10:42 AM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: The questions to be answered in the BN s.13(1)(a) s.15(1)

[redacted]

[redacted]

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

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

[redacted]

Karen

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

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Audcent, Karen
Sent: 2016-Jun-17 1:38 PM
To: Angers, Lucie; Wong, Normand; Thérien, Michelle
Cc: Sansom, Gareth
Subject: [redacted]

[redacted] does this work? Michelle I also revised the approval slip, revised slip is attached. Karen

s.15(1)

[redacted] Approval Slip v2.docx

From: Angers, Lucie
Sent: 2016-Jun-17 1:33 PM
To: Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: [redacted]

Thanks! [redacted]

Could we clarify in the TPs? Thanks, Lucie

From: Wong, Normand
Sent: Friday, June 17, 2016 1:04 PM
To: Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: [redacted]

Am forwarding this to Michelle to get approved. Martine came looking for it. Michelle you can send Martine the e-version too. I reviewed the version Gareth just sent and am fine with it.

Normand Wong
613.941.2341 o
613.791.4669 m

From: Sansom, Gareth
Sent: 2016-Jun-17 12:49 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: [redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Made a minor tweak to first bullet.
-Gareth

<< File: Talking Points [redacted] v2.docx >>
From: Audcent, Karen
Sent: Friday, June 17, 2016 12:29 PM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: [redacted]

Here is a quick TP mash up of Gareth's TPs and Norm's TPs, does this work? You'll note that I am now the author, which I did for convenience only and am happy to revise to either or both of you if you wish to see your name on this.
Karen

<< File: Talking Points [redacted] .docx >> s.15(1)

From: Sansom, Gareth
Sent: 2016-Jun-17 12:14 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: [redacted]

Although the request has now changed to be simply Talking Points, attached is the draft briefing note I prepared this morning to answer the two questions. It incorporates Norm's input on [redacted]

So, this may not be needed any longer but here it is anyway.

[redacted]
Regards,
Gareth

From: Audcent, Karen
Sent: Friday, June 17, 2016 10:42 AM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: The questions to be answered in the BN

s.13(1)(a)
s.15(1)

[redacted]

Released under the Access to Information Act
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.13(1)(a)
s.15(1)

[redacted]

[redacted]

Karen

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

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Department of Justice Canada | Ministère de la Justice Canada

Fiche d'approbation
Approval Slip

À remplir par le secteur / To be completed by sector **DOSSIER/FILE** #2016-001959

Objet / Subject: TPs for the [redacted] s.15(1)

Préparée par /
Prepared by: Karen Audcent

Cote de sécurité /
Security level: Unclassified

Personnel de soutien /
Administrative personnel: Michelle Therien

Numéro de téléphone /
Telephone number: 946-2212

Nombre de pièces jointes /
# of attachments:

Date limite à l'ULM /
Due at MLU: _____

Soumise pour approbation à **Sector approvals as required**	**Initiales** **Initials**	**Année** **Year**	**Mois** **Month**	**Journée** **Day**
LUCIE ANGERS, Directrice et AG, SPMDP – Director and GC, CLPS, External Relations				
CAROLE MORENCY, DG et AGP, SPMDP - DG and SGC, CLPS				
DONALD K. PIRAGOFF, SADM				
WILLIAM F. PENTNEY, Deputy Minister				
Équipe du SM / DM-Team				

Approbation/signature/examen/du ministre demandé pour le :
Minister's signature/approval/review requested by: _____

Remarques / remarks: _____

À remplir par l'ULM / To be completed by MLU

À la demande de /Requested by:/ Veuillez faire parvenir à :/Please forward to: _____

Revue interne / Seen by: _____

Rédaction par/ Edited by: _____

Reçue / received: _____

Received in MLU: _____

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Department of Justice Canada

Ministère de la Justice Canada

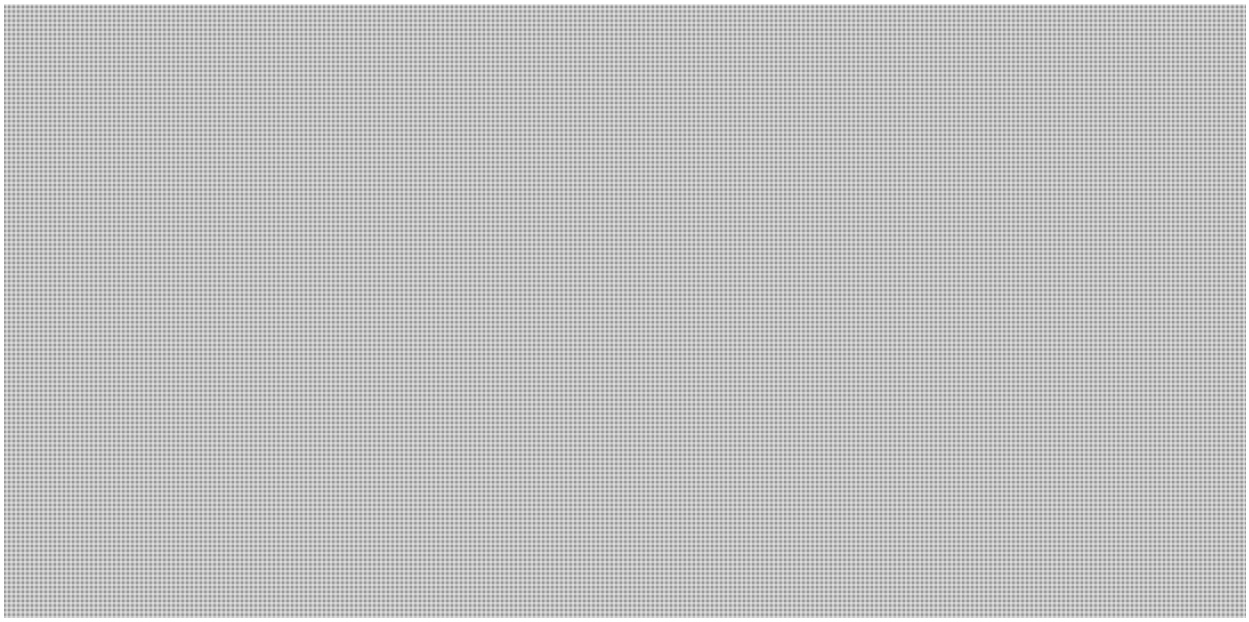
UNCLASSIFIED
2016-001959

Talking Points

[redacted]

s.15(1)
s.21(1)(a)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.



s.15(1)
s.21(1)(a)

PREPARED BY
Karen Audcent
Senior Counsel
Criminal Law Policy Section
613-957-4733

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Angers, Lucie
Sent: 2016-Jun-17 1:38 PM
To: Sansom, Gareth; Audcent, Karen; Wong, Normand
Subject:

Thanks, I'm sure we'll be able to use it in a not so distant future!

s.15(1)

From: Sansom, Gareth
Sent: Friday, June 17, 2016 12:14 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject:

Although the request has now changed to be simply Talking Points, attached is the draft briefing note I prepared this morning to answer the two questions. It incorporates Norm's input on

So, this may not be needed any longer but here it is anyway.

Regards,
Gareth

From: Audcent, Karen
Sent: Friday, June 17, 2016 10:42 AM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: The questions to be answered in the BN

s.13(1)(a)
s.15(1)

s.21(1)(a)
s.23 000475

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Karen

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Thérien, Michelle
Sent: 2016-Jun-17 1:38 PM
To: Audcent, Karen
Subject: [redacted]

Merci

Michelle L. Therien
Administrative Assistant | Adjointe administrative
Policy Sector/Secteur des politiques |
Criminal Law Policy Section | Politique en matière de droit pénal
284 Wellington Street | 284, rue Wellington
EMB-5053 | ECE-5053 Ottawa, ON K1A 0H8
michelle.therien@justice.gc.ca
Tel | : 613 946-2215
Fax | : 613 941-9310
Government of Canada | Gouvernement du Canada
Pensez vert avant d'imprimer / Before printing, think green

s.15(1)

From: Audcent, Karen
Sent: 2016-Jun-17 1:38 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: [redacted]

[redacted] does this work? Michelle I also revised the approval slip, revised slip is attached. Karen

<< File: Talking Points [redacted] v3.docx >> << File: Approval Slip v2.docx >>

From: Angers, Lucie
Sent: 2016-Jun-17 1:33 PM
To: Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: [redacted]

Thanks! [redacted]

Could we clarify in the TPs? Thanks, Lucie

From: Wong, Normand
Sent: Friday, June 17, 2016 1:04 PM
To: Thérien, Michelle <Michelle.Therien@justice.gc.ca>

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

Am forwarding this to Michelle to get approved. Martine came looking for it. Michelle you can send Martine the e-version too. I reviewed the version Gareth just sent and am fine with it.

Normand Wong
613.941.2341 o
613.791.4669 m

s.15(1)

From: Sansom, Gareth
Sent: 2016-Jun-17 12:49 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject:

Made a minor tweak to first bullet.
-Gareth

<< File: Talking Points v2.docx >>

From: Audcent, Karen
Sent: Friday, June 17, 2016 12:29 PM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject:

Here is a quick TP mash up of Gareth's TPs and Norm's TPs, does this work? You'll note that I am now the author, which I did for convenience only and am happy to revise to either or both of you if you wish to see your name on this.
Karen

<< File: Talking Points .docx >>

From: Sansom, Gareth
Sent: 2016-Jun-17 12:14 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject:

Although the request has now changed to be simply Talking Points, attached is the draft briefing note I prepared this morning to answer the two questions. It incorporates Norm's input on

So, this may not be needed any longer but here it is anyway.
<<
Regards,

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Gareth

From: Audcent, Karen
Sent: Friday, June 17, 2016 10:42 AM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: The questions to be answered in the BN

s.13(1)(a)
s.15(1)

[redacted]

[redacted]

Karen

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

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Audcent, Karen
Sent: 2016-Jun-17 1:56 PM
To: Angers, Lucie; Wong, Normand; Thérien, Michelle
Cc: Sansom, Gareth
Subject:

With a change from Norm to the fourth bullet. Karen

s.15(1)
s.21(1)(a)

From: Audcent, Karen
Sent: 2016-Jun-17 1:46 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

Here is a further change – although it is hard to get into much detail re is this helpful? Karen

<< File: Talking Points -v4.docx >>

From: Audcent, Karen
Sent: 2016-Jun-17 1:38 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

does this work? Michelle I also revised the approval slip, revised slip is attached. Karen

< << File: Approval Slip v2.docx >>

From: Angers, Lucie
Sent: 2016-Jun-17 1:33 PM
To: Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Thanks!

Could we clarify in the TPs? Thanks, Lucie

From: Wong, Normand
Sent: Friday, June 17, 2016 1:04 PM
To: Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

s.15(1)

Am forwarding this to Michelle to get approved. Martine came looking for it. Michelle you can send Martine the e-version too. I reviewed the version Gareth just sent and am fine with it.

Normand Wong
613.941.2341 o
613.791.4669 m

From: Sansom, Gareth
Sent: 2016-Jun-17 12:49 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject:

Made a minor tweak to first bullet.
-Gareth

<< File: Talking Points v2.docx >>

From: Audcent, Karen
Sent: Friday, June 17, 2016 12:29 PM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject:

Here is a quick TP mash up of Gareth's TPs and Norm's TPs, does this work? You'll note that I am now the author, which I did for convenience only and am happy to revise to either or both of you if you wish to see your name on this.
Karen

<

From: Sansom, Gareth
Sent: 2016-Jun-17 12:14 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: [redacted]

s.15(1)

Although the request has now changed to be simply Talking Points, attached is the draft briefing note I prepared this morning to answer the two questions. It incorporates Norm's input on [redacted]

So, this may not be needed any longer but here it is anyway.
[redacted]
Regards,
Gareth

From: Audcent, Karen
Sent: Friday, June 17, 2016 10:42 AM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: The questions to be answered in the BN

s.13(1)(a)
s.15(1)

[redacted]

[redacted]

Karen

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

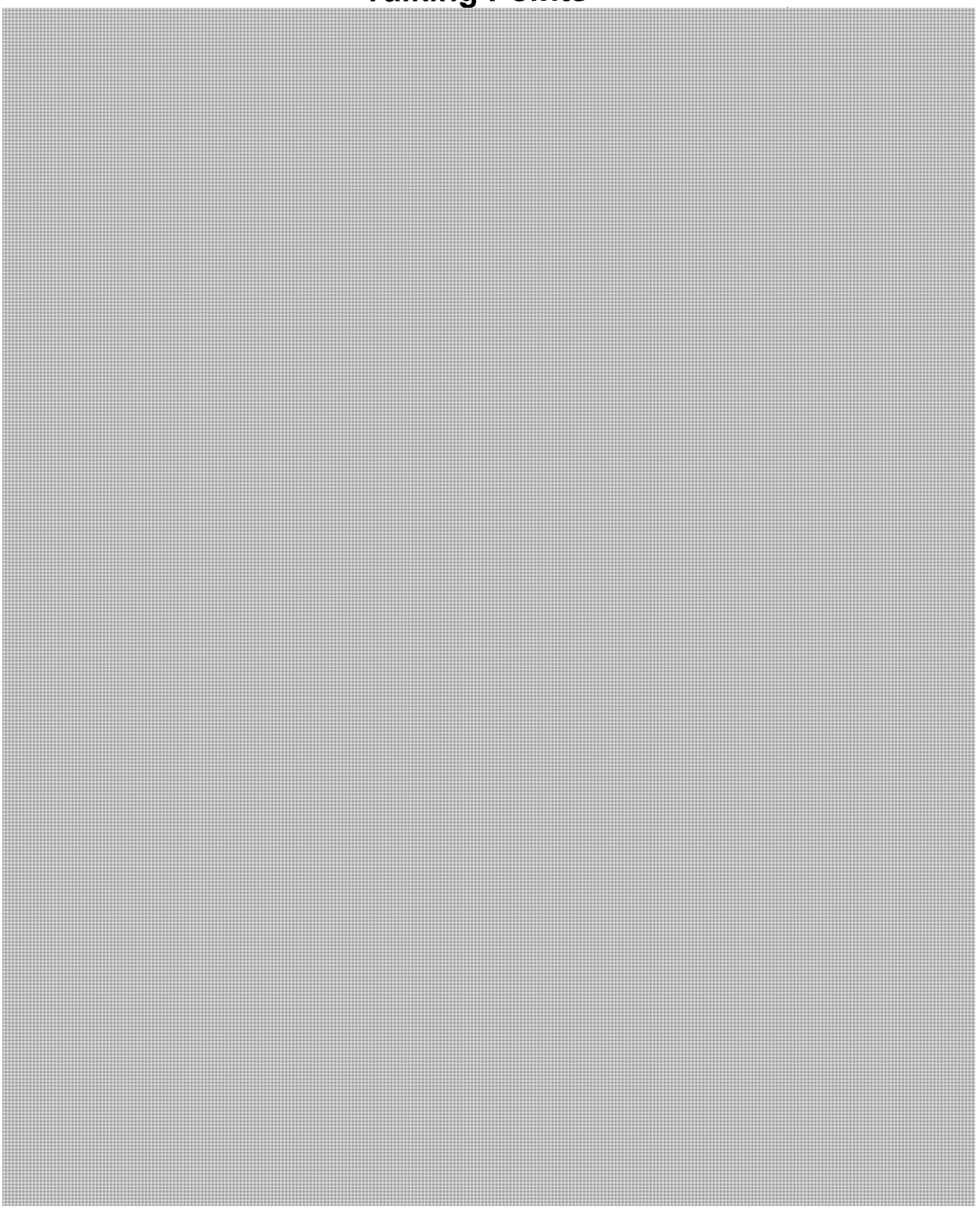
Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Department of Justice Canada | Ministère de la Justice Canada

UNCLASSIFIED
2016-001959

s.15(1)
s.21(1)(a)

Talking Points



Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.15(1)
s.21(1)(a)

PREPARED BY
Karen Audcent
Senior Counsel
Criminal Law Policy Section
613-957-4733

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Angers, Lucie
Sent: 2016-Jun-17 1:59 PM
To: Audcent, Karen; Wong, Normand; Thérien, Michelle
Cc: Sansom, Gareth
Subject: [redacted]

Talking Points [redacted]

s.15(1)

My concern was with the first bullet and I did some moving around. What about this?

From: Audcent, Karen
Sent: Friday, June 17, 2016 1:46 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: [redacted]

Here is a further change – although it is hard to get into much detail re [redacted] is this helpful? Karen

[redacted]

From: Audcent, Karen
Sent: 2016-Jun-17 1:38 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: [redacted]

[redacted] does this work? Michelle I also revised the approval slip, revised slip is attached. Karen

[redacted] << File: Approval Slip v2.docx >>

From: Angers, Lucie
Sent: 2016-Jun-17 1:33 PM
To: Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: [redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Thanks!

Could we clarify in the TPs? Thanks, Lucie

From: Wong, Normand
Sent: Friday, June 17, 2016 1:04 PM
To: Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

Am forwarding this to Michelle to get approved. Martine came looking for it. Michelle you can send Martine the e-version too. I reviewed the version Gareth just sent and am fine with it.

Normand Wong s.15(1)
613.941.2341 o
613.791.4669 m

From: Sansom, Gareth
Sent: 2016-Jun-17 12:49 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject:

Made a minor tweak to first bullet.
-Gareth

<< File: Talking Points v2.docx >>
From: Audcent, Karen
Sent: Friday, June 17, 2016 12:29 PM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject:

Here is a quick TP mash up of Gareth's TPs and Norm's TPs, does this work? You'll note that I am now the author, which I did for convenience only and am happy to revise to either or both of you if you wish to see your name on this.
Karen

From: Sansom, Gareth
Sent: 2016-Jun-17 12:14 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: [redacted] s.15(1) s.21(1)(a) s.23

Although the request has now changed to be simply Talking Points, attached is the draft briefing note I prepared this morning to answer the two questions. It incorporates Norm's input on [redacted]

So, this may not be needed any longer but here it is anyway.
[redacted]
Regards,
Gareth

From: Audcent, Karen
Sent: Friday, June 17, 2016 10:42 AM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca> s.13(1)(a)
Subject: The questions to be answered in the BN s.15(1)

[redacted]

[redacted]

Karen

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

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Department of Justice Canada | Ministère de la Justice Canada

UNCLASSIFIED
2016-001959

Talking Points

s.15(1)
s.21(1)(a)

[redacted]

Formatted: No bullets or numbering

Formatted: Bulleted + Level: 1 + Aligned at: 0 cm + Tab after: 0.64 cm + Indent at: 0.64 cm

Formatted: No bullets or numbering

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

[redacted]

s.15(1)

s.21(1)(a)

Formatted: Normal, Bulleted + Level: 1 + Aligned at: 0 cm + Tab after: 0.64 cm + Indent at: 0.64 cm

PREPARED BY
Karen Audcent
Senior Counsel
Criminal Law Policy Section
613-957-4733

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Sansom, Gareth
Sent: 2016-Jun-17 2:17 PM
To: Angers, Lucie; Audcent, Karen; Wong, Normand; Thérien, Michelle
Subject:

Works for me. In case you want greater precision I added a short sentence to the 4th (?) bullet – highlighted.

Talking Points

s.15(1)

-Gareth

From: Angers, Lucie
Sent: Friday, June 17, 2016 1:59 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject

<
My concern was with the first bullet and I did some moving around. What about this?

From: Audcent, Karen
Sent: Friday, June 17, 2016 1:46 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

Here is a further change – although it is hard to get into much detail re
), is this helpful? Karen

From: Audcent, Karen
Sent: 2016-Jun-17 1:38 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

[redacted] does this work? Michelle I also revised the approval slip, revised slip is attached. Karen

[redacted] << File: Approval Slip v2.docx >>

From: Angers, Lucie
Sent: 2016-Jun-17 1:33 PM
To: Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject [redacted]

Thanks! [redacted]

Could we clarify in the TPs? Thanks, Lucie

---

s.15(1)

From: Wong, Normand
Sent: Friday, June 17, 2016 1:04 PM
To: Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: [redacted]

Am forwarding this to Michelle to get approved. Martine came looking for it. Michelle you can send Martine the e-version too. I reviewed the version Gareth just sent and am fine with it.

Normand Wong
613.941.2341 o
613.791.4669 m

From: Sansom, Gareth
Sent: 2016-Jun-17 12:49 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: [redacted]

Made a minor tweak to first bullet.
-Gareth

<< [redacted] v2.docx >>
From: Audcent, Karen
Sent: Friday, June 17, 2016 12:29 PM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: [redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Here is a quick TP mash up of Gareth's TPs and Norm's TPs, does this work? You'll note that I am now the author, which I did for convenience only and am happy to revise to either or both of you if you wish to see your name on this.
Karen

<

s.15(1)

From: Sansom, Gareth
Sent: 2016-Jun-17 12:14 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject:

Although the request has now changed to be simply Talking Points, attached is the draft briefing note I prepared this morning to answer the two questions. It incorporates Norm's input on

So, this may not be needed any longer but here it is anyway.

Regards,
Gareth

From: Audcent, Karen
Sent: Friday, June 17, 2016 10:42 AM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: The questions to be answered in the BN

s.13(1)(a)
s.15(1)

Karen

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

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Department of Justice Canada | Ministère de la Justice Canada

UNCLASSIFIED
2016-001959

Talking Points

[redacted]

s.15(1)
s.21(1)(a)

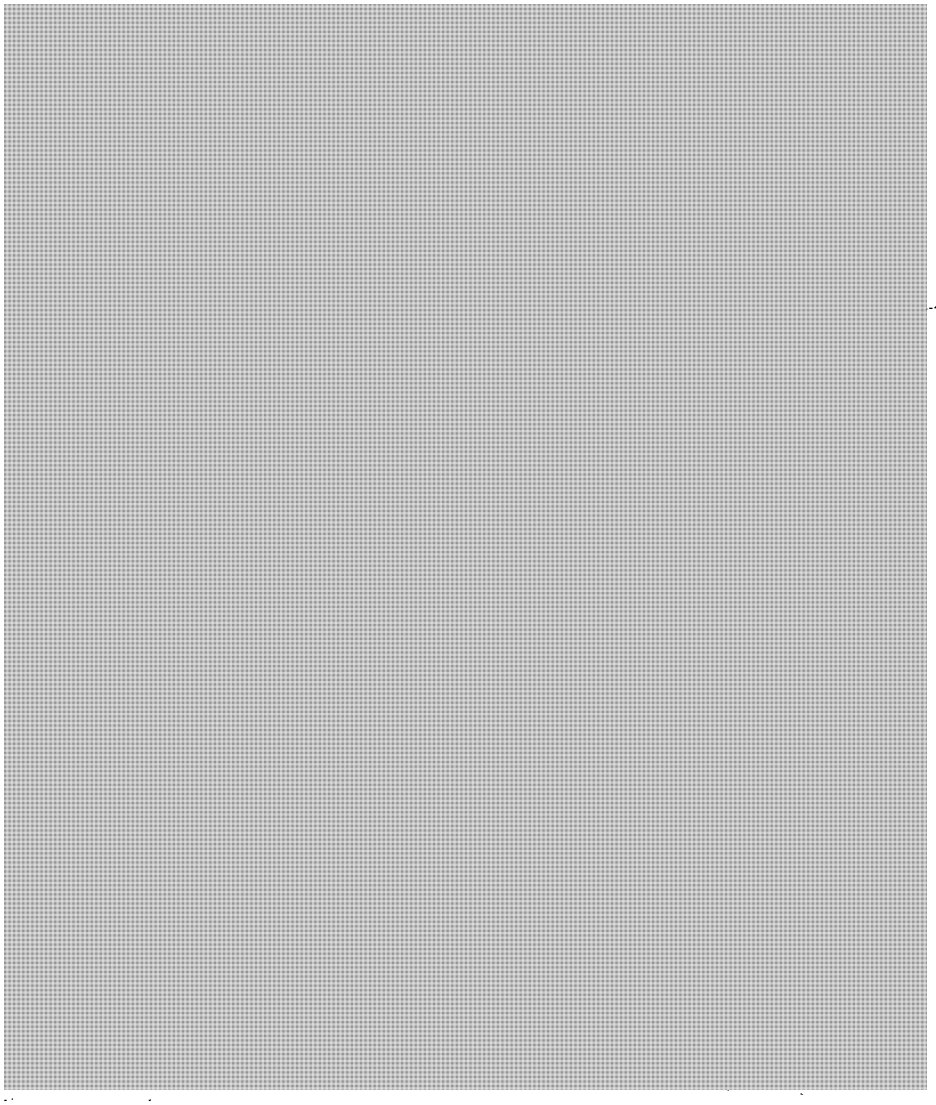
Formatted: No bullets or numbering

Formatted: Bulleted + Level: 1 + Aligned at: 0 cm + Tab after: 0.64 cm + Indent at: 0.64 cm

Formatted: No bullets or numbering

Formatted: Highlight

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.



s.15(1)
s.21(1)(a)

Formatted: Normal, Bulleted + Level: 1 + Aligned at: 0 cm + Tab after: 0.64 cm + Indent at: 0.64 cm

PREPARED BY
Karen Audcent
Senior Counsel
Criminal Law Policy Section
613-957-4733

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Audcent, Karen
Sent: 2016-Jun-17 2:23 PM
To: Angers, Lucie; Wong, Normand; Thérien, Michelle
Cc: Sansom, Gareth
Subject: [redacted]

With revisions to Lucie's version discussed on the phone with her. I'll do a changes accepted version and circulate it also. Karen

Talking Points [redacted]

s.15(1)

From: Angers, Lucie
Sent: 2016-Jun-17 1:59 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: [redacted]

[redacted]
My concern was with the first bullet and I did some moving around. What about this?

From: Audcent, Karen
Sent: Friday, June 17, 2016 1:46 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: [redacted]

Here is a further change – although it is hard to get into much detail re [redacted] is this helpful? Karen

<< File: [redacted] v4.docx >>

From: Audcent, Karen
Sent: 2016-Jun-17 1:38 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: [redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

[redacted] does this work? Michelle I also revised the approval slip, revised slip is attached. Karen

< [redacted] > << File: Approval Slip v2.docx >>

---

s.15(1)

From: Angers, Lucie
Sent: 2016-Jun-17 1:33 PM
To: Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: [redacted]

Thanks! [redacted]

Could we clarify in the TPs? Thanks, Lucie

From: Wong, Normand
Sent: Friday, June 17, 2016 1:04 PM
To: Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: [redacted]

Am forwarding this to Michelle to get approved. Martine came looking for it. Michelle you can send Martine the e-version too. I reviewed the version Gareth just sent and am fine with it.

Normand Wong
613.941.2341 o
613.791.4669 m

From: Sansom, Gareth
Sent: 2016-Jun-17 12:49 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: [redacted]

Made a minor tweak to first bullet.
-Gareth

[redacted]
v2.docx >>
From: Audcent, Karen
Sent: Friday, June 17, 2016 12:29 PM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: [redacted]

Here is a quick TP mash up of Gareth's TPs and Norm's TPs, does this work? You'll note that I am now the author, which I did for convenience only and am happy to revise to either or both of you if you wish to see your name on this.
Karen

s.15(1)

[redacted]

From: Sansom, Gareth
Sent: 2016-Jun-17 12:14 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: [redacted]

Although the request has now changed to be simply Talking Points, attached is the draft briefing note I prepared this morning to answer the two questions. It incorporates Norm's input on [redacted]

So, this may not be needed any longer but here it is anyway.
[redacted]
Regards,
Gareth

From: Audcent, Karen
Sent: Friday, June 17, 2016 10:42 AM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: The questions to be answered in the BN

s.13(1)(a)
s.15(1)

[redacted]

[redacted]

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

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Karen

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Department of Justice Canada | Ministère de la Justice Canada

UNCLASSIFIED
2016-001959

Talking Points

[redacted]

s.15(1)
s.21(1)(a)

Formatted: No bullets or numbering

Formatted: Bulleted + Level: 1 + Aligned at: 0 cm + Tab after: 0.64 cm + Indent at: 0.64 cm

Formatted: No bullets or numbering

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

[redacted]

s.15(1)
s.21(1)(a)

Formatted: Normal, Bulleted + Level: 1 + Aligned at: 0 cm + Tab after: 0.64 cm + Indent at: 0.64 cm

PREPARED BY
Karen Audcent
Senior Counsel
Criminal Law Policy Section
613-957-4733

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Audcent, Karen
Sent: 2016-Jun-17 2:27 PM
To: Angers, Lucie; Wong, Normand; Thérien, Michelle
Cc: Sansom, Gareth
Subject:

With changes accepted. Karen

Talking Points

s.15(1)

From: Audcent, Karen
Sent: 2016-Jun-17 2:23 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

With revisions to Lucie's version discussed on the phone with her. I'll do a changes accepted version and circulate it also. Karen

---

From: Angers, Lucie
Sent: 2016-Jun-17 1:59 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

My concern was with the first bullet and I did some moving around. What about this?

From: Audcent, Karen
Sent: Friday, June 17, 2016 1:46 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Here is a further change – although it is hard to get into much detail re [redacted] is this helpful? Karen

[redacted]

s.15(1)

From: Audcent, Karen
Sent: 2016-Jun-17 1:38 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: [redacted]

[redacted] does this work? Michelle I also revised the approval slip, revised slip is attached. Karen

[redacted] << File: Approval Slip v2.docx >>

From: Angers, Lucie
Sent: 2016-Jun-17 1:33 PM
To: Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: [redacted]

Thanks! [redacted]

Could we clarify in the TPs? Thanks, Lucie

From: Wong, Normand
Sent: Friday, June 17, 2016 1:04 PM
To: Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: [redacted]

Am forwarding this to Michelle to get approved. Martine came looking for it. Michelle you can send Martine the e-version too. I reviewed the version Gareth just sent and am fine with it.

Normand Wong
613.941.2341 o
613.791.4669 m

From: Sansom, Gareth
Sent: 2016-Jun-17 12:49 PM

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: [redacted]

s.15(1)

Made a minor tweak to first bullet.
-Gareth

[redacted]
v2.docx >>
From: Audcent, Karen
Sent: Friday, June 17, 2016 12:29 PM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: [redacted]

Here is a quick TP mash up of Gareth's TPs and Norm's TPs, does this work? You'll note that I am now the author, which I did for convenience only and am happy to revise to either or both of you if you wish to see your name on this.
Karen

[redacted]

From: Sansom, Gareth
Sent: 2016-Jun-17 12:14 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: [redacted]

Although the request has now changed to be simply Talking Points, attached is the draft briefing note I prepared this morning to answer the two questions. It incorporates Norm's input on [redacted]

So, this may not be needed any longer but here it is anyway.
[redacted]
Regards,
Gareth

From: Audcent, Karen
Sent: Friday, June 17, 2016 10:42 AM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: The questions to be answered in the BN

s.13(1)(a)
s.15(1)

[redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.13(1)(a)

s.15(1)

[redacted]

[redacted]

Karen

s.21(1)(a)

s.23

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Department of Justice Canada | Ministère de la Justice Canada

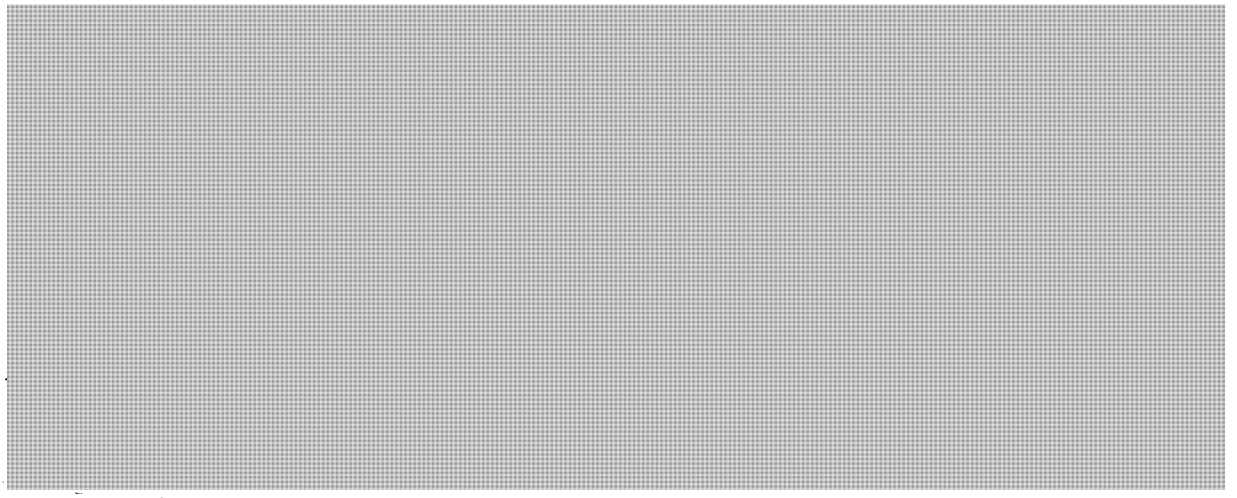
UNCLASSIFIED
2016-001959

Talking Points

[redacted]

s.15(1)
s.21(1)(a)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.



s.15(1)
s.21(1)(a)

PREPARED BY
Karen Audcent
Senior Counsel
Criminal Law Policy Section
613-957-4733

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Angers, Lucie
Sent: 2016-Jun-17 2:31 PM
To: Sansom, Gareth; Audcent, Karen; Wong, Normand; Thérien, Michelle
Subject: [redacted]

Beautiful, thanks (as I was just telling Karen ☺)!

s.15(1)

From: Sansom, Gareth
Sent: Friday, June 17, 2016 2:28 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Subject [redacted]

I am fine with it. My one tweak is to bullet four in case it is not obvious on a quick read. I suggest:

[redacted]

From: Audcent, Karen
Sent: Friday, June 17, 2016 2:23 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: [redacted]

With revisions to Lucie's version discussed on the phone with her. I'll do a changes accepted version and circulate it also. Karen

[redacted]

From: Angers, Lucie
Sent: 2016-Jun-17 1:59 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: [redacted]

<< [redacted]
My concern was with the first bullet and I did some moving around. What about this?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

From: Audcent, Karen
Sent: Friday, June 17, 2016 1:46 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: s.15(1)

Here is a further change – although it is hard to get into much detail re

is this helpful? Karen

<< File: Talking Points /4.docx >>

From: Audcent, Karen
Sent: 2016-Jun-17 1:38 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

does this work? Michelle I also revised the approval slip, revised slip is attached. Karen

<< File: Approval Slip v2.docx >>

From: Angers, Lucie
Sent: 2016-Jun-17 1:33 PM
To: Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

Thanks!

Could we clarify in the TPs? Thanks, Lucie

From: Wong, Normand
Sent: Friday, June 17, 2016 1:04 PM
To: Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Am forwarding this to Michelle to get approved. Martine came looking for it. Michelle you can send Martine the e-version too. I reviewed the version Gareth just sent and am fine with it.

Normand Wong
613.941.2341 o
613.791.4669 m

From: Sansom, Gareth
Sent: 2016-Jun-17 12:49 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: [redacted] **s.15(1)**

Made a minor tweak to first bullet.
-Gareth

<[redacted]
v2.docx >>
From: Audcent, Karen
Sent: Friday, June 17, 2016 12:29 PM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: [redacted]

Here is a quick TP mash up of Gareth's TPs and Norm's TPs, does this work? You'll note that I am now the author, which I did for convenience only and am happy to revise to either or both of you if you wish to see your name on this.
Karen

[redacted]

From: Sansom, Gareth
Sent: 2016-Jun-17 12:14 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: [redacted]

Although the request has now changed to be simply Talking Points, attached is the draft briefing note I prepared this morning to answer the two questions. It incorporates Norm's input on [redacted]

So, this may not be needed any longer but here it is anyway.
[redacted]
Regards,
Gareth

From: Audcent, Karen
Sent: Friday, June 17, 2016 10:42 AM

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: The questions to be answered in the BN

s.13(1)(a)

s.15(1)

[redacted]

[redacted]

Karen

s.21(1)(a)

s.23

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Audcent, Karen
Sent: 2016-Jun-17 2:34 PM
To: Angers, Lucie; Sansom, Gareth; Wong, Normand; Thérien, Michelle
Subject:

With Gareth's changes. Karen

Talking Points

From: Angers, Lucie
Sent: 2016-Jun-17 2:31 PM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Subject: s.15(1)

Also beautiful!

From: Sansom, Gareth
Sent: Friday, June 17, 2016 2:31 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Subject:

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

Last bullet possible modification to explain

From: Audcent, Karen
Sent: Friday, June 17, 2016 2:27 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

With changes accepted. Karen

<

s.15(1)

From: Audcent, Karen
Sent: 2016-Jun-17 2:23 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

With revisions to Lucie's version discussed on the phone with her. I'll do a changes accepted version and circulate it also. Karen

---

From: Angers, Lucie
Sent: 2016-Jun-17 1:59 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

My concern was with the first bullet and I did some moving around. What about this?

From: Audcent, Karen
Sent: Friday, June 17, 2016 1:46 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

Here is a further change – although it is hard to get into much detail re

is this helpful? Karen

<

From: Audcent, Karen
Sent: 2016-Jun-17 1:38 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

[redacted] does this work? Michelle I also revised the approval slip, revised slip is attached. Karen

<< [redacted] >> << File: Approval Slip v2.docx >>

s.15(1)

From: Angers, Lucie
Sent: 2016-Jun-17 1:33 PM
To: Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: [redacted]

Thanks! [redacted]

Could we clarify in the TPs? Thanks, Lucie

From: Wong, Normand
Sent: Friday, June 17, 2016 1:04 PM
To: Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: [redacted]

Am forwarding this to Michelle to get approved. Martine came looking for it. Michelle you can send Martine the e-version too. I reviewed the version Gareth just sent and am fine with it.

Normand Wong
613.941.2341 o
613.791.4669 m

From: Sansom, Gareth
Sent: 2016-Jun-17 12:49 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: [redacted]

Made a minor tweak to first bullet.
-Gareth

<[redacted] v2.docx >>
From: Audcent, Karen
Sent: Friday, June 17, 2016 12:29 PM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: [redacted]

Here is a quick TP mash up of Gareth's TPs and Norm's TPs, does this work? You'll note that I am now the author, which I did for convenience only and am happy to revise to either or both of you if you wish to see your name on this.
Karen

[redacted]> s.15(1)

From: Sansom, Gareth
Sent: 2016-Jun-17 12:14 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: [redacted]

Although the request has now changed to be simply Talking Points, attached is the draft briefing note I prepared this morning to answer the two questions. It incorporates Norm's input on [redacted]

So, this may not be needed any longer but here it is anyway.
[redacted]
Regards,
Gareth

From: Audcent, Karen
Sent: Friday, June 17, 2016 10:42 AM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject: The questions to be answered in the BN

s.13(1)(a)
s.15(1)

[redacted]

[redacted]

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

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Karen

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Department of Justice Canada

Ministère de la Justice Canada

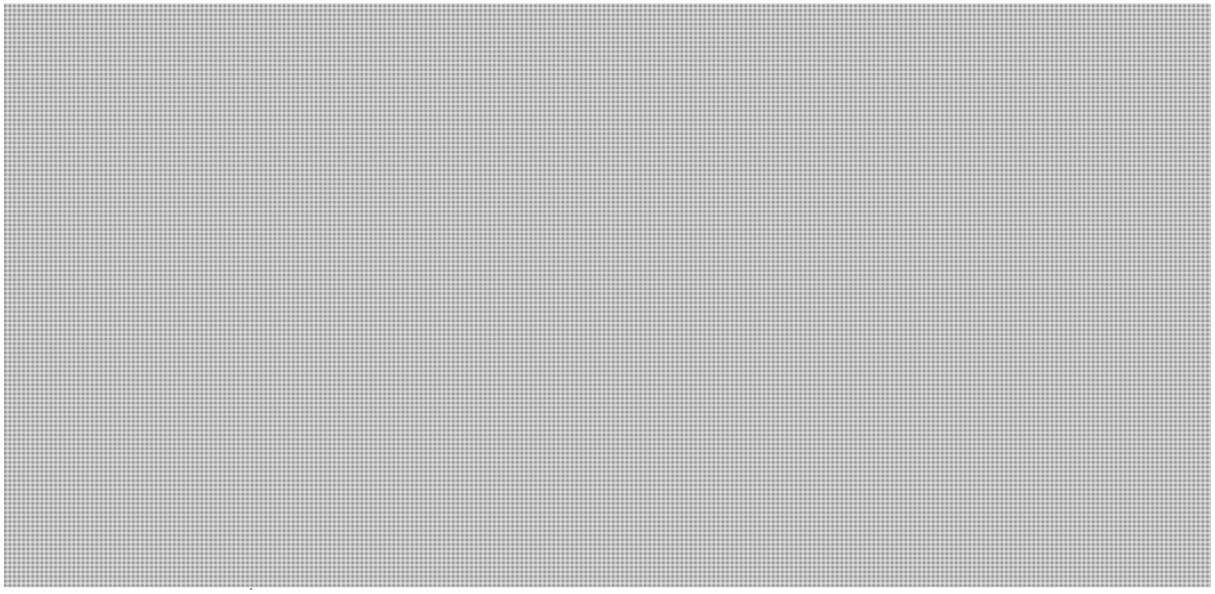
UNCLASSIFIED
2016-001959

Talking Points

[redacted]

s.15(1)
s.21(1)(a)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.



s.15(1)
s.21(1)(a)

PREPARED BY
Karen Audcent
Senior Counsel
Criminal Law Policy Section
613-957-4733

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Angers, Lucie
Sent: 2016-Jun-17 2:36 PM
To: Audcent, Karen; Sansom, Gareth; Wong, Normand; Thérien, Michelle
Subject:

Excellent, thanks!

s.15(1)

From: Audcent, Karen
Sent: Friday, June 17, 2016 2:34 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Subject:

With Gareth's changes. Karen

From: Angers, Lucie
Sent: 2016-Jun-17 2:31 PM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Subject

Also beautiful!

From: Sansom, Gareth
Sent: Friday, June 17, 2016 2:31 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Subject:

Last bullet possible modification to explain why national laws may not work:

From: Audcent, Karen
Sent: Friday, June 17, 2016 2:27 PM

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

With changes accepted. Karen s.15(1)

<

From: Audcent, Karen
Sent: 2016-Jun-17 2:23 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject

With revisions to Lucie's version discussed on the phone with her. I'll do a changes accepted version and circulate it also. Karen

---

From: Angers, Lucie
Sent: 2016-Jun-17 1:59 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

My concern was with the first bullet and I did some moving around. What about this?

From: Audcent, Karen
Sent: Friday, June 17, 2016 1:46 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

Here is a further change – although it is hard to get into much detail re is this helpful? Karen

<< File: v4.docx >>

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

From: Audcent, Karen
Sent: 2016-Jun-17 1:38 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

does this work? Michelle I also revised the approval slip, revised slip is attached. Karen

<< << File: Approval Slip v2.docx >>

From: Angers, Lucie
Sent: 2016-Jun-17 1:33 PM
To: Wong, Normand <Normand.Wong@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca> s.15(1)
Subject:

Thanks!

Could we clarify in the TPs? Thanks, Lucie

From: Wong, Normand
Sent: Friday, June 17, 2016 1:04 PM
To: Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

Am forwarding this to Michelle to get approved. Martine came looking for it. Michelle you can send Martine the e-version too. I reviewed the version Gareth just sent and am fine with it.

Normand Wong
613.941.2341 o
613.791.4669 m

From: Sansom, Gareth
Sent: 2016-Jun-17 12:49 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject:

Made a minor tweak to first bullet.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

-Gareth

---

v2.docx >>
From: Audcent, Karen
Sent: Friday, June 17, 2016 12:29 PM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca> s.15(1)
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject:

Here is a quick TP mash up of Gareth's TPs and Norm's TPs, does this work? You'll note that I am now the author, which I did for convenience only and am happy to revise to either or both of you if you wish to see your name on this.
Karen

From: Sansom, Gareth
Sent: 2016-Jun-17 12:14 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject:

Although the request has now changed to be simply Talking Points, attached is the draft briefing note I prepared this morning to answer the two questions. It incorporates Norm's input on

So, this may not be needed any longer but here it is anyway.

Regards,
Gareth

From: Audcent, Karen
Sent: Friday, June 17, 2016 10:42 AM
To: Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca> s.13(1)(a)
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca> s.15(1)
Subject: The questions to be answered in the BN

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

[redacted]

Karen

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

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Thérien, Michelle
Sent: 2016-Jun-17 2:39 PM
To: Audcent, Karen
Subject: [redacted]

Ok I am coming with the print version.

s.15(1)

Michelle L. Therien
Administrative Assistant | Adjointe administrative
Policy Sector/Secteur des politiques |
Criminal Law Policy Section | Politique en matière de droit pénal
284 Wellington Street | 284, rue Wellington
EMB-5053 | ECE-5053 Ottawa, ON K1A 0H8
michelle.therien@justice.gc.ca
Tel | : 613 946-2215
Fax | : 613 941-9310
Government of Canada | Gouvernement du Canada
Pensez vert avant d'imprimer / Before printing, think green

From: Audcent, Karen
Sent: 2016-Jun-17 2:38 PM
To: Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Subject: [redacted]

yes

From: Thérien, Michelle
Sent: 2016-Jun-17 2:37 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>
Subject: [redacted]

Karen,

Fixed the font for the classification. Is version 8 ready to go know.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

s.15(1)

From: Valin, Martine
Sent: 2016-Jun-17 2:53 PM
To: Douglas, Michelle; Nesrallah, Tania
Cc: Audcent, Karen; Wong, Normand; Angers, Lucie; Sansom, Gareth
Subject:
Attachments:

Approved by / approuvé par Carole Morency, Director General and SGC.

Martine Valin
Adjointe exécutive /Executive Assistant
Politique en matière de droit pénal / Criminal Law Policy
284 Wellington Street, Room 5093
Justice Canada
Ottawa, Ontario K1A 0H8
Tel: (613) 948-7423
Fax: (613) 957-6374
martine.valin@justice.gc.ca

From: Thérien, Michelle
Sent: June 17, 2016 2:42 PM
To: * CLP SGC/Admin <CLP_SGC_Admin@JUSTICE.GC.CA>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Millette, Pierre <Pierre.Millette@justice.gc.ca>
Subject:

As requested TP for

Michelle L. Therien
Administrative Assistant | Adjointe administrative
Policy Sector/Secteur des politiques |
Criminal Law Policy Section | Politique en matière de droit pénal
284 Wellington Street | 284, rue Wellington
EMB-5053 | ECE-5053 Ottawa, ON K1A 0H8
michelle.therien@justice.gc.ca
Tel | : 613 946-2215
Fax | : 613 941-9310
Government of Canada | Gouvernement du Canada
Pensez vert avant d'imprimer / Before printing, think green

From: Thérien, Michelle
Sent: 2016-Jun-17 1:29 PM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>
Subject:

Karen/Lucie

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

For your approval pls.. Martine is waiting for it. Thank you!

Michelle L. Therien
Administrative Assistant | Adjointe administrative
Policy Sector/Secteur des politiques |
Criminal Law Policy Section | Politique en matière de droit pénal
284 Wellington Street | 284, rue Wellington
EMB-5053 | ECE-5053 Ottawa, ON K1A 0H8
michelle.therien@justice.gc.ca
Tel | : 613 946-2215
Fax | : 613 941-9310
Government of Canada | Gouvernement du Canada
Pensez vert avant d'imprimer / Before printing, think green

s.15(1)

From: Thérien, Michelle
Sent: 2016-Jun-17 11:25 AM
To: Audcent, Karen <Karen.Audcent@justice.gc.ca>
Cc: Wong, Normand <Normand.Wong@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject:

Karen,

I have attached the approval slip for your review. Could Norm and Gareth send me the BN and TP once completed for formatting and I will print and bring you the hard copies for approval.

NOTE: pls. attach the documents to this e-mail.

Michelle L. Therien
Administrative Assistant | Adjointe administrative
Policy Sector/Secteur des politiques |
Criminal Law Policy Section | Politique en matière de droit pénal
284 Wellington Street | 284, rue Wellington
EMB-5053 | ECE-5053 Ottawa, ON K1A 0H8
michelle.therien@justice.gc.ca
Tel | : 613 946-2215
Fax | : 613 941-9310
Government of Canada | Gouvernement du Canada
Pensez vert avant d'imprimer / Before printing, think green

From: Valin, Martine
Sent: 2016-Jun-17 10:45 AM
To: Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Subject:

Looks like they are combining both into one BN and one set of TPs

Martine

From: Audcent, Karen
Sent: June 17, 2016 10:33 AM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Douglas, Michelle <Michelle.Douglas@justice.gc.ca>; Breithaupt, Doug <Doug.Breithaupt@justice.gc.ca>
Cc: Nesrallah, Tania <Tania.Nesrallah@justice.gc.ca>; Valin, Martine <Martine.Valin@justice.gc.ca>; Morency, Carole

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

<Carole.Morency@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Subject:

I've discussed with Gareth and with Norm, Gareth will draft a BN and TPs, Norm will draft some text and TPs on and provide the text and TPs to Gareth to include in his note. Norm thought it would be difficult to give the Minister TPs to us the easiest approach. We think we can have the BN and TPs drafted by end of day.

s.15(1)
s.21(1)(a)
s.21(1)(b)

Karen

From: Angers, Lucie
Sent: 2016-Jun-17 8:27 AM
To: Douglas, Michelle <Michelle.Douglas@justice.gc.ca>; Breithaupt, Doug <Doug.Breithaupt@justice.gc.ca>
Cc: Nesrallah, Tania <Tania.Nesrallah@justice.gc.ca>; Valin, Martine <Martine.Valin@justice.gc.ca>; Morency, Carole <Carole.Morency@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>
Subject:

Given the earlier material, Gareth should be able to do it first thing this morning by updating the BN and TP to reflect the question asked. Norm and Karen, what about the other request? If we could do only TPs on this one it could probably also be done today. Michelle, would that work? Thanks, Lucie

Sent from my BlackBerry 10 smartphone on the Rogers network.

From: Douglas, Michelle
Sent: Friday, June 17, 2016 8:21 AM
To: Angers, Lucie; Breithaupt, Doug
Cc: Nesrallah, Tania; Valin, Martine; Morency, Carole; Audcent, Karen; Sansom, Gareth; Wong, Normand
Subject:

Thanks, Lucie.

The package is going to the Minister's Office at noon today. In light of the timing, I suspect that this is information best put in the hands of the DM as he will be attending the meeting with the Minister. Do you think we could get something by end of day or early Monday?

Something quite brief or even some TPS (Q&A type thing) might be a good way to approach this.

The TPs should be prepared in English, please. The meeting will be fully interpreted.

Thanks very much!
Michelle

Sent from my BlackBerry

From: Angers, Lucie
Sent: Friday, June 17, 2016 7:56 AM
To: Douglas, Michelle; Breithaupt, Doug
Cc: Nesrallah, Tania; Valin, Martine; Morency, Carole; Audcent, Karen; Sansom, Gareth; Wong, Normand
Subject:

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.15(1)

s.21(1)(b)

Hi Michelle, Gareth could prepare a BN. He prepared an excellent one for FPT DMS and could use part of it for for the first issue. [redacted] would it be you Norm? I vaguely remember one of you doing a BN on this year's ago?? Thanks, Lucie

Sent from my BlackBerry 10 smartphone on the Rogers network.

From: Douglas, Michelle
Sent: Thursday, June 16, 2016 12:18 PM
To: Angers, Lucie; Breithaupt, Doug
Cc: Nesrallah, Tania
Subject: [redacted]

Hi Doug and Lucie,

[redacted]

Kindly advise.

Thanks,
Michelle

s.13(1)(a)

[redacted]

Pages 528 to / à 529

are withheld pursuant to section

sont retenues en vertu de l'article

13(1)(a)

of the Access to Information Act

de la Loi sur l'accès à l'information

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Department of Justice Canada | Ministère de la Justice Canada

UNCLASSIFIED
2016-001959

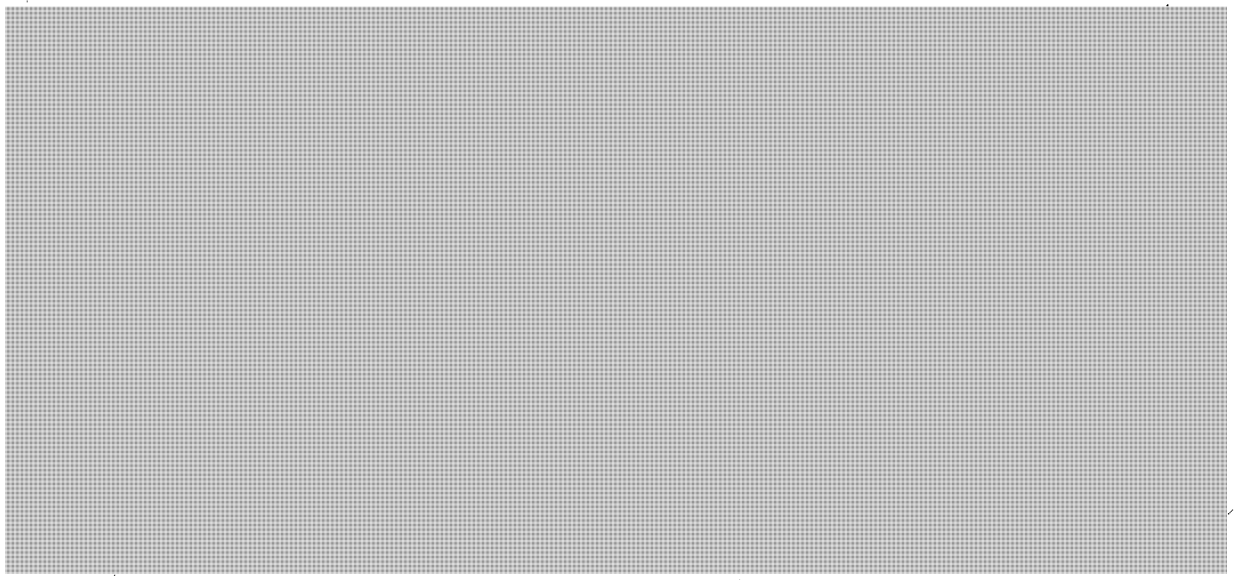
Talking Points

[redacted]

s.15(1)
s.21(1)(a)

000530

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.



s.15(1)
s.21(1)(a)

PREPARED BY
Karen Audcent
Senior Counsel
Criminal Law Policy Section
613-957-4733

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Sansom, Gareth
Sent: 2016-Jun-26 11:30 AM
To: Wong, Normand; Angers, Lucie
Cc: Audcent, Karen
Subject: Technical Annex - Encryption - revised
Attachments: 20160623 Lawful Access - Annex - Encryption _ [redacted] -GS-mod.docx

s.21(1)(a)

Hi Folks,
In order to help out Norm, I have given a close read to the most recent (I believe) amended version which [redacted] on Friday morning (via Lindsey).

In general, I am ok with [redacted] actual changes and most of their comments.

I have explicitly fixed one of the sentences they correctly suggested was unclear. I also fixed the "cryptography" versus ""encryption" (or appropriate verb tense) in a few spots which was mentioned at the outset. I made some minor tweaks and raised a comment of my own (but you can ignore it if you wish – it is the MLAT-IAG example).

Overall this should hopefully provide some assistance in sending back a reply to Lindsey on Monday.

Cheers,
Gareth

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

ANNEX Z

ENCRYPTION

INTRODUCTION

As our society and economy becomes ever more interwoven with the internet, encryption has become a critically important tool for safety, security and privacy online. Widely regarded as a best practice, encryption enhances security and protects privacy online and is commonly used to protect individual messages, personal devices and transmission channels. Encryption is central to electronic commerce, banking, cybersecurity, data and intellectual property protection. The use of encryption technologies has grown tremendously in both availability and use with the growth of the internet.

Cryptography is the practice and study of communications and the procedures, processes, and methods of making and using secret communications, such as codes or ciphers. One of the main fields in cryptography is encryption. To encrypt, means to make hidden or secret. Encryption uses a process or algorithm (sometimes known as a cipher) and converts a readable message into an unreadable encrypted message. In order to access the hidden or secret message, the user must have the key (which can be an algorithm or another type of code) to unlock it. Encryption plays an important role as it allows users to authenticate and safeguard sensitive data, and other information stored on computers or transmitted over closed or public networks.

While this technology provides tremendous benefits, it also gives criminals and terrorists additional means to avoid discovery, investigation and prosecution by concealing their activities. Law enforcement and national security agencies' concern relative to encryption is primarily that investigative techniques employed, under judicial authority, to obtain information, including interception of private communications (wiretap), production orders, and search warrants, can be made ineffective by the use of encryption. Encryption can be used by criminals or terrorists to prevent ~~an~~ investigators from being able to use the information obtained, which is needed to solve a crime or address a threat to Canada or Canada's interests. Encryption can also prevent law enforcement ~~and~~ from accessing information held by victims of crime (i.e. in the case of murdered, lost or missing individuals). Additionally, victims of technology-enabled crimes, such as theft, fraud, extortion (ransomware), are often surprised to learn that law enforcement agencies lack investigative techniques and authorities appropriately tailored toward cybercrime-related investigations. Left ~~completely undeterred~~unchecked, the costs of technology-enabled crime will likely increase, and may potentially lessen society's trust in the integrity of e-commerce, social media, and other telecom-enabled technology.

s.21(1)(a)

s.23

s.21(1)(a)

The lack of means whereby encrypted data can be decrypted and read within a reasonable time and reasonable expenditure of resources presents challenges for agencies involved in law enforcement and national security investigations in Canada. In order to be able to

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.23

effectively respond and adhere to their individual mandates, the agencies involved in law enforcement and national security investigations in Canada require appropriate solutions that provide them with the tools they need to keep Canada safe and secure while respecting Canadians' privacy and human rights. There is a tremendous benefit to having law enforcement and national security agencies that have the investigative tools required to achieve their individual mandates in an evolving digital world. Having the capability, with appropriate judicial authorization, to decrypt evidence that is encrypted. ~~This~~ would also assist Canada in meeting its international obligations to foreign partners.~~,~~

[redacted]

To date, this issue has not been directly addressed in law in Canada, and the question of if, or how, to address this challenge continues to make headlines in many jurisdictions around the world. In trying to address the challenges faced by law enforcement and national security agencies, some of the issues raised relate to:

- human rights, including privacy rights, freedom of expression, and the right against self-incrimination,
- commercial interests, such as competitiveness and the protection of intellectual property;
- jurisdictional implications; and
- the need for encryption to enable modern e-commerce, e-banking and all types of cybersecurity and protect critical infrastructure.

[redacted]

These issues, along with others, will be discussed further in this annex.

Commented [A6]: This sentence is a bit awkwardly worded and unclear.

Commented [A7]: This sentence is a bit awkwardly worded and unclear.

Commented [A8]: Agree that sentence was unclear – proposed the current revision.

TYPES OF ENCRYPTION

Encryption is technology that can be applied to data-in-use and data-at-rest. Any of these could have various layers of encryption applied to it by any or all of the following: the end user, third party applications, and telecommunication service providers.

Data-in-use, otherwise known as active data, is data that is live and under constant change and manipulation by an application. Data-in-use is physically stored in databases, ~~data warehouses,~~ spreadsheets, etc.. Data-at-rest is inactive data stored physically in ~~databases,~~ data warehouses, ~~spreadsheets,~~ archives, hard drives, tapes, off-site backups, mobile devices, etc.

In addition, encryption can be applied to more specific items such as the message itself (i.e. email, text message, or photo), the storage media of the device (i.e. the cell phone, the computer, the tablet), or the transmission network and/or channel (i.e. a VPN network, an enterprise server, or even the communication service provider's network).

[redacted]

s.21(1)(a)

POLICY AND LEGISLATION

THE GOVERNMENT OF CANADA'S ELECTRONIC COMMERCE STRATEGY & THE POLICY ON CRYPTOGRAPHY)

As of June 20, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Almost 20 years ago, in 1997-1998, Aan extensive review of Canada's Cryptography policy was undertaken ~~in 1997-1998~~ under the leadership of Industry Canada (now Innovation, Science, and Economic Development Canada) in the context of Canada's e-commerce policy but extended to the issues of law enforcement access and national security considerations. In 1998, Canada's Minister of Industry announced its Cryptography policy and, this policy remains in place today. In this policy, the Government affirmed the following principles:

1) The freedom of Canadians to develop, import and use whatever cryptography they wished;
2) Support for private sector research and development
3) The Government would not implement mandatory key recovery requirements or licensing regimes for certification authorities or trusted third parties;
4) Export controls would continue to be consistent with Canada's international obligations; and
5) The Government would explore legislative and other options to protect consumer privacy and to assist law enforcement and national security agencies.

The policy emphasized the importance of maintaining a balanced approach to a complex problem.

A number of key considerations played a role in helping shape Canada's Cryptography policy. The following were some significant developments that helped guide the policy development process:

s.21(1)(a)

- The increasing use of strong encryption software and computers powerful enough to encrypt and decrypt data easily were commonly available;
- The rapidly increasing use of telecommunications media suitable for encryption (e.g. email and other data conveyed via the Internet and other computer-based media) for both personal and commercial communications;
- The increasing use of wireless cellular telephones, which had created pressure for the development of digital equipment and had led to the encryption of their signals in some cases; and
- The increasing reliance on computers and computer networks for commercial activities and the need to protect privacy and security, which had led companies to store business records in secure computer facilities and in encrypted forms.

Notably, many of these developments are still relevant today given the proliferation of and reliance on the use of technology, encryption and digital communications. Both then, and now, encryption forms part of the core framework that allows electronic commerce to flourish.
In an effort to develop a cryptography framework, specific considerations were given to the areas of electronic commerce,

To date, these remain some of the key considerations

As of June 20, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Electronic Commerce

In 1998, more and more transactions were shifting from closed networks to open networks and cryptography became essential for the conduct of electronic commerce. Open networks allowed for more global trading, but came with a variety of security challenges including concerns over the authentication of communicating parties, the integrity of the data being communicated, the confidentiality of the proprietary or personal data, and the assurance that transactions have been authorized by legitimate users. Without cryptography, these challenges may not have been addressed.

The aims of law enforcement and business align when cryptography protects proprietary information, trade secrets, and in general, helps defend industry and consumers against fraud and other unlawful activities. In addition, cryptography meets national security objectives to the extent that it helps protect Canada, and its national critical infrastructure and valuable information.

The policy challenge was, and continues to be, the need to find solutions that will address the investigative challenges faced by law enforcement and national security agencies without interfering with legitimate business, institutional or individual interests and without weakening the security of the network infrastructure for all users. Furthermore, consideration will now need to be given to the current digital environment and the trend towards the use of end-to-end encryption by many companies within the information and communication technology sector.

A recent dispute in the U.S. between Apple and the FBI highlighted challenges in this alignment, when Apple refused to create a 'key' or 'backdoor' bypassing the encryption protecting (or locking) a suspect's iPhone. Ultimately, the FBI accessed the phone through a third party, but the dispute highlighted the complex issues faced in finding solutions to the challenges stemming from the widespread use of encryption

s.23

Investigative Challenges in a Digital Age

The development of new technologies has been transformative for law enforcement and national security agencies, playing an increasingly crucial role in their daily work, such as providing a number of additional tools to help advance their investigations. Courts too are relying more and more on digital evidence in legal proceedings. Yet, we have also seen new forms of criminal activity and threats, new methods of committing old crimes, and new ways of concealing evidence. The widespread use of ~~cryptography~~ encryption can raise concerns in this context because it can create obstacles to the detection and investigation of criminal activities and security threats, as well as the inspection of computer records subject to investigation.

Commented [A13]: This section seems to duplicate a portion of the introduction. Suggest it be shortened/ focussed as it reads somewhat redundant.

The roles and responsibilities of the law enforcement and national security agencies involved in investigations are diverse but include aspects such as: identifying threats and detecting, investigating and prosecuting matters related to terrorism, crimes of violence and related to property, and abuses of domestic and international commercial and financial systems. The

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

effectiveness of these agencies in monitoring criminal activities and threats to Canada's security, and in investigating and prosecuting offenders in Canada has depended on their lawful ability to conduct judicially authorized interception of specific private communications, or to search and inspect places and materials, including computers, where relevant information may be kept.

Commented [A14]: For example, this could be removed/combined with the text up front.

The increase in the use of ~~cryptography~~ encryption can provide concurrent, yet competing, outcomes; while it can provide enhanced technical protection for confidential information, it can also impede the ability to conduct lawful and authorized electronic surveillance. Notwithstanding the receipt of judicial authorizations for the interception of communications, intercepted data in an encrypted form may be unreadable and undecipherable for authorities. This makes it difficult for authorities to decipher the information, or to do so in time to be able to effectively use it or take action to prevent harm from occurring. As a result, law enforcement and national security agencies are challenged to effectively respond and adhere to their individual mandates in the face of undecipherable encrypted communications. Having appropriate, Charter-compliant investigative authorities tailored towards digital investigations would not only be a tremendous benefit to law enforcement and national security agencies in Canada, but it would also benefit Canada's international cooperation efforts as Canada's Mutual Legal Assistance in Criminal Matters Act generally requires that a court order be obtained to send evidence to a foreign partner. To obtain such an order, it is necessary to describe the evidence to be sent, which becomes impossible when potentially relevant electronic evidence is encrypted.

s.23

[redacted]

Human rights and civil liberties

The rights of Canadians to privacy and to express themselves freely are constitutionally protected. Section 8 of the *Charter* guarantees Canadians the right to be free from "unreasonable search or seizure" which has been interpreted through jurisprudence [redacted], and the right to freedom of expression may extend to both the production of cryptographic products and their use to protect the messages being expressed or data being stored. The protection of a reasonable expectation of privacy, and invasions of that privacy must be justified, must be authorized in law and generally require specific pre-authorization by the courts.

~~Canadians also have human rights protections under international human rights law with regard to privacy and freedom of expression. Canada is a State party to the International Covenant on Civil and Political Rights. Article 17 of the Covenant prohibits interferences with privacy that are arbitrary or unlawful and Article 19 guarantees an individual's freedom of expression.~~

[redacted]

WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES

Canada is one of 41 participating states to the Wassenaar Arrangement which was established to contribute to regional and international security and stability, by promoting transparency and

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

greater responsibility in transfers of conventional arms and dual-use goods and technologies. Participating states seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities. The aim is also to prevent the acquisition of these items by terrorists.
Participating States control all items set forth in the Munitions List (items designed for military use) and the List of Dual-Use Goods and Technologies (items having both civilian and military applications such as encryption software),with the objective of preventing unauthorized transfers or re-transfers of those items.
The participating states have an agreement to maintain national export controls on listed items, which are implemented via national legislation; are guided by agreed upon best practices, guidelines or elements; have agreed to report on transfers and denials of specific controlled items to destinations outside of the arrangement; and exchange information on sensitive dual-use goods and technologies.

BILL C-30 – *PROTECTING CHILDREN FROM INTERNET PREDATORS ACT*, 2012

In the past, in the context of work on lawful access issues, and most recently in former Bill C-30 (*Protecting Children from Internet Predators Act*, 2012, 41st Parliament, 1st session), legislative proposals were introduced, but did not come into force, to create requirements for telecommunications service providers to decrypt communications where it was readily possible for the service provide to do so, in the context of lawful interception. However, telecommunications service providers were not required to develop specific decryption techniques themselves. For example, if interception was successful but the data retrieved was encrypted by a tool that was implemented directly by the service provider, rather than the user, then the service provider would be asked to decrypt the data.

These proposals were supported by law enforcement and national security agencies. However, in the larger picture, these proposals would not have solved the problem posed by encryption in whole, nor did they purport to do so. This is particularly true given that many major IT companies have built mobile and other digital devices that enable individuals to encrypt and decrypt data at the user level.

JURISDICTIONAL AND INTERNATIONAL CONSIDERATIONS

Law enforcement and national security agencies also face challenges when attempting to compel communication service providers to decrypt communications. Many communication service providers, particularly software and application service providers, do not have physical premises in Canada, and may not be subject to Canadian jurisdiction. In order to be able to obtain information held by these companies, currently the principal process available is through the use of Mutual Legal Assistance Treaties (MLATs). Currently, MLAT processes are not always timely enough for the exigencies of investigations involving electronic evidence, nor were they designed for a high volume of requests that could ensue given the trend toward global inter-connectivity and challenges in relation to jurisdiction in the context of modern communications.

As of June 20, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

It is important to note that the complex challenges involving encryption ~~and~~ are the topic of on-going discussion and work in various international fora. The subject of how best to address the challenges for law enforcement and national security agencies arising from the use of encryption while supporting its many beneficial uses is an issue also being explored by many of Canada's closest allies.

DRAFT

As of June 20, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Angers, Lucie
Sent: 2016-Jun-27 8:24 AM
To: Sansom, Gareth; Wong, Normand
Cc: Audcent, Karen
Subject: RE: Technical Annex - Encryption - revised
Attachments: 20160623 Lawful Access - Annex - Encryption [redacted]GS-mod rev la.docx

s.21(1)(a)

I agree with Gareth that this document needs a bit more work and needs to be tightened. I added a few more comments in his revised version. Thanks, Lucie

---

From: Sansom, Gareth
Sent: Sunday, June 26, 2016 11:30 AM
To: Wong, Normand <Normand.Wong@justice.gc.ca>; Angers, Lucie <Lucie.Angers@justice.gc.ca>
Cc: Audcent, Karen <Karen.Audcent@justice.gc.ca>
Subject: Technical Annex - Encryption - revised

Hi Folks,
In order to help out Norm, I have given a close read to the most recent (I believe) amended version which [redacted] on Friday morning (via Lindsey).

In general, I am ok with the [redacted] actual changes and most of their comments.

I have explicitly fixed one of the sentences they correctly suggested was unclear. I also fixed the "cryptography" versus ""encryption" (or appropriate verb tense) in a few spots which was mentioned at the outset. I made some minor tweaks and raised a comment of my own (but you can ignore it if you wish – it is the MLAT-IAG example).

Overall this should hopefully provide some assistance in sending back a reply to Lindsey on Monday.

Cheers,
Gareth

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

ANNEX Z

ENCRYPTION

INTRODUCTION

As our society and economy becomes ever more interwoven with the internet, encryption has become a critically important tool for safety, security and privacy online. Widely regarded as a best practice, encryption enhances security and protects privacy online and is commonly used to protect individual messages, personal devices and transmission channels. Encryption is central to electronic commerce, banking, cybersecurity, data and intellectual property protection. The use of encryption technologies has grown tremendously in both availability and use with the growth of the internet.

Cryptography is the practice and study of communications and the procedures, processes, and methods of making and using secret communications, such as codes or ciphers. One of the main fields in cryptography is encryption. To encrypt, means to make hidden or secret. Encryption uses a process or algorithm (sometimes known as a cipher) and converts a readable message into an unreadable encrypted message. In order to access the hidden or secret message, the user must have the key (which can be an algorithm or another type of code) to unlock it. Encryption plays an important role as it allows users to authenticate and safeguard sensitive data, and other information stored on computers or transmitted over closed or public networks.

Commented [A1]: Another pass through this document is required to standardize the use of 'encryption' vs 'cryptography'.

This paragraph does a good job of describing encryption as a composite element of the science of cryptography. Later in the document, however (pages 4-5), 'cryptography' pops up again in the generic sense (subsections on Electronic Commerce; and Investigative Challenges in a Digital Age).

Commented [A2]: I agree with the above comment. Both terms are properly used in this paragraph. I have made two amendments below changing "cryptography" to "encryption" (or its verb) where it was appropriate.

While this technology provides tremendous benefits, it also gives criminals and terrorists additional means to avoid discovery, investigation, and prosecution by concealing their activities. Law enforcement and national security agencies' concern relative to encryption is primarily that investigative techniques employed, under judicial authority, to obtain information, including interception of private communications (wiretap), production orders, and search warrants, can be made ineffective by the use of encryption. Encryption can be used by criminals or terrorists to prevent ~~an~~ investigators from being able to use the information obtained, which is needed to solve a crime or address a threat to Canada or Canada's interests. Encryption can also prevent law enforcement [redacted] from accessing information held by victims of crime (i.e., in the case of murdered, lost or missing individuals). ~~Additionally, victims of technology-enabled crimes, such as theft, fraud, extortion (ransomware), are often surprised to learn that law enforcement agencies lack investigative techniques and authorities appropriately tailored toward cybercrime-related investigations.~~ Left ~~completely undeterred~~unchecked, the costs of technology-enabled crime will likely increase, and may potentially lessen society's trust in the integrity of e-commerce, social media, and other telecom-enabled technology.

s.21(1)(a)

s.23

Commented [A3]: Not clearly relevant.

[redacted] The lack of means whereby encrypted data can be decrypted and read within a reasonable time and reasonable expenditure of resources presents challenges for agencies involved in law enforcement and national security investigations in Canada. In order to be able to

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.23

effectively respond and adhere to their individual mandates, these agencies ~~involved in law enforcement and national security investigations in Canada~~ require appropriate solutions that provide them with the tools they need to keep Canada safe and secure while respecting Canadians' privacy and human rights. There is a tremendous benefit to having law enforcement and national security agencies that have the investigative tools required to achieve their individual mandates in an evolving digital world. Having the capability, with appropriate judicial authorization, to decrypt evidence that is encrypted. ~~This~~ would also assist Canada in meeting its international obligations to foreign partners.

[redacted]

Commented [A7]: This sentence is a bit awkwardly worded and unclear.

Commented [A8]: This sentence is a bit awkwardly worded and unclear.

Commented [A9]: Agree that sentence was unclear – proposed the current revision.

To date, this issue has not been ~~directly~~ addressed in law in Canada, and the question of if, or how, to address this challenge continues to make headlines in many jurisdictions around the world. In trying to address the challenges faced by law enforcement and national security agencies, some of the issues raised relate to:

- human rights, including privacy rights, freedom of expression, and the right against self-incrimination,
- commercial interests, such as competitiveness and the protection of intellectual property;
- jurisdictional implications; and
- the need for encryption to enable modern e-commerce, e-banking and all types of cybersecurity and protect critical infrastructure.

[redacted]

These issues, along with others, will be discussed further in this annex.

TYPES OF ENCRYPTION

Encryption is technology that can be applied to data-in-use and data-at-rest. Any of these could have various layers of encryption applied to it by any or all of the following: the end user, third party applications, and telecommunication service providers.

s.21(1)(a)

Data-in-use, otherwise known as active data, is data that is live and under constant change and manipulation by an application. Data-in-use is physically stored in databases, ~~data warehouses,~~ spreadsheets, etc.. Data-at-rest is inactive data stored physically in ~~databases, data~~ warehouses, ~~spreadsheets,~~ archives, hard drives, tapes, off-site backups, mobile devices, etc.

[redacted]

In addition, encryption can be applied to more specific items such as the message itself (i.e. email, text message, or photo), the storage media of the device (i.e. the cell phone, the computer, the tablet), or the transmission network and/or channel (i.e. a VPN network, an enterprise server, or even the communication service provider's network).

POLICY AND LEGISLATION

THE GOVERNMENT OF CANADA'S ELECTRONIC COMMERCE STRATEGY & THE POLICY ON CRYPTOGRAPHY)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Almost 20 years ago, in 1997-1998, Aan extensive review of Canada's Cryptography policy was undertaken ~~in 1997-1998~~ under the leadership of Industry Canada (now Innovation, Science, and Economic Development Canada) in the context of Canada's e-commerce policy but extended to the issues of law enforcement access and national security considerations. In 1998, Canada's Minister of Industry announced its Cryptography policy and, this policy remains in place today. In this policy, the Government affirmed the following principles:

1) The freedom of Canadians to develop, import and use whatever cryptography they wished;
2) Support for private sector research and development;
3) The Government would not implement mandatory key recovery requirements or licensing regimes for certification authorities or trusted third parties;
4) Export controls would continue to be consistent with Canada's international obligations; and
5) The Government would explore legislative and other options to protect consumer privacy and to assist law enforcement and national security agencies.

s.21(1)(a)

The policy emphasized the importance of maintaining a balanced approach to a complex problem.

A number of key considerations played a role in helping shape Canada's Cryptography policy. The following were some significant developments that helped guide the policy development process:

- The increasing use of strong encryption software and computers powerful enough to encrypt and decrypt data easily were commonly available;
- The rapidly increasing use of telecommunications media suitable for encryption (e.g., email and other data conveyed via the Internet and other computer-based media) for both personal and commercial communications;
- The increasing use of wireless cellular telephones, which had created pressure for the development of digital equipment and had led to the encryption of their signals in some cases; and
- The increasing reliance on computers and computer networks for commercial activities and the need to protect privacy and security, which had led companies to store business records in secure computer facilities and in encrypted forms.

Notably, many of these developments are still relevant today given the proliferation of and reliance on the use of technology, encryption and digital communications. Both then, and now, encryption forms part of the core framework that allows electronic commerce to flourish.
In an effort to develop a cryptography framework, specific considerations were given to the areas of electronic commerce,

To date, these remain some of the key considerations

As of June 20, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Electronic Commerce

In 1998, more and more transactions were shifting from closed networks to open networks and cryptography became essential for the conduct of electronic commerce. Open networks allowed for more global trading, but came with a variety of security challenges including concerns over the authentication of communicating parties, the integrity of the data being communicated, the confidentiality of the proprietary or personal data, and the assurance that transactions have been authorized by legitimate users. Without cryptography, these challenges may not have been addressed.

The aims of law enforcement and business align when cryptography protects proprietary information, trade secrets, and in general, helps defend industry and consumers against fraud and other unlawful activities. In addition, cryptography meets national security objectives to the extent that it helps protect Canada, and its national critical infrastructure and valuable information.

The policy challenge was, and continues to be, the need to find solutions that will address the investigative challenges faced by law enforcement and national security agencies without interfering with legitimate business, institutional or individual interests and without weakening the security of the network infrastructure for all users. Furthermore, consideration will now need to be given to the current digital environment and the trend towards the use of end-to-end encryption by many companies within the information and communication technology sector.

s.23

A recent dispute in the U.S. between Apple and the FBI highlighted challenges in this alignment, when Apple refused to create a 'key' or 'backdoor' bypassing the encryption protecting (or locking) a suspect's iPhone. Ultimately, the FBI accessed the phone through a third party, but the dispute highlighted the complex issues faced in finding solutions to the challenges stemming from the widespread use of encryption.

Investigative Challenges in a Digital Age

Commented [A14]: This section seems to duplicate a portion of the introduction. Suggest it be shortened/ focussed as it reads somewhat redundant.

The development of new technologies has been transformative for law enforcement and national security agencies, playing an increasingly crucial role in their daily work, such as providing a number of additional tools to help advance their investigations. Courts too are relying more and more on digital evidence in legal proceedings. Yet, we have also seen new forms of criminal activity and threats, new methods of committing old crimes, and new ways of concealing evidence. The widespread use of ~~cryptography~~ encryption can raise concerns in this context because it can create obstacles to the detection and investigation of criminal activities and security threats, as well as the inspection of computer records subject to investigation.

The roles and responsibilities of the law enforcement and national security agencies involved in investigations are diverse but include aspects such as: identifying threats and detecting, investigating and prosecuting matters related to terrorism, crimes of violence and related to property, and abuses of domestic and international commercial and financial systems. The

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

effectiveness of these agencies in monitoring criminal activities and threats to Canada's security, and in investigating and prosecuting offenders in Canada has depended on their lawful ability to conduct judicially authorized interception of specific private communications, or to search and inspect places and materials, including computers, where relevant information may be kept.

Commented [A15]: For example, this could be removed/combined with the text up front.

The increase in the use of ~~cryptography~~ encryption can provide concurrent, yet competing, outcomes; while it can provide enhanced technical protection for confidential information, it can also impede the ability to conduct lawful and authorized electronic surveillance. Notwithstanding the receipt of judicial authorizations for the interception of communications, intercepted data in an encrypted form may be unreadable and undecipherable for authorities. This makes it difficult for authorities to decipher the information, or to do so in time to be able to effectively use it or take action to prevent harm from occurring. As a result, law enforcement and national security agencies are challenged to effectively respond and adhere to their individual mandates in the face of undecipherable encrypted communications. Having appropriate, Charter-compliant investigative authorities tailored towards digital investigations would not only be a tremendous benefit to law enforcement and national security agencies in Canada, but it would also benefit Canada's international cooperation efforts as Canada's Mutual Legal Assistance in Criminal Matters Act generally requires that a court order be obtained to send evidence to a foreign partner. To obtain such an order, it is necessary to describe the evidence to be sent, which becomes impossible when potentially relevant electronic evidence is encrypted.

s.23

[redacted]

Human rights and civil liberties

The rights of Canadians to privacy and to express themselves freely are constitutionally protected. Section 8 of the *Charter* guarantees Canadians the right to be free from "unreasonable search or seizure" which has been interpreted through jurisprudence as [redacted] and the right to freedom of expression may extend to both the production of cryptographic products and their use to protect the messages being expressed or data being stored. The protection of a reasonable expectation of privacy, and invasions of that privacy must be justified, must be authorized in law and generally require specific pre-authorization by the courts.

[redacted]

~~Canadians also have human rights protections under international human rights law with regard to privacy and freedom of expression. Canada is a State party to the International Covenant on Civil and Political Rights. Article 17 of the Covenant prohibits interferences with privacy that are arbitrary or unlawful and Article 19 guarantees an individual's freedom of expression.~~

WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES

Canada is one of 41 participating states to the Wassenaar Arrangement which was established to contribute to regional and international security and stability, by promoting transparency and

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

greater responsibility in transfers of conventional arms and dual-use goods and technologies. Participating states seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities. The aim is also to prevent the acquisition of these items by terrorists.

Participating States control all items set forth in the Munitions List (items designed for military use) and the List of Dual-Use Goods and Technologies (items having both civilian and military applications such as encryption software), with the objective of preventing unauthorized transfers or re-transfers of those items.

s.21(1)(a)

The participating states have an agreement to maintain national export controls on listed items, which are implemented via national legislation; are guided by agreed upon best practices, guidelines or elements; have agreed to report on transfers and denials of specific controlled items to destinations outside of the arrangement; and exchange information on sensitive dual-use goods and technologies.

Commented [A22]: The relevance of this section with encryption needs to be better explained for the general public to understand the link.

FORMER BILL C-30 – *PROTECTING CHILDREN FROM INTERNET PREDATORS ACT*, 2012

In the past, in the context of work on lawful access issues, and most recently in former Bill C-30 (*Protecting Children from Internet Predators Act*, 2012, 41st Parliament, 1st session), legislative proposals were introduced, but did not come into force, to create requirements for telecommunications service providers to decrypt communications where it was readily possible for the service provide to do so, in the context of lawful interception. However, telecommunications service providers were not required to develop specific decryption techniques themselves. For example, if interception was successful but the data retrieved was encrypted by a tool that was implemented directly by the service provider, rather than the user, then the service provider would be asked to decrypt the data.

Commented [A23]: Not sure that 2012 qualifies as being recent?

These proposals were supported by law enforcement and national security agencies. However, ~~in the larger picture,~~ these proposals would not have solved the problem posed by encryption in whole, nor did they purport to do so. This is particularly true given that many major IT companies have built mobile and other digital devices that enable individuals to encrypt and decrypt data at the user level.

JURISDICTIONAL AND INTERNATIONAL CONSIDERATIONS

Law enforcement and national security agencies also face challenges when attempting to compel communication service providers to decrypt communications. Many communication service providers, particularly software and application service providers, do not have physical premises in Canada, and may not be subject to Canadian jurisdiction. In order to be able to obtain information held by these companies, currently the principal process available is through the use of Mutual Legal Assistance Treaties (MLATs). Currently, MLAT processes are not always timely enough for the exigencies of investigations involving electronic evidence, nor were they designed for a high volume of requests that could ensue given the trend toward global inter-connectivity and challenges in relation to jurisdiction in the context of modern communications.

As of June 20, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

It is important to note that the complex challenges involving encryption ~~and~~ are the topic of on-going discussion and work in various international fora. The subject of how best to address the challenges for law enforcement and national security agencies arising from the use of encryption while supporting its many beneficial uses is an issue also being explored by many of Canada's closest allies.

DRAFT

As of June 20, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

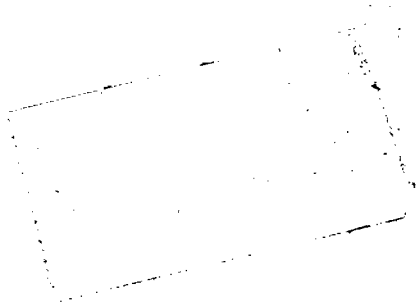
Audcent, Karen

From: Wong, Normand
Sent: 2016-Jun-27 4:10 PM
To: 'Oakes, Lindsey (PS/SP)'
Cc: Angers, Lucie; Audcent, Karen; Sansom, Gareth
Subject: 20160623 Lawful Access - Annex - Encryption _ GS-mod rev la nw.docx
Attachments: 20160623 Lawful Access - Annex - Encryption _ GS-mod rev la nw.docx

Our comments. They are mainly comments and not suggested text although I did provide some suggested text. I think we are generally of the view that it needs work to tighten up. The part on the history is good,

I'll look at the data retention piece now.

s.21(1)(a)



Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

ANNEX Z

[redacted]

s.23

INTRODUCTION

As our society and economy becomes ever more interwoven with the internet, encryption has become a critically important tool for safety, security and privacy online. Widely regarded as a best practice, encryption enhances security and protects privacy online and is commonly used to protect individual messages, personal devices and transmission channels. Encryption is central to electronic commerce, banking, cybersecurity, data and intellectual property protection. The use of encryption technologies has grown tremendously in both availability and use with the growth of the internet.

s.21(1)(a)

Cryptography is the practice and study of ~~communications and~~ the procedures, processes, and methods of making and using secret communications, such as codes or ciphers. One of the main fields in cryptography is encryption. To encrypt, means to make hidden or secret. Encryption uses a process, often an ~~or~~ algorithm (sometimes known as a cipher) ~~and~~ to converts a readable message into an unreadable encrypted message. In order to access the hidden or secret message, the user must have the key (which can be an algorithm or another type of code) to unlock it. Encryption plays an important role as it allows users to authenticate and safeguard sensitive data, and other information stored on computers or transmitted over closed or public networks.

Commented [A2]: Another pass through this document is required to standardize the use of 'encryption' vs 'cryptography'.

This paragraph does a good job of describing encryption as a composite element of the science of cryptography. Later in the document, however (pages 4-5), 'cryptography' pops up again in the generic sense (subsections on Electronic Commerce; and Investigative Challenges in a Digital Age).

Commented [A3]: I agree with the above comment. Both terms are properly used in this paragraph. I have made two amendments below changing "cryptography" to "encryption" (or its verb) where it was appropriate.

While this technology provides tremendous benefits, it also gives criminals and terrorists additional means to avoid discovery, investigation, and prosecution by concealing their activities. Law enforcement and national security agencies' concern relative to encryption is primarily that investigative techniques employed, under judicial authority, to obtain information, including interception of private communications (wiretap), production orders, and search warrants, can be made ineffective by the use of encryption. Encryption can be used by criminals or terrorists to prevent ~~an~~ investigators from being able to use the information obtained, which is needed to solve a crime or address a threat to Canada or Canada's interests. Encryption can also prevent law enforcement [redacted] from accessing information held by victims of crime (i.e., in the case of murdered, ~~lost~~ or missing individuals). ~~Additionally, victims of technology-enabled crimes, such as theft, fraud, extortion (ransomware), are often surprised to learn that law enforcement agencies lack investigative techniques and authorities appropriately tailored toward cybercrime-related investigations.~~ Left ~~completely undeterred~~unchecked, the costs of technology-enabled crime will likely increase, and may potentially lessen society's trust in the integrity of e-commerce, social media, and other telecom-enabled technology.

s.23

Commented [A4]: Not clearly relevant.

[redacted] The lack of means whereby encrypted data can be decrypted and read within a reasonable time and reasonable expenditure of resources presents challenges for agencies involved in law enforcement and national security investigations in Canada. In order to be able to

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

effectively respond and adhere to their individual mandates, these agencies ~~involved in law enforcement and national security investigations in Canada~~ require appropriate solutions that provide them with the tools they need to keep Canada safe and secure while respecting Canadians' privacy and human rights. There is a tremendous benefit to having law enforcement and national security agencies that have the investigative tools required to achieve their individual mandates in an evolving digital world. Having the capability, with appropriate judicial authorization, to decrypt evidence that is encrypted. ~~This~~ would also assist Canada in meeting its international obligations to foreign partners.

s.23

[redacted]

To date, this issue has not been ~~directly~~ addressed in law in Canada, and the question of if, or how, to address this challenge continues to make headlines in many jurisdictions around the world. In trying to address the challenges faced by law enforcement and national security agencies, some of the issues raised relate to:

- human rights, including privacy rights, freedom of expression, and the right against self-incrimination,
- commercial interests, such as competitiveness and the protection of intellectual property;
- jurisdictional implications; and
- the need for encryption to enable modern e-commerce, e-banking and all types of cybersecurity and protect critical infrastructure.

[redacted]

Commented [A9]: This sentence is a bit awkwardly worded and unclear.

Commented [A10]: This sentence is a bit awkwardly worded and unclear.

Commented [A11]: Agree that sentence was unclear – proposed the current revision.

These issues, along with others, will be discussed further in this annex.

TYPES OF ENCRYPTION

Encryption is technology that can be applied to data-in-use and data-at-rest. Any of these could have various layers of encryption applied to it by any or all of the following: the end user, third party applications, and telecommunication service providers.

s.21(1)(a)

[redacted]

Data-in-use, otherwise known as active data, is data that is live and under constant change and manipulation by an application. Data-in-use is physically stored in databases, ~~data warehouses,~~ spreadsheets, etc.. Data-at-rest is inactive data stored physically in ~~databases,~~ data warehouses, ~~spreadsheets,~~ archives, hard drives, tapes, off-site backups, mobile devices, etc.

In addition, encryption can be applied to more specific items such as the message itself (i.e. email, text message, or photo), the storage media of the device (i.e. the cell phone, the computer, the tablet), or the transmission network and/or channel (i.e. a VPN network, an enterprise server, or even the communication service provider's network).

POLICY AND LEGISLATION

THE GOVERNMENT OF CANADA'S ELECTRONIC COMMERCE STRATEGY & THE POLICY ON CRYPTOGRAPHY)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Electronic Commerce

In 1998, more and more transactions were shifting from closed networks to open networks and cryptography became essential for the conduct of electronic commerce. Open networks allowed for more global trading, but came with a variety of security challenges including concerns over the authentication of communicating parties, the integrity of the data being communicated, the confidentiality of the proprietary or personal data, and the assurance that transactions have been authorized by legitimate users. Without cryptography, these challenges may not have been addressed.

The aims of law enforcement and business align when cryptography protects proprietary information, trade secrets, and in general, helps defend industry and consumers against fraud and other unlawful activities. In addition, cryptography meets national security objectives to the extent that it helps protect Canada, and its national critical infrastructure and valuable information.

The policy challenge was, and continues to be, the need to find solutions that will address the investigative challenges faced by law enforcement and national security agencies without interfering with legitimate business, institutional or individual interests and without weakening the security of the network infrastructure for all users. Furthermore, consideration will now need to be given to the current digital environment and the trend towards the use of end-to-end encryption by many companies within the information and communication technology sector.

A recent dispute in the U.S. between Apple and the FBI highlighted challenges in this alignment, when Apple refused to create a 'key' or 'backdoor' bypassing the encryption protecting (or locking) a suspect's iPhone. Ultimately, the FBI accessed the phone through a third party, but the dispute highlighted the complex issues faced in finding solutions to the challenges stemming from the widespread use of encryption ~~importance service providers and their clients place on privacy rights and the challenges faced by law enforcement~~.

s.23

Investigative Challenges in a Digital Age

The development of new technologies has been transformative for law enforcement and national security agencies, playing an increasingly crucial role in their daily work, such as providing a number of additional tools to help advance their investigations. Courts too are relying more and more on digital evidence in legal proceedings. Yet, we have also seen new forms of criminal activity and threats, new methods of committing old crimes, and new ways of concealing evidence. The widespread use of ~~cryptography~~ encryption can raise concerns in this context because it can create obstacles to the detection and investigation of criminal activities and security threats, as well as the inspection of computer records subject to investigation.

Commented [A17]: This section seems to duplicate a portion of the introduction. Suggest it be shortened/ focussed as it reads somewhat redundant.

The roles and responsibilities of the law enforcement and national security agencies involved in investigations are diverse but include aspects such as: identifying threats and detecting, investigating and prosecuting matters related to terrorism, crimes of violence and related to

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Almost 20 years ago, in 1997-1998, ~~A~~an extensive review of Canada's Cryptography policy was undertaken ~~in 1997-1998~~ under the leadership of Industry Canada (now Innovation, Science, and Economic Development Canada) in the context of Canada's e-commerce policy but extended to the issues of law enforcement access and national security considerations. In 1998, Canada's Minister of Industry announced its Cryptography policy and, this policy remains in place today.

In this policy, the Government affirmed the following principles:

1) The freedom of Canadians to develop, import and use whatever cryptography they wished;
2) Support for private sector research and development;
3) The Government would not implement mandatory key recovery requirements or licensing regimes for certification authorities or trusted third parties;
4) Export controls would continue to be consistent with Canada's international obligations; and
5) The Government would explore legislative and other options to protect consumer privacy and to assist law enforcement and national security agencies.

The policy emphasized the importance of maintaining a balanced approach to a complex problem.

s.21(1)(a)

A number of key considerations played a role in helping shape Canada's Cryptography policy. The following were some significant developments that helped guide the policy development process:

- The increasing use of strong encryption software and computers powerful enough to encrypt and decrypt data easily were commonly available;
- The rapidly increasing use of telecommunications media suitable for encryption (e.g., email and other data conveyed via the Internet and other computer-based media) for both personal and commercial communications;
- The increasing use of wireless cellular telephones, which had created pressure for the development of digital equipment and had led to the encryption of their signals in some cases; and
- The increasing reliance on computers and computer networks for commercial activities and the need to protect privacy and security, which had led companies to store business records in secure computer facilities and in encrypted forms.

Notably, many of these developments are still relevant today given the proliferation of and reliance on the use of technology, encryption and digital communications. Both then, and now, encryption forms part of the core framework that allows electronic commerce to flourish.
In an effort to develop a cryptography framework, specific considerations were given to the areas of electronic commerce,

To date, these remain some of the key considerations

As of June 20, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Canada is one of 41 participating states to the Wassenaar Arrangement which was established to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies. Participating states seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities. The aim is also to prevent the acquisition of these items by terrorists.

Participating States control all items set forth in the Munitions List (items designed for military use) and the List of Dual-Use Goods and Technologies (items having both civilian and military applications such as encryption software),with the objective of preventing unauthorized transfers or re-transfers of those items.

The participating states have an agreement to maintain national export controls on listed items, which are implemented via national legislation; are guided by agreed upon best practices, guidelines or elements; have agreed to report on transfers and denials of specific controlled items to destinations outside of the arrangement; and exchange information on sensitive dual-use goods and technologies.

s.21(1)(a)

[redacted]

FORMER BILL C-30 – *PROTECTING CHILDREN FROM INTERNET PREDATORS ACT*, 2012

In the past, in the context of work on lawful access issues, and most recently in former Bill C-30 (*Protecting Children from Internet Predators Act*, 2012, 41st Parliament, 1st session), legislative proposals were introduced, but did not come into force, to create requirements for telecommunications service providers to decrypt communications where it was readily possible for the service provide to do so, in the context of lawful interception. However, telecommunications service providers were not required to develop specific decryption techniques themselves. For example, if interception was successful but the data retrieved was encrypted by a tool that was implemented directly by the service provider, rather than the user, then the service provider would be asked to decrypt the data.

[redacted]

These proposals were supported by law enforcement and national security agencies. However, ~~in the larger picture,~~ these proposals would not have solved the problem posed by encryption in whole, nor did they purport to do so. This is particularly true given that many major IT companies have built mobile and other digital devices that enable individuals to encrypt and decrypt data at the user level.

JURISDICTIONAL AND INTERNATIONAL CONSIDERATIONS

Law enforcement and national security agencies also face challenges when attempting to compel communication service providers to decrypt communications. Many communication service providers, particularly software and application service providers, do not have physical premises in Canada, and may not be subject to Canadian jurisdiction. In order to be able to obtain information held by these companies, currently the principal process available is through the use of Mutual Legal Assistance Treaties (MLATs). Currently, MLAT processes are not always timely enough for the exigencies of investigations involving electronic evidence, nor were they designed for a high volume of requests that could ensue given the trend toward global inter-connectivity and challenges in relation to jurisdiction in the context of modern communications.

As of June 20, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

property, and abuses of domestic and international commercial and financial systems. The effectiveness of these agencies in monitoring criminal activities and threats to Canada's security, and in investigating and prosecuting offenders in Canada has depended on their lawful ability to conduct judicially authorized interception of specific private communications, or to search and inspect places and materials, including computers, where relevant information may be kept.

Commented [A18]: For example, this could be removed/combined with the text up front.

The increase in the use of ~~cryptography~~ encryption can provide concurrent, yet competing, outcomes; while it can provide enhanced technical protection for confidential information, it can also impede the ability to conduct lawful and authorized electronic surveillance. Notwithstanding the receipt of judicial authorizations for the interception of communications, intercepted data in an encrypted form may be unreadable and undecipherable for authorities. This makes it difficult for authorities to decipher the information, or to do so in time to be able to effectively use it or take action to prevent harm from occurring. As a result, law enforcement and national security agencies are challenged to effectively respond and adhere to their individual mandates in the face of undecipherable encrypted communications. Having appropriate, Charter-compliant investigative authorities tailored towards digital investigations would not only be a tremendous benefit to law enforcement and national security agencies in Canada, but it would also benefit Canada's international cooperation efforts as Canada's Mutual Legal Assistance in Criminal Matters Act generally requires that a court order be obtained to send evidence to a foreign partner. To obtain such an order, it is necessary to describe the evidence to be sent, which becomes impossible when potentially relevant electronic evidence is encrypted.

s.23

[redacted]

Human rights and civil liberties

The rights of Canadians to privacy and to express themselves freely are constitutionally protected. Section 8 of the *Charter* guarantees Canadians the right to be free from "unreasonable search or seizure" which has been interpreted through jurisprudence [redacted] and the right to freedom of expression may extend to both the production of cryptographic products and their use to protect the messages being expressed or data being stored. The protection of a reasonable expectation of privacy, and invasions of that privacy must be justified, must be authorized in law and generally require specific pre-authorization by the courts.

[redacted]

~~Canadians also have human rights protections under international human rights law with regard to privacy and freedom of expression. Canada is a State party to the International Covenant on Civil and Political Rights. Article 17 of the Covenant prohibits interferences with privacy that are arbitrary or unlawful and Article 19 guarantees an individual's freedom of expression.~~

WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES

[redacted]

As of June 20, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

It is important to note that the complex challenges involving encryption ~~and~~ are the topic of on-going discussion and work in various international fora. The subject of how best to address the challenges for law enforcement and national security agencies arising from the use of encryption while supporting its many beneficial uses is an issue also being explored by many of Canada's closest allies.

As of June 20, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Wong, Normand
Sent: 2016-Jun-28 8:08 AM
To: 'Oakes, Lindsey (PS/SP)'
Cc: Angers, Lucie; Audcent, Karen; Sansom, Gareth; Adamowski, Andrew (PS/SP)
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ -GS-mod rev la nw.docx

Most of the comments were Gareth's and Lucie's. Sorry about the version confusion. I worked on the version that both Gareth and Lucie commented on. I didn't see the point in sending you two versions.

Normand Wong
613.941.2341 o
613.791.4669 m

From: Oakes, Lindsey (PS/SP) [mailto:lindsey.oakes@canada.ca]
Sent: 2016-Jun-28 7:08 AM
To: Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Adamowski, Andrew (PS/SP) <andrew.adamowski@canada.ca> s.23
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ -GS-mod rev la nw.docx

Hi Norm,

I've reviewed your comments, at least the ones that I can identify are yours.
The version you were working off of, rather than the latest version that I sent out yesterday, I can make the text changes that you have s.21(1)(b) recommended to the latest version and can re-send.

I am happy to re-distribute the comments you have shared with them and ask them to revise.

I'll be in touch with an updated version this morning.

Lindsey Oakes
Telephone: 613-990-8020
Blackberry: 613-410-6057
E-mail | Courriel: lindsey.oakes@canada.ca

Public Safety Canada | Sécurité publique Canada

From: Wong, Normand [mailto:Normand.Wong@justice.gc.ca]
Sent: Monday, June 27, 2016 4:10 PM
To: Oakes, Lindsey (PS/SP)
Cc: Angers, Lucie; Audcent, Karen; Sansom, Gareth s.21(1)(a)
Subject: 20160623 Lawful Access - Annex - Encryption _ -GS-mod rev la nw.docx

Our comments. They are mainly comments and not suggested text although I did provide some suggested text. I think we are generally of the view that it needs work to tighten up. The part on the history is good,

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

[redacted]

I'll look at the data retention piece now.

s.21(1)(a)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Oakes, Lindsey (PS/SP) <lindsey.oakes@canada.ca>
Sent: 2016-Jun-28 8:11 AM
To: Wong, Normand
Cc: Angers, Lucie; Audcent, Karen; Sansom, Gareth; Adamowski, Andrew (PS/SP)
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ GS-mod rev la nw.docx
Attachments: PS-SP-#1866700-5-Lawful Access - Annex - Encryption .DOCX

Hi Norm,

Please find attached the updated version which incorporates the additional changes to the text that you provided. If Lucie and Gareth want to take another peak given the changes between the two previous versions and let me know if there is anything further, that would be great.

s.23

Lindsey Oakes
Telephone: 613-990-8020
Blackberry: 613-410-6057
E-mail | Courriel: lindsey.oakes@canada.ca

Public Safety Canada | Sécurité publique Canada

From: Wong, Normand [mailto:Normand.Wong@justice.gc.ca]
Sent: Monday, June 27, 2016 4:10 PM
To: Oakes, Lindsey (PS/SP)
Cc: Angers, Lucie; Audcent, Karen; Sansom, Gareth
Subject: 20160623 Lawful Access - Annex - Encryption _ GS-mod rev la nw.docx

Our comments. They are mainly comments and not suggested text although I did provide some suggested text. I think we are generally of the view that it needs work to tighten up. The part on the history is good,

I'll look at the data retention piece now.

s.21(1)(a)

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Wong, Normand
Sent: 2016-Jun-28 8:55 AM
To: Watts, Heather
Cc: Angers, Lucie; Audcent, Karen; Sargent, Laurie; Sansom, Gareth; 'Oakes, Lindsey (PS/SP)'
Subject: FW: 20160623 Lawful Access - Annex - Encryption _[redacted]-GS-mod rev la nw.docx
Attachments: PS-SP-#1866700-5-Lawful Access - Annex - Encryption .DOCX

Heather: I think this is you, but if not let me know who could take a look at this. It's part of the National Security Green Paper – Annex on encryption. [redacted]

Thanks,

s.23

Norm

Normand Wong
613.941.2341 o
613.791.4669 m

From: Oakes, Lindsey (PS/SP) [mailto:lindsey.oakes@canada.ca]
Sent: 2016-Jun-28 8:11 AM
To: Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Adamowski, Andrew (PS/SP) <andrew.adamowski@canada.ca>
Subject: RE: 20160623 Lawful Access - Annex - Encryption _[redacted]GS-mod rev la nw.docx

Hi Norm,

Please find attached the updated version which incorporates the additional changes to the text that you provided. If Lucie and Gareth want to take another peak given the changes between the two previous versions and let me know if there is anything further, that would be great.

[redacted]

Lindsey Oakes
Telephone: 613-990-8020
Blackberry: 613-410-6057
E-mail | Courriel: lindsey.oakes@canada.ca

Public Safety Canada | Sécurité publique Canada

From: Wong, Normand [mailto:Normand.Wong@justice.gc.ca]
Sent: Monday, June 27, 2016 4:10 PM
To: Oakes, Lindsey (PS/SP)
Cc: Angers, Lucie; Audcent, Karen; Sansom, Gareth
Subject: 20160623 Lawful Access - Annex - Encryption _[redacted]GS-mod rev la nw.docx

s.21(1)(a)

Our comments. They are mainly comments and not suggested text although I did provide some suggested text. I think we are generally of the view that it needs work to tighten up. The part on the history is good, [redacted]

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

[redacted]

I'll look at the data retention piece now.

s.21(1)(a)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

ANNEX Z

ENCRYPTION

INTRODUCTION

As our society and economy becomes ever more interwoven with the internet, encryption has become an important tool for safety, security and privacy online. Widely regarded as a best practice, encryption enhances security and protects privacy online and is commonly used to protect individual messages, personal devices and transmission channels. Encryption is central to electronic commerce, banking, cybersecurity, data and intellectual property protection. The use of encryption technologies has grown in both availability and use with the growth of the internet.

Cryptography is the practice and study of ~~communications and~~ the procedures, processes, and methods of making and using secret communications, such as codes or ciphers. One of the main fields in cryptography is encryption. To encrypt, means to make hidden or secret. Encryption uses a process, often an ~~or~~ algorithm (sometimes known as a cipher) ~~and~~ to converts a readable message into an unreadable encrypted message. In order to access the hidden message, the user must have the key (which can be an algorithm or another type of code) to unlock it. Encryption plays an important role as it allows users to authenticate and safeguard sensitive data, and other information stored on computers or transmitted over closed or public networks.

The ubiquitous nature of technology has led to a transformation for all, including the justice system. As Canadians have moved their lives online, so too has the evidentiary trail. The development of new technologies has played an increasingly crucial role in for law enforcement and national security[1] agencies in their daily work by providing a number of additional tools to help advance their investigations. In fact, in some circumstances, evidence required to advance investigations can only be found in the digital realm (i.e. such as on mobile devices, or in stored data), therefore, digital evidence has become important in legal proceedings. Yet, we have also seen new forms of criminal activity and threats, new methods of committing old crimes, and new ways of concealing evidence. The widespread use of encryption can raise concerns in this context because it can create obstacles to the detection and investigation of criminal activities and security threats, as well as the inspection of computer records subject to investigation. Interestingly, the amount of digital communication that took place in the PC-only ear (between 1977 and 2007) is minimal compared to the amount of digital communications that is facilitated by mobile devices.

Law enforcement and national security agencies' concern relative to encryption is primarily that investigative techniques employed, under judicial authority, to obtain information, including interception of private communications (wiretap), production orders, and search warrants, can be

[1] Please note that, as a foreign intelligence and information technology security agency, the Communications Security Establish Canada (CSE) does not conduct national security or law enforcement investigations. It also does not direct its foreign intelligence or cyber security activities at Canadians or anyone in Canada. As such, the tools discussed in this annex do not relate to CSE.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

made ineffective by the use of encryption. Encryption, as well as anonymizing technologies[2], can be used by criminals or terrorists to prevent ~~an~~ investigators from being able to use the information obtained, which is needed to solve a crime or address a threat to Canada or Canada's interests. Encryption can also prevent law enforcement and ~~national security agencies~~ from accessing information held by victims of crime (i.e. in the case of murdered, lost or missing individuals). Additionally, encryption can also prevent law enforcement from accessing information to assist victims of technology-enabled crimes, such as theft, fraud, extortion (ransomware[3]). Left unchecked, the costs of technology-enabled crime will likely increase, and may potentially lessen society's trust in the integrity of e-commerce, social media, and other telecom-enabled technology.

[redacted]

s.21(1)(a)

To date, this issue has not been ~~directly~~ addressed in law in Canada, and the question of if, or how, to address this challenge continues to make headlines in many jurisdictions around the world. In trying to address the challenges faced by law enforcement and national security agencies, some of the key issues raised relate to:

- human rights, including but not limited to privacy rights, freedom of expression, and the right against self-incrimination;
- commercial interests, such as competitiveness and the protection of intellectual property;
- jurisdictional implications; and
- the need for encryption to enable modern e-commerce, e-banking and all types of cybersecurity and protect critical infrastructure.

[2] Some online applications channel web traffic through anonymizing networks, while other online services provide encrypted and disposable email services that can generate a new, random email address with only one click. These encryption and anonymity tools are increasing in availability too, with new applications for phones and tablets that allow for anonymous web browsing, email and instant messaging, and large file transfers. Moreover, most of the Internet is unindexed and cannot be navigated through common search engines, such as Google or Yahoo. This part of the Internet – the 'Deep Web' – may be used for licit or illicit purposes, similar to encryption and anonymizing technologies. In terms of illicit use, criminals may use 'darknets' or anonymizing networks and related technologies to avoid detection by law enforcement and traffic illegal drugs online, buy and sell counterfeit goods, share child sexual exploitation material, among other criminal activity.

[3] Encryption may also form an integral component of a criminal offence that targets victims online through computers and other information technologies. One example of this capability is known as a 'ransomware' scam. This scam involves a malicious type of software ('malware') that can lock a computer and its data content, and uses social engineering tactics, such as threats, to coerce victims into paying fees for regained computer access.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

These issues will be discussed further in this annex.

THE APPLICATION OF ENCRYPTION

Encryption is technology that can be applied to data-in-use and data-at-rest. Any of these could have various layers of encryption applied to it by any or all of the following: the end user, third party applications, and telecommunication service providers.

Data-in-use, otherwise known as active data, is data that is live and under constant change and manipulation by an application. Data-in-use is physically stored in databases, spreadsheets, etc. Data-at-rest is inactive data stored physically in data warehouses, archives, hard drives, tapes, off-site backups, mobile devices, etc.

In addition, encryption can be applied to more specific items such as the message itself (i.e. email, text message, or photo), the storage media of the device (i.e. the cell phone, the computer, the tablet), or the transmission network and/or channel (i.e. a VPN network, an enterprise server, or even the communication service provider's network).

POLICY AND LEGISLATION

THE GOVERNMENT OF CANADA'S ELECTRONIC COMMERCE STRATEGY & THE POLICY ON CRYPTOGRAPHY)

Almost 20 years ago, in 1997-1998, an extensive review of Canada's Cryptography policy was undertaken under the leadership of Industry Canada (now Innovation, Science, and Economic Development Canada) in the context of Canada's e-commerce policy but extended to the issues of law enforcement access and national security considerations. In 1998, Canada's Minister of Industry announced its Cryptography policy and, this policy remains in place today.

In this policy, the Government affirmed the following principles:

1) The freedom of Canadians to develop, import and use whatever cryptography they wished;
2) Support for private sector research and development
3) The Government would not implement mandatory key recovery requirements or licensing regimes for certification authorities or trusted third parties;
4) Export controls would continue to be consistent with Canada's international obligations; and
5) The Government would explore legislative and other options to protect consumer privacy and to assist law enforcement and national security agencies.

The policy emphasized the importance of maintaining a balanced approach to a complex problem.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

A number of key considerations played a role in helping shape Canada's Cryptography policy. The following were some significant developments that helped guide the policy development process:

- The increasing use of strong encryption software and computers powerful enough to encrypt and decrypt data easily were commonly available;
- The rapidly increasing use of telecommunications media suitable for encryption (e.g. email and other data conveyed via the Internet and other computer-based media) for both personal and commercial communications;
- The increasing use of wireless cellular telephones, which had created pressure for the development of digital equipment and had led to the encryption of their signals in some cases; and
- The increasing reliance on computers and computer networks for commercial activities and the need to protect privacy and security, which had led companies to store business records in secure computer facilities and in encrypted forms.

Notably, many of these developments are still relevant today given the proliferation of and reliance on the use of technology, encryption and digital communications. Both then and now, encryption forms part of the core framework that allow electronic commerce to flourish. s.21(1)(a)
In an effort to develop a cryptography framework, specific considerations were given to the areas of: electronic commerce; [redacted] involved in any discussion of encryption.

Electronic Commerce

In 1998, an increasing number of transactions were shifting from closed networks to open networks and encryption became essential for the conduct of electronic commerce. Open networks allowed for more global trading, but came with a variety of security challenges including concerns over the authentication of communicating parties, the integrity of the data being communicated, the confidentiality of the proprietary or personal data, and the assurance that transactions have been authorized by legitimate users. Without encryption, these challenges may not have been addressed.

The aims of law enforcement and business align when encryption protects proprietary information, trade secrets, and in general, helps defend industry and consumers against fraud and other unlawful activities. In addition, encryption helps protect information that is important to the objectives of law enforcement and national security agencies by protecting Canada, its industry and valuable information.

The policy challenge was, and continues to be, the need to find solutions that will address the investigative challenges faced by law enforcement and national security agencies without interfering with legitimate business, institutional or individual interests and without weakening the security of the network infrastructure for all users. Furthermore, consideration will now need to be given to the current digital environment and the trend towards the use of default encrypted

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

devices, compared to the use of back end encryption software, in addition to end-to-end encryption by many companies within the information and communication technology sector.

A recent dispute in the U.S. between Apple and the FBI highlighted challenges in this alignment, when Apple refused to create a 'key' or 'backdoor' bypassing the encryption protecting (or locking) a suspect's iPhone. Ultimately, the FBI accessed the phone through a third party, but the dispute highlighted the complex issues faced in finding solution to the challenges stemming from the widespread use of encryption.

Investigative Challenges in a Digital Age

The roles and responsibilities of the law enforcement and national security agencies involved in investigations are diverse but include aspects such as: identifying threats and detecting; investigating and prosecuting matters related to terrorism; crimes of violence and related to property; and abuses of domestic and international commercial and financial systems. The effectiveness of these agencies in monitoring criminal activities and threats to Canada's security, and in investigating and prosecuting offenders in Canada has depended on their lawful ability to conduct judicially authorized interception of specific private communications, or to search and inspect places and materials, including computers, where relevant information may be kept.

The increased use of encryption can provide concurrent, yet competing, outcomes; while it can provide enhanced technical protection for confidential information, it can also impede the ability to conduct lawful and authorized electronic surveillance. Notwithstanding the receipt of judicial authorizations for the interception of communications, intercepted data in an encrypted form may be unreadable and undecipherable for authorities. This makes it difficult for authorities to decipher the information, or to do so in time to be able to effectively use it or take action to prevent harm from occurring. As a result, law enforcement and national security agencies are challenged to effectively respond and adhere to their individual mandates in the face of undecipherable encrypted communications. Having appropriate, Charter-compliant investigative authorities tailored towards digital investigations would not only be a benefit to Canadians and law enforcement and national security agencies in Canada, but it would also benefit Canada's international cooperation efforts, as Canada's Mutual Legal Assistance in Criminal Matters Act generally requires that a court order be obtained to send evidence to a foreign partner. To obtain such an order, it is necessary to describe the evidence to be sent, which becomes impossible when potentially relevant electronic evidence is encrypted.

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

Human rights and civil liberties

The rights of Canadians to privacy and to express themselves freely are constitutionally protected. Section 8 of the *Charter* guarantees Canadians the right to be free from "unreasonable search or seizure" which has been interpreted through jurisprudence

The protection of a reasonable expectation of privacy, and invasions of that privacy must be justified, must be authorized in law and generally require specific pre-authorization by the courts. In this context,

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.21(1)(a)

and the right to freedom of expression may extend to both the production of encryption products and their use to protect the messages being expressed or data being stored.

It is important to note that Canadians also have human rights protections under international human rights law with regard to privacy and freedom of expression. Canada is a State party to the International Covenant on Civil and Political Rights. Article 17 of the Covenant prohibits interferences with privacy that are arbitrary or unlawful and Article 19 guarantees an individual's freedom of expression.

WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES

While Canada has not addressed encryption challenges in law, Canada is one of 41 participating states to the Wassenaar Arrangement which was established to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies. Participating States seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities. The aim is also to prevent the acquisition of these items by terrorists.

Participating States control all items set forth in the Munitions List (items designed for military use) and the List of Dual-Use Goods and Technologies (items having both civilian and military applications such as encryption software),with the objective of preventing unauthorized transfers or re-transfers of those items.

The Participating States have an agreement to maintain national export controls on listed items, which are implemented via national legislation; are guided by agreed upon best practices, guidelines or elements; have agreed to report on transfers and denials of specific controlled items to destinations outside of the arrangement; and have agreed to exchange information on sensitive dual-use goods and technologies.

FORMER BILL C-30 -- *PROTECTING CHILDREN FROM INTERNET PREDATORS ACT*, 2012

In the past, in the context of work on lawful access issues, under former Bill C-30 (*Protecting Children from Internet Predators Act*, 2012, 41st Parliament, 1st session), legislative proposals were introduced, but did not come into force, to create requirements for telecommunications service providers to decrypt communications where it was readily possible for the service provide to do so, in the context of lawful interception. However, telecommunications service providers were not required to develop specific decryption techniques themselves. For example, if interception was successful but the data retrieved was encrypted by a tool that was implemented directly by the service provider, rather than the user, then the service provider would be asked to decrypt the data.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.21(1)(a)

~~These proposals were supported by law enforcement and national security agencies.~~ However, ~~in the larger picture,~~ these proposals would not have solved the problem posed by encryption in whole, nor did they purport to do so. This is particularly true given that many major IT companies have built mobile and other digital devices that enable individuals to encrypt and decrypt data at the user level.

JURISDICTIONAL AND INTERNATIONAL CONSIDERATIONS

Law enforcement and national security agencies also face challenges when attempting to compel communication service providers to decrypt communications. Many communication service providers, particularly software and application service providers, do not have physical premises in Canada, and may not be subject to Canadian jurisdiction. In order to be able to obtain information held by these companies, currently the principal process available is through the use of Mutual Legal Assistance Treaties (MLATs). Currently, MLAT processes are not always timely enough for the exigencies of investigations involving electronic evidence, nor were they designed for a high volume of requests that could ensue given the trend toward global inter-connectivity and challenges in relation to jurisdiction in the context of modern communications.

It is important to note that the complex challenges involving encryption ~~and~~ are the topic of on-going discussion and work in various international fora. The subject of how best to address the challenges for law enforcement and national security agencies arising from the use of encryption while supporting its many beneficial uses is an issue also being explored by many of Canada's closest allies.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Watts, Heather
Sent: 2016-Jun-28 9:12 AM
To: Wong, Normand; MacCallum, Raymond
Cc: Angers, Lucie; Audcent, Karen; Sargent, Laurie; Sansom, Gareth; 'Oakes, Lindsey (PS/SP)'
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ GS-mod rev la nw.docx

Hi Norm,

Thanks for forwarding,

Heather

s.23

From: Wong, Normand
Sent: 2016-Jun-28 8:55 AM
To: Watts, Heather
Cc: Angers, Lucie; Audcent, Karen; Sargent, Laurie; Sansom, Gareth; 'Oakes, Lindsey (PS/SP)'
Subject: FW: 20160623 Lawful Access - Annex - Encryption _ GS-mod rev la nw.docx

Heather: I think this is you, but if not let me know who could take a look at this. It's part of the National Security Green Paper – Annex on encryption.

Thanks,

Norm

Normand Wong
613.941.2341 o
613.791.4669 m

From: Oakes, Lindsey (PS/SP) [mailto:lindsey.oakes@canada.ca]
Sent: 2016-Jun-28 8:11 AM
To: Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Adamowski, Andrew (PS/SP) <andrew.adamowski@canada.ca>
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ GS-mod rev la nw.docx

Hi Norm,

Please find attached the updated version which incorporates the additional changes to the text that you provided. If Lucie and Gareth want to take another peak given the changes between the two previous versions and let me know if there is anything further, that would be great.

s.23

Lindsey Oakes
Telephone: 613-990-8020

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Blackberry: 613-410-6057
E-mail | Courriel: lindsey.oakes@canada.ca

Public Safety Canada | Sécurité publique Canada

From: Wong, Normand [mailto:Normand.Wong@justice.gc.ca]
Sent: Monday, June 27, 2016 4:10 PM
To: Oakes, Lindsey (PS/SP) s.21(1)(a)
Cc: Angers, Lucie; Audcent, Karen; Sansom, Gareth
Subject: 20160623 Lawful Access - Annex - Encryption _ [redacted]-GS-mod rev la nw.docx

Our comments. They are mainly comments and not suggested text although I did provide some suggested text. I think we are generally of the view that it needs work to tighten up. The part on the history is good, [redacted]

I'll look at the data retention piece now.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Oakes, Lindsey (PS/SP) <lindsey.oakes@canada.ca>
Sent: 2016-Jun-28 1:38 PM
To: MacCallum, Raymond; Watts, Heather; Wong, Normand
Cc: Angers, Lucie; Audcent, Karen; Sargent, Laurie; Sansom, Gareth
Subject: RE: 20160623 Lawful Access - Annex - Encryption [redacted]GS-mod rev la nw.docx
Attachments: PS-SP-#1866700-5-Lawful Access - Annex - Encryption .DOCX

Hi Ray,

Please see attached s.23

Thanks

Lindsey Oakes
Telephone: 613-990-8020
Blackberry: 613-410-6057
E-mail | Courriel: lindsey.oakes@canada.ca

Public Safety Canada | Sécurité publique Canada

From: MacCallum, Raymond [mailto:Raymond.MacCallum@justice.gc.ca]
Sent: Tuesday, June 28, 2016 1:34 PM
To: Watts, Heather; Wong, Normand
Cc: Angers, Lucie; Audcent, Karen; Sargent, Laurie; Sansom, Gareth; Oakes, Lindsey (PS/SP)
Subject: RE: 20160623 Lawful Access - Annex - Encryption _[redacted]GS-mod rev la nw.docx

Can someone please forward me the attachment?

Thanks.

From: Watts, Heather
Sent: June 28, 2016 9:12 AM
To: Wong, Normand <Normand.Wong@justice.gc.ca>; MacCallum, Raymond <Raymond.MacCallum@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sargent, Laurie <Laurie.Sargent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; 'Oakes, Lindsey (PS/SP)' <lindsey.oakes@canada.ca>
Subject: RE: 20160623 Lawful Access - Annex - Encryption _[redacted]GS-mod rev la nw.docx

Hi Norm,

Thanks for forwarding, [redacted]

Heather

From: Wong, Normand
Sent: 2016-Jun-28 8:55 AM
To: Watts, Heather

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Cc: Angers, Lucie; Audcent, Karen; Sargent, Laurie; Sansom, Gareth; 'Oakes, Lindsey (PS/SP)'
Subject: FW: 20160623 Lawful Access - Annex - Encryption _ [redacted] GS-mod rev la nw.docx

Heather: I think this is you, but if not let me know who could take a look at this. It's part of the National Security Green Paper – Annex on encryption. [redacted]

Thanks,

Norm

Normand Wong
613.941.2341 o
613.791.4669 m

From: Oakes, Lindsey (PS/SP) [mailto:lindsey.oakes@canada.ca] s.23
Sent: 2016-Jun-28 8:11 AM
To: Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Adamowski, Andrew (PS/SP) <andrew.adamowski@canada.ca>
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ [redacted] GS-mod rev la nw.docx

Hi Norm,

Please find attached the updated version which incorporates the additional changes to the text that you provided.
If Lucie and Gareth want to take another peak given the changes between the two previous versions and let me know if there is anything further, that would be great.

[redacted]

Lindsey Oakes
Telephone: 613-990-8020
Blackberry: 613-410-6057
E-mail | Courriel: lindsey.oakes@canada.ca

Public Safety Canada | Sécurité publique Canada

From: Wong, Normand [mailto:Normand.Wong@justice.gc.ca]
Sent: Monday, June 27, 2016 4:10 PM
To: Oakes, Lindsey (PS/SP)
Cc: Angers, Lucie; Audcent, Karen; Sansom, Gareth
Subject: 20160623 Lawful Access - Annex - Encryption [redacted] GS-mod rev la nw.docx s.21(1)(a)

Our comments. They are mainly comments and not suggested text although I did provide some suggested text. I think we are generally of the view that it needs work to tighten up. The part on the history is good, [redacted]

I'll look at the data retention piece now.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

ANNEX Z

ENCRYPTION

INTRODUCTION

As our society and economy becomes ever more interwoven with the internet, encryption has become an important tool for safety, security and privacy online. Widely regarded as a best practice, encryption enhances security and protects privacy online and is commonly used to protect individual messages, personal devices and transmission channels. Encryption is central to electronic commerce, banking, cybersecurity, data and intellectual property protection. The use of encryption technologies has grown in both availability and use with the growth of the internet.

Cryptography is the practice and study of ~~communications and~~ the procedures, processes, and methods of making and using secret communications, such as codes or ciphers. One of the main fields in cryptography is encryption. To encrypt, means to make hidden or secret. Encryption uses a process, often an ~~or~~ algorithm (sometimes known as a cipher) ~~and~~ to converts a readable message into an unreadable encrypted message. In order to access the hidden message, the user must have the key (which can be an algorithm or another type of code) to unlock it. Encryption plays an important role as it allows users to authenticate and safeguard sensitive data, and other information stored on computers or transmitted over closed or public networks.

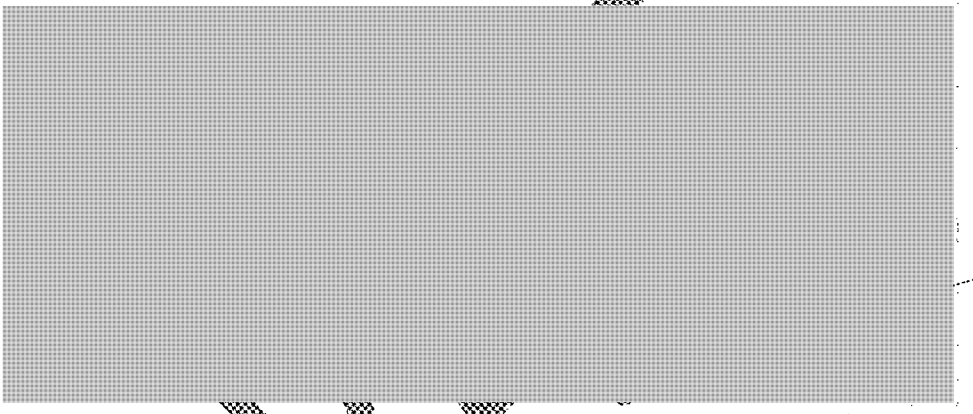
The ubiquitous nature of technology has led to a transformation for all, including the justice system. As Canadians have moved their lives online, so too has the evidentiary trail. The development of new technologies has played an increasingly crucial role in for law enforcement and national security[1] agencies in their daily work by providing a number of additional tools to help advance their investigations. In fact, in some circumstances, evidence required to advance investigations can only be found in the digital realm (i.e. such as on mobile devices, or in stored data), therefore, digital evidence has become important in legal proceedings. Yet, we have also seen new forms of criminal activity and threats, new methods of committing old crimes, and new ways of concealing evidence. The widespread use of encryption can raise concerns in this context because it can create obstacles to the detection and investigation of criminal activities and security threats, as well as the inspection of computer records subject to investigation. Interestingly, the amount of digital communication that took place in the PC-only ear (between 1977 and 2007) is minimal compared to the amount of digital communications that is facilitated by mobile devices.

Law enforcement and national security agencies' concern relative to encryption is primarily that investigative techniques employed, under judicial authority, to obtain information, including interception of private communications (wiretap), production orders, and search warrants, can be

[1] Please note that, as a foreign intelligence and information technology security agency, the Communications Security Establish Canada (CSE) does not conduct national security or law enforcement investigations. It also does not direct its foreign intelligence or cyber security activities at Canadians or anyone in Canada. As such, the tools discussed in this annex do not relate to CSE.

Released under the Access to Information Act /
Divulgé(s) en vèrtu de la Loi sur l'accès à l'information.

-made ineffective by the use of encryption. Encryption, as well as anonymizing technologies[2], can be used by criminals or terrorists to prevent ~~an~~ investigators from being able to use the information obtained, which is needed to solve a crime or address a threat to Canada or Canada's interests. Encryption can also prevent law enforcement and ~~national security agencies~~ from accessing information held by victims of crime (i.e. in the case of murdered, lost or missing individuals). Additionally, encryption can also prevent law enforcement from accessing information to assist victims of technology-enabled crimes, such as theft, fraud, extortion (ransomware[3]). Left unchecked, the costs of technology-enabled crime will likely increase, and may potentially lessen society's trust in the integrity of e-commerce, social media, and other telecom-enabled technology.



s.21(1)(a)

Formatted: Highlight

To date, this issue has not been ~~directly~~ addressed in law in Canada, and the question of if, or how, to address this challenge continues to make headlines in many jurisdictions around the world. In trying to address the challenges faced by law enforcement and national security agencies, some of the key issues raised relate to:

- human rights, including but not limited to, privacy rights, freedom of expression, and the right against self-incrimination,
- commercial interests, such as competitiveness and the protection of intellectual property;
- jurisdictional implications; and

[2] Some online applications channel web traffic through anonymizing networks, while other online services provide encrypted and disposable email services that can generate a new, random email address with only one click. These encryption and anonymity tools are increasing in availability too, with new applications for phones and tablets that allow for anonymous web browsing, email and instant messaging, and large file transfers. Moreover, most of the Internet is unindexed and cannot be navigated through common search engines, such as Google or Yahoo. This part of the Internet – the 'Deep Web' – may be used for licit or illicit purposes, similar to encryption and anonymizing technologies. In terms of illicit use, criminals may use 'darknets' or anonymizing networks and related technologies to avoid detection by law enforcement and traffic illegal drugs online, buy and sell counterfeit goods, share child sexual exploitation material, among other criminal activity.

[3] Encryption may also form an integral component of a criminal offence that targets victims online through computers and other information technologies. One example of this capability is known as a 'ransomware' scam. This scam involves a malicious type of software ('malware') that can lock a computer and its data content, and uses social engineering tactics, such as threats, to coerce victims into paying fees for regained computer access.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- the need for encryption to enable modern e-commerce, e-banking and all types of cybersecurity and protect critical infrastructure.

These issues will be discussed further in this annex.

THE APPLICATION OF ENCRYPTION

Encryption is technology that can be applied to data-in-use and data-at-rest. Any of these could have various layers of encryption applied to it by any or all of the following: the end user, third party applications, and telecommunication service providers.

Data-in-use, otherwise known as active data, is data that is live and under constant change and manipulation by an application. Data-in-use is physically stored in databases, spreadsheets, etc. Data-at-rest is inactive data stored physically in data warehouses, archives, hard drives, tapes, off-site backups, mobile devices, etc.

In addition, encryption can be applied to more specific items such as the message itself (i.e. email, text message, or photo), the storage media of the device (i.e. the cell phone, the computer, the tablet), or the transmission network and/or channel (i.e. a VPN network, an enterprise server, or even the communication service provider's network).

POLICY AND LEGISLATION

THE GOVERNMENT OF CANADA'S ELECTRONIC COMMERCE STRATEGY & THE POLICY ON CRYPTOGRAPHY)

Almost 20 years ago, in 1997-1998, an extensive review of Canada's Cryptography policy was undertaken under the leadership of Industry Canada (now Innovation, Science, and Economic Development Canada) in the context of Canada's e-commerce policy but extended to the issues of law enforcement access and national security considerations. In 1998, Canada's Minister of Industry announced its Cryptography policy and, this policy remains in place today.

In this policy, the Government affirmed the following principles:

1) The freedom of Canadians to develop, import and use whatever cryptography they wished;
2) Support for private sector research and development
3) The Government would not implement mandatory key recovery requirements or licensing regimes for certification authorities or trusted third parties;
4) Export controls would continue to be consistent with Canada's international obligations; and
5) The Government would explore legislative and other options to protect consumer privacy and to assist law enforcement and national security agencies.

The policy emphasized the importance of maintaining a balanced approach to a complex problem.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

A number of key considerations played a role in helping shape Canada's Cryptography policy. The following were some significant developments that helped guide the policy development process:

- The increasing use of strong encryption software and computers powerful enough to encrypt and decrypt data easily were commonly available;
- The rapidly increasing use of telecommunications media suitable for encryption (e.g. email and other data conveyed via the Internet and other computer-based media) for both personal and commercial communications;
- The increasing use of wireless cellular telephones, which had created pressure for the development of digital equipment and had led to the encryption of their signals in some cases; and
- The increasing reliance on computers and computer networks for commercial activities and the need to protect privacy and security, which had led companies to store business records in secure computer facilities and in encrypted forms.

Notably, many of these developments are still relevant today, given the proliferation of and reliance on the use of technology, encryption and digital communications. Both then and now, encryption forms part of the core framework that allows electronic commerce to flourish.
In an effort to develop a cryptography framework, specific considerations were given to the areas of: electronic commerce; [redacted] involved in any discussion of encryption.

Electronic Commerce

In 1998, an increasing number of transactions were shifting from closed networks to open networks and encryption became essential for the conduct of electronic commerce. Open networks allowed for more global trading, but came with a variety of security challenges including concerns over the authentication of communicating parties, the integrity of the data being communicated, the confidentiality of the proprietary or personal data, and the assurance that transactions have been authorized by legitimate users. Without encryption, these challenges may not have been addressed.

s.21(1)(a)

The aims of law enforcement and business align when encryption protects proprietary information, trade secrets, and in general, helps defend industry and consumers against fraud and other unlawful activities. In addition, encryption helps protect information that is important to the objectives of law enforcement and national security agencies by protecting Canada, its industry and valuable information.

The policy challenge was, and continues to be, the need to find solutions that will address the investigative challenges faced by law enforcement and national security agencies without interfering with legitimate business, institutional or individual interests and without weakening the security of the network infrastructure for all users. Furthermore, consideration will now need

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

to be given to the current digital environment and the trend towards the use of default encrypted devices, compared to the use of back end encryption software, in addition to end-to-end encryption by many companies within the information and communication technology sector.

A recent dispute in the U.S. between Apple and the FBI highlighted challenges in this alignment, when Apple refused to create a 'key' or 'backdoor' bypassing the encryption protecting (or locking) a suspect's iPhone. Ultimately, the FBI accessed the phone through a third party, but the dispute highlighted the complex issues faced in finding solution to the challenges stemming from the widespread use of encryption.

[redacted]

Formatted: Highlight

Formatted: Highlight

Human rights and civil liberties

The rights of Canadians to privacy and to express themselves freely are constitutionally protected. Section 8 of the *Charter* guarantees Canadians the right to be free from "unreasonable search or seizure" which has been interpreted through jurisprudence [redacted] The protection of a reasonable expectation of privacy, and invasions of that privacy must be justified, must be authorized in law and generally require specific pre-authorization by the courts. In this context, [redacted] and the right to

s.21(1)(a)

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

freedom of expression may extend to both the production of encryption products and their use to protect the messages being expressed or data being stored.

It is important to note that Canadians also have human rights protections under international human rights law with regard to privacy and freedom of expression. Canada is a State party to the International Covenant on Civil and Political Rights. Article 17 of the Covenant prohibits interferences with privacy that are arbitrary or unlawful and Article 19 guarantees an individual's freedom of expression.

WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES

While Canada has not addressed encryption challenges in law, Canada is one of 41 participating states to the Wassenaar Arrangement which was established to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies. Participating States seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities. The aim is also to prevent the acquisition of these items by terrorists.

Participating States control all items set forth in the Munitions List (items designed for military use) and the List of Dual-Use Goods and Technologies (items having both civilian and military applications such as encryption software),with the objective of preventing unauthorized transfers or re-transfers of those items.

The Participating States have an agreement to maintain national export controls on listed items, which are implemented via national legislation; are guided by agreed upon best practices, guidelines or elements; have agreed to report on transfers and denials of specific controlled items to destinations outside of the arrangement; and have agreed to exchange information on sensitive dual-use goods and technologies.

FORMER BILL C-30 – *PROTECTING CHILDREN FROM INTERNET PREDATORS ACT*, 2012

In the past, in the context of work on lawful access issues, under former Bill C-30 (*Protecting Children from Internet Predators Act*, 2012, 41st Parliament, 1st session), legislative proposals were introduced, but did not come into force, to create requirements for telecommunications service providers to decrypt communications where it was readily possible for the service provide to do so, in the context of lawful interception. However, telecommunications service providers were not required to develop specific decryption techniques themselves. For example, if interception was successful but the data retrieved was encrypted by a tool that was implemented directly by the service provider, rather than the user, then the service provider would be asked to decrypt the data.

s.21(1)(a)

~~[These proposals were supported by law enforcement and national security agencies].~~ However, ~~in the larger picture,~~ these proposals would not have solved the problem posed by encryption in

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

whole, nor did they purport to do so. This is particularly true given that many major IT companies have built mobile and other digital devices that enable individuals to encrypt and decrypt data at the user level.

JURISDICTIONAL AND INTERNATIONAL CONSIDERATIONS

Law enforcement and national security agencies also face challenges when attempting to compel communication service providers to decrypt communications. Many communication service providers, particularly software and application service providers, do not have physical premises in Canada, and may not be subject to Canadian jurisdiction. In order to be able to obtain information held by these companies, currently the principal process available is through the use of Mutual Legal Assistance Treaties (MLATs). Currently, MLAT processes are not always timely enough for the exigencies of investigations involving electronic evidence, nor were they designed for a high volume of requests that could ensue given the trend toward global inter-connectivity and challenges in relation to jurisdiction in the context of modern communications.

It is important to note that the complex challenges involving encryption ~~and~~ are the topic of on-going discussion and work in various international fora. The subject of how best to address the challenges for law enforcement and national security agencies arising from the use of encryption while supporting its many beneficial uses is an issue also being explored by many of Canada's closest allies.

DRAFT

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Angers, Lucie
Sent: 2016-Jun-28 5:45 PM
To: Wong, Normand; Audcent, Karen; Sansom, Gareth
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ [redacted]GS-mod rev la nw.docx

Why don't you check with Lindsay? I'm surprised that they did not see any of the annexes before...

From: Wong, Normand
Sent: Tuesday, June 28, 2016 4:57 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: Fw: 20160623 Lawful Access - Annex - Encryption _ [redacted]GS-mod rev la nw.docx

Any idea of how I should reply to Ray?

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

Sent from my BlackBerry 10 smartphone on the Rogers network.

From: MacCallum, Raymond <Raymond.MacCallum@justice.gc.ca>
Sent: Tuesday, June 28, 2016 16:53
To: Wong, Normand
Cc: 'lindsey.oakes@canada.ca'
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ [redacted]GS-mod rev la nw.docx

Norm, [redacted]

Ray

From: Watts, Heather
Sent: June 28, 2016 9:12 AM
To: Wong, Normand <Normand.Wong@justice.gc.ca>; MacCallum, Raymond <Raymond.MacCallum@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sargent, Laurie <Laurie.Sargent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; 'Oakes, Lindsey (PS/SP)' <lindsey.oakes@canada.ca>
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ [redacted]GS-mod rev la nw.docx

Hi Norm,

Thanks for forwarding. [redacted]

Heather

From: Wong, Normand
Sent: 2016-Jun-28 8:55 AM
To: Watts, Heather

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Cc: Angers, Lucie; Audcent, Karen; Sargent, Laurie; Sansom, Gareth; 'Oakes, Lindsey (PS/SP)'
Subject: FW: 20160623 Lawful Access - Annex - Encryption [redacted]GS-mod rev la nw.docx

Heather: I think this is you, but if not let me know who could take a look at this. It's part of the National Security Green Paper – Annex on encryption. [redacted]

Thanks,

Norm

Normand Wong
613.941.2341 o
613.791.4669 m

From: Oakes, Lindsey (PS/SP) [mailto:lindsey.oakes@canada.ca]
Sent: 2016-Jun-28 8:11 AM
To: Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Adamowski, Andrew (PS/SP) <andrew.adamowski@canada.ca>
Subject: RE: 20160623 Lawful Access - Annex - Encryption [redacted]GS-mod rev la nw.docx

s.23

Hi Norm,

Please find attached the updated version which incorporates the additional changes to the text that you provided. If Lucie and Gareth want to take another peak given the changes between the two previous versions and let me know if there is anything further, that would be great.

[redacted]

Lindsey Oakes
Telephone: 613-990-8020
Blackberry: 613-410-6057
E-mail | Courriel: lindsey.oakes@canada.ca

Public Safety Canada | Sécurité publique Canada

From: Wong, Normand [mailto:Normand.Wong@justice.gc.ca]
Sent: Monday, June 27, 2016 4:10 PM
To: Oakes, Lindsey (PS/SP)
Cc: Angers, Lucie; Audcent, Karen; Sansom, Gareth
Subject: 20160623 Lawful Access - Annex - Encryption [redacted]-GS-mod rev la nw.docx

s.21(1)(a)

Our comments. They are mainly comments and not suggested text although I did provide some suggested text. I think we are generally of the view that it needs work to tighten up. The part on the history is good, [redacted]

I'll look at the data retention piece now.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Oakes, Lindsey (PS/SP) <lindsey.oakes@canada.ca>
Sent: 2016-Jun-29 7:11 AM
To: MacCallum, Raymond; Wong, Normand
Cc: Adamowski, Andrew (PS/SP)
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ [redacted] GS-mod rev la nw.docx
Attachments: [redacted]

Hi Ray,

[redacted]

Would Justice be okay with this approach?
Happy to discuss further.

Thanks again,

s.23

Lindsey Oakes
Telephone: 613-990-8020
Blackberry: 613-410-6057
E-mail | Courriel: lindsey.oakes@canada.ca

Public Safety Canada | Sécurité publique Canada

From: MacCallum, Raymond [mailto:Raymond.MacCallum@justice.gc.ca]
Sent: Tuesday, June 28, 2016 4:53 PM
To: Wong, Normand
Cc: Oakes, Lindsey (PS/SP)
Subject: RE: 20160623 Lawful Access - Annex - Encryption _[redacted]GS-mod rev la nw.docx

Norm, [redacted]

Ray

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

From: Watts, Heather
Sent: June 28, 2016 9:12 AM
To: Wong, Normand <Normand.Wong@justice.gc.ca>; MacCallum, Raymond <Raymond.MacCallum@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sargent, Laurie <Laurie.Sargent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; 'Oakes, Lindsey (PS/SP)' <lindsey.oakes@canada.ca>
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ -GS-mod rev la nw.docx

Hi Norm,

Thanks for forwarding,

Heather

s.23

From: Wong, Normand
Sent: 2016-Jun-28 8:55 AM
To: Watts, Heather
Cc: Angers, Lucie; Audcent, Karen; Sargent, Laurie; Sansom, Gareth; 'Oakes, Lindsey (PS/SP)'
Subject: FW: 20160623 Lawful Access - Annex - Encryption _ -GS-mod rev la nw.docx

Heather: I think this is you, but if not let me know who could take a look at this. It's part of the National Security Green Paper – Annex on encryption.

Thanks,

Norm

Normand Wong
613.941.2341 o
613.791.4669 m

From: Oakes, Lindsey (PS/SP) [mailto:lindsey.oakes@canada.ca]
Sent: 2016-Jun-28 8:11 AM
To: Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Adamowski, Andrew (PS/SP) <andrew.adamowski@canada.ca>
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ -GS-mod rev la nw.docx

Hi Norm,

Please find attached the updated version which incorporates the additional changes to the text that you provided.
If Lucie and Gareth want to take another peak given the changes between the two previous versions and let me know if there is anything further, that would be great.

Lindsey Oakes
Telephone: 613-990-8020
Blackberry: 613-410-6057
E-mail | Courriel: lindsey.oakes@canada.ca

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

From: Wong, Normand [mailto:Normand.Wong@justice.gc.ca]
Sent: Monday, June 27, 2016 4:10 PM
To: Oakes, Lindsey (PS/SP)
Cc: Angers, Lucie; Audcent, Karen; Sansom, Gareth
Subject: 20160623 Lawful Access - Annex - Encryption _ [redacted] GS-mod rev la nw.docx

s.21(1)(a)

Our comments. They are mainly comments and not suggested text although I did provide some suggested text. I think we are generally of the view that it needs work to tighten up. The part on the history is good, [redacted]

I'll look at the data retention piece now.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

ANNEX Z

ENCRYPTION

INTRODUCTION

As our society and economy becomes ever more interwoven with the internet, encryption has become an important tool for safety, security and privacy online. Widely regarded as a best practice, encryption enhances security and protects privacy online and is commonly used to protect individual messages, personal devices and transmission channels. Encryption is central to electronic commerce, banking, cybersecurity, data and intellectual property protection. The use of encryption technologies has grown in both availability and use with the growth of the internet.

Cryptography is the practice and study of ~~communications and~~ the procedures, processes, and methods of making and using secret communications, such as codes or ciphers. One of the main fields in cryptography is encryption. To encrypt, means to make hidden or secret. Encryption uses a process, often an ~~or~~ algorithm (sometimes known as a cipher) ~~and~~ to converts a readable message into an unreadable encrypted message. In order to access the hidden message, the user must have the key (which can be an algorithm or another type of code) to unlock it. Encryption plays an important role as it allows users to authenticate and safeguard sensitive data, and other information stored on computers or transmitted over closed or public networks.

The ubiquitous nature of technology has led to a transformation for all, including the justice system. As Canadians have moved their lives online, so too has the evidentiary trail. The development of new technologies has played an increasingly crucial role in for law enforcement and national security[1] agencies in their daily work by providing a number of additional tools to help advance their investigations. In fact, in some circumstances, evidence required to advance investigations can only be found in the digital realm (i.e. such as on mobile devices, or in stored data), therefore, digital evidence has become important in legal proceedings. Yet, we have also seen new forms of criminal activity and threats, new methods of committing old crimes, and new ways of concealing evidence. The widespread use of encryption can raise concerns in this context because it can create obstacles to the detection and investigation of criminal activities and security threats, as well as the inspection of computer records subject to investigation. Interestingly, the amount of digital communication that took place in the PC-only ear (between 1977 and 2007) is minimal compared to the amount of digital communications that is facilitated by mobile devices.

Law enforcement and national security agencies' concern relative to encryption is primarily that investigative techniques employed, under judicial authority, to obtain information, including interception of private communications (wiretap), production orders, and search warrants, can be

[1] Please note that, as a foreign intelligence and information technology security agency, the Communications Security Establish Canada (CSE) does not conduct national security or law enforcement investigations. It also does not direct its foreign intelligence or cyber security activities at Canadians or anyone in Canada. As such, the tools discussed in this annex do not relate to CSE.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

-made ineffective by the use of encryption. Encryption, as well as anonymizing technologies[2], can be used by criminals or terrorists to prevent ~~an~~ investigators from being able to use the information obtained, which is needed to solve a crime or address a threat to Canada or Canada's interests. Encryption can also prevent law enforcement and ~~national security agencies~~ from accessing information held by victims of crime (i.e. in the case of murdered, lost or missing individuals). Additionally, encryption can also prevent law enforcement from accessing information to assist victims of technology-enabled crimes, such as theft, fraud, extortion (ransomware[3]). Left unchecked, the costs of technology-enabled crime will likely increase, and may potentially lessen society's trust in the integrity of e-commerce, social media, and other telecom-enabled technology.

[redacted] s.21(1)(a)

Formatted: Highlight

To date, this issue has not been ~~directly~~ addressed in law in Canada, and the question of if, or how, to address this challenge continues to make headlines in many jurisdictions around the world. In trying to address the challenges faced by law enforcement and national security agencies, some of the key issues raised relate to:

- human rights, including but not limited to, privacy rights, freedom of expression, and the right against self-incrimination,
- commercial interests, such as competitiveness and the protection of intellectual property;
- jurisdictional implications; and

[2] Some online applications channel web traffic through anonymizing networks, while other online services provide encrypted and disposable email services that can generate a new, random email address with only one click. These encryption and anonymity tools are increasing in availability too, with new applications for phones and tablets that allow for anonymous web browsing, email and instant messaging, and large file transfers. Moreover, most of the Internet is unindexed and cannot be navigated through common search engines, such as Google or Yahoo. This part of the Internet – the 'Deep Web' – may be used for licit or illicit purposes, similar to encryption and anonymizing technologies. In terms of illicit use, criminals may use 'darknets' or anonymizing networks and related technologies to avoid detection by law enforcement and traffic illegal drugs online, buy and sell counterfeit goods, share child sexual exploitation material, among other criminal activity.

[3] Encryption may also form an integral component of a criminal offence that targets victims online through computers and other information technologies. One example of this capability is known as a 'ransomware' scam. This scam involves a malicious type of software ('malware') that can lock a computer and its data content, and uses social engineering tactics, such as threats, to coerce victims into paying fees for regained computer access.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- the need for encryption to enable modern e-commerce, e-banking and all types of cybersecurity and protect critical infrastructure.

These issues will be discussed further in this annex.

THE APPLICATION OF ENCRYPTION

Encryption is technology that can be applied to data-in-use and data-at-rest. Any of these could have various layers of encryption applied to it by any or all of the following: the end user, third party applications, and telecommunication service providers.

Data-in-use, otherwise known as active data, is data that is live and under constant change and manipulation by an application. Data-in-use is physically stored in databases, spreadsheets, etc. Data-at-rest is inactive data stored physically in data warehouses, archives, hard drives, tapes, off-site backups, mobile devices, etc.

In addition, encryption can be applied to more specific items such as the message itself (i.e. email, text message, or photo), the storage media of the device (i.e. the cell phone, the computer, the tablet), or the transmission network and/or channel (i.e. a VPN network, an enterprise server, or even the communication service provider's network).

POLICY AND LEGISLATION

THE GOVERNMENT OF CANADA'S ELECTRONIC COMMERCE STRATEGY & THE POLICY ON CRYPTOGRAPHY)

Almost 20 years ago, in 1997-1998, an extensive review of Canada's Cryptography policy was undertaken under the leadership of Industry Canada (now Innovation, Science, and Economic Development Canada) in the context of Canada's e-commerce policy but extended to the issues of law enforcement access and national security considerations. In 1998, Canada's Minister of Industry announced its Cryptography policy and, this policy remains in place today.

In this policy, the Government affirmed the following principles:

1) The freedom of Canadians to develop, import and use whatever cryptography they wished;
2) Support for private sector research and development
3) The Government would not implement mandatory key recovery requirements or licensing regimes for certification authorities or trusted third parties;
4) Export controls would continue to be consistent with Canada's international obligations; and
5) The Government would explore legislative and other options to protect consumer privacy and to assist law enforcement and national security agencies.

The policy emphasized the importance of maintaining a balanced approach to a complex problem.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

A number of key considerations played a role in helping shape Canada's Cryptography policy. The following were some significant developments that helped guide the policy development process:

- The increasing use of strong encryption software and computers powerful enough to encrypt and decrypt data easily were commonly available;
- The rapidly increasing use of telecommunications media suitable for encryption (e.g. email and other data conveyed via the Internet and other computer-based media) for both personal and commercial communications;
- The increasing use of wireless cellular telephones, which had created pressure for the development of digital equipment and had led to the encryption of their signals in some cases; and
- The increasing reliance on computers and computer networks for commercial activities and the need to protect privacy and security, which had led companies to store business records in secure computer facilities and in encrypted forms.

Notably, many of these developments are still relevant today given the proliferation of and reliance on the use of technology, encryption and digital communications. Both then and now, encryption forms part of the core framework that allows electronic commerce to flourish.
In an effort to develop a cryptography framework, specific considerations were given to the areas of: electronic commerce; [redacted] nvolved in any discussion of encryption. s.21(1)(a)

Electronic Commerce

In 1998, an increasing number of transactions were shifting from closed networks to open networks and encryption became essential for the conduct of electronic commerce. Open networks allowed for more global trading, but came with a variety of security challenges including concerns over the authentication of communicating parties, the integrity of the data being communicated, the confidentiality of the proprietary or personal data, and the assurance that transactions have been authorized by legitimate users. Without encryption, these challenges may not have been addressed.

The aims of law enforcement and business align when encryption protects proprietary information, trade secrets, and in general, helps defend industry and consumers against fraud and other unlawful activities. In addition, encryption helps protect information that is important to the objectives of law enforcement and national security agencies by protecting Canada, its industry and valuable information.

The policy challenge was, and continues to be, the need to find solutions that will address the investigative challenges faced by law enforcement and national security agencies without interfering with legitimate business, institutional or individual interests and without weakening the security of the network infrastructure for all users. Furthermore, consideration will now need

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

to be given to the current digital environment and the trend towards the use of default encrypted devices, compared to the use of back end encryption software, in addition to end-to-end encryption by many companies within the information and communication technology sector.

A recent dispute in the U.S. between Apple and the FBI highlighted challenges in this alignment, when Apple refused to create a 'key' or 'backdoor' bypassing the encryption protecting (or locking) a suspect's iPhone. Ultimately, the FBI accessed the phone through a third party, but the dispute highlighted the complex issues faced in finding solution to the challenges stemming from the widespread use of encryption.

[redacted]

Formatted: Highlight

Formatted: Highlight

Human rights and civil liberties

The rights of Canadians to privacy and to express themselves freely are constitutionally protected. Section 8 of the *Charter* guarantees Canadians the right to be free from "unreasonable search or seizure" which has been interpreted through jurisprudence [redacted]

s.21(1)(a)

The protection of a reasonable expectation of privacy, and invasions of that privacy must be justified, must be authorized in law and generally require specific pre-authorization by the courts. In this context, [redacted] and the right to

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

freedom of expression may extend to both the production of encryption products and their use to protect the messages being expressed or data being stored.

It is important to note that Canadians also have human rights protections under international human rights law with regard to privacy and freedom of expression. Canada is a State party to the International Covenant on Civil and Political Rights. Article 17 of the Covenant prohibits interferences with privacy that are arbitrary or unlawful and Article 19 guarantees an individual's freedom of expression.

WASSENAAR ARRANGEMENT ON EXPORT CONTROLS FOR CONVENTIONAL ARMS AND DUAL-USE GOODS AND TECHNOLOGIES

While Canada has not addressed encryption challenges in law, Canada is one of 41 participating states to the Wassenaar Arrangement which was established to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies. Participating States seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities. The aim is also to prevent the acquisition of these items by terrorists.

Participating States control all items set forth in the Munitions List (items designed for military use) and the List of Dual-Use Goods and Technologies (items having both civilian and military applications such as encryption software),with the objective of preventing unauthorized transfers or re-transfers of those items.

The Participating States have an agreement to maintain national export controls on listed items, which are implemented via national legislation; are guided by agreed upon best practices, guidelines or elements; have agreed to report on transfers and denials of specific controlled items to destinations outside of the arrangement; and have agreed to exchange information on sensitive dual-use goods and technologies.

FORMER BILL C-30 – *PROTECTING CHILDREN FROM INTERNET PREDATORS ACT*, 2012

In the past, in the context of work on lawful access issues, under former Bill C-30 (*Protecting Children from Internet Predators Act*, 2012, 41st Parliament, 1st session), legislative proposals were introduced, but did not come into force, to create requirements for telecommunications service providers to decrypt communications where it was readily possible for the service provide to do so, in the context of lawful interception. However, telecommunications service providers were not required to develop specific decryption techniques themselves. For example, if interception was successful but the data retrieved was encrypted by a tool that was implemented directly by the service provider, rather than the user, then the service provider would be asked to decrypt the data.

s.21(1)(a)

~~These proposals were supported by law enforcement and national security agencies.~~ However, ~~in the larger picture,~~ these proposals would not have solved the problem posed by encryption in

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

whole, nor did they purport to do so. This is particularly true given that many major IT companies have built mobile and other digital devices that enable individuals to encrypt and decrypt data at the user level.

JURISDICTIONAL AND INTERNATIONAL CONSIDERATIONS

Law enforcement and national security agencies also face challenges when attempting to compel communication service providers to decrypt communications. Many communication service providers, particularly software and application service providers, do not have physical premises in Canada, and may not be subject to Canadian jurisdiction. In order to be able to obtain information held by these companies, currently the principal process available is through the use of Mutual Legal Assistance Treaties (MLATs). Currently, MLAT processes are not always timely enough for the exigencies of investigations involving electronic evidence, nor were they designed for a high volume of requests that could ensue given the trend toward global inter-connectivity and challenges in relation to jurisdiction in the context of modern communications.

It is important to note that the complex challenges involving encryption and are the topic of on-going discussion and work in various international fora. The subject of how best to address the challenges for law enforcement and national security agencies arising from the use of encryption while supporting its many beneficial uses is an issue also being explored by many of Canada's closest allies.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Oakes, Lindsey (PS/SP) <lindsey.oakes@canada.ca>
Sent: 2016-Jun-29 9:56 AM
To: Wong, Normand
Cc: Angers, Lucie; Sansom, Gareth; Audcent, Karen
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ [redacted] GS-mod rev la nw.docx
Attachments: RE: 20160623 Lawful Access - Annex - Encryption _ [redacted] GS-mod rev la nw.docx

Hey Norm, s.21(1)(a) s.23

See attached my response to you and Ray this morning.

Happy to remove it entirely and leave it to what is discussed in the GP only.

Lindsey Oakes
Telephone: 613-990-8020
Blackberry: 613-410-6057
E-mail | Courriel: lindsey.oakes@canada.ca

Public Safety Canada | Sécurité publique Canada

From: Wong, Normand [mailto:Normand.Wong@justice.gc.ca]
Sent: Wednesday, June 29, 2016 9:54 AM
To: Oakes, Lindsey (PS/SP)
Cc: Angers, Lucie; Sansom, Gareth; Audcent, Karen
Subject: FW: 20160623 Lawful Access - Annex - Encryption _ [redacted] GS-mod rev la nw.docx

Lindsey – Ray MacCallum's reply is below. [redacted]

Normand Wong
613.941.2341 o
613.791.4669 m

From: Angers, Lucie
Sent: 2016-Jun-28 5:45 PM
To: Wong, Normand <Normand.Wong@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ [redacted] GS-mod rev la nw.docx

Why don't you check with Lindsay? I'm surprised that they did not see any of the annexes before...

From: Wong, Normand
Sent: Tuesday, June 28, 2016 4:57 PM
To: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: Fw: 20160623 Lawful Access - Annex - Encryption _ [redacted] GS-mod rev la nw.docx

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Any idea of how I should reply to Ray?

Sent from my BlackBerry 10 smartphone on the Rogers network.

From: MacCallum, Raymond <Raymond.MacCallum@justice.gc.ca>
Sent: Tuesday, June 28, 2016 16:53
To: Wong, Normand
Cc: 'lindsey.oakes@canada.ca' s.23
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ GS-mod rev la nw.docx

Norm,

Ray

From: Watts, Heather
Sent: June 28, 2016 9:12 AM
To: Wong, Normand <Normand.Wong@justice.gc.ca>; MacCallum, Raymond <Raymond.MacCallum@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sargent, Laurie <Laurie.Sargent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; 'Oakes, Lindsey (PS/SP)' <lindsey.oakes@canada.ca>
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ GS-mod rev la nw.docx

Hi Norm,

Thanks for forwarding

Heather

From: Wong, Normand
Sent: 2016-Jun-28 8:55 AM
To: Watts, Heather
Cc: Angers, Lucie; Audcent, Karen; Sargent, Laurie; Sansom, Gareth; 'Oakes, Lindsey (PS/SP)'
Subject: FW: 20160623 Lawful Access - Annex - Encryption _ GS-mod rev la nw.docx

Heather: I think this is you, but if not let me know who could take a look at this. It's part of the National Security Green Paper – Annex on encryption.

Thanks,

Norm

Normand Wong
613.941.2341 o
613.791.4669 m

From: Oakes, Lindsey (PS/SP) [mailto:lindsey.oakes@canada.ca]
Sent: 2016-Jun-28 8:11 AM
To: Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

<Gareth.Sansom@justice.gc.ca>; Adamowski, Andrew (PS/SP) <andrew.adamowski@canada.ca>
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ [redacted]GS-mod rev la nw.docx

Hi Norm,

Please find attached the updated version which incorporates the additional changes to the text that you provided. If Lucie and Gareth want to take another peak given the changes between the two previous versions and let me know if there is anything further, that would be great.

[redacted] s.23

Lindsey Oakes
Telephone: 613-990-8020
Blackberry: 613-410-6057
E-mail | Courriel: lindsey.oakes@canada.ca

Public Safety Canada | Sécurité publique Canada

From: Wong, Normand [mailto:Normand.Wong@justice.gc.ca]
Sent: Monday, June 27, 2016 4:10 PM
To: Oakes, Lindsey (PS/SP)
Cc: Angers, Lucie; Audcent, Karen; Sansom, Gareth
Subject: 20160623 Lawful Access - Annex - Encryption _ [redacted]GS-mod rev la nw.docx s.21(1)(a)

Our comments. They are mainly comments and not suggested text although I did provide some suggested text. I think we are generally of the view that it needs work to tighten up. The part on the history is good, [redacted]

I'll look at the data retention piece now.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Oakes, Lindsey (PS/SP) <lindsey.oakes@canada.ca>
Sent: 2016-Jun-29 1:34 PM
To: Wong, Normand; MacCallum, Raymond; Audcent, Karen; Angers, Lucie; Sansom, Gareth
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ GS-mod rev la nw.docx

Okay, thanks Norm. Much appreciated.

Lindsey Oakes
Telephone: 613-990-8020
Blackberry: 613-410-6057
E-mail | Courriel: lindsey.oakes@canada.ca

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

Public Safety Canada | Sécurité publique Canada

From: Wong, Normand [mailto:Normand.Wong@justice.gc.ca]
Sent: Wednesday, June 29, 2016 1:33 PM
To: Oakes, Lindsey (PS/SP); MacCallum, Raymond; Audcent, Karen; Angers, Lucie; Sansom, Gareth
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ GS-mod rev la nw.docx

[redacted]

Normand Wong
613.941.2341 o
613.791.4669 m

From: Oakes, Lindsey (PS/SP) [mailto:lindsey.oakes@canada.ca]
Sent: 2016-Jun-29 11:50 AM
To: Wong, Normand <Normand.Wong@justice.gc.ca>; MacCallum, Raymond <Raymond.MacCallum@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Angers, Lucie <Lucie.Angers@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ -GS-mod rev la nw.docx

Hi Norm and Ray,

[redacted]

Lindsey Oakes
Telephone: 613-990-8020
Blackberry: 613-410-6057
E-mail | Courriel: lindsey.oakes@canada.ca

Public Safety Canada | Sécurité publique Canada

From: Wong, Normand [mailto:Normand.Wong@justice.gc.ca]
Sent: Wednesday, June 29, 2016 11:44 AM
To: Oakes, Lindsey (PS/SP); MacCallum, Raymond; Audcent, Karen; Angers, Lucie; Sansom, Gareth
Subject: Fw: 20160623 Lawful Access - Annex - Encryption _ GS-mod rev la nw.docx

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

I've forwarded your thoughts to lindsey which were the same as mine. PS will decide I think.

Sent from my BlackBerry 10 smartphone on the Rogers network.

From: MacCallum, Raymond <Raymond.MacCallum@justice.gc.ca> s.21(1)(a)
Sent: Wednesday, June 29, 2016 11:36 s.23
To: Wong, Normand
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ GS-mod rev la nw.docx

Thanks Norm.

Ray

From: Wong, Normand
Sent: June 29, 2016 9:56 AM
To: MacCallum, Raymond <Raymond.MacCallum@justice.gc.ca>
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ GS-mod rev la nw.docx

Ray: I'm inquiring with Lindsey what we should do. You make a good point that

Normand Wong
613.941.2341 o
613.791.4669 m

From: MacCallum, Raymond
Sent: 2016-Jun-28 4:53 PM
To: Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: 'lindsey.oakes@canada.ca' <lindsey.oakes@canada.ca>
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ -GS-mod rev la nw.docx

Norm,

Ray

From: Watts, Heather
Sent: June 28, 2016 9:12 AM
To: Wong, Normand <Normand.Wong@justice.gc.ca>; MacCallum, Raymond <Raymond.MacCallum@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sargent, Laurie <Laurie.Sargent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; 'Oakes, Lindsey (PS/SP)'

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

<lindsey.oakes@canada.ca>
Subject: RE: 20160623 Lawful Access - Annex - Encryption _ [redacted] GS-mod rev la nw.docx

Hi Norm,

Thanks for forwarding, [redacted]

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

Heather

From: Wong, Normand
Sent: 2016-Jun-28 8:55 AM
To: Watts, Heather
Cc: Angers, Lucie; Audcent, Karen; Sargent, Laurie; Sansom, Gareth; 'Oakes, Lindsey (PS/SP)'
Subject: FW: 20160623 Lawful Access - Annex - Encryption [redacted] GS-mod rev la nw.docx

Heather: I think this is you, but if not let me know who could take a look at this. It's part of the National Security Green Paper – Annex on encryption. [redacted]

Thanks,

Norm

Normand Wong
613.941.2341 o
613.791.4669 m

From: Oakes, Lindsey (PS/SP) [mailto:lindsey.oakes@canada.ca]
Sent: 2016-Jun-28 8:11 AM
To: Wong, Normand <Normand.Wong@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Audcent, Karen <Karen.Audcent@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>; Adamowski, Andrew (PS/SP) <andrew.adamowski@canada.ca>
Subject: RE: 20160623 Lawful Access - Annex - Encryption [redacted] GS-mod rev la nw.docx

Hi Norm,

Please find attached the updated version which incorporates the additional changes to the text that you provided.
If Lucie and Gareth want to take another peak given the changes between the two previous versions and let me know if there is anything further, that would be great.

[redacted]

Lindsey Oakes
Telephone: 613-990-8020
Blackberry: 613-410-6057
E-mail | Courriel: lindsey.oakes@canada.ca

Public Safety Canada | Sécurité publique Canada

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

From: Wong, Normand [mailto:Normand.Wong@justice.gc.ca]
Sent: Monday, June 27, 2016 4:10 PM
To: Oakes, Lindsey (PS/SP)
Cc: Angers, Lucie; Audcent, Karen; Sansom, Gareth
Subject: 20160623 Lawful Access - Annex - Encryption _ [redacted] GS-mod rev la nw.docx

s.21(1)(a)

Our comments. They are mainly comments and not suggested text although I did provide some suggested text. I think we are generally of the view that it needs work to tighten up. The part on the history is good, [redacted]

I'll look at the data retention piece now.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Bindman, Stephen
Sent: 2016-Jul-03 10:31 AM
To: Angers, Lucie; Assad, Michael; Audcent, Karen; Breithaupt, Doug; Bryden, Cathleen; Colaianni, Anna; Cormier, Sophie M.; Douglas, Michelle; Duffy, Michael; Eid, Elisabeth; Geh, Sarah; Gilmour, Glenn; Glushek, Phaedra; Hébert, Nathalie; Holthuis, Annemieke; Hoover, Doug; Koster, Greg; Leclerc, Caroline; Legault, Yanike; Lidstone, Bonnie; Lobo, Betty Ann; McCann, Tracey; Melanson, Janice; Nesbitt, Scott; Patry, Claudine; Piragoff, Donald; Pollard, Dorette; Scrivens, Mark; Sheppard, Ann; Sugunasiri, Shalin (PS); Wilkins, Keith
Subject: FW: Encryption creating a barrier for police, documents suggest | Toronto Star

Stephen Bindman
Special Advisor on Wrongful Convictions//Conseiller spécial, erreurs judiciaires
Policy Sector | Secteur des politiques
Department of Justice Canada | Ministère de la Justice Canada
Ottawa, ON K1A 0H8
sbindman@justice.gc.ca
Telephone | Téléphone 613-894-7495 (cell)
Facsimile | Télécopieur 613-957-9949
Government of Canada | Gouvernement du Canada

From: Morgan, Ed (HC/SC) [mailto:ed.morgan@canada.ca]
Sent: July-02-16 8:00 AM
Subject: Encryption creating a barrier for police, documents suggest | Toronto Star

https://www.thestar.com/news/canada/2016/07/02/encryption-creating-a-barrier-for-police-documents-suggest.html

Sent from my BlackBerry 10 smartphone on the Rogers network.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Holthuis, Annemieke
Sent: 2016-Jul-07 12:38 PM
To: Sansom, Gareth; McKey, Erin; Ram, Christopher; Audcent, Karen; Wong, Normand
Cc: Angers, Lucie
Subject: FYI - article on encryption issues

FYI – note the first item on the encryption debate.

Erin: The article states: "Little is known about the two US iMessage and WhatsApp cases — why DOJ backed off in the former, how the latter turned out, what orders the two courts entered, how Apple and Facebook responded, or the legal arguments made on each side." Would this be something you might ask your G7 colleagues?

Annemieke

From: Just Security [mailto:info=justsecurity.org@mail164.atl121.mcsv.net] **On Behalf Of** Just Security
Sent: Wednesday, July 06, 2016 3:05 PM
To: Holthuis, Annemieke <Annemieke.Holthuis@justice.gc.ca>
Subject: Posts from Just Security for 07/06/2016

Today on *Just Security* for **07/06/2016**

View this email in your browser

JUST SECURITY
A FORUM ON LAW, RIGHTS, AND U.S. NATIONAL SECURITY

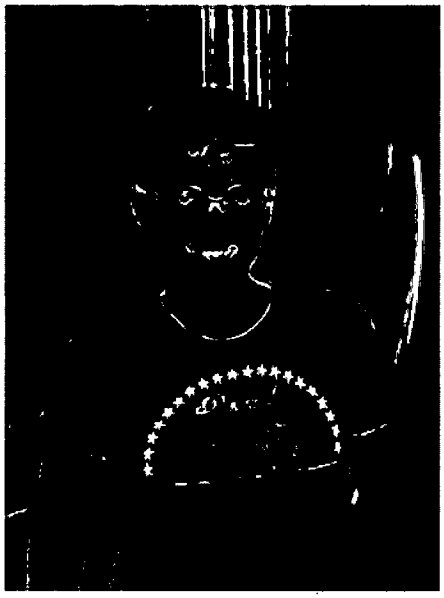
Share | Tweet | Forward | +1 | Read Later

Missed anything on *Just Security* today? We've got you covered. You can find all our posts from the last 24 hours right here with **Today on *Just Security***....

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Excerpts:

The Encryption Debate: All Quiet on the Western Front?



Riana Pfefferkorn

The US war on encryption has quieted down recently. The San Bernardino and Brooklyn court cases concerning encrypted iPhones both ended this spring not with a bang, but with a whimper. The disastrous Burr-Feinstein anti-crypto bill has gone dormant — for now. Likewise, similar measures proposed in the New York, California, and Louisiana legislatures have either been formally killed off or left to wither away in committee. The tragic massacre in Orlando may have helped defeat a proposed amendment to a defense appropriations bill that would have *protected* encryption. But on the bright side, it has not spurred a renewed offensive *against* encryption like what we saw after the Paris and San Bernardino attacks last winter (though some politicians and national security experts continue to claim that defeating terrorism requires reaching a "middle ground" on encryption).

While encryption has fallen off the front page in US news, the current round of the Crypto Wars continues elsewhere and behind the scenes. Internationally, governments are quite active on this issue. The lower and upper houses of

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Russia's legislature have just passed a bill that, if approved by the Kremlin (as is expected), would mandate state security services be able to access Russians' encrypted communications and would allow them to obtain providers' encryption keys without a court order. Within the same week, India's high court rejected a petition to ban end-to-end encrypted messaging apps and mandate crypto backdoors. The court, while dismissing the case, urged the petitioner to take the matter to the appropriate state agencies. In the space of a week, the fate of secure communications turned grim for 143 million Russians and was left up in the air for over 1.3 billion Indians. With national governments watching each other closely on encryption issues, the ramifications of these two powerful countries' encryption policies won't be confined within their borders.

This international activity supports my suspicion that end-to-end encrypted messaging tools are probably the next frontier in the current Crypto War here in the US as well. FBI Director Jim Comey has promised more litigation over government access to encrypted data. One of the next big court showdowns will probably involve a demand that an app's provider somehow decrypt encrypted communications intercepted *in transit* pursuant to a wiretap order, rather than access to encrypted data *in storage* on a device for which the government has a warrant.

Director Comey alluded to this possible move in a May speech. He claimed that one out of every eight devices involved in active FBI investigations now can't be unlocked — an eyebrow-raisingly high number. He also predicted that messaging apps' rising adoption of end-to-end encryption will further increase that number. While this remark didn't seem to distinguish between searches of encrypted devices and interception of encrypted messages on the wire, it nevertheless indicates that US law enforcement officials are thinking about their next move vis-à-vis encrypted messaging. At present, the newly-released wiretap report for 2015 has been read to indicate that encryption remains a negligible problem for law enforcement intercepts. However, the reports contain few details relating to encryption, and Comey and Deputy Attorney General Sally Yates have cautioned in the past against drawing that conclusion from the report (namely the 2014

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

version, when *more* instances of encryption were reportedly encountered than in 2015).

So who will be up at bat for the coming fight over end-to-end encrypted messaging apps? If popularity is any prediction, the most likely contenders are Apple's iMessage, with its heavy US traffic, or Facebook-owned WhatsApp, which roughly one-seventh of the Earth's population uses. (While it's the darling of privacy and security advocates, Signal has a relatively tiny user base, meaning it probably doesn't come up much in the garden-variety cases that dominate law enforcement's time.)

Last winter, before WhatsApp deployed end-to-end encryption by default, Julian Sanchez speculated that the company was already getting numerous wiretap orders. But, he pointed out that law enforcement would no longer be able to intercept readable messages once WhatsApp finished rolling out end-to-end encryption, which it completed in April (using Signal's encryption protocol). In the intervening months, the public has learned little about US law enforcement's response. Are they still bothering to get wiretap orders for WhatsApp users? Can they somehow obtain legible WhatsApp messages, and if so, how? Are police getting court authorization to mount a man-in-the-middle attack, as Sanchez suggested? Has Facebook been ordered to provide decrypted WhatsApp messages to police, or to give them other assistance to enable them to do so?

Those are the sorts of court scenarios that might arise in the end-to-end encryption fight. Indeed, iMessage and WhatsApp specifically have already gotten caught up in court disputes in the US and abroad. In the US, the Justice Department was reportedly figuring out how to proceed in a recent wiretap matter involving WhatsApp. The Indian high court petition sought to ban WhatsApp and other end-to-end encrypted messaging tools because Indian police and intelligence services can't read users' messages. In Brazil, WhatsApp's inability, by design, to comply with orders to hand over user data led a judge to have a local Facebook executive briefly jailed and to block the app country-wide — twice. And a US court showdown over Apple's iMessage was supposedly averted last year when DOJ backed down.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The paucity of cases in this area (at least cases that the public knows about) makes it unclear how a battle over end-to-end encrypted messages might turn out, when and if the government finds the right test case. Little is known about the two US iMessage and WhatsApp cases — why DOJ backed off in the former, how the latter turned out, what orders the two courts entered, how Apple and Facebook responded, or the legal arguments made on each side.

If courts are ruling on tech companies' legal obligations to assist law enforcement vis-à-vis encrypted communications, it's happening in secret. The government's unusual choice to conduct the San Bernardino case in public backfired spectacularly. The federal government surely hasn't stopped making demands for access to encrypted smartphones, it's merely filing them under seal. That would keep the companies subjected to those demands from talking about them openly unless and until the matter is unsealed. That's why we know next to nothing about the iMessage and WhatsApp wiretap cases, and why we're not aware of any other attempts to compel providers to decrypt encrypted communications, if they do exist. Any gag orders directed to those providers as part of the surveillance demands might endure for years.

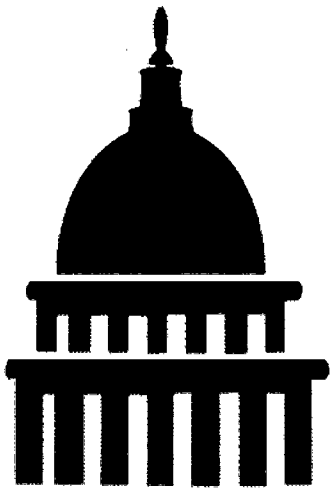
Sealing surveillance requests is doubtless appropriate initially, but too often these demands and orders remain sealed forever. This secrecy creates, as Magistrate Judge Stephen W. Smith has written, a "lacuna of law from which little light escapes." This is particularly a problem now that communications security is on the line. Single judges are secretly making decisions that can affect the security and availability of communications for entire populations. The public deserves to know how courts are "marking the bounds of legitimate government intrusion into our electronic lives." That's why we at the Stanford Center for Internet and Society are working to uncover and analyze provider-assistance court cases involving encryption, such as through FOIA requests we've filed on our own and with the ACLU. If and when we discover that end-to-end encrypted communication is the next front in the Crypto War, we intend to let you know.

Read on Just Security »

Read on »

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Highlights From the Chilcot Report



Just Security

Earlier today, the UK's Iraq Inquiry Committee released the report of its seven year investigation into the country's role in the Iraq War. Started in 2009 at the direction of then-Prime Minister Gordon Brown, the committee, chaired by retired civil servant Sir John Chilcot, was asked to investigate two questions: whether it was right and necessary to invade Iraq in March 2003; and whether the UK could — and should — have been better prepared for what followed. While the 6,400 page report will take time to read through and process, there are a few sections and conclusions we wanted to flag for our readers.

First, Section 5 of the report is particularly noteworthy for its focus on the role government lawyers played in the UK's participation in the war. Labeled "Advice on the legal basis for military action, November 2002 to March 2003," the section includes an in-depth discussion of legal advice given to senior British government officials by Lord Peter Goldsmith, then-Attorney General for England, Wales and Northern Ireland, in the run-up to the war.

Key findings from Section 5 include the notion that senior government officials were not given an explanation of legal advice that helped the British government determine Iraq failed to meet its disarmament obligations under UN Security

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Council Resolution 1441 and thereby opened the door for the UK's use of force against the regime of Saddam Hussein:

Cabinet [consisting of senior British government officials and MP's] was provided with the text of Lord Goldsmith's Written Answer to Baroness Ramsey setting out the legal basis for military action. That document represented a statement of the Government's legal position – it did not explain the legal basis of the conclusion that Iraq had failed to take "the final opportunity" to comply with its disarmament obligations offered by [UN] resolution 1441. Cabinet was not provided with written advice which set out, as the advice of 7 March had done, the conflicting arguments regarding the legal effect of resolution 1441 and whether, in particular, it authorised military action without a further resolution of the Security Council. The advice should have been provided to Ministers and senior officials whose responsibilities were directly engaged and should have been made available to Cabinet.

Second, in his statement accompanying the report, Chilcot wrote that, in response to the question of whether it was right and necessary to invade Iraq in 2003, the Committee determined that "the UK chose to join the invasion of Iraq before the peaceful options for disarmament had been exhausted. Military action at that time was not a last resort." He went on to say that the Committee's other key conclusions include:

The judgements about the severity of the threat posed by Iraq's weapons of mass destruction – WMD – were presented with a certainty that was not justified. Despite explicit warnings, the consequences of the invasion were underestimated. The planning and preparations for Iraq after Saddam Hussein were wholly inadequate. The Government failed to achieve its stated objectives.

Third, the Executive Summary contains key findings (starting on p. 111) and lessons learned (starting on p. 129) that cover the entire time under investigation (2001–2009). While the report obviously has more in-depth explanations and discussions of each, those sections are a good place to start.

The report itself covers only part of the total documentation the Committee made available. The Committee also published reams of witness and documentary

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

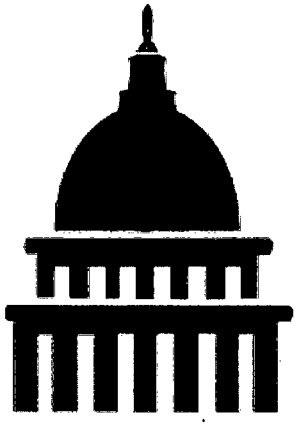
evidence it considered during the inquiry. Additionally, the Committee has published some of the various other materials it considered during its investigation, and included details about those materials where it did not publish the information itself.

There will of course be much to say about the report once our editors and contributors have had a chance to read it through more comprehensively, so keep watching this space for more.

Read on Just Security »

Read on »

The Early Edition: July 6, 2016



Zoë Chapman

Before the start of business, *Just Security* provides a curated summary of up-to-the-minute developments at home and abroad. Here's today's news.

IRAQ and SYRIA

Turkey is building a giant concrete wall to block the Syrian border close to the Turkish city of Gaziantep, a region that has been a thoroughfare for thousands of extremist fighters joining the Islamic State in Syria. Turkey has always denied it has permitted this movement, though documents obtained by Dominique Soguel and Aya Batrawy of the AP indicate a "pattern of porousness"

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

along Turkey's border with Syria, those who are documented as entering by that route making up "between 25 to 40 percent of the estimated total of IS's foreign recruits."

Recent Islamic State-linked attacks in four countries indicate the "limitations" of US-led efforts to oust the group from Syria and Iraq, write Warren Strobel and John Walcott for Reuters. That said, the Obama administration's portrayal of the Islamic State's attacks worldwide as a direct consequence of the US-led military successes in Iraq and Syria is "overly simplistic and understates how Islamic State's influence has spread beyond the territory it controls."

The latest attacks "reveal an enemy that is adapting, becoming more sophisticated than Al Qaeda, and nurturing a far-flung network of operations, including in the West." This requires a "complex response," suggests the New York Times editorial board, with improved intelligence, coordinated attempts to locate terrorist before they attack, and improved strategies to counter extremist propaganda as necessary as bombing.

Al-Qaeda is "the principal benefactor" of Syrian President Assad's continued survival, for whom, as things stand, there is no reason to view the political process "as anything less than a game in which to taunt and kill his adversaries, while compelling his allies to double-down in defense of his regime." Charles Lister blames the US's failure to solve the Syrian crisis, which he says is prompting Syrians to see al-Qaeda as "a more loyal protector of their lives" than the US. [The Daily Beast]

A suicide bombing outside a bakery in Syria's Hassakeh province killed at least ten yesterday, Syria's state-run news agency and the London-based Syrian Observatory for Human Rights which puts the death toll at 16 – have reported. [AP]

Three people were killed in a mortar attack on a camp for displaced Iraqis close to Baghdad late last night, according to the UN. The camp is populated by

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

families who fled there in the wake of the Islamic State. No one has claimed responsibility for the attack. [AP]

US-led airstrikes continue. US and coalition forces carried out 11 airstrikes against Islamic State targets in Syria on July 4. Separately, partner forces conducted 11 strikes against targets in Iraq. [Central Command]

THE CHILCOT REPORT

The Chilcot report on the Iraq War has been released today, finding that the UK did not exhaust all peaceful options before joining the invasion of Iraq, that judgments about Iraq's weapons of mass destruction "were presented with a certainty that was not justified," and that post-war planning was "wholly inadequate." Speaking ahead of the report's release at 11:35 GMT, enquiry head Sir John Chilcot said he hoped that future military action on such a scale would only be possible in future with more careful analysis and political judgment. [BBC]

Live coverage is being provided by the BBC and the Guardian.

Whatever the report establishes, there are "at least three deeper truths about Iraq," writes David Gardner for the Financial Times. First, it revealed the "limits to US power" – to which Britain was a "side show" – and its lack of ability to "shape the broader Middle East." Second, "Iraq led to Syria." Third, the West's "recklessness" in Iraq, and then its "fecklessness" in Syria, have led to "inescapable if unintended consequences," at least for the UK and the EU.

HILLARY CLINTON EMAIL CONTROVERSY

FBI Director James Comey recommended yesterday that no criminal charges be brought against Hillary Clinton in relation to her use of a private email server to handle classified information while serving as secretary of state. [New York Times' Mark Landler and Eric Lichtblau]

However, Comey did describe Clinton's behavior as "extremely careless" in a 15-minute statement at FBI headquarters, adding that "any reasonable person" in Clinton's position would have known that the sensitive information she was

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

handling warranted greater security. [Wall Street Journal's Kate O'Keeffe and Byron Tau]

This will undercut the argument she has consistently made, that the whole issue is the result of over-zealous, after-the-fact classification of emails as they were publicized under the Freedom of Information Act, suggests Steven Lee Myers in the New York Times.

"Rigged for the powerful." The most "revealing" part of Comey's statement was the following, suggests the Wall Street Journal editorial board: "This is not to suggest that in similar circumstances, a person who engaged in this activity would face no consequences." This exposes double standards within the FBI, insists the board.

Comey's comments may have been "unusual," but they were a "justifiable departure from normal practice," writes Ruth Marcus. Comey's statement took this bad situation and "made it better," revealing to the public information that is not sufficient to support criminal charges, but which will be deemed by many to be relevant to their assessment of Clinton's suitability for presidency. [Washington Post]

It is possible that Clinton's email system was accessed by "hostile actors," Comey said, though the FBI investigation did not uncover any successful hacks on her "homebrew" setup. Comey said that, given the nature of the attackers, he "wouldn't expect to see any evidence." The most likely suspects are apparently Russia, China, and Israel. [Politico's Eric Geller and Martin Matishak]

The State Department has taken issue with Comey's comment that its "security culture" is "generally lacking in the kind of care for classified information found elsewhere in the government." The FBI's investigation into Hillary Clinton's former email habits uncovered a number of shortcomings, in particular the State Department's habit of using unclassified email systems to discuss sensitive information. [The Hill's Julian Hattem]

BAGHDAD BOMBING

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The death toll from Sunday's bombing in Iraq's capital has risen to 250, the Iraqi government has confirmed. This is now the deadliest such attack since the 2003 US-led invasion of Iraq, reports the BBC.

Iraq's interior minister Muhammad Ghabban has resigned following the bombing, making the announcement at a news conference yesterday. His resignation will only be official, however, if Prime Minister Haider al-Abadi approves it. [Reuters]

DHAKA ATTACK

Bangladesh's politicians' inability to work together and habit of using attacks for political gain may have helped extremist groups to gain a foothold in the country, political scientists and terrorism researchers worry. This "long-toxic political atmosphere" has continued following the attack in Dhaka, reports Syed Zain Al-Mahmood for the Wall Street Jounal.

A hostage in the attack on the Holey Artisan Bakery in Dhaka last Friday was shot by police who mistook him for one of the gunmen, subsequently releasing his picture along with the other attackers. [BBC]

SAUDI ARABIA

Saudi Arabia's King Salman bin Abdulaziz Al Saud has vowed to "strike with an iron fist" those responsible for Monday's suicide attacks, the death toll as a consequence of which has now risen to four, as well as those responsible. [Al Jazeera]

The triple suicide-attack "can hardly be thought of as incidental," writes the Wall Street Journal editorial board: the Islamic State, it suggests – though the group has not claimed responsibility for the attacks – would like nothing more than to destroy the "pro-American" House of Saud and take Islam's holiest cities for themselves.

EUROPE

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Fifteen people were sentenced for their involvement in a terror plot that was thwarted in Belgium in 2015, yesterday. The plot is believed to have been orchestrated by Abdelhamid Abaaoud, who was the on-the-ground coordinator for the November Paris attacks. [New York Times' Alissa J Rubin]

"Our country was not ready; now we must get ready." Further details of the report of a French parliamentary commission set up to assess the failure to prevent a series of terror attacks in France in 2015 have been provided by Angelique Chrisafis in the Guardian. The report highlights "global failure" among French intelligence services, and recommends replacing them with a US-style national counter-terrorism agency.

SOUTH CHINA SEA

The Philippines is prepared to talk to China if the arbitration panel in The Hague rules in its favor, rather than go to war, its new President Rodrigo Duterte said yesterday, adding that the Philippines will accept and abide by the ruling if, conversely, it does not go in its favor. [AP's Tersa Cerojano]

Veteran Chinese foreign policy maker Dai Bingguo urged the US to scale back its "heavy-handed intervention" in the South China Sea in a speech in Washington yesterday. [Washington Post's Chun Han Wong]

OTHER DEVELOPMENTS

Brazilian authorities are attempting to find missing former Guantánamo Bay detainee Abu Wa'el Dhiab, whom Uruguay, where Dhiab was resettled after his release, continues to insist is visiting Brazil. [AP]

The US criticized Israel's plans to build hundreds of new homes in the occupied West Bank and East Jerusalem, State Department spokesperson John Kirby calling the plans the "latest step ... in a systematic process of land seizure." [BBC] Israel's Prime Minister Benjamin Netanyahu has authorized the building of over a thousand new homes, according to an Israeli official, presenting

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

the move as a response to a series of attacks by Palestinians against Jewish settlers, reports Josef Federman for the AP.

The UN is "screwing up" the political process in Libya by trying to impose an unfeasible agreement on the country's various factions, Libya's prime minister – the head of a weak interim government based in eastern Libya and rival to the UN-brokered presidency council based in Tripoli – said yesterday. [AP's Maggie Michael]

An ex-National Guardsman has been arrested for allegedly offering to obtain weapons for what he believed was going to be an Islamic State attack on US soil, the Justice Department said yesterday. [The Hill]

A suicide car bomb in the southern Yemeni port city of Aden has killed at least 10 inside a military and security compound located next to the city's international airport today. No group has immediately claimed responsibility for the attack, reports Ahmen Al-Haj for the AP.

The UK faces being treated like other non-European countries when it comes to transferring personal data when it leaves the EU, writes Duncan Robinson for the Financial Times. Personal data can easily be transferred between EU countries under EU privacy rules, but can only be transferred outside the bloc if certain criteria are fulfilled.

Read on Just Security »
Read on »

The Encryption Debate: All Quiet on the Western Front?

By Riana Pfefferkorn on Jul 06, 2016 01:00 pm

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Riana Pfefferkorn

The US war on encryption has quieted down recently. The San Bernardino and Brooklyn court cases concerning encrypted iPhones both ended this spring not with a bang, but with a whimper. The disastrous Burr-Feinstein anti-crypto bill has gone dormant — for now. Likewise, similar measures proposed in the New York, California, and Louisiana legislatures have either been formally killed off or left to wither away in committee. The tragic massacre in Orlando may have helped defeat a proposed amendment to a defense appropriations bill that would have *protected* encryption. But on the bright side, it has not spurred a renewed offensive *against* encryption like what we saw after the Paris and San Bernardino attacks last winter (though some politicians and national security experts continue to claim that defeating terrorism requires reaching a "middle ground" on encryption).

While encryption has fallen off the front page in US news, the current round of the Crypto Wars continues elsewhere and behind the scenes. Internationally, governments are quite active on this issue. The lower and upper houses of Russia's legislature have just passed a bill that, if approved by the Kremlin (as is expected), would mandate state security services be able to access Russians' encrypted communications and would allow them to obtain providers' encryption keys without a court order. Within the same week, India's high court rejected a

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

petition to ban end-to-end encrypted messaging apps and mandate crypto backdoors. The court, while dismissing the case, urged the petitioner to take the matter to the appropriate state agencies. In the space of a week, the fate of secure communications turned grim for 143 million Russians and was left up in the air for over 1.3 billion Indians. With national governments watching each other closely on encryption issues, the ramifications of these two powerful countries' encryption policies won't be confined within their borders.

This international activity supports my suspicion that end-to-end encrypted messaging tools are probably the next frontier in the current Crypto War here in the US as well. FBI Director Jim Comey has promised more litigation over government access to encrypted data. One of the next big court showdowns will probably involve a demand that an app's provider somehow decrypt encrypted communications intercepted *in transit* pursuant to a wiretap order, rather than access to encrypted data *in storage* on a device for which the government has a warrant.

Director Comey alluded to this possible move in a May speech. He claimed that one out of every eight devices involved in active FBI investigations now can't be unlocked — an eyebrow-raisingly high number. He also predicted that messaging apps' rising adoption of end-to-end encryption will further increase that number. While this remark didn't seem to distinguish between searches of encrypted devices and interception of encrypted messages on the wire, it nevertheless indicates that US law enforcement officials are thinking about their next move vis-à-vis encrypted messaging. At present, the newly-released wiretap report for 2015 has been read to indicate that encryption remains a negligible problem for law enforcement intercepts. However, the reports contain few details relating to encryption, and Comey and Deputy Attorney General Sally Yates have cautioned in the past against drawing that conclusion from the report (namely the 2014 version, when *more* instances of encryption were reportedly encountered than in 2015).

So who will be up at bat for the coming fight over end-to-end encrypted messaging apps? If popularity is any prediction, the most likely contenders are Apple's

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

iMessage, with its heavy US traffic, or Facebook-owned WhatsApp, which roughly one-seventh of the Earth's population uses. (While it's the darling of privacy and security advocates, Signal has a relatively tiny user base, meaning it probably doesn't come up much in the garden-variety cases that dominate law enforcement's time.)

Last winter, before WhatsApp deployed end-to-end encryption by default, Julian Sanchez speculated that the company was already getting numerous wiretap orders. But, he pointed out that law enforcement would no longer be able to intercept readable messages once WhatsApp finished rolling out end-to-end encryption, which it completed in April (using Signal's encryption protocol). In the intervening months, the public has learned little about US law enforcement's response. Are they still bothering to get wiretap orders for WhatsApp users? Can they somehow obtain legible WhatsApp messages, and if so, how? Are police getting court authorization to mount a man-in-the-middle attack, as Sanchez suggested? Has Facebook been ordered to provide decrypted WhatsApp messages to police, or to give them other assistance to enable them to do so?

Those are the sorts of court scenarios that might arise in the end-to-end encryption fight. Indeed, iMessage and WhatsApp specifically have already gotten caught up in court disputes in the US and abroad. In the US, the Justice Department was reportedly figuring out how to proceed in a recent wiretap matter involving WhatsApp. The Indian high court petition sought to ban WhatsApp and other end-to-end encrypted messaging tools because Indian police and intelligence services can't read users' messages. In Brazil, WhatsApp's inability, by design, to comply with orders to hand over user data led a judge to have a local Facebook executive briefly jailed and to block the app country-wide — twice. And a US court showdown over Apple's iMessage was supposedly averted last year when DOJ backed down.

The paucity of cases in this area (at least cases that the public knows about) makes it unclear how a battle over end-to-end encrypted messages might turn out, when and if the government finds the right test case. Little is known about the two US iMessage and WhatsApp cases — why DOJ backed off in the former, how the

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

latter turned out, what orders the two courts entered, how Apple and Facebook responded, or the legal arguments made on each side.

If courts are ruling on tech companies' legal obligations to assist law enforcement vis-à-vis encrypted communications, it's happening in secret. The government's unusual choice to conduct the San Bernardino case in public backfired spectacularly. The federal government surely hasn't stopped making demands for access to encrypted smartphones, it's merely filing them under seal. That would keep the companies subjected to those demands from talking about them openly unless and until the matter is unsealed. That's why we know next to nothing about the iMessage and WhatsApp wiretap cases, and why we're not aware of any other attempts to compel providers to decrypt encrypted communications, if they do exist. Any gag orders directed to those providers as part of the surveillance demands might endure for years.

Sealing surveillance requests is doubtless appropriate initially, but too often these demands and orders remain sealed forever. This secrecy creates, as Magistrate Judge Stephen W. Smith has written, a "lacuna of law from which little light escapes." This is particularly a problem now that communications security is on the line. Single judges are secretly making decisions that can affect the security and availability of communications for entire populations. The public deserves to know how courts are "marking the bounds of legitimate government intrusion into our electronic lives." That's why we at the Stanford Center for Internet and Society are working to uncover and analyze provider-assistance court cases involving encryption, such as through FOIA requests we've filed on our own and with the ACLU. If and when we discover that end-to-end encrypted communication is the next front in the Crypto War, we intend to let you know.

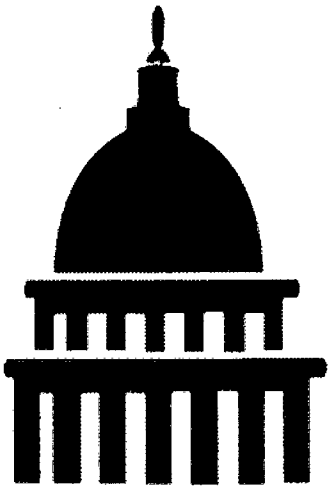
Read on Just Security »

Tweet Like

Highlights From the Chilcot Report

By Just Security on Jul 06, 2016 11:10 am

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.



Just Security

Earlier today, the UK's Iraq Inquiry Committee released the report of its seven year investigation into the country's role in the Iraq War. Started in 2009 at the direction of then-Prime Minister Gordon Brown, the committee, chaired by retired civil servant Sir John Chilcot, was asked to investigate two questions: whether it was right and necessary to invade Iraq in March 2003; and whether the UK could — and should — have been better prepared for what followed. While the 6,400 page report will take time to read through and process, there are a few sections and conclusions we wanted to flag for our readers.

First, Section 5 of the report is particularly noteworthy for its focus on the role government lawyers played in the UK's participation in the war. Labeled "Advice on the legal basis for military action, November 2002 to March 2003," the section includes an in-depth discussion of legal advice given to senior British government officials by Lord Peter Goldsmith, then-Attorney General for England, Wales and Northern Ireland, in the run-up to the war.

Key findings from Section 5 include the notion that senior government officials were not given an explanation of legal advice that helped the British government determine Iraq failed to meet its disarmament obligations under UN Security

000617

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Council Resolution 1441 and thereby opened the door for the UK's use of force against the regime of Saddam Hussein:

Cabinet [consisting of senior British government officials and MP's] was provided with the text of Lord Goldsmith's Written Answer to Baroness Ramsey setting out the legal basis for military action. That document represented a statement of the Government's legal position – it did not explain the legal basis of the conclusion that Iraq had failed to take "the final opportunity" to comply with its disarmament obligations offered by [UN] resolution 1441. Cabinet was not provided with written advice which set out, as the advice of 7 March had done, the conflicting arguments regarding the legal effect of resolution 1441 and whether, in particular, it authorised military action without a further resolution of the Security Council. The advice should have been provided to Ministers and senior officials whose responsibilities were directly engaged and should have been made available to Cabinet.

Second, in his statement accompanying the report, Chilcot wrote that, in response to the question of whether it was right and necessary to invade Iraq in 2003, the Committee determined that "the UK chose to join the invasion of Iraq before the peaceful options for disarmament had been exhausted. Military action at that time was not a last resort." He went on to say that the Committee's other key conclusions include:

The judgements about the severity of the threat posed by Iraq's weapons of mass destruction – WMD – were presented with a certainty that was not justified. Despite explicit warnings, the consequences of the invasion were underestimated. The planning and preparations for Iraq after Saddam Hussein were wholly inadequate. The Government failed to achieve its stated objectives.

Third, the Executive Summary contains key findings (starting on p. 111) and lessons learned (starting on p. 129) that cover the entire time under investigation (2001–2009). While the report obviously has more in-depth explanations and discussions of each, those sections are a good place to start.

The report itself covers only part of the total documentation the Committee made available. The Committee also published reams of witness and documentary

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

evidence it considered during the inquiry. Additionally, the Committee has published some of the various other materials it considered during its investigation, and included details about those materials where it did not publish the information itself.

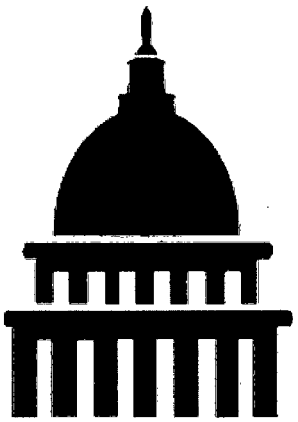
There will of course be much to say about the report once our editors and contributors have had a chance to read it through more comprehensively, so keep watching this space for more.

Read on Just Security »

Tweet Like

The Early Edition: July 6, 2016

By Zoë Chapman on Jul 06, 2016 08:00 am



Zoë Chapman

Before the start of business, *Just Security* provides a curated summary of up-to-the-minute developments at home and abroad. Here's today's news.

IRAQ and SYRIA

Turkey is building a giant concrete wall to block the Syrian border close to the Turkish city of Gaziantep, a region that has been a thoroughfare for thousands of extremist fighters joining the Islamic State in Syria. Turkey has always denied it has permitted this movement, though documents obtained by

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Dominique Soguel and Aya Batrawy of the AP indicate a "pattern of porousness" along Turkey's border with Syria, those who are documented as entering by that route making up "between 25 to 40 percent of the estimated total of IS's foreign recruits."

Recent Islamic State-linked attacks in four countries indicate the "limitations" of US-led efforts to oust the group from Syria and Iraq, write Warren Strobel and John Walcott for Reuters. That said, the Obama administration's portrayal of the Islamic State's attacks worldwide as a direct consequence of the US-led military successes in Iraq and Syria is "overly simplistic and understates how Islamic State's influence has spread beyond the territory it controls."

The latest attacks "reveal an enemy that is adapting, becoming more sophisticated than Al Qaeda, and nurturing a far-flung network of operations, including in the West." This requires a "complex response," suggests the New York Times editorial board, with improved intelligence, coordinated attempts to locate terrorist before they attack, and improved strategies to counter extremist propaganda as necessary as bombing.

Al-Qaeda is "the principal benefactor" of Syrian President Assad's continued survival, for whom, as things stand, there is no reason to view the political process "as anything less than a game in which to taunt and kill his adversaries, while compelling his allies to double-down in defense of his regime." Charles Lister blames the US's failure to solve the Syrian crisis, which he says is prompting Syrians to see al-Qaeda as "a more loyal protector of their lives" than the US. [The Daily Beast]

A suicide bombing outside a bakery in Syria's Hassakeh province killed at least ten yesterday, Syria's state-run news agency and the London-based Syrian Observatory for Human Rights which puts the death toll at 16 – have reported. [AP]

Three people were killed in a mortar attack on a camp for displaced Iraqis close to Baghdad late last night, according to the UN. The camp is populated by

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

families who fled there in the wake of the Islamic State. No one has claimed responsibility for the attack. [AP]

US-led airstrikes continue. US and coalition forces carried out 11 airstrikes against Islamic State targets in Syria on July 4. Separately, partner forces conducted 11 strikes against targets in Iraq. [Central Command]

THE CHILCOT REPORT

The Chilcot report on the Iraq War has been released today, finding that the UK did not exhaust all peaceful options before joining the invasion of Iraq, that judgments about Iraq's weapons of mass destruction "were presented with a certainty that was not justified," and that post-war planning was "wholly inadequate." Speaking ahead of the report's release at 11:35 GMT, enquiry head Sir John Chilcot said he hoped that future military action on such a scale would only be possible in future with more careful analysis and political judgment. [BBC]

Live coverage is being provided by the BBC and the Guardian.

Whatever the report establishes, there are "at least three deeper truths about Iraq," writes David Gardner for the Financial Times. First, it revealed the "limits to US power" – to which Britain was a "side show" – and its lack of ability to "shape the broader Middle East." Second, "Iraq led to Syria." Third, the West's "recklessness" in Iraq, and then its "fecklessness" in Syria, have led to "inescapable if unintended consequences," at least for the UK and the EU.

HILLARY CLINTON EMAIL CONTROVERSY

FBI Director James Comey recommended yesterday that no criminal charges be brought against Hillary Clinton in relation to her use of a private email server to handle classified information while serving as secretary of state. [New York Times' Mark Landler and Eric Lichtblau]

However, Comey did describe Clinton's behavior as "extremely careless" in a 15-minute statement at FBI headquarters, adding that "any reasonable person" in Clinton's position would have known that the sensitive information she was

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

handling warranted greater security. [Wall Street Journal's Kate O'Keeffe and Byron Tau]

This will undercut the argument she has consistently made, that the whole issue is the result of over-zealous, after-the-fact classification of emails as they were publicized under the Freedom of Information Act, suggests Steven Lee Myers in the New York Times.

"Rigged for the powerful." The most "revealing" part of Comey's statement was the following, suggests the Wall Street Journal editorial board: "This is not to suggest that in similar circumstances, a person who engaged in this activity would face no consequences." This exposes double standards within the FBI, insists the board.

Comey's comments may have been "unusual," but they were a "justifiable departure from normal practice," writes Ruth Marcus. Comey's statement took this bad situation and "made it better," revealing to the public information that is not sufficient to support criminal charges, but which will be deemed by many to be relevant to their assessment of Clinton's suitability for presidency. [Washington Post]

It is possible that Clinton's email system was accessed by "hostile actors," Comey said, though the FBI investigation did not uncover any successful hacks on her "homebrew" setup. Comey said that, given the nature of the attackers, he "wouldn't expect to see any evidence." The most likely suspects are apparently Russia, China, and Israel. [Politico's Eric Geller and Martin Matishak]

The State Department has taken issue with Comey's comment that its "security culture" is "generally lacking in the kind of care for classified information found elsewhere in the government." The FBI's investigation into Hillary Clinton's former email habits uncovered a number of shortcomings, in particular the State Department's habit of using unclassified email systems to discuss sensitive information. [The Hill's Julian Hattem]

BAGHDAD BOMBING

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The death toll from Sunday's bombing in Iraq's capital has risen to 250, the Iraqi government has confirmed. This is now the deadliest such attack since the 2003 US-led invasion of Iraq, reports the BBC.

Iraq's interior minister Muhammad Ghabban has resigned following the bombing, making the announcement at a news conference yesterday. His resignation will only be official, however, if Prime Minister Haider al-Abadi approves it. [Reuters]

DHAKA ATTACK

Bangladesh's politicians' inability to work together and habit of using attacks for political gain may have helped extremist groups to gain a foothold in the country, political scientists and terrorism researchers worry. This "long-toxic political atmosphere" has continued following the attack in Dhaka, reports Syed Zain Al-Mahmood for the Wall Street Jounal.

A hostage in the attack on the Holey Artisan Bakery in Dhaka last Friday was shot by police who mistook him for one of the gunmen, subsequently releasing his picture along with the other attackers. [BBC]

SAUDI ARABIA

Saudi Arabia's King Salman bin Abdulaziz Al Saud has vowed to "strike with an iron fist" those responsible for Monday's suicide attacks, the death toll as a consequence of which has now risen to four, as well as those responsible. [Al Jazeera]

The triple suicide-attack "can hardly be thought of as incidental," writes the Wall Street Journal editorial board: the Islamic State, it suggests – though the group has not claimed responsibility for the attacks – would like nothing more than to destroy the "pro-American" House of Saud and take Islam's holiest cities for themselves.

EUROPE

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Fifteen people were sentenced for their involvement in a terror plot that was thwarted in Belgium in 2015, yesterday. The plot is believed to have been orchestrated by Abdelhamid Abaaoud, who was the on-the-ground coordinator for the November Paris attacks. [New York Times' Alissa J Rubin]

"Our country was not ready; now we must get ready." Further details of the report of a French parliamentary commission set up to assess the failure to prevent a series of terror attacks in France in 2015 have been provided by Angelique Chrisafis in the Guardian. The report highlights "global failure" among French intelligence services, and recommends replacing them with a US-style national counter-terrorism agency.

SOUTH CHINA SEA

The Philippines is prepared to talk to China if the arbitration panel in The Hague rules in its favor, rather than go to war, its new President Rodrigo Duterte said yesterday, adding that the Philippines will accept and abide by the ruling if, conversely, it does not go in its favor. [AP's Tersa Cerojano]

Veteran Chinese foreign policy maker Dai Bingguo urged the US to scale back its "heavy-handed intervention" in the South China Sea in a speech in Washington yesterday. [Washington Post's Chun Han Wong]

OTHER DEVELOPMENTS

Brazilian authorities are attempting to find missing former Guantánamo Bay detainee Abu Wa'el Dhiab, whom Uruguay, where Dhiab was resettled after his release, continues to insist is visiting Brazil. [AP]

The US criticized Israel's plans to build hundreds of new homes in the occupied West Bank and East Jerusalem, State Department spokesperson John Kirby calling the plans the "latest step … in a systematic process of land seizure." [BBC] Israel's Prime Minister Benjamin Netanyahu has authorized the building of over a thousand new homes, according to an Israeli official, presenting

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

the move as a response to a series of attacks by Palestinians against Jewish settlers, reports Josef Federman for the AP.

The UN is "screwing up" the political process in Libya by trying to impose an unfeasible agreement on the country's various factions, Libya's prime minister – the head of a weak interim government based in eastern Libya and rival to the UN-brokered presidency council based in Tripoli – said yesterday. [AP's Maggie Michael]

An ex-National Guardsman has been arrested for allegedly offering to obtain weapons for what he believed was going to be an Islamic State attack on US soil, the Justice Department said yesterday. [The Hill]

A suicide car bomb in the southern Yemeni port city of Aden has killed at least 10 inside a military and security compound located next to the city's international airport today. No group has immediately claimed responsibility for the attack, reports Ahmen Al-Haj for the AP.

The UK faces being treated like other non-European countries when it comes to transferring personal data when it leaves the EU, writes Duncan Robinson for the Financial Times. Personal data can easily be transferred between EU countries under EU privacy rules, but can only be transferred outside the bloc if certain criteria are fulfilled.

Read on Just Security »

Tweet Like

Recent Articles:

National Security-Related Congressional Hearings, July 4–8

The Updated First Geneva Convention Commentary, DOD's Law of War Manual, and a More Perfect Law of War

The Early Edition: July 5, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The Fourth of July

The Good and Bad in the US Government's Civilian Casualties Announcement

Copyright © 2016 Just Security, All rights reserved.
You are receiving this email because you opted in at Just Security.

Our mailing address is:
Just Security
Wilf Hall, 5th Floor
139 MacDougal Street
New York, NY 10012

Add us to your address book

unsubscribe from this list update subscription preferences

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

11 July 2016

EMBARGOED
Do not distribute

COUNTER-TERRORISM GREEN PAPER

MESSAGE FROM THE MINISTERS

A fundamental obligation of the Government of Canada is the responsibility to protect our safety and security at home and abroad. Equally fundamental is the responsibility to uphold the Constitution of Canada, and to ensure all laws respect the rights and freedoms we enjoy as people living in a free and democratic country.

When former Bill C-51, the *Anti-terrorism Act, 2015* (ATA, 2015), was tabled in the House of Commons, many Canadians voiced concern with the Government's approach to these responsibilities and whether the proposed legislation appropriately balanced security with rights and freedoms. Those concerns have not diminished since the passage of the ATA, 2015.

The Government is committed to openness, transparency, and accountability. An early demonstration of this commitment was making public the Prime Minister's mandate letters to Ministers, so that Canadians could see our full list of priorities. Reflecting the seriousness with which the Government regards the concerns about the ATA, 2015, our mandate letters direct us to work together to repeal its problematic elements and introduce new legislation that strengthens accountability and national security. In this respect, we have made commitments to:

- guarantee that all Canadian Security Intelligence Service (CSIS) warrants comply with the *Canadian Charter of Rights and Freedoms* (the *Charter*);
- ensure all Canadians are not limited from lawful protest and advocacy;
- enhance the redress process related to the Passenger Protect Program and address the issue of false positive matches to the list;
- narrow overly broad definitions, such as defining "terrorist propaganda" more clearly; and
- require a statutory review of the ATA, 2015 after three years.

In addition, we are establishing a statutory national security and intelligence committee of parliamentarians with broad access to classified information to examine how national security institutions are working. Further, we are also launching the Office of the community outreach and counter-radicalization coordinator to provide national coordination on preventing radicalization to violence; work with partners across communities, provinces, stakeholders and experts to ensure community resiliency; and, to develop a national strategy involving programming, policy and research.

These are our commitments, but we know more can be done. We do not view this as a simple exercise of repealing some legislative provisions and enacting new ones. Our aim is to ensure that the right tools are available to law enforcement and security officials, that they are appropriate, and that they are in keeping with Canadian values.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

We consider this as an opportunity to engage you and your fellow Canadians in a discussion about certain aspects of our country's national security framework. This discussion is necessary if Canadians are to be appropriately informed about national security matters and empowered to contribute to – and influence - elements of that framework.

This Green Paper has been prepared to facilitate the process of providing us with your views. It will also serve as the background document and foundation for the consultation that will take place in the coming months.

We sincerely hope that you will take the time to read this material and join in this discussion. We look forward to your contributions to what, we are sure you will agree, is a timely and truly important national initiative. Together we can ensure that the Government appropriately achieves a framework that upholds both security and rights.

Hon. Ralph Goodale, P.C., M.P.
Minister of Public Safety and Emergency Preparedness

Hon. Jody Wilson-Raybould, P.C., M.P.
Minister of Justice and Attorney General of Canada

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

11 July 2016

EMBARGOED
Do not distribute

CONTENTS

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

11 July 2016

EMBARGOED
Do not distribute

INTRODUCTION

Setting the Scene

Canada has long dealt with terrorism threats from a diverse set of groups. Some threats resulted in tragic terrorist attacks. For example, a terrorist bomb exploded aboard Air India Flight 182 in 1985, killing 329 passengers and crew. In a related incident, a second bomb exploded at Narita airport in Japan, killing two more individuals. This remains the worst terrorist attack in Canadian history.

s.21(1)(a)

In 2001, following the September 11 attacks in the United States, Canada enacted [redacted] the *Anti-terrorism Act*. The Act recognized the unique nature of terrorism and created offences addressing specific aspects of terrorism. These offences included contributing to the activities of a terrorist group, instructing someone to carry out a terrorist activity, and harbouring a terrorist.

Since 2001, threats to Canadian and international security have continued to evolve. Groups inspired by al-Qaida have emerged in many parts of the world. In early 2014, one of these groups, al-Qaida in Iraq, severed ties with al-Qaida and emerged anew as the Islamic State of Iraq and the Levant (ISIL).[1] Since the start of the Syrian conflict in 2011, increasing numbers of Canadians have travelled to Syria and Iraq to join ISIL's predecessor and then ISIL itself. ISIL's declaration of a "caliphate" led to even more of these "extremist travellers" from Canada joining ISIL abroad. Some later returned to Canada, leaving trained and connected terrorist actors in our presence.

Extremist narratives have also inspired an increasing number of Canadians to plot and pursue attacks. Sometimes their targets are domestic, such as the 2014 attacks in Ottawa and Saint-Jean-sur-Richelieu. Other times, their targets are outside Canada, such as the Algerian gas plant attacked by terrorists, including two Canadians, in 2013.

The Minister of Public Safety and Emergency Preparedness recently released the *2016 Public Report on the Terrorist Threat to Canada*. The Report noted that the principal terrorist threat to Canada remains that posed by violent extremists who could be inspired to carry out an attack within Canada. Violent extremist ideologies espoused by terrorist groups like ISIL and al-Qaida continue to appeal to certain individuals in Canada.

Both the threat of terrorism and the counter-terrorism tools we use to respond have evolved over the years. However, there has been one constant imperative from Canada's perspective. That is to ensure that any actions by the Government respect Canadian values, including the rights and freedoms guaranteed by the *Charter*.

National security institutions in Canada are professional, responsible and effective in the work they do. They work within a well-defined set of legal authorities and respect Canadian law. Their core duty is to keep Canadians safe—and they do so daily. National security institutions in Canada are

[1] ISIL is also known as DAESH, the Islamic State, and the Islamic State of Iraq and Syria.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

subject to measures that make them accountable. These accountability measures ensure that these institutions are acting within the law and are being effective. Accountability for national security institutions is, therefore, an important part of any discussion on national security, as it offers protections and safeguards.

The Government is aware that its actions in security matters can impact rights. In protecting national security, the Government must find an appropriate balance between the actions it takes to keep Canadians safe and the impact of those actions on the rights we cherish. The question is: what is an appropriate and reasonable impact?

The Canadian public, stakeholders, experts and those in government institutions will have a variety of views on what constitutes an appropriate balance. Canadians rightly expect strong justifications to limits their rights. This means that we must look at measures to protect national security to see whether they are effective, if there are potential alternatives and if they have properly taken into account the rights they affect.

Human Rights

Canada is founded upon the rule of law, of which the Constitution is the "supreme law." This means that all laws enacted by Parliament and all actions taken by the Government of Canada must be consistent with the Constitution, which includes the *Charter*. The *Charter* reflects our basic values and guarantees our fundamental rights and freedoms, including freedom of expression and association, and the rights to equality, privacy, and the presumption of innocence. The purpose of the *Charter* is to ensure that we are governed in accordance with our basic values. Any laws of Parliament and actions of government that are inconsistent with the *Charter* are unconstitutional and can be declared so by the courts.

The rights and freedoms guaranteed in the *Charter* are not absolute. They can be limited in accordance with the law, if justifiable. Justifiable limitations are generally those that pursue important objectives and that impact rights or freedoms as little as reasonably possible in the circumstances. Also, limitations are only justifiable if, overall, the benefits from these limitations outweigh the harm to the right.

The need for balance is acutely important in the national security context, where *Charter* rights and freedoms regularly come into play. Measures to protect national security are aimed at fulfilling the Government's primary mandate, which is to safeguard the people, institutions and values of Canada. Preserving national security includes protecting what defines Canada, including democracy, multiculturalism, and respect for the rule of law and fundamental rights and freedoms.

The *Charter* establishes a minimum standard of conduct by governments in Canada. Governments are free to produce legislation or policies, or carry out activities, that give greater protection to rights and freedoms than the *Charter* requires. In some cases, the appropriate balance between national security concerns and *Charter* rights may result in greater protection. The Government is interested

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

in the views of Canadians about when it may be appropriate in national security matters to give greater protection to rights and freedoms than that required by the *Charter*.

Privacy

In recent years, many countries have experienced high-profile public controversies about privacy impacts of national security activities.

It is difficult to hold an informed public debate about whether privacy intrusions are appropriate. In part, this is because revealing some details about national security operations can undermine their effectiveness.

That said, effective and sustainable anti-terrorism measures should reflect a robust democratic consensus, at least at the level of principles. In matters involving privacy in particular, it might not be enough to achieve that consensus if anti-terrorism activities merely satisfy the minimum constitutional and legal standards. The Government is interested in the views of Canadians to help determine where the consensus lies.

Consultation Process

How best to respond to terrorism while protecting rights and freedoms is a highly complex issue. As the Government examines possible changes to Canada's counter-terrorism framework, it is asking Canadians to become active partners in finding an appropriate balance between security and rights. These consultations will help the Government develop more informed policies in this complex area.

Each chapter of this Green Paper describes a terrorism issue and the related laws, challenges and potential effects that government responses might have on rights and freedoms. Each chapter also contains hypothetical scenarios to illustrate the issues.

As well, other documents posted online will provide more detailed, technical information about these issues. All Canadians are invited to respond online to the issues raised in this Green Paper. Responses will be accepted until November 1, 2016.

The Government will consider the responses and use them to help develop any new laws and policies. The Government will also keep Canadians up to date on the progress of consultations.

Hypothetical scenarios will be presented throughout this document to illustrate issues. The roles of the characters used in these scenarios are set out in Annex A.

Our main scenario starts as follows...

Mr. A is a charismatic speaker who holds weekly meetings in a local community centre. He has strong views on social and political issues. He invites individuals with similar interests to attend. Some of these individuals have become friends with each other, and with Mr. A. They are also his most devoted followers.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Mr. A believes that things in Canada need to change. He is looking for people who are willing to get involved and make this happen. Over time, his calls for political and social change start taking on a more violent tone.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

ACCOUNTABILITY

Some government agencies have unique intelligence collection and enforcement powers to protect national security. They must exercise these powers according to specific laws and in a manner consistent with the *Charter*. These powers are potentially intrusive, and can impact rights and freedoms. For this reason, these powers must be exercised with great care.

Much work of these agencies occurs in secret. This is because the public disclosure of sensitive information could harm national security by putting investigations, sources of information and investigative techniques at risk. As a result, effective accountability mechanisms are key to maintaining the public's trust in these agencies. Accountability mechanisms provide assurance that agencies act responsibly, strictly within the law and with respect for Canadians' rights and freedoms.

Ministerial Oversight

The Minister of Public Safety and Emergency Preparedness and the Minister of National Defence have important responsibilities with regard to the national security and intelligence agencies in their respective portfolios.

The Minister of Public Safety and Emergency Preparedness is responsible for three national security agencies: the Canada Border Services Agency (CBSA), the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP). The Minister is also responsible for Public Safety Canada.

The Minister of National Defence is responsible for the Communications Security Establishment (CSE), the Department of National Defence (DND) and the Canadian Armed Forces (CAF).

The Ministers are accountable to Parliament for the activities of their respective agencies.

If the activities of CSE or of CSIS employees are believed to have contravened the law, the minister responsible for the relevant agency is engaged and the Attorney General of Canada is informed.[2]

Ministers can issue formal directions that establish guidelines on the conduct and management of operations, although the principle of police independence limits direct ministerial involvement in day-to-day law enforcement operations. Ministerial Directions (MDs) may also specify reporting requirements and procedures for obtaining approval for agency activities.

A number of MDs are currently in effect for the CBSA, CSE, CSIS and the RCMP. For example, in 2011, MDs on information sharing with foreign entities were issued to CBSA, CSE, CSIS and the RCMP. In the current global security environment, the frequent exchange of sensitive information with foreign entities is vital to protect Canada. The MDs establish a clear and consistent process for

[2] In the case of CSE, it is the CSE Commissioner who informs the Minister and Attorney General of Canada. Reports to the Attorney General of Canada about CSIS employees must also be provided to the Security Intelligence Review Committee.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

deciding whether to share information with foreign entities where there may be a risk of mistreatment stemming from the sharing of information. The MDs state that Canada opposes in the strongest possible terms the mistreatment of any individual by any foreign entity for any purpose. They also affirm that all decisions agencies make about whether to share information must be made in accordance with Canada's laws and legal obligations.

The Courts

Courts are involved in national security matters in several ways. Judges decide whether to issue warrants for agencies to use intrusive powers when investigating threats. Judges ensure that agencies meet the legal requirements to obtain warrants and that the warrants comply with the *Charter*. Judges also have the discretion to include in warrants any terms and conditions that are advisable in the public interest. For example, a judge might limit how long a government institution can keep the information it obtains.

More generally, judges decide whether activities leading to an individual's arrest and criminal prosecution are justifiable and proper. For example, judges examine whether investigators respected constitutional rights during investigations and whether evidence was properly collected and should be admitted at trial. Judges also have the authority to provide remedies to citizens who show law enforcement misconduct.

The Federal Court may also hear applications for judicial review of administrative decisions made by the Government in national security matters. Judicial review is a process by which the courts ensure that government decisions are fair and comply with the law. For example, the Court could review decisions made under national security programs such as the Passenger Protect Program.

Independent Review

Canada has a long-standing system of independent, non-partisan bodies reviewing the activities of certain agencies that deal with national security matters. Review bodies operate at arm's-length from government. Their main task is to ensure that national security and intelligence agencies comply with the law and MDs.

At present, there are three such bodies:

- the Civilian Review and Complaints Commission (CRCC), responsible for reviewing RCMP activities;
- the Security Intelligence Review Committee (SIRC), responsible for reviewing CSIS activities; and
- the Office of the Communications Security Establishment Commissioner (OCSEC), responsible for reviewing CSE activities.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Governor-in-Council (cabinet) appointees head the CRCC and SIRC. The Governor-in-Council appoints a supernumerary judge or retired judge of a superior court to head OCSEC. Each review body has an independent research staff and legal counsel to help it.

All three review bodies have a mandate to review the activities of, and hear complaints against, the particular agency for which they are responsible. They have robust access to information held by the agency. Each review body produces a public report every year summarizing its activities, including findings and recommendations from reviews and complaints.

The authority of these three review bodies does not extend beyond the specific agency for which each review body is responsible. As a result, review bodies do not share classified information with each other or conduct joint reviews of national security and intelligence activities.

Parliament

Parliament has several roles in national security matters. It holds ministers to account for the actions of the institutions for which they are responsible. Parliament reviews, refines and enacts proposed legislation on national security matters. This process often involves calling witnesses to provide expert evidence about the issues raised by the proposed legislation.

Some laws contain provisions requiring a review of the law after a set period. For example, the Government has made a commitment to require a review of the ATA, 2015 after three years. Some laws might also require that a provision expires on a set date unless renewed. Other laws may require an annual report about the use of a particular provision – a search power, for example.

House of Commons and Senate committees can also examine national security policy issues and conduct studies of government activities and existing legislation.

Normally, however, parliamentarians do not see classified information. This limits their ability to examine national security issues in depth. To resolve this, the Government has tabled a bill [worth adding a footnote with hyperlink to bill?] to create a national security and intelligence committee of parliamentarians with broad access to classified information. The committee would examine how institutions are working together to keep Canadians safe from national security threats. It would also seek to ensure that institutions comply with Canada's laws and respect fundamental values, the democratic nature of our open society and the rights and freedoms of Canadians.

Agents of Parliament

Certain agents of Parliament scrutinize the national security activities of all federal institutions in relation to their specific mandates. For example, the Privacy Commissioner of Canada can examine their handling of personal information. The Privacy Commissioner also has a mandate to review the operations of the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) every two years. The Information Commissioner of Canada investigates complaints about the

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Government's handling of access to information requests. The Auditor General can conduct "value-for-money" audits of national security programs.[3]

Commissions of Inquiry

Commissions of inquiry provide another means to keep government institutions accountable. Commissions of inquiry are "established by the Governor in Council (Cabinet) to fully and impartially investigate issues of national importance."[4] Within the last decade, the O'Connor, Iacobucci and Major Commissions[5] each reported on the activities of various national security institutions. Many, but not all, of their recommendations have been implemented. For example, Commissioner O'Connor made a number of detailed recommendations for changes to the framework for national security accountability in Canada that have not been implemented.

[3] For example, in spring 2013, the Auditor General (AG) reported on its audit of government spending on the Public Security and Anti-Terrorism Initiative; in fall 2012, the AG reported on the government's efforts to protect Canadian critical infrastructure against cyber threats; and in March 2009, the AG reported on intelligence and information sharing in relation to national security.

[4] Privy Council Office, Commissions of Inquiry.

[5] Specifically, the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (report released September 18, 2006); the Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin (report released 22 October 2008); and the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 (report released 17 June 2010).

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

What are other countries doing?

Some of our closest allies, including Australia and the United Kingdom (UK), share democratic traditions and institutions. As such, their experiences ensuring the accountability of national security and intelligence services are useful to consider when reflecting on Canada's own accountability mechanisms.

For instance, both Australia and the UK have parliamentary committees with access to classified information dedicated to national security. Indeed, the UK's Intelligence and Security Committee can, with the Government's consent, review specific national security operations.

Australia and the UK also take different approaches to independent review of national security activities. In the UK, a number of different commissioners concentrate on a specific aspect of national security and intelligence across a range of agencies. These include:

- The Interception of Communications Commissioner ensures the propriety of communications interception activities;
- The Intelligence Service Commissioner's Office and the Office of Surveillance Commissioners review covert surveillance activities other than communications intercepts; and
- The Investigatory Powers Tribunal hears complaints and can authorize compensation and other redress.

The UK's system may change shortly, however; the *Investigatory Powers Bill*, currently before the UK Parliament, would consolidate the current bodies into a single Investigatory Powers Commission, and would also establish Judicial Commissioners charged with approving warrants.

Australia, for its part, has long had a consolidated model. There, the Inspector General of Intelligence and Security reviews all key intelligence and security agencies for compliance with the law, ministerial directives, and in regard to human rights.

In addition to its commissions and tribunals, the UK's Independent Reviewer of Terrorism Legislation provides expert commentary on proposed legislation, and reviews the use of powers granted by certain key pieces of existing legislation. In carrying out these duties, the Reviewer – who is appointed from outside of government – has access to classified information.

What do you think?

Should existing review bodies – CRCC, OCSEC and SIRC – have greater capacity to review and investigate complaints against their respective agencies?

Should the existing review bodies be permitted to collaborate on reviews?

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Should the Government introduce independent review mechanisms of other departments and agencies that have national security responsibilities, such as the CBSA?

The proposed committee of parliamentarians will have a broad mandate to examine the national security and intelligence activities of all departments and agencies. In light of this, is there a need for an independent review body to look at national security activities across Government, as Commissioner O'Connor recommended?

The Government has made a commitment to require a statutory review of the ATA, 2015 after three years. What other measures might be needed to increase parliamentary accountability for this legislation?

PREVENTION

A new phrase has appeared in the Canadian lexicon: radicalization to violence. Radicalization to violence is a process where people take up an ideological position that moves them towards extremism and ultimately, terrorist activity.

Semantics are important here. It is not a crime to be a radical. Throughout history, change has been brought about by individuals whose radical ideas have inspired new ways of thinking. What is a crime is terrorism – violence committed in the name of radical ideologies or beliefs. As a Government, as a society, we are obliged to respond to criminal violence, whatever form it takes.

When someone decides to use violence to reach a political, ideological or religious goal, they have "**radicalized to violence**." This is where terrorism takes root. This person may be formally linked to a terrorist group, inspired by a terrorist group, or radicalized to violence through their own beliefs. The question is, how does radicalization to violence begin? And, more important, what can be done to prevent it?

What Plays a Role?

We know that highly specific "narratives" drive radicalization to violence. These narratives reduce an individual's understanding of global events to a few highly simplistic propositions. Radicalization is also a social process occurring within networks and communities, both virtual and physical. People can be influenced by friends, mentors and other individuals in their lives.

Associating with others ascribing to violent radical ideologies can influence individuals to move further down the path to radicalization to violence. For example, it is no accident that many people who become extremist travellers – individuals who go abroad to join or contribute to terrorist groups – know others like them who have gone abroad. Extremist travellers who return to Canada have the experience to plan and carry out terrorist attacks at home, as well as the credibility to recruit, encourage, mentor and facilitate the actions of aspiring terrorists.

The Internet also plays an important role in radicalization to violence. Terrorist groups use websites, chat rooms and social media as key propaganda and recruitment tools. For example, in the conflict

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

in Iraq and Syria, some individuals and groups regularly post content and video clips on social media. These boast of battlefield victories and seek to justify terrorist attacks and recruit young people from around the globe to join the fight.

Consider a scenario...

Mr. B is 17 years old and in his final year of high school. He was born and raised in a large suburban area. His neighbours think he is polite and he has no criminal record. Several months ago, a friend encouraged Mr. B to attend weekly discussion group meetings hosted by Mr. A. His charisma, moving speeches about global politics and self-confidence immediately drew in Mr. B. Over time, Mr. A's extremist views and promotion of violence began to resonate with Mr. B.

Between weekly meetings, Mr. B now spends much of his time on the family computer, watching violent videos that Mr. A has posted online. Some friends have noticed changes in Mr. B's behaviour and that he spends more time alone than before. Some teachers have noticed that he is less engaged in the classroom and intolerant of the views of his peers during class discussions. His association with Mr. A worries Mr. B's parents, but their attempts to talk to him about it have failed. They want to know what they can do and where they can go for help to prevent their son from becoming fully committed to a violent radical ideology.

What Can be Done?

All levels of government, communities and other stakeholders must work together to steer at-risk individuals away from radicalization to violence. They also need to give at-risk individuals the support they need to choose an alternative path that reflects Canadian values of peace and acceptance.

Law enforcement organizations play an important role. They seek to support individuals at risk of radicalization to violence and respond if individuals progress to criminal activities. The RCMP train law enforcement officers and front-line personnel to recognize early warning signs and lead interventions to divert individuals from the path to radicalization to violence. As well, Correctional Services Canada conducts tailored interventions for inmates who have radicalized to violence or who are at risk of doing so.

Family members, friends and others close to at-risk individuals can also play a key role in countering radicalization to violence. They are often aware of the individual's beliefs and intentions. Individuals who are early on in the process of radicalization may have many questions and doubts. At this early stage, it may be possible to steer individuals away from radicalization to violence. For this reason, it is essential to support local communities to address this issue.

National Leadership

The Government is also exploring new ideas and innovative approaches to counter radicalization to violence. Budget 2016 announced $35 million over five years, with $10 million ongoing, to create an

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Office of the community outreach and counter-radicalization coordinator. The Office will lead Canada's response to radicalization to violence, coordinate federal, provincial, territorial and international initiatives, and support community outreach and research. The material immediately below describes in greater detail what the Office could do.

Work with Communities

The most effective way to prevent radicalization to violence often lies within communities. It involves working with local leaders to develop early intervention programs. A key focus for the new Office is to reach out to Canadians and build constructive relationships with communities across Canada, raise general awareness about threats and means to address them, and maintain a continual dialogue with those communities.

Engaging with Canadians will help identify priorities for the Office and inform the development of a national strategy to counter radicalization to violence. The Office is seeking to support programs that focus on individuals at risk of radicalization to violence. These programs can include community capacity-building, mentorship, multi-agency interventions and training and support for those involved in front-line intervention work (such as youth workers, corrections and parole officers, social service providers, faith leaders and mental health practitioners).

The City of Montreal is also working in this area. It has established a Centre for the Prevention of Radicalization Leading to Violence. The Centre brings together partners from various sectors, including health and social services, public safety and education. The goal is to develop expertise, define areas of prevention and intervention, and empower communities to address radicalization to violence. We can learn from Montreal's experience and adopt its best practices in future programming.

Engage Youth and Women

Radicalization to violence affects young people disproportionately. Engaging with youth is therefore important in addressing this issue. Early in the process of radicalization they may have many questions and doubts. They turn to the guidance that is available. At this early stage, tailored outreach has the potential to steer at-risk youth away from radicalization to violence. The Office is looking to start a positive conversation with young people, raise their awareness about the dangers of becoming radicalized to violence, and empower them to respond to the issue.

Women can play a key role in this area. Research has shown that the involvement of women – in different capacities and roles, in both the private and public spheres – is essential to effective prevention efforts. As gatekeepers to their communities, they are often well-positioned to serve as credible, resonant voices against violent radical ideologies. The Office can support local initiatives that engage, inform and empower women to better identify and address violent radicalization in their families and communities. The Office can also develop and share tools, resources and information to support women – and men – in responding to this issue.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Promote Alternative Narratives

Terrorist groups often aim to influence potential recruits by promoting and spreading certain messages. Promoting positive, alternative narratives is one way to counter such messages.

The Office is looking for ways to support credible voices and empower community actors—particularly youth and women —to develop programs, messaging or other tools that reflect the local realities. These measures can be used to challenge violent radical narratives and promote critical thinking. For example, terrorist groups use the Internet and social media to spread violent radical ideologies and messaging quickly and broadly. The Office can support programs that harness these tools for positive uses.

Foster Research

Research is a key element in countering radicalization to violence. It can inform policy development, improve the design of programs and tools, and help identify appropriate and effective ways to counter radicalization to violence. The Government is looking to engage with academics, think tanks and others to determine research priorities, identify best practices and lessons learned and develop effective tools to measure the success of programs.

Through the Kanishka Project [footnote explaining Kanishka], the Government has invested in research about radicalization to violence and identified lessons learned and best practices. There is more to learn, and the demand for that information and research is great. Support for action-oriented research is important. Such research produces guides, tools and other resources to assist the public, as well as mechanisms to evaluate programs and measure their success. Evaluation tools will help develop more effective programs to counter radicalization to violence. Knowing what works will also inform policies and priorities, and can contribute to the success of Canada's overall approach to the issue.

What are other countries doing?

Countering radicalization to violence is a priority for the international community. The United Nations emphasized the importance of prevention efforts in United Nations Security Council Resolution 2178, which was unanimously adopted in September 2014. Also, in January 2016, the United Nations released a Plan of Action to Prevent Violent Extremism, which encourages countries to develop national strategies for addressing radicalization to violence. Canada strongly supports this initiative,

Like Canada, other countries have begun to develop policies and programs to respond to this issue. Working with communities, engaging youth and women, promoting alternative narratives, and conducting research are also key areas of focus for our international partners.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Examples

Community engagement is a cornerstone of a number of countries' national strategies to counter radicalization to violence. For example, to enhance social cohesion and harmony, Singapore's Community Engagement Programme brings together Singaporeans from different communities – from religious groups, to unions, to educational institutions, to the media – to strengthen inter-communal bonds, build partnerships and enhance social resilience. Also, to better inform citizens on radicalization to violence, Australia has created a website called Living Safe Together as a central online location where people can read about how Australia addresses this issue, seek information and advice on radicalization to violence, and access other resources. The Office could develop similar initiatives that are tailored to the Canadian experience.

Some countries have also explored programs focusing on youth. For example, in Sweden, there is a youth centre called "Fryshust" that promotes confidence, responsibility, and understanding to enable young people to develop their innate abilities and find their way into society. Also, in Denmark, an organization called "My House" aims to pair individuals at risk of radicalization to violence with mentors that face similar challenges and come from similar backgrounds, but that can show an alternative, positive path to explore.

Finally, engaging women in prevention efforts is an important element of some countries' approaches to this issue. For example, in the United Kingdom, "Project Shanaz" was developed in 2011 to understand the perception women have of activities related to the country's national strategy to counter radicalization to violence. This project led to the establishment of the Shanaz Network, an independent body of 50 women community leaders that contributes to the development of policies and strategies related to radicalization to violence. A similar model in Canada could help inform the development of a new strategy to counter radicalization to violence.

What do you think?

The Government would like your views about what shape a national strategy to counter radicalization to violence should take. In particular, it is looking to identify policy, research and program priorities for the Office of the community outreach and counter-radicalization coordinator. What should the priorities be for the national strategy?

What should the role of the Government be in efforts to counter radicalization to violence?

Research and experience has shown that working with communities is the most effective way to prevent radicalization to violence. How can the Government best work with communities? How can tensions between security concerns and prevention efforts be managed?

Efforts to counter radicalization to violence cannot be "one size fits all." Different communities have different needs and priorities. How can the Office identify and address these particular needs? What should be the priorities in funding efforts to counter radicalization to violence?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Radicalization to violence is a complex, evolving issue. It is important for research to keep pace. Which research should receive priority?

What information and other tools do you need to help you prevent and respond to radicalization to violence in your communities? What further research do you think is necessary?

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

THREAT REDUCTION

Since its creation in 1984, the Canadian Security Intelligence Service (CSIS) has collected information and intelligence on threats to the security of Canada, at home and abroad.[6] CSIS uses the information to advise other institutions of government, such as law enforcement, about these threats. These institutions then in turn act on the information.

The *Anti-terrorism Act, 2015* (ATA, 2015) revised the CSIS mandate to enable it to reduce threats to the security of Canada. CSIS can now do more than share information. It can also take direct action against threats to reduce the danger they pose. Threat reduction (also called disruption) seeks to prevent or discourage people who pose a threat from carrying out their plans.

The threats facing Canada have evolved significantly in recent years. In part, this flows from the trend away from complex terrorist operations towards loosely organized small-scale attacks, the growing use of the Internet and mobile communications, and the ease with which people can move about the globe. These changes have made it harder for security agencies to prevent attacks.

The RCMP have long had a crime prevention mandate. This allows them to act pre-emptively to prevent threats from materializing. However, the roles and responsibilities of CSIS and the RCMP differ. These include different priorities, different approaches, access to different information and a different international presence. For these reasons, during the development of the ATA, 2015, it was felt that CSIS was at times better placed than the RCMP to take timely action to reduce threats. Even before the debate about the ATA, 2015, a threat reduction mandate for CSIS was being discussed. A 2010 report by the Security Intelligence Review Committee (SIRC) recommended that CSIS seek guidance and direction on the issue of threat reduction. In 2011, the Senate Special Committee on Anti-terrorism also considered threat reduction and issued recommendations.

The CSIS threat reduction mandate does not give it law enforcement powers. For instance, CSIS cannot arrest individuals. CSIS continues to work in consultation with the RCMP and other law enforcement agencies.

The Threat Reduction Mandate

For some threat reduction measures CSIS requires a warrant from the Federal Court. Whether a warrant is needed hinges on whether the proposed actions by CSIS would affect *Charter* rights or would, without a warrant, be against the law.

---

[6] "Threats to the security of Canada" are defined in section 2 of the *CSIS Act*, and encompass terrorism (or more precisely "acts of serious violence… for the purpose of achieving a political, religious or ideological objective"), espionage and sabotage, foreign-influenced activities that are clandestine, deceptive, or threaten a person, as well as domestic subversion aimed at the overthrow by violence of the constitutional order of government. Lawful advocacy, protest and dissent are excluded, unless carried out in conjunction with any of the activities referred to above.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Consider a scenario where a warrant is not needed...

Mr. C, a Canadian citizen, attends Mr. A's weekly meetings. He has even voiced support for terrorist activity in Canada in response to terrorist propaganda encouraging attacks in the West. Mr. C is seeking employment as a guard for a firm that provides security at major concerts and other events. CSIS approaches the firm and provides information about Mr. C. Once aware of Mr. C's support for terrorist activity, the firm launches an investigation and decides to restrict Mr. C's work. As a result, Mr. C does not gain privileged access to major events where he could pose a security threat.

Consider a scenario where a warrant is needed...

Mr. D, an associate of Mr. A, is promoting extremism on his personal website by posting videos supporting a terrorist group. His website is hosted outside Canada and also includes how-to guides for making bombs and suicide vests. CSIS obtains a threat reduction warrant from the Federal Court allowing it to modify the website's how-to guides. CSIS replaces some of the terrorism-related details with misinformation that will make the devices fail. Mr. D and his followers do not notice the changes. In short, the actions of CSIS have reduced the support to terrorism provided by the website.

The table below explains when CSIS threat reduction measures do or do not require a warrant.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

	No warrant required	Warrant required
Examples	– Interviews – Asking friends to intervene – Reporting extremist content to social media providers	– Disrupting financial transactions – Interfering with terrorist communications – Manipulating goods intended for terrorist use
Procedure CSIS must follow to take threat reduction measures	– CSIS must have reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada – CSIS must demonstrate that the proposed measure is reasonable and proportional in the circumstances – CSIS must obtain internal approval, perform a risk assessment, and consult law enforcement and other agencies as appropriate	– CSIS must have reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada – CSIS must demonstrate that the proposed measure is reasonable and proportional in the circumstances – CSIS must obtain internal approval, perform a risk assessment, and consult law enforcement and other agencies as appropriate – **CSIS must obtain approval from the Minister of Public Safety and Emergency Preparedness for a warrant application** – **The Federal Court then reviews the warrant application and decides whether to issue the warrant**

Threat reduction measures that would cause death or bodily harm, violate a person's sexual integrity or interfere in the course of justice are prohibited.[7]

Potential Impacts on *Charter* Rights

Threat reduction measures may affect Canadians' *Charter* rights and freedoms.

[7] See *CSIS Act*, section 12.2.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

CSIS must obtain a warrant from the Federal Court before it can take threat reduction measures that would affect rights protected under the *Charter*. The *Charter* recognizes that rights and freedoms are not absolute and that at times they may justifiably be limited. A warrant shows that the Court has determined in advance that the proposed threat reduction measures are reasonable and proportional in the circumstances.

Warrants have long been used to balance government objectives and *Charter* rights. Since 1984, CSIS has sought warrants from the Federal Court to collect intelligence using techniques that limit privacy rights protected by section 8 of the *Charter*. Police wiretaps and search warrants work in a similar way. Threat reduction warrants are a departure from previous warrant regimes. They can limit additional *Charter* rights, not just privacy rights under section 8.

What are other countries doing?

Intelligence and security services in many of Canada's allies have the mandate to reduce threats to national security and a range of threat reduction powers. There is no standard approach to threat reduction, however, as each country has a unique system of government, making direct comparisons difficult. In some countries, responsibility for national security and intelligence is divided between foreign and domestic services. In others, responsibility is divided between intelligence and law enforcement. In the US, for example, there are distinct domestic and international agencies. Domestically, the FBI has both intelligence and law enforcement responsibilities.

Nonetheless, various allied intelligence and security services have the authority to take direct action against threats, domestically and/or abroad, subject to various limitations. In the United Kingdom (UK), for instance, the Security Service (also known as MI5) has legal authority to take action to protect national security, including against the threat of terrorism. The Australian Secret Intelligence Service has a broad mandate to undertake "other activities", including threat reduction measures outside of Australia. French authorities can also disrupt threats to France and French interests abroad.

Internationally, the means by which threat reduction activity is legally authorized takes various forms. Canada's framework requires court warrants for measures that would affect *Charter* rights. In other countries, senior members of the executive branch authorize intrusive threat reduction measures.

In the current international environment, the threat reduction mandate allows CSIS to contribute to a broader range of allied operations against terrorism and other shared threats than was previously the case.

What do you think?

The Government wants to know what you think about CSIS's new threat reduction mandate:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

CSIS' threat reduction mandate was the subject of extensive public debate during the passage of Bill C-51, which became the ATA, 2015. Given the nature of the threats facing Canada, what scope should CSIS have to reduce these threats?

Are the safeguards around CSIS's threat reduction powers sufficient to ensure that CSIS uses them responsibly and effectively? If current safeguards are not sufficient, what additional safeguards are needed?

The Government has committed to ensuring that all CSIS activities comply with the *Charter*. Should subsection 12.1(3) of the *Canadian Security Intelligence Service Act*[8] be amended to make it clear that CSIS warrants can never violate the *Charter*? What alternatives might the Government consider?

[8] Subsection 12.1(3) of the Act states that CSIS "shall not take measures to reduce a threat to the security of Canada if those measures will contravene a right or freedom guaranteed by the *Canadian Charter of Rights and Freedoms* or will be contrary to other Canadian law, unless [CSIS] is authorized to take them by a warrant...."

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

DOMESTIC NATIONAL SECURITY INFORMATION SHARING

National security institutions need information to detect, analyze, investigate and prevent threats. It often takes multiple pieces of information to provide a complete threat picture, and today's national security threats can evolve rapidly, heightening the need for timely and complete information.

Yet information needed for national security purposes is held in different places by various institutions of government. Because of this, the sharing of information is an important part of national security work today. The report of the Air India inquiry[9] stressed this point.

Federal institutions with national security responsibilities can collect information to carry out lawful duties and responsibilities. This collection may be authorized by an Act of Parliament, the common law or the Crown Prerogative. Even institutions that do not have a national security mandate (such as the Department of Fisheries and Oceans) sometimes hold information that could be significant for national security institutions. Non-national security institutions must be able to disclose that information to institutions that have a mandate to act on it.

Government institutions must follow certain rules when sharing information, especially information about individuals. These rules protect privacy rights. However, their complexity can sometimes make it difficult to know whether a given institution is permitted to share information. This can prevent information from getting to the right institution in time.

The *Privacy Act*

The *Privacy Act* protects individuals' personal information by regulating how federal government institutions collect, use, retain and disclose it. The Act limits the collection of personal information by government institutions to that which relates directly to their work. It also limits when this information can be used and disclosed without the consent of the individual to whom it relates.

The *Privacy Act* recognizes that personal information may be disclosed without consent in some situations, including those involving national security. The main exceptions to the rule preventing disclosure without consent are as follows:

1. "Consistent use": One federal institution may share information with another institution for the purpose for which the information was collected or for a use consistent with that purpose (for an example, see the scenario below).

2. "Investigative bodies": Some institutions are listed as "investigative bodies" in the Act (for example, the RCMP and CSIS). An investigative body can ask another federal institution to provide it with personal information to assist it in carrying out its activities. However, the other institution must be asked first. It cannot decide on its own to share personal information with an investigative body.

3. "Public interest": The head of a federal institution may disclose personal information if the head determines that the public interest benefit in disclosure clearly outweighs any invasion of privacy. In the national security context, communicating what the benefit is to a non-national security institution to obtain disclosure may not be possible (because of operational

[9] Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

sensitivities). This makes it difficult for the head of the non-national security institution to decide whether to disclose personal information in the pubic interest.

4. "Lawful authority": the *Privacy Act* permits disclosure of personal information where another Act of Parliament authorizes it.

Consider a scenario...

A foreign national, Ms. E, sends an application for permanent resident status to Immigration, Refugees and Citizenship Canada (IRCC). This application contains the personal information that the Government needs to process her request to become a permanent resident and to determine whether she is admissible to Canada under the *Immigration and Refugee Protection Act*. To assess her application for security concerns, IRCC discloses some of Ms. E's personal information to CSIS, which has a security screening mandate under the immigration program. This type of sharing between IRCC and CSIS is an example of sharing that takes place under the "consistent use" exception of the *Privacy Act*.

The *Security of Canada Information Sharing Act*

Objective

The ATA, 2015 enacted the *Security of Canada Information Sharing Act* (SCISA) to facilitate national security information sharing. The SCISA provides greater certainty about when institutions can share information for national security reasons. Because it is an Act of Parliament that authorizes disclosure, it satisfies the "lawful authority" exception under the *Privacy Act*, as explained above.

What the SCISA Does

The SCISA authorizes all federal institutions to disclose information (including information about individuals) related to "activities that undermine the security of Canada."[10] This concept covers a broad range of national security-related activities and is intended to provide flexibility to accommodate new threats that may arise. The SCISA includes examples of these activities.

Information may be disclosed to 17 federal institutions listed in the SCISA (referred to as "recipients" throughout this document).[11] To be disclosed, the information must be *relevant*[12] to the recipient's lawful national security jurisdiction or responsibilities.

Consider a scenario...

During a routine check, a passport official at IRCC contacts the references of Mr. F, who has

[10] "Activity that undermines the security of Canada" is defined as any activity that "undermines the sovereignty, security or territorial integrity of Canada or the lives or the security of the people of Canada" (section 2 of the SCISA).

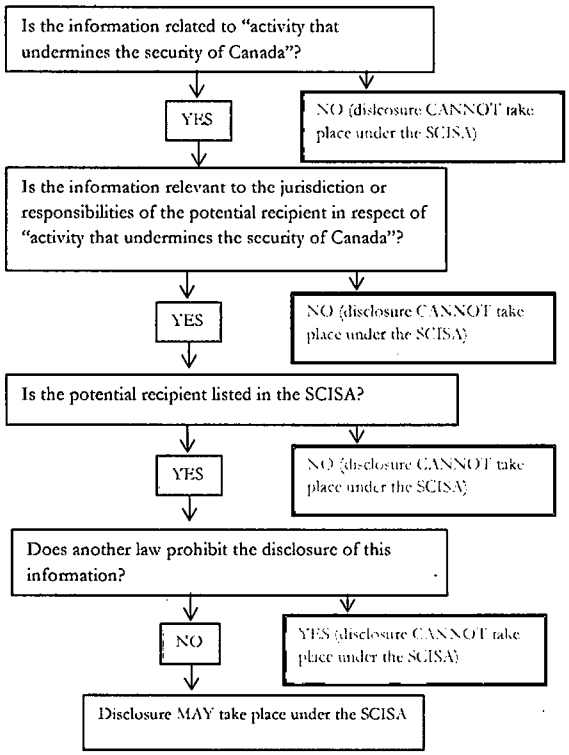
[11] These 17 recipients already have legal authorities to collect information for national security reasons. The SCISA neither expands nor changes these collection authorities.

[12] Relevant: Because national security information sharing often engages privacy rights, the SCISA requires that information be disclosed only if it is actually—and not potentially or possibly—relevant to the recipient's lawful responsibilities for activity that undermines the security of Canada. There must be a reasonable basis to conclude that the information is related to the recipient's exercise of their responsibilities for such activity. Reliability and accuracy are also important factors in determining whether information is relevant under the SCISA.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

applied for a passport. Mr. F has been attending Mr. A's weekly meetings. Without prompting, one referee tells the passport official that she is worried that Mr. F may be travelling to a country to become a fighter with a terrorist group, since he supports the group's goals. IRCC relies on the SCISA to proactively share the information with CSIS and the RCMP, which have responsibilities for investigating this type of activity.

To decide whether they can disclose information under the SCISA, federal institutions go through the following process:



When the SCISA Can and Cannot be Used:

The definition of "activity that undermines the security of Canada" only includes activities that have an impact on national security. Some Canadians expressed concern during the parliamentary examination of the bill that became the ATA, 2015 that the SCISA might inappropriately limit their right to lawful protest. The SCISA was amended to make it clear the activities of advocacy, protest, dissent, and artistic expression *do not* fall within the definition of "activity that undermines the security of Canada." As a result, information about these activities cannot be disclosed under the SCISA.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

However, if violent actions take place that meet the definition of "activity that undermines the security of Canada," they cannot be considered to be advocacy, protest, dissent or artistic expression. Information about these violent actions can be disclosed under the SCISA.

Consider another scenario...

A national park is located near a natural gas pipeline, a critical infrastructure site. An official at the park notices a group gathering to protest near the pipeline. Even though this information deals with critical infrastructure, the official cannot disclose this information under the SCISA to another federal institution. This is because protest, advocacy, dissent, and artistic expression are explicitly excluded from the definition of "activity that undermines the security of Canada" under the SCISA.

What the SCISA Does Not Do

The SCISA cannot be used to bypass other laws prohibiting or limiting disclosure. If another law restricts use or sharing of information, these restrictions take priority over the SCISA. For example, Employment and Social Development Canada's program legislation addresses how it protects and discloses personal information. The SCISA does not override this program legislation.

Who Decides Whether to Use the SCISA?

The institution disclosing information is responsible for determining whether the information may be disclosed. The disclosing institution may need discussions with the potential recipient to see if the information relates to the national security responsibilities of the recipient. These discussions should not require the recipient sharing sensitive operational information.

An institution has the discretion whether or not to disclose information under the SCISA. This decision always rests with the disclosing institution even if all the SCISA requirements for disclosure are met.

Who Receives the Information?

All recipients under the SCISA have national security responsibilities. However, not all parts of the recipient institutions will carry out these responsibilities. The SCISA requires that information be provided to the head of the institution or to delegates of the head. This helps to ensure that only officials who need the information receive it.[13]

Potential Impacts on *Charter* Rights

The *Charter* protects individuals against unreasonable government intrusions on their privacy. However, as noted earlier, these rights are not absolute. The *Charter* allows intrusions into privacy that are authorized by a reasonable law. In some cases, disclosure of information among federal institutions could impact privacy rights.

Information sharing practices under the SCISA may be reviewed like other instances of government information sharing. In particular, the *Privacy Act* allows the Privacy Commissioner of Canada to

[13] Once information is disclosed to a recipient under the SCISA, the recipient may further disclose it under the SCISA or under another authority outside the SCISA. The recipient's use of the information disclosed to it under the SCISA continues to be governed by authorities found outside the SCISA.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

review institutions' handling of personal information and to hold institutions accountable by releasing public reports. Some institutions – the RCMP, CSIS and the CSE – also have specific bodies review their work, including information sharing practices that are part of this work.

The SCISA includes a power to make regulations to supplement the provisions of the Act. For example, regulations could outline record-keeping requirements. However, however no regulations have yet been made.

A number of Government-wide information sharing guidance and support resources are available for federal institutions. Public Safety Canada has prepared a deskbook and a public framework to guide institutions in using the SCISA. Federal institutions may also set policies and give guidance on how their officials should use the SCISA.

What are other countries doing?

Many countries seek to promote the sharing of information for national security purposes, while protecting the privacy rights of individuals. As each country has a unique legislative and policy framework for the sharing of information for national security purposes, the challenges they face in this area vary considerably across jurisdictions. Some countries allow the sharing of information between government agencies without express consent to do so in each case. Others have more explicit powers or policies.

The United Kingdom's information sharing provisions are included in its *Counter-Terrorism Act, 2008*. These provide broad information sharing powers, including from persons to UK security agencies. Denmark has express authority in privacy legislation (the *Act on Processing of Personal Data*) to share personal information for national security purposes. Australia has a 10-year plan (Vision 2020) to enhance national security information sharing, which includes a harmonized policy and legislative framework.

What do you think?

The Government has made a commitment to ensure that Canadians are not prevented from carrying out lawful protest and advocacy. The SCISA explicitly states that the activities of advocacy, protest, dissent, and artistic expression do not fall within the definition of "activity that undermines the security of Canada." Would adding a principle to the SCISA beyond what is already stated in the Act make it clearer that the Act does not apply to lawful advocacy and protest?

Should the Government make it clear in the SCISA that institutions receiving information must use that information only as the lawful authorities that apply to them allow?

Under the *Privacy Act*, the Privacy Commissioner can conduct reviews – at his or her discretion – about the collection, retention, use, protection and disclosure of personal information by government institutions. Should the law be changed to require the Commissioner to make an annual report to Parliament about information disclosed under the SCISA, and to make the results of the report public?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

To facilitate any review, for example, by the Privacy Commissioner, of how SCISA is being used, should the Government introduce regulations requiring institutions to keep a record of disclosures under the SCISA?

Some individuals have questioned why some institutions are listed as potential recipients when their core duties do not relate to national security. This is because only part of their jurisdiction or responsibilities relate to national security. Should the SCISA be clearer about the requirements for listing potential recipients? Should the list of eligible recipients be reduced or expanded?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

11 July 2016

EMBARGOED
Do not distribute

THE PASSENGER PROTECT PROGRAM

Air travel is an important means of transportation, both within Canada and abroad. Without appropriate security measures, air travel is vulnerable to criminal and national security threats. Tragedies such as the 1985 Air India bombing, the attacks of September 11, 2001, and the October 2015 bombing of a Russian airliner in Egypt, each demonstrate the cost in lives, economic and social disruption that terrorist attacks in the air can impose.

Direct threats to aviation security, such as terrorists bringing or placing explosive devices aboard aircraft, continue to be of concern. In addition, concern is growing about individuals travelling abroad, often by air, to engage in terrorism offences. These individuals are known as "extremist travellers." They pose a threat at home and also pose a threat abroad when they participate in conflicts in countries as Syria and Iraq. These individuals are involved in training, fundraising and other terrorist activities on behalf of groups such as ISIL. Trained, radicalized and experienced extremist travellers pose another serious risk if they return to Canada. Here, they might launch or inspire domestic attacks.

The Government provides aviation security in part by preventing individuals who have the intent and capability to harm passengers and aircraft from boarding. The ATA, 2015 enacted the *Secure Air Travel Act* (SATA). Under the SATA, the Government can use the Passenger Protect Program (PPP) – an air passenger identity screening program – to prevent individuals from boarding a flight if they pose a threat to transportation security or are seeking to travel by air to commit certain terrorism offences.

Consider a scenario...

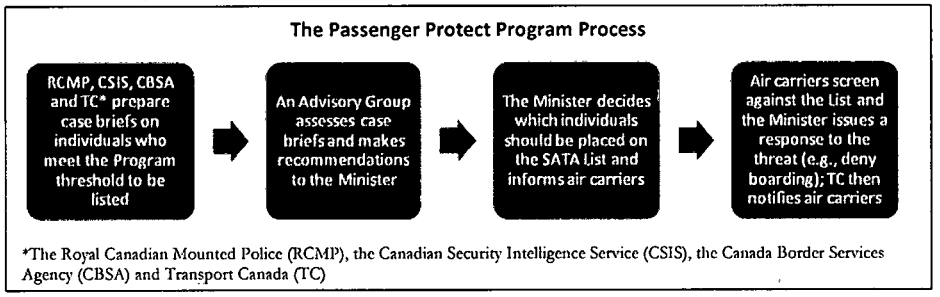
Ms. G is a 22-year-old high school graduate who has been drifting between jobs over the past few years. She attends Mr. A's discussion meetings in her neighbourhood and has rapidly radicalized to violence.

Ms. G is keen to travel overseas to join a terrorist group. Mr. A has been communicating with a terrorist overseas to plan Ms. G's departure. The goal is for Ms. G to get weapons and explosives training and fight for her cause. She then wants to return to Canada and train others to become terrorists.

The RCMP become aware of Ms. G's plans and alert Public Safety Canada. Based on this information, the Minister of Public Safety and Emergency Preparedness adds Ms. G to the list created under the SATA. If Ms. G attempts to check in for a flight, Public Safety Canada will be alerted and may issue a direction to deny her boarding.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The PPP, as governed by the SATA, works as follows:



Through the PPP, the Minister of Public Safety and Emergency Preparedness (the Minister[14]) has the authority to establish a list of individuals (known as the SATA List) who may (1) pose a threat to transportation security or (2) travel by air to commit certain terrorism offences.[15] Listed individuals can be prevented from flying. To list an individual, the Minister must have reasonable grounds to suspect that the individual will engage in at least one of these two acts. For example, individuals [reasonably?] suspected of [travelling, intending to travel?] by air to commit certain terrorism offences,[16] such as participating in the activity of a terrorist group, can be listed under the PPP.

The listing process is conducted confidentially and is based on intelligence and other information from investigations. Public Safety Canada chairs an advisory group composed of the RCMP, CSIS, CBSA, TC and Immigration, Refugees and Citizenship Canada. The advisory group nominates individuals for addition to the SATA List, assesses the information supporting the nominations and recommends to the Minister who should be listed. The SATA List is reviewed at least every 90 days to ensure that there are still reasonable grounds to suspect that individuals on the List pose a threat to transportation security and/or will travel by air to commit certain terrorism offences.

Once an individual is listed, the Minister can direct an air carrier how to respond when the individual attempts to board an aircraft. The direction will be issued to air carriers only once an individual's identity is verified and confirmed to be a positive match to the SATA List, and after any new information is considered. These responses are tailored to the specific situation, based on what is reasonable and necessary to prevent the threat from being carried out. For example, individuals who are assessed as posing a high risk to transportation security may be denied boarding to protect both passengers and aircraft. Other listed individuals may undergo additional screening to provide greater certainty that they are not, for example, carrying any weapons or prohibited items.

[14] The Minister can delegate his or her authority to take any action under the SATA.

[15] Pursuant to paragraphs 8(1)(*a*) and (*b*) of the SATA.

[16] The SATA refers to offences under sections 83.18, 83.19 and 83.2 of the *Criminal Code*.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

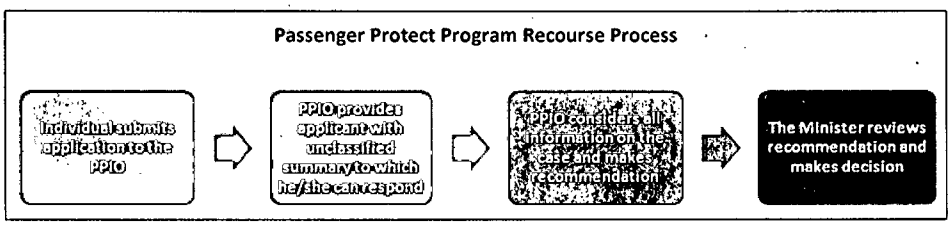
Potential Impacts on *Charter* Rights

A direction to deny boarding can impact a citizen's right to enter and leave Canada. Section 6 of the *Charter* protects this right. Individuals also have an interest in not being delayed or prevented from travelling by air. However, the Minister will issue a direction to deny boarding only if the Minister considers it is reasonable and necessary to prevent a listed person from taking a specific action.

Recourse

s.21(1)(a)

~~impacted,~~ an individual who has been denied boarding under the PPP may apply in writing for recourse to the Passenger Protect Inquiries Office (PPIO) within 60 days of being denied boarding.[17] The application seeks to have the individual's name removed from the List. The applicant receives an unclassified summary of the information used to support the listing and has an opportunity to respond. The Minister may take up to 90 days[18] to review the application and decide whether reasonable grounds remain to list the applicant. If the Minister does not make a decision within 90 days,[19] the Minister is deemed to have decided not to remove the applicant's name from the List. This is done to err on the side of caution, while the 90-day deadline ensures that the person has timely access to the Federal Court, as explained below.



If an individual is not satisfied with the Minister's decision, the individual may appeal the decision to the Federal Court. Most decisions made under the PPP rely on sensitive information that, if disclosed, could injure national security or endanger the safety of a person. The judge hearing the appeal can see all information relevant to the Government's decision. To protect against disclosure of sensitive information, the applicant can see only a summary of the relevant sensitive information. The applicant can also introduce new information to respond to the Government's case. The judge may appoint an *amicus curiae* to assist the Court with any aspect of the proceeding, including during the closed portion of the proceedings where the applicant cannot be present because sensitive information is being presented.

[17] Subsection 15(2) of the SATA allows the Minister to extend that limit if there are exceptional circumstances.

[18] Subsection 15(6) of the SATA allows this period to be extended, as agreed by the applicant and the Minister.

[19] Or a further period agreed upon between the applicant and the Minister.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Consider a scenario...

Mr. H intends to fly to Florida for the Labour Day weekend but is delayed at the airline ticket counter while the desk agent contacts his supervisor. After a few minutes, Mr. H is allowed to continue, but he leaves on his flight frustrated. He suspects that his name is similar to that of someone on Canada's aviation security list. He contacts the Passenger Protect Inquiries Office, which works with relevant partners to help facilitate his future travel.

Redress

The SATA List is not the only reason for delaying an individual or preventing them from flying. There can be many other reasons, unrelated to the SATA, including air carriers' own security lists and/or aviation security lists maintained by other countries. As well, a false positive match to an aviation security list, whether that of an air carrier, a foreign country or the SATA List itself, may cause travel to be delayed.

The PPIO provides assistance to air travellers who have experienced delays or difficulties related to aviation security lists. The PPIO can assist the traveller in identifying the reason for this situation and suggest what to do next. Following a joint announcement by the Prime Minister of Canada and the President of the United States on March 10, 2016, the governments established the Canada-U.S. Redress Working Group. The Working Group is a bilateral mechanism. It allows the PPIO to collaborate closely with the U.S. on certain matters of redress and recourse about Canadian and American citizens and permanent residents who may be affected because of their potential presence on the SATA List or the U.S. No Fly List.

In addition, the Government is considering possible changes to regulations [redacted] to help reduce instances of false positive matches to the SATA List. The objective is to provide redress numbers to individuals who have experienced a false positive match. These individuals can avoid delays by providing the number to their air carrier when they want to fly.

What are other countries doing?

A number of Canada's key international partners, including the United States (U.S.), the United Kingdom, Australia and New Zealand have some form of air passenger screening prior to departure. In most cases, these programs are designed to determine an individual's admissibility status before they can travel to that country, and/or whether they pose a security risk. The U.S., for example, operates a number of air passenger screening programs that address both immigration and security considerations.

Canada's PPP does not operate in conjunction with the U.S. No Fly list or with any other countries' and organizations' aviation security programs. While the SATA permits the Minister of Public Safety to share information with another country to address potential threats, both countries' programs will continue to operate independently and subject to their respective laws, as well as listing and operational procedures.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

What do you think?

At present, if the Minister does not make a decision within 90 days about an individual's application for removal from the SATA List, the individual's name remains on the List. Should this be changed, so that if the Minister does not decide within 90 days, the individual's name would subsequently be removed from the List?

To reduce false positive matches to the SATA List, and air travel delays [and denials?] that may follow, the Government has made a commitment to enhance the redress process related to the PPP. [How might the Government help resolve problems faced by air travellers whose names nonetheless generate a false positive?]

Are there any additional measures that could enhance procedural fairness in appeals of decisions made under section 8 and directions issued under section 9 of the SATA?

s.21(1)(a)

CRIMINAL CODE TERRORISM PROVISIONS

The *Criminal Code* defines terms such as "terrorist activity," "terrorism offence" and "terrorist group." It sets out a wide range of terrorism offences, provides a process to "list" entities as terrorist groups and outlines a range of anti-terrorism powers for law enforcement.[20] Many of the terrorism provisions were enacted in 2001 and amended in 2013 to include specific terrorist travel offences. Since 2001, a number of people have been convicted of terrorism offences in Canada, with some receiving life sentences. The courts have found key *Criminal Code* terrorism provisions to be consistent with the *Charter*.[21]

Some provisions of the ATA, 2015 introduced changes to *Criminal Code* terrorism provisions. The Code was amended to accomplish several goals:

- to make it easier for peace officers to detain individuals temporarily, and to apply to a court to have reasonable conditions imposed on individuals to prevent the carrying out of terrorist activity and the commission of terrorism offences;
- to create a new offence that criminalizes the advocacy or promotion of the commission of terrorism offences in general;

[20] "Terrorist activity" is a term made up of a list of specific offences that implement Canada's international obligations, as well as a general definition. It is used as the basis for many of the terrorism offences in the *Criminal Code*, such as facilitating a terrorist activity

[21] See, for example, *R. v. Khawaja, 2012*, [2012], 3 SCR 555.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- to give the courts the authority to order the seizure and forfeiture of tangible terrorist propaganda material and the removal of online terrorist propaganda from Canadian websites; and,
- to provide additional protection to witnesses and other participants in national security proceedings and prosecutions.

Preventive Law Enforcement Tools (Recognizance with Conditions and Terrorism Peace Bond)

Canadian criminal law generally focuses on prosecuting offences that have already occurred. However, criminal courts can also impose **preventive conditions** on an individual where there is evidence that the individual is likely to commit an offence in future. Two specific tools allow for a court to impose conditions to prevent terrorism: the **recognizance with conditions** and the **terrorism peace bond**. Some aspects of these tools first appeared in 2001 when the *Anti-terrorism Act* came into force.

A **terrorism peace bond** is used to prevent a specific individual from committing a specific terrorism offence, such as leaving or attempting to leave Canada to commit an offence for a terrorist group.

A **recognizance with conditions** is used when the police suspect someone is connected in some way to the carrying out of a terrorist activity. For example, they suspect that someone is connected to a broad plot to attack Parliament, but the person's exact role may not be known.

Both the terrorism peace bond and the recognizance with conditions aim to prevent individuals from carrying out terrorist acts.

Consider a scenario where a terrorism peace bond could be used...

A family notifies the RCMP that they feel their son, Mr. I, has become radicalized to violence. He is a good friend of Mr. A. The RCMP investigate and learn that Mr. I has told a number of people close to him that he plans to join a terrorist group active in a conflict zone abroad. The RCMP also learn that Mr. I has been pricing air travel to a country that borders an ongoing conflict zone where the group is active.

The RCMP now suspect that Mr. I may commit a terrorism offence – travelling or attempting to travel abroad to participate in the activity of a terrorist group. They seek the consent of the Attorney General of Canada to apply to a judge for a terrorism peace bond to prevent Mr. I from travelling abroad.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Consider a scenario where a recognizance with conditions could be used...

The police conduct an urgent investigation into a group of ten people based on an anonymous tip. Some of these people attend Mr. A's weekly meetings. Some members of the group are apparently planning to bomb an unknown public gathering that week. Further investigation reveals that one person in the group, Ms. J, recently downloaded bomb-making instructions. The police hope to obtain a recognizance with conditions to stop Ms. J from making, providing or using an explosive device. They seek the consent of the Attorney General of Canada to apply to a judge for a recognizance with conditions.

The judge considers the application and is satisfied that a terrorist activity may be carried out. The judge also has reasonable grounds to suspect that the imposition of the recognizance with conditions is likely to prevent the carrying out of the terrorist activity. As a result, the judge issues a recognizance with conditions.

The ATA, 2015 amended the provisions on recognizance with conditions and the terrorism peace bond. The amendments were designed to make it easier for police to apply to provincial court for the imposition of reasonable conditions, such as travel restrictions.

The 2015 amendments did the following:

- lowered the threshold to obtain a **recognizance with conditions** to where a peace officer believes on reasonable grounds that a terrorist activity "*may be* carried out." Previously, the law required that police believe on reasonable grounds that a terrorist activity "*will be* carried out." The amendments also replaced the former requirement that a recognizance is "*necessary* to prevent" the carrying out of a terrorist activity with "is *likely* to prevent."

- increased the period of preventative [preventive; check wording of statute] detention under a recognizance with conditions to a total of up to seven days, which includes periodic review by a judge. Previously, preventative detention could last only up to three days.

  Further periods of detention beyond the possible 24-hour initial police detention are allowed only if the judge finds that it is necessary to ensure public safety, to ensure that the person attends the hearing or to maintain confidence in the administration of justice. In addition, there are two new possible 48-hour periods of judge-ordered detention. In these instances, it must also be demonstrated that the investigation in relation to which the person is being detained is being conducted "diligently and expeditiously." If these criteria are not met, the person must be released – with or without conditions – but will be required to return to court for the hearing on whether conditions should be imposed on them.

- lowered the threshold to obtain a **terrorism peace bond** so that it may be obtained when a person believes an individual "*may* commit" a terrorism offence. Previously, the threshold was "*will* commit" a terrorism offence.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- for both the recognizance with conditions and the terrorism peace bond, there are now additional requirements for the judge to consider whether to impose a geographical restrictions condition on the person and whether to require the person to surrender their passport(s) or other travel documents.
- increased the length of time these measures can be applied if the person has been previously convicted of a terrorism offence. For the recognizance with conditions, the conditions can apply for up to two years. For the terrorism peace bond, the conditions can apply for up to five years.
- if a person breached their conditions under a recognizance with conditions or a terrorism peace bond, increased the maximum penalty to four years imprisonment (from a maximum of two years).
- sought to improve the efficiency and effectiveness of the recognizance with conditions and peace bonds across Canada by allowing for the use of video conferencing and for [redacted] between provinces.

Potential Impacts on *Charter* Rights

s.21(1)(a)

The terrorism peace bonds and recognizance with conditions impact liberty interests protected under the *Charter*. Persons subject to these measures may face detention and other restrictions on their liberty without being charged with or convicted of an offence.

The consent of the Attorney General of Canada or of a province is required [redacted] before the police can even apply to a judge for a] recognizance with conditions or terrorism peace bond. In addition, the Crown or the affected person may apply to change any of the conditions. The recognizance with conditions also continues to be subject to a requirement [redacted] annually on its use. Finally, the provisions on these recognizances are subject to a five-year sunset clause. This means that the [law [recognizance provisions]] will no longer be in force five years after July 15, 2013, unless Parliament renews them.

Criminalizing the Advocacy or Promotion of Terrorism Offences in General

The ATA, 2015 added a new *Criminal Code* offence on advocating or promoting the commission of terrorism offences in general.

Consider a scenario...

Ms. K has also been attending Mr. A's weekly discussion groups. She feels that what Mr. A is saying should be known by more people and that Mr. A's views deserve a wider audience. To do this, Ms. K has started posting some of her views online. Over time, she has gained some followers on social

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

media. She is now clearly stating that violence should be used as the only way to change the government's position on foreign policy.

Ms. K has been communicating with some of her online followers. One has stated that they would be willing to "take direct action." In response to what she believes is support for her views, she decides to use her latest post to appear in a video message dressed in military clothing. In the video, she urges her followers to support a terrorist group by saying, "Do not wait for us to tell you what to do. From now on, you have permission to do whatever you want, do whatever is in your capability. Just act."

As noted above, the 2015 change to the *Criminal Code* makes it a criminal offence for a person, by communicating statements, to knowingly advocate or promote the commission of terrorism offences in general. To commit the offence, the person must *know* that any of those offences will be committed or *be reckless* as to whether any of those offences may be committed as a result of such communication.

Counselling generally involves one person procuring, soliciting or inciting another to commit a criminal offence. Counselling is a long-standing offence. It requires some specificity about the offence or type of offence being counselled.

The definition of "terrorism offence" in the *Criminal Code* includes a broad range of conduct – from violence against people and destruction of property to providing financial and material support and recruitment. [Previously, Before the 2015 change to the *Criminal Code*,] the scope of the offence of counselling was unclear. There was some uncertainty about whether it constituted counselling if a person actively encouraged committing terrorism offences but was not specific about the offences or the type of offences (for example, whether terrorist bombing or terrorist financing). There was also uncertainty about what the penalty would be. This new offence makes it clear that such conduct is criminal. The new offence is modelled on the existing law of counselling. It extends the concept of counselling to cases where *no specific* terrorism offence is being counselled, but where it is evident nonetheless that *terrorism offences* are being counselled.

The maximum penalty for the new offence is five years imprisonment. This is [comparable to the maximum sentence / the same maximum as that] for advocating or promoting genocide against an identifiable group, the most serious of the three hate propaganda offences in the *Criminal Code*.

Potential Impacts on *Charter* Rights

Because this offence criminalizes communicating statements, it could be viewed as limiting freedom of expression. However, it is important to consider that the expression in question is generally directed at violent activities. As well, this offence involves more than mere expression. The offence is not simply an attempt to criminalize glorification of terrorism or praise of terrorism. The offence prohibits *active encouragement to commit terrorism offences*, not mere expressions of opinion about the acceptability of terrorism.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

To ensure appropriate oversight, the prior consent of the appropriate Attorney General is needed to begin proceedings in respect of terrorism offences.

Seizure and Forfeiture (or Removal) of Terrorist Propaganda

The ATA, 2015 created two new warrants of seizure (court orders that allow police to seize materials) in the *Criminal Code* to apply to "terrorist propaganda" material. This is material counselling the commission of a terrorism offence or advocating or promoting the commission of terrorism offences in general. Some Canadians raised concerns about terrorist propaganda [redacted] during the debate about the ATA, 2015. The Government has made a commitment to address the issue.

s.21(1)(a)

The new provisions allow a judge to order the seizure and forfeiture of terrorist propaganda material that is in printed form or is in the form of audio recordings. A judge may also order the removal of terrorist propaganda when it is in electronic form and is made available to the public through a Canadian Internet service provider (ISP).

Continuing the scenario from above...

Ms. K's posts on social media are made available through a Canadian ISP. Her posts have clearly been promoting the commission of terrorism offences in general.

With the consent of the Attorney General, the police seek a warrant from a judge requiring the Canadian ISP to remove this content from the site.

Potential Impacts on *Charter* Rights

The new warrants could impact the right to free expression. However, the warrants are similar to those already available under the *Criminal Code* for the seizure of material deemed criminal, such as hate propaganda. As well, the consent of the Attorney General is needed before the police can apply for a warrant, to ensure that the Attorney General considers public interest issues, such as protecting freedom of expression.

Protections for Witnesses and Other Justice System Participants

The ATA, 2015 introduced changes to the *Criminal Code* to improve protection of witnesses, in particular in proceedings involving security information or criminal intelligence information. Security certificate proceedings under the *Immigration and Refugee Protection Act* are examples.

The changes on how witnesses can testify include the following:

- Judges can order that witnesses testify behind a device, such as a screen, to prevent the public from seeing them while they testify;

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Judges must consider whether a witness has responsibilities relating to national security or criminal intelligence when deciding whether to allow that witness to testify using a pseudonym or via closed-circuit television; and
- Judges have explicit authority to make any order necessary to protect the security of any witness, including those who have responsibilities relating to national security. One such order could be to allow a witness to testify while partially disguised.

In addition, the Act [ATA, 2015 or the *Criminal Code* as revised by the ATA] better protects justice system participants from intimidation. The *Criminal Code* prohibits their intimidation and provides a maximum of 14 years imprisonment for the offence. The Act [ATA, 2015 or the *Criminal Code* as revised by the ATA] expanded the definition of "justice system participant" to include persons who play a role in proceedings that involve various types of information, including security information and criminal intelligence information. This ensures that punishment for intimidation is proportional to the gravity of the conduct, its effect on the victims and, more broadly, its effect on the proper functioning of the justice system.

The Act [ATA, 2015 or the *Criminal Code* as revised by the ATA] also removed the requirement to publish the names of federally-designated prosecutors and peace officers who have obtained authorizations to intercept private communications ("wiretap" authorizations). This increases protection from intimidation or retaliation for federal prosecutors and law enforcement officers who obtain such authorizations. The amendment puts them in the same situation as their provincial counterparts. The Minister of Public Safety and Emergency Preparedness will continue to report annually [redacted] on the number of federally-designated prosecutors and peace officers who have obtained authorizations for wiretaps. This maintains ministerial accountability for their use.

s.21(1)(a)

Potential Impacts on *Charter* Rights

[redacted]

s.23

What are other countries doing?

Terrorism Peace Bonds and Recognizance with Conditions

The recognizance with conditions and peace bond provisions are consistent with counter-terrorism laws in countries such as the United Kingdom and Australia.

The United Kingdom, for example, currently allows for preventative detention for up to 14 days, which also requires independent review on grounds similar to those contained in the *Anti-terrorism Act, 2015*. They also have a tool similar to a peace bond, called a Terrorism Prevention and Investigation Measure, which allows for the imposition of conditions on individuals where satisfied,

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

on the balance of probabilities, that the individual is or has been involved in terrorism-related activity.

Australia also allows for preventative detention which, under federal law, can last for three days. Australian law also permits the imposition of "Control Orders," which are similar to peace bonds and which can result in the imposition of conditions on individuals where evidence establishes that, for example, making the order would substantially assist in preventing a terrorist act.

Advocacy or Promotion of Terrorism Offences in General

Since 2006, the United Kingdom has had an offence of direct or indirect encouragement to commit acts of terrorism. For the purposes of the offence, it is irrelevant whether the encouragement relates to one or more particular acts of terrorism or acts of terrorism generally. Indirect encouragement is defined to include a statement which glorifies the commission of such acts and which members of the public could reasonably be expected to infer that what is being glorified is being glorified as conduct that should be emulated by them in existing circumstances.

In 2014, Australia created a new offence of advocating the doing of a terrorist act or the commission of a terrorism offence, while being reckless as to whether another person will engage in a terrorist act or commit a terrorism offence. "Advocates" is defined to include promoting. It applies where one terrorism act or offence is being advocated or more than one of such acts or offences are being advocated. There are statutory defences that may apply depending on the circumstances, such as publishing in good faith a report or commentary about a matter of public interest. The maximum punishment is five years imprisonment.

As the Canadian offence in *Anti-terrorism Act, 2015* is based on the knowing and active encouragement of the commission of terrorism offences in general, it more closely resembles the Australian rather than the United Kingdom model.

Seizing Terrorist Propaganda

The measures are similar to laws that already exist in the United Kingdom and Australia. For example, the United Kingdom legislation, which allows for the takedown of websites and social media feeds, has been in existence since 2006. In Australia, complaints about on-line content are made to the Australian Communications and Media Authority (ACMA). If the ACMA determines that the content is restricted (i.e., if it incites violence or advocates a terrorist act), it issues a notice and takedown order to the service provider.

Protecting those Involved in National Security Proceedings/Prosecutions

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The United Kingdom, New Zealand, and Australia have all developed legislative regimes that provide ways for witnesses to testify which seek to mitigate any adverse consequences that may arise from their giving testimony, while protecting the interests of an accused.

What do you think?

Are the thresholds for obtaining the recognizance with conditions and terrorism peace bond appropriate?

Advocating and promoting the commission of terrorism in general is a variation or the existing offence of counselling. Would it be useful to clarify the advocacy offence so that it more clearly resembles counselling?

Should the part of the definition of terrorist propaganda referring to the advocacy or promotion of terrorism offences in general be removed from the definition?

What other changes, if any, should be made to the protections that witnesses and other participants in the justice system received under the ATA, 2015?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

11 July 2016

EMBARGOED
Do not distribute

PROCEDURES FOR "LISTING" TERRORIST ENTITIES

Listing an individual or group as a "terrorist entity" is a public means of identifying their involvement with terrorism and curtailing support for them. Listing is one component of the international and domestic response to terrorism. All United Nations (UN) member states have an obligation to implement UN Security Council resolutions that deal with terrorism.

s.21(1)(a)

There are three ways for Canada to list a terrorist entity. Two are established under Canada's *United Nations Act*[22] and a third was created by an amendment to the *Criminal Code* in 2001. Canada relies mainly on the *Criminal Code* process. The Code process both helps to fulfill Canada's international obligations and supports domestic counter-terrorism measures. An entity listed under the *Criminal Code* is considered to be a terrorist group [The *Criminal Code* defines any entity listed under the Code as a terrorist group]. Any funds the group has in Canada are immediately frozen and may be seized by, and forfeited to, government.

More than 50 terrorist entities are now listed under the *Criminal Code*. These include al-Qaida, the Taliban, ISIL, al-Shabaab, Boko Haram, the World Tamil Movement, and Hizballah. To date, most listed entities are based overseas, though members or supporters can also be found in Canada. Entities originating in Canada can also be listed.

The *Criminal Code* listing process begins with the RCMP or CSIS producing criminal or security intelligence reports on an entity. The Minister of Public Safety and Emergency Preparedness may recommend to the federal Cabinet that an entity be listed if the Minister has reasonable grounds to believe that the entity:

- knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity; or
- is knowingly acting on behalf of, at the direction of, or in association with an entity that has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity.

To list an entity, Cabinet must also be satisfied that the above test is met. The name of the listed entity is then published in the *Canada Gazette*. A complete list is available on Public Safety Canada's website.

Consider a scenario...

The 123 Group has committed terrorist attacks overseas and is being investigated by CSIS. CSIS informs Public Safety Canada about 123 Group's involvement in these attacks and its links to

[22] These are the *UN Al-Qaida and Taliban Regulations* and the *Regulations Implementing the UN Resolution on the Suppression of Terrorism*.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Canada. The Minister of Public Safety and Emergency Preparedness recommends to Cabinet adding the 123 Group to the list of terrorist entities established under the *Criminal Code* because the group has knowingly carried out a terrorist activity. Cabinet approves the listing. All financial assets belonging to 123 Group in Canada are frozen and can be seized by government.

The entity and the public are not made aware that the Government is planning to list the entity until the listing takes effect. This is to prevent the entity removing its Canadian assets from Canada before the listing freezes them.

Once an entity is listed, the *Criminal Code* deems it a "terrorist group" in Canada. This can help with investigating and prosecuting terrorism offences, since it is not necessary for investigators and prosecutors to prove independently that the group is a terrorist group. It is not a crime simply to be a terrorist group, but many *Criminal Code* terrorism offences contain the term "terrorist group" in the description of the offence. For example, it is an offence to do any of the following:

- knowingly participate in, or contribute to any activity of, a terrorist group for the purpose of enhancing the ability of any terrorist group to facilitate or carry out terrorist activity;
- leave Canada to participate in the activities of a terrorist group;
- collect money or property knowing that it will benefit a terrorist group; and,
- instruct anyone to carry out an activity for the benefit of a terrorist group.

The listing process also makes it easier to apply other provisions relating to terrorist groups, such as using the *Charities Registration (Security Information) Act* to de-register a charity or refuse to register an organization as a charity.

Canada's closest allies, including the United States, United Kingdom, Australia and New Zealand, have similar terrorist listing regimes that include mechanisms for freezing assets in compliance with international obligations.

Potential Impacts on *Charter* Rights

Being listed as a terrorist entity or being associated with a terrorist entity could impact *Charter* rights. Specifically, section 7 of the *Charter* protects against the deprivation of life, liberty and security of the person, except in accordance with the principles of fundamental justice.

Procedural safeguards have been put in place because of the possible impact on these rights. An entity has the right to apply to the Minister of Public Safety and Emergency Preparedness to be de-listed. If the Minister decides not to de-list the entity, the entity can ask the Federal Court for judicial review of the Minister's decision.

Some evidence relating to the listing will be sensitive and the Government may wish to protect it from disclosure to the entity. However, this evidence can be withheld only if a Federal Court judge determines that its disclosure would injure national security or endanger the safety of any person. If evidence is withheld on these grounds, the judge must provide an unclassified summary to ensure

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

that [redacted] the entity can understand the basis of the listing decision. As part of this process [redacted] the entity can also make submissions to the Federal Court. If the judge determines listing to be unreasonable, the judge will order de-listing.

s.21(1)(a)

The Government is also required to review all entities on the list every two years and confirm whether they should remain on the list.

Listing an entity could harm individuals and groups with a similar name. To prevent harm from mistaken identity, individuals and groups may apply to the Minister of Public Safety and Emergency Preparedness for a certificate confirming that they are not the entity on the list.

What are other countries doing?

Canada's closest allies all have similar terrorist listing regimes that include mechanisms for freezing assets in compliance with international obligations. The manner in which international obligations are domestically implemented has led to a variety of different terrorist listing regimes across our closest allies and among all UN Member States.

The United Kingdom (UK), for example, implements its international obligations in relation to UNSC Resolution 1267 using regulations made pursuant to the *European Communities Act 1972*. UNSC Resolution 1373 is implemented under Part 1 of the *Terrorist Asset-Freezing etc. Act 2010*. As well, under the UK's *Terrorism Act 2000*, the Home Secretary may proscribe an organization if it commits or participates in acts of terrorism, prepares for terrorism, promotes or encourages terrorism or is otherwise concerned with terrorism. Membership in a proscribed organization is a criminal offence. Proscribed entities may apply to the Home Office to be de-listed and, if denied, an appeal process to a special commission, as well as judicial review of its decision, is available.

Australia, like Canada, has a listing process in its *Criminal Code*. The government may list an entity if the Attorney-General is satisfied on reasonable grounds that it is directly or indirectly engaged in preparing, planning, assisting or fostering the doing of a terrorist act, or advocates the doing of a terrorist act. The Australian government reviews listed entities every three years from the date that they were originally listed. Any person or organisation is entitled to make a de-listing application to the Attorney-General and judicial review of the legality of a decision to list an organisation is also available in the courts. Australia also implements UNSC Resolution 1373 by regulations made under the *Charter of the United Nations Act 1945*, and implements UNSC Resolution 1267 by automatically incorporating the United Nations sanctions list by regulations made under the same Act.

New Zealand's *Terrorism Suppression Act 2002* provides for a list of terrorist entities to be established and maintained. The police are responsible for coordinating requests to the Prime Minister for designation of a terrorist entity. A designation in New Zealand, like in Canada, has the effect of freezing the entity's assets. It is also a criminal offence to participate in or support the activities of the designated terrorist entity. This includes dealing with the property of the designated terrorist entity or making property or financial services available to the entity. Also, New Zealand implements

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

the UNSC Resolution 1267 and automatically incorporates the United Nations sanctions list by regulations made under their *United Nations Act 1946*.

The lists kept by the U.S. government are more complex and diverse. The U.S. implements its obligations relating to financial sanctions under both UNSCR 1267 and UNSCR 1373 primarily through Executive Order (E.O.) 13224. The Office of Foreign Assets Control (OFAC) administers and enforces E.O. 13224 and maintains a public list of groups and individuals designated under the Order as well as those designated under the *Immigration and Nationality Act* as Foreign Terrorist Organizations. There are some general similarities with Canada's listing processes. For example, entities are not informed that they may be listed and they cannot provide evidence or submissions before the listing process is completed.

What do you think?

The Government is interested in your views about the listing of terrorist entities.

Does listing meet our domestic needs and international obligations?

The *Criminal Code* allows the Government to list groups and individuals in Canada and abroad. Most listed entities are groups based overseas. On which types of individuals and groups should Canada focus its listing efforts in the future?

What could be done to improve the efficiency of the listing processes and how can listing be used more effectively to reduce terrorism?

Do current safeguards provide an appropriate balance to adequately protect the rights of Canadians? If not, what should be done?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

TERRORIST FINANCING

Canada has a stable, open economy, an accessible and advanced financial system, and strong democratic institutions. However, those seeking to raise, transfer and use funds for terrorism purposes try to do so by exploiting some of these strengths. In confronting the evolving challenges of terrorist financing, the Government must ensure that it does not compromise fundamental Canadian values.

Terrorist financing is a multi-faceted global phenomenon. Terrorists (individuals and groups) raise, collect and transfer funds across the globe to carry out attacks and finance day-to-day operations. They raise funds from criminal activities and from legitimate sources, such as donations or business profits. Terrorists use a variety of methods to move their funds. These include the formal banking system, international trade, money services businesses, informal money transfer systems, digital platforms, and the physical transportation of cash or certain high value goods, such as gold or precious stones.

Individuals also finance terrorist activities by raising money themselves to travel abroad for terrorist purposes or to purchase materials for attacks. Since funds are vital to terrorist organizations, depriving them of these funds is one effective mechanism to counter terrorism.

For example, one of the five priorities of the Global Coalition against ISIL is to reduce ISIL's capabilities by cutting off its access to financing and funding [redacted]IL is likely the wealthiest terrorist group in the world [verify that this is consistent with statement (about Hizballah?) in 2015 Public Report on Terrorist Threat to Canada], due to its access to proceeds generated in the territory it controls. Its wealth allows it to carry out attacks, recruit and pay members, provide training and indoctrination, maintain communications networks and disseminate propaganda. Reducing access to funds will diminish ISIL's capability.

s.21(1)(a)

Canada's Approach to Counter Terrorist Financing

In Canada, the Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) regime involves 11 federal departments and agencies.[23] Together, they work to prevent, detect, deter, investigate and prosecute the financing of terrorist activities. A key component of Canada's regime is the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), which establishes the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

The PCMLTFA imposes obligations on more than 31,000 financial service providers and financial intermediaries. The Act makes them active partners in the fight against money laundering and terrorist financing. Under the Act, these entities must keep certain records, know their customers,

[23] Department of Finance, Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), the Royal Canadian Mounted Police (RCMP), the Canada Border Services Agency (CBSA), the Canadian Security Intelligence Service (CSIS), the Canada Revenue Agency (CRA), Department of Justice Canada, Public Prosecution Service of Canada (PPSC), Public Safety Canada (PS), Office of the Superintendent of Financial Institutions (OSFI), and Global Affairs Canada.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

and report certain transactions to FINTRAC.[24] FINTRAC assesses entities' compliance with these requirements and can fine them for non-compliance. FINTRAC also has the authority to analyze financial transaction reports and to disclose certain information to law enforcement and intelligence agencies if it has reasonable grounds to suspect that it would be relevant to the investigation or prosecution of a money laundering or a terrorist financing offence.

Law enforcement and intelligence agencies use this information and that from other sources to identify and disrupt terrorist activities. Law enforcement agencies can also lay criminal charges. The *Criminal Code* contains three terrorist financing offences. These prohibit (1) providing or collecting property for terrorist-related activities; (2) providing or making available property or services for terrorist purposes; and (3) using or possessing property for terrorist purposes. As noted earlier,[25] the *Criminal Code* also provides for a process to list individuals or groups as terrorist entities. The listing of a terrorist entity results in its funds being frozen immediately. The funds may then be seized and forfeited to the Government.

Consider a scenario...

Ms. L is a friend of Mr. A. She supports the 123 Group and wants to send it money abroad. Ms. L goes to a bank to send a wire transfer of $11,000 to a country where it is known that 123 Group operates. Because the amount is more than $10,000, the PCMLTFA requires the bank to report the transaction to FINTRAC. FINTRAC concludes that the transaction is suspicious (given its destination and other indicators) and provides the information to RCMP investigators.

Canada's Contribution to International Efforts

Terrorist financing is a global problem that requires a well-coordinated, multilateral response. The Financial Action Task Force (FATF), of which Canada is an active member, is an international organization that sets standards for combating money laundering and terrorist financing, which ensures all members' AML/ATF regimes are held to the same expectation. The FATF also monitors the implementation of these standards among the 37 FATF members and the more than 190 countries in the global FATF network through peer reviews and public reporting. FATF is currently evaluating Canada against these standards and is expected to finalize and publish the results in summer 2016.

As well, Canada works with international partners through fora such as the United Nations, the G7/G20 and the Counter-ISIL Finance Group. Canada also implements several UN Security Council Resolutions to freeze and seize the assets of persons and entities engaged in terrorism. In addition, Canada supports developing regions that are at higher risk for having terrorist financing activities on their soil, such as the Middle East and North Africa. Canada does this through technical

[24] International electronic fund transfers (EFTs), cash transactions, disbursement from casinos over $10,000; transactions suspected of being related to ML or TF; and terrorist property reports must be reported to FINTRAC.

[25] See chapter "Terrorist Entity Listing Procedures"

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

assistance on counter-terrorist financing. This assistance is designed to strengthen the capacity of financial systems in these regions to avoid being exploited as vehicles for terrorist financing.

Potential Impacts on *Charter* Rights

The current approach requires certain businesses to disclose private financial information to FINTRAC. FINTRAC may decide to disclose it to law enforcement and intelligence agencies for investigation. This could impact privacy rights protected by section 8 of the *Charter*.

Because of the potential impact on section 8 privacy rights, the PCMLTFA has safeguards in place. For example, the Act prescribes the information that FINTRAC can receive and disclose. The PCMLTFA also identifies the law enforcement and intelligence agencies that can receive FINTRAC's financial intelligence. The Act also limits when FINTRAC can disclose information to these agencies. It must have reasonable grounds to suspect that the information would be relevant to the investigation or prosecution of a money laundering or a terrorist financing offence. FINTRAC is independent from law enforcement agencies and does not conduct investigations.

To ensure that the terrorist financing regime addresses emerging risks and maintains appropriate safeguards, Parliament reviews the PCMLTFA every five years. As well, the PCMLTFA permits the Privacy Commissioner of Canada to conduct a review [of FINTRAC, the Act?] every two years. This is to ensure that FINTRAC protects the information it receives as part of its operations. The Privacy Commissioner reports the findings of the review to Parliament.

Finally, the Government continues to monitor its AML/ATF regime to ensure that it aligns with international standards and that it takes into consideration Government policy priorities, including its impact on businesses and the rights of individuals.

Challenges

Canada's financial sector has evolved significantly since the PCMLFTA came into force in 2001. The Act has been amended several times in the past ten [15?] years, but staying current in the changing financial environment presents challenges. Financial technology is changing rapidly. The regime needs to keep pace with evolving techniques using new platforms for illicit fundraising or financial transfers. In addition, the reporting thresholds under the Act may be set too high in terrorism matters. Banks and other financial institutions do not need to report to FINTRAC any transactions below these thresholds unless they deem them suspicious. For example, the $10,000 threshold for reporting international funds transfers may be appropriate for investigations involving money laundering, but terrorists often transfer much smaller amounts. Enhanced coverage of new technologies and a lower reporting threshold would provide more information for investigations. However, it would also increase the personal information collected by FINTRAC, and the number of businesses required to report.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Consider a scenario...

Ms. L sends $3,000 to a member of the 123 Group outside Canada. As the transaction is below the $10,000 threshold, it is not reported to FINTRAC. The business transferring the funds has no information causing it to consider the transaction suspicious and so does not notify FINTRAC of the transaction. FINTRAC has no information to pass on to law enforcement agencies through legislated reporting mechanisms. Had FINTRAC known about the transfer, the PCMLTFA would have allowed it to inform law enforcement if it had reasonable suspicion that the transfer was related to the financing of a terrorist activity.

Terrorists are adaptable and may exploit weaknesses to avoid detection, impeding Canada's efforts to reduce terrorist financing. In addition, terrorists can procure goods or services without actual transfers of funds, limiting the value of FINTRAC's monitoring of the financial system. Terrorists have also used financial professionals with no ties with or sympathies for the terrorist's cause to help move money and resources between countries.

Terrorist financing investigations require extensive resources and significant sharing of information within Canada and with other countries. Investigations also require cooperation within the private sector and between the private and the public sectors. Effective partnerships require a clear understanding by both the public and private sectors of terrorist financing methods and trends, to better and more accurately identify suspicious behaviour. These challenges suggest that an approach that adapts to technological advances and strengthens partnerships between government and the private sector, may be the most effective way to deny terrorists the resources they need.

What do you think?

The Government would like your views about how best to address gaps and other challenges in the regime.

What additional measures could the Government undertake with the private sector and international partners to reduce terrorist financing?

What measures might strengthen cooperation between the Government and the private sector?

Are the safeguards in the regime sufficient to protect individual rights and the interests of Canadian businesses?

What changes could make counter-terrorist financing measures more effective, yet ensure respect for individual rights and minimize the impact on Canadian businesses?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

INVESTIGATIVE CAPABILITIES IN A DIGITAL WORLD

Evolving technology has changed the way Canadians communicate and live their lives. Canadians are increasingly active online. They may use multiple communications devices and a wide variety of tools such as email, Internet banking, instant messaging and various social media applications. This evolution provides enormous benefits for Canadian society, but criminals and terrorists can use these same technologies. Digital communications are now a fundamental tool for terrorism-related activities, including radicalization to violence, facilitation of travel for terrorist purposes, acquisition of funding and equipment, and even training for terrorist actions. The potential harm of evolving technologies is not limited to national security. Traditional criminal activity – from planning violent crime to committing frauds – also relies on these technologies. New public safety challenges continue to appear via the Internet, such as the distribution of terrorist propaganda and child pornography, cyberbullying, and the "Dark Web" and its associated criminal marketplace.

Digital information is sometimes more important than physical evidence or intelligence in investigating national security threats, solving crimes and prosecuting offenders.

To protect Canadians from crime or threats to safety and security, Canada's law enforcement and national intelligence investigators must be able to work as effectively in the digital world as they do in the physical. They must also have the ability to cooperate effectively with their international partners who seek digital evidence from Canada to further their criminal investigations and prosecutions. The laws governing the collection of information and evidence have not, however, kept pace with the rapid advancements of digital technology in the last 20 years and the role technology plays in the lives of Canadians today. Whether information comes from more traditional sources or from within the increasingly complex digital landscape, investigators need access to that information to investigate terrorist threats and criminal activity, and to cooperate with foreign partners in a timely manner.

The term "lawful access" has been used as an umbrella term to refer to certain legally authorized procedural powers and techniques, as well as criminal laws, that may come into play when national security and law enforcement agencies conduct investigations.[26] The Government has attempted to ensure that investigative tools are adequate to deal with new forms and uses of technology. These efforts include multiple public consultations on "lawful access"[27] and updating cybercrime and

[26] Please note that, as a foreign intelligence and information technology security agency, CSE does not conduct national security or law enforcement investigations. It also does not direct its foreign intelligence or cyber security activities at Canadians or anyone in Canada. As such, the tools discussed in this chapter do not relate to CSE.

[27] These include the 2002-2003 Lawful Access Consultations, details of which can be found at www.justice.gc.ca/eng/cons/la-al/index.html.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

cyberbullying laws through the *Protecting Canadians from Online Crime Act.*[28] Canada's digital environment, however, continues to change dramatically. More data has been created in the last five years than ever before. As we move forward, discussions of the investigative capabilities of law enforcement and national security agencies in a digital world must take into account technological advances, [redacted] the legal context and the current threat environment.

Potential Impacts on *Charter* Rights

Access by national security and law enforcement agencies to digital communications, information for investigative or intelligence purposes, or both, it could impact the privacy rights protected by the *Charter.* Some aspects of the issues discussed here could also impact freedom of expression or the right against self-incrimination, also protected under the *Charter.*

These issues are complex. Each raises specific concerns about its intersection with considerations of security and individual rights, including privacy. International and economic considerations also come into play.

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

Challenges

In the physical world, law enforcement and national security agencies use a variety of tools to collect information and evidence to further their investigations and to assist foreign counterparts. For example, investigators at a crime scene may look for physical evidence such as DNA, fingerprints, weapons or other items of importance that may relate to the crime. The *Criminal Code* and other statutes, such as the *CSIS Act* and *the Mutual Legal Assistance in Criminal Matters Act*, authorize the use of these tools. In the digital world, [redacted] In the digital world, for example, investigators may be looking for information and evidence (data) such as online addresses (website or IP addresses), the types of communication that took place, with whom, and for how long.

Law enforcement and national security agencies obtain access to such data as authorized by law. However, the legislation providing for certain investigative tools may not be adequate to deal with the complexity, diversity, and rapid pace of change in the digital world. Current challenges impacting investigative capabilities include the following:

- lack of consistent and timely access to *basic subscriber information* to help identify the subscriber to a communications service;
- lack of consistent and reliable technical *intercept capability* on domestic telecommunication networks;

[28] Some of the measures introduced by this Act were new production orders that allow for authority to obtain tracking data, tracing communication, and transmission data, new powers for preservation of data, and the creation of a new offence for the non-consensual distribution of intimate images, known as "revenge porn." The Act also introduced measures to adapt some existing investigative tools to current technology and aligned those changes with privacy safeguards and requirements for judicial oversight.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- diminished ability to investigate due to the use of *encryption*, and
- inconsistent *retention* of communications data.

These challenges are discussed in order below.

In addition, cyberspace is not easily bound by domestic borders and laws. Many communication service providers have no infrastructure or business presence in Canada, but provide Internet-based communications services. These providers operate in Canada but may fall beyond the reach of Canadian law. This can cause investigative agencies in Canada significant challenges and delays in acquiring the information necessary to advance investigations. It can also lead to critical intelligence and evidence being unobtainable.

Basic Subscriber Information

Consider a scenario…

There is suspicion that Mr. A. has inspired Mr. M. to begin planning a terrorist attack in Canada with an unidentified person. Much of Mr. M's collaboration happens through exchanges over the Internet, such as through online forums.

As part of the investigation of this suspicious activity, a police officer wants to request the identity (subscriber information) related to a particular Internet Protocol (IP) address that has been involved in these online exchanges. However, to get the information from the Internet service provider (ISP), the officer would need a court order. The officer is in the early stages of the investigation and does not have enough information to meet the threshold for obtaining this court order, since getting an order requires more than suspicion that the activities are taking place. As a result, the officer is unable to pursue an investigative lead in a timely and effective manner.

"Basic subscriber information" (BSI) consists of basic identifying information that corresponds to a customer's telecommunications subscription. This can include name, home address, phone number, email address, and/or IP address. BSI does not include the contents of communications. BSI provides law enforcement and national security agencies with key information. This information is particularly useful at the outset of an investigation and may also be used to follow investigative leads further. The information allows the police and national security agencies to identify an individual.

s.23

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

In 2014, in *R. v. Spencer*, the Supreme Court of Canada decided ~~found~~ that the police could not request the name and address of a person in relation to his or her IP address where it would reveal intimate details of his or her anonymous online activities, except in an emergency situation or pursuant to a reasonable law. The Court ~~recognized~~ concluded that obtaining such information interfered with privacy interests protected by the *Charter*.

Without specific legislation permitting access, law enforcement and national security agencies have had difficulty getting timely and effective access to BSI since the *Spencer* decision. As a result, law enforcement agencies have used tools already available in the *Criminal Code*, such as general

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

production orders. These are designed for a large search scope. They are meant for situations such as seeking the complete browsing history, medical records or financial history of an individual. Because of this a high degree of judicial scrutiny is necessary.

The use of these tools for BSI presents the following challenges, especially during early stages of an investigation:

- The information needed to apply for a court order -- for example, a general production order -- may not be available at the beginning of an investigation. The existing information may not attain the threshold required for a court to grant an order.

- The process to obtain a search warrant or a general production order can be slow and involve considerable work. These requirements may be excessive when the only information investigators are seeking is BSI, even if the requirements are appropriate in other situations involving greater privacy intrusions.

The extensive requirements for attaining the threshold to obtain these warrants or orders can significantly hinder criminal investigations. Key evidence may be lost and opportunities to prevent a crime from happening missed. A tool designed to access BSI specifically could, with appropriate safeguards, both enhance investigative capabilities and respect privacy interests.

Laws in many foreign jurisdictions specifically permit law enforcement and national security agencies to obtain BSI. In many cases, this can occur without prior judicial authorization (generally, obtaining BSI without prior judicial authorization is called administrative access). These foreign jurisdictions include the United States, the United Kingdom, Australia, Germany, Sweden, Ireland, Denmark, Spain, Finland, the Netherlands and Norway.

The laws and regulations in these jurisdictions vary in how they limit and safeguard administrative access to BSI. Some jurisdictions give certain agencies access to BSI administratively but require other agencies to obtain judicial authorization first. In some cases, a general administrative scheme for obtaining BSI operates, but an order from a judge may be required under certain conditions. These conditions requiring a court order may include when BSI is stored as part of a data retention requirement, or when certain categories of BSI are sought, such as an IP address or other data unique to mobile cellular devices, such as an International Mobile Subscriber Identity (IMSI) number. Other limitations in getting administrative access to BSI include requirements for senior police officers to approve requests and limiting BSI access to certain types of crime, or including prosecutors in the process to obtain some types of BSI.

Any measures to address the need for consistent and timely access to BSI would have to take into consideration the investigative needs of law enforcement and national security agencies and the impact of those measures on industry. The measures would also have to protect privacy rights in accordance with the *Spencer* decision.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Interception Capability for Communications Services

Law enforcement and national security agencies intercept private communications under the *Criminal Code* and the *Canadian Security Intelligence Service Act* to obtain communications when investigating certain crimes (as listed in the *Criminal Code*) or threats to national security. Each Act sets out procedures to obtain judicial authorization to use interception techniques. These procedures are designed to uphold privacy rights.

In some cases, law enforcement and national security agencies obtain the necessary court orders to intercept communications. However, communications service providers (CSPs) may not be able to perform the interception because the technical capability to intercept communications has not been built into the CSP's infrastructure. This hinders investigations that are being pursued under judicial authorization. In turn, this prevents law enforcement and national security agencies from fulfilling their mandates.

Canada does not impose a general requirement for CSPs to have interception capabilities on their networks. Many other countries do. Australia, the United States, the United Kingdom and [many?] other European nations require CSPs to have an interception capability. In the U.S., for example, the *Communications Assistance for Law Enforcement Act*, usually referred to as CALEA, imposes this obligation. The US Federal Communications Commission (FCC) website explains CALEA.[29] Because of CALEA, traditional voice switches in the U.S. today include an intercept feature.

Commented [KA4]: Discussed with Norm, we think "many?" is ok.
Formatted: Highlight
Formatted: Highlight
Formatted: Highlight

Continuing the scenario from above...

The investigation has now proceeded to a point well beyond suspicion and the police have received an authorization from a judge to intercept the communications of Mr. M.

However, when the police contact the telecommunications service provider, they learn that the service provider has not built a capability to intercept communications into its infrastructure. The service provider cannot complete the work required to develop and implement this intercept capability before the authorization expires. As a result, the police miss out on obtaining key evidence, even though they had court authority to intercept the communications.

Several issues need to be taken into account when discussing whether to require CSPs to introduce intercept capabilities. These include the impact on privacy, the investigative needs of law enforcement and national security agencies, and how introducing requirements for intercept capabilities affects the costs and competitiveness of the industry.

Formatted: Highlight

Encryption

Encryption converts a readable electronic message into an unreadable message. To decrypt the message (make it readable again), the reader must use one or more specific decryption "keys."

[29] https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Encryption is widely regarded as a best practice to enhance security and protect privacy online. It is commonly used to protect individual messages, personal devices and transmission channels. Secure encryption is also vital to cybersecurity, e-commerce, data and intellectual property protection, and the commercial interests of the communications industry. Canada's policy on cryptography ([redacted] established in 1998) underlines the importance of encryption to the viability, stability and growth of the economy and e-marketplace and encourages the use of encryption to protect privacy, personal information and data. Today, free encryption technologies and services are widely available. These include encryption that often operates without the users' knowledge or need to activate it. Encryption technologies may be built in to a user's communication service.

Commented [JNW5]: established

Formatted: Highlight

However, encryption technology also helps criminals and terrorists to avoid discovery, investigation and prosecution by making their communications unreadable to outsiders. The international availability of encryption tools and the complexities of encryption make law enforcement and national security investigations more difficult, including those involving foreign partners against serious international crimes.

It is difficult to address~~limit~~ the problematic use of encryption without also impairing ~~reducing~~ its use and benefits. As a result, very few countries have proceeded to limit encryption through the law in the interests of protecting law enforcement and national security agency capabilities. This is despite the challenges posed by encryption for law enforcement and national security agencies being well known. Encryption has been the subject of concern and discussion in many jurisdictions since the 1990s.

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

The United Kingdom is among the few countries to impose limits on encryption through law – in this case, the *Regulation of Investigatory Powers Act, 2000*. The Act gives legally authorized persons (such as law enforcement, security and intelligence agencies) the authority to serve notices on individuals or bodies requiring the disclosure of protected (for example, encrypted) information in an intelligible form. This can be done through decryption or disclosure of encryption keys that the person is believed to hold. These provisions have attracted controversy.

s.21(1)(a)

In the 1990s, a series of legislative initiatives (sometimes referred to as "Clipper Chip" proposals) were suggested in the U.S. to impose built-in decryption capabilities. These proposals were highly controversial and attracted vigorous opposition from privacy and civil liberties groups and from groups concerned about the potential damage to industry [redacted] None of these proposals became law. However, vigorous debate about encryption continues in the U.S., as do concerns of law enforcement about encryption. This was seen most recently in the controversy that arose when the US government asked Apple [redacted] associated with the San Bernardino terrorist incident.

Formatted: Highlight

Continuing the scenario from above...

The police were finally able to develop intercept capability and obtain court authority again to intercept the communications of Mr. M.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

To avoid having his plans discovered, however, Mr. M had encrypted his communications, which were unreadable to the police as a result. In addition, the service provider advised the police that it could not help decrypt the communications. After months of investigative delays and despite court authority to intercept the communications of Mr. M, the police cannot read them to obtain potential evidence. As a result, Mr. M's communications remain protected from law enforcement.

Even when law enforcement or national security agencies can intercept a communication, with assistance from a service provider under a court order, the data that is obtained is often unreadable due to the layers of encryption that cannot be decrypted or otherwise removed. Encryption challenges also apply to the court-ordered production of historical data, such as e-mail, text messages, photos and videos from lawfully seized smartphones, computer hard drives and other digital devices. Since encryption can be used by anyone, a private sector organization may not be able to help law enforcement and national security agencies decrypt communications because the organization might not have the technical ability to [redacted].

s.23

No provisions specifically designed to compel decryption are found in the *Criminal Code*, the *Canadian Security Intelligence Service Act* or in other Canadian laws. In other words, there is no law in Canada designed to ~~can~~ force a person or organization to decrypt their communications.

Formatted: Highlight

Formatted: Highlight

Discussion about encryption and decryption must involve the potential impact on the following:

- human rights, including privacy rights, freedom of expression, and the right against self-incrimination;
- the investigative needs of law enforcement and national security agencies;
- commercial interests, such as competitiveness and the protection of intellectual property;
- how compelling decryption could weaken existing IT infrastructure models and systems;
- cybersecurity; and
- e-commerce.

Data Retention

"Data retention" refers to the general requirements to store certain elements of subscribers' telecommunications data, such telephone numbers dialed, call length, time of call, and Internet equivalents. This is done to support law enforcement and national security investigations. These data can provide key pieces of intelligence and evidence. Data retention ensures that this information will be kept for a specified period so that law enforcement and national security agencies might be able to obtain this information with a warrant. To date, Canada has not pursued a telecommunications data retention requirement for law enforcement and national security purposes.

Formatted: Highlight

Continuing the scenario from above...

As part of its ongoing investigation, the police learn that Mr. M had used his mobile phone over

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

three weeks in July 2015 to communicate with individuals linked to terrorist groups. The police seek a court order to obtain telecommunications data associated with Mr. M's mobile phone account. However, the company keeps records for business purposes only for nine months. As a result, the company has already deleted data from July 2015 and the data are not available to the police.

Parliament recently introduced *preservation* powers into the *Criminal Code* when it enacted the *Protecting Canadians from Online Crime Act*. These powers allow law enforcement agencies to seek a court order or demand the preservation of specific computer data belonging to specific persons for a brief time to assist in investigations.

However, some business practices are changing and companies are deleting data more quickly than before, sometimes before law enforcement can seek a court order for or demand preservation. This poses a new challenge. In addition, the length of time data is held varies from company to company. General data retention requirements would provide for companies to keep data for a standardized period. However, this might mean that companies might have to store data for longer than they require strictly for business purposes. Requiring data retention for a given period could also increase risks to personal information held by companies. The longer personal information is kept, the longer it is vulnerable to attack.

General requirements for data retention already exist in some foreign jurisdictions or have been proposed or debated there. In the U.S., some data retention bills have been introduced in Congress, but none have been enacted. Australia recently enacted data retention requirements. On March 15, 2006, the European Union (EU) issued a Data Retention Directive (DRD) to impose data retention requirements for telecommunications data on its member states.

The DRD required that data retention be implemented through legislation enacted by EU member states at the national level. The manner of the implementation varied significantly among member states, in part because of controversy over these requirements in some states. On April 8, 2014, the Court of Justice of the European Union struck down the DRD, calling it inconsistent with privacy rights in Europe.

EU member states are now looking at their respective national laws to determine if and how their national laws on data retention need adjustment after the court decision. Some countries, such as Germany, have already introduced changes. The Federal Constitutional Court of Germany declared the country's own domestic legislation unconstitutional in March 2010. A new data retention law came into effect in Germany on January 4, 2016. The law introduced many safeguards, such as reducing [redacted] from six months to ten weeks and restricting access to such data to [redacted] "serious crimes" only.

The discussion of telecommunications data retention requirements should take into account several issues, including the following: the investigative needs of law enforcement and national security

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

agencies, the impact on privacy interests and the impact on the costs and competitiveness of companies resulting from ~~by~~ data retention requirements.

Formatted: Highlight

What do you think?

How can the Government address challenges to law enforcement and national security investigations posed by the evolving technological landscape in a manner that is consistent with Canadian values, including respect for privacy, provision of security and the protection of economic interests?

In the physical world, if the police obtain a search warrant from a judge to enter your home to conduct an investigation, you must allow them access. Should investigative agencies operate any differently in the digital world?

Currently, investigative agencies have tools in the digital world similar to those in the physical world. As this document shows, there is concern that these tools may not be as effective in the digital world as in the physical world. Should the government update these tools to better support digital/online investigations?

Is your expectation of privacy different in the digital world than in the physical world?

Basic Subscriber Information (BSI)

Since the *Spencer* decision, police and national security agencies have had difficulty obtaining BSI in a timely and efficient manner. This has limited their ability to carry out their mandates, including investigating crimes. If the Government developed legislation to respond to this problem, under what circumstances should BSI (such as name, address, telephone number and email address) be available to these agencies? For example, would it be appropriate to make such information available in emergency circumstances, to help find a missing person, if there is suspicion of a crime, to further an investigative lead, or in other specific situations?

Do you consider your basic identifying information identified through BSI (such as name, home address, phone number and email address) to be as private as the contents of your emails? your personal diary? your financial records? your medical records? Why or why not?

s.23

Do you see a difference between the police having access to your name, home address and phone number, and the police having access to your Internet address, such as your IP address or email address?

Interception Capability

The Government has made previous attempts to enact interception capability legislation. This legislation would have required ~~attempted to compel~~ domestic communications service providers to create and maintain networks that would be technically capable of intercepting communications if a court order authorized the interception. These ~~attempts to enact law~~ legislative proposals were

Formatted: Highlight

Formatted: Highlight

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

controversial with Canadians. Some were concerned about privacy intrusions. As well, the Canadian communications industry was concerned about how such laws might affect it.

Should Canada's laws help to ensure that consistent interception capabilities are available through domestic telecommunications service provider networks when a court order authorizing the intercepting is granted by the courts?

Encryption

If the Government were to consider options to address the challenges encryption poses in police and national security investigations, in what circumstances, if any, should investigators have the ability to compel individuals or companies to assist with decryption?

How can law enforcement and national security agencies reduce the effectiveness of encryption for individuals and organizations involved in crime or terrorist activities, yet not limit the beneficial uses of encryption by those not involved in illegal activities?

Data Retention

Should the law require Canadian service providers to keep telecommunications data for a certain period to ensure that it is available if police and national security agencies need it for their investigations and a court authorizes access?

If the Government of Canada were to enact a general data retention requirement, what type of data should be included or excluded? How long should this information be kept?

INTELLIGENCE AND EVIDENCE

National security information needs to be protected from unnecessary public disclosure. At the same time, there is a need to facilitate its use in legal proceedings, when appropriate, while maintaining the fairness of the proceedings and the integrity of the justice system.

The challenge is significant in criminal and related proceedings involving constitutionally protected interests. National security information might also, for example, be important in advancing or defending against a civil case. The Government might also use such information when making administrative decisions, which in turn can be judicially reviewed.

When national security information is involved—or potentially involved—in a legal proceeding, it brings into play issues of fundamental justice, the rule of law and the confidence of Canadians in the justice system. The potential disclosure of national security information may also limit the effectiveness of national security agencies and make it more difficult to assure foreign partners that national security information they have shared with Canada is protected.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Key Principles

The discussion of intelligence and evidence raises several important principles, including the following:

- the requirement that laws be consistent with the *Charter*;
- the obligation of the Government to protect sensitive sources, capabilities and techniques, and its relationships with international partners, in the interests of national security and international relations;
- the ability of courts and tribunals to consider as much relevant material as possible to ensure that judgments are based on a complete picture of the facts and that justice is done; and
- the need for legislative tools to be flexible enough to apply in a broad range of circumstances.

Section 38 of the *Canada Evidence Act* (CEA) provides the framework for the disclosure and use of national security information in a broad range of legal proceedings. Under section 38, a Federal Court judge must assess whether or not the disclosure would be injurious to international relations, national defence or national security. If disclosure would be injurious, the judge must then consider whether the public interest in disclosure outweighs the public interest in non-disclosure. The process under section 38 of the CEA is conducted in Federal Court even though the information may relate to a proceeding in a different court.

This two-part process, also known as a bifurcated process, has been the subject of criticism.

The Supreme Court of Canada concluded that this bifurcated approach is constitutional in a criminal proceeding (*R. v. Ahmad (2011)*). Still, the Court invited the Government to consider its policy choice of using a bifurcated system. The issues surrounding intelligence and evidence have also been addressed in a number of reports, including reports of parliamentary committees and the Air India Inquiry.[30] Intelligence and evidence has also been the subject of consultations in New Zealand and the United Kingdom.

Intelligence and evidence issues can be expected to continue to arise for several reasons, including that a number of federal agencies are involved in national security investigations. In some cases, the need for cooperation between federal institutions has resulted in an increasing number of government actions being informed by national security information.

[30] Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Criminal Proceedings

The Federal Court does not hear criminal cases, unlike the criminal courts in the provinces and territories. However, issues relating to the disclosure of national security information in these cases are largely addressed by Federal Court judges.

This means that, in some instances, the criminal court in a province may be unable to see the national security information and may only be able to rely on unclassified summaries provided by the Federal Court.

s.21(1)(a)

In other cases, an [redacted] to allow disclosure in court of national security information under certain conditions, determined case by case. However, these proceedings are unable to incorporate the protections for national security information built into the *Canada Evidence Act*. Nor can they benefit from using the Federal Court's secure facilities or relying on its administrative expertise in handling national security information.

Consider a scenario...

After a long investigation, the RCMP lay criminal charges in the superior court of the province against Mr. M for planning a terrorist attack. Information provided by CSIS was essential to the RCMP investigation. This information was obtained from a foreign agency, which provided it on condition that it not be further disclosed without the agency's consent. The foreign agency refuses to consent to the disclosure. Revealing this national security information without the foreign agency's consent would damage CSIS's relationship with it.

To protect against the disclosure of the information provided by the foreign agency, the Attorney General of Canada makes an application under the *Canada Evidence Act* for the Federal Court to decide whether it is in the public interest to protect or disclose the information. The Federal Court judge decides to protect the national security information, which means that the actual information will not be given to the judge of the superior court or be relied on during the prosecution.

However, the judge of the Federal Court also decides to prepare an unclassified summary of the information, which is provided to Mr. M and the judge of the superior court. Mr. M uses this summary to defend himself against the charges and the judge of the superior court may consider it during the proceedings. Because this information is an important part of the prosecution's case, not being able to rely on the complete information in the superior court could cause the prosecution to fail.

National security agencies collect information to advise government, but the information is not generally intended to be used as evidence In some circumstances, the obligation on the prosecutor to make disclosure in criminal cases may require the prosecutor to approach these agencies to see if they have information relevant to the case. The prosecutor must do this even if the agencies did not provide that information to law enforcement for the criminal investigation. This is one way for national security agencies to get drawn into criminal proceedings.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Potential Impacts on *Charter* Rights

When trying to protect national security information in a criminal case, the Government must ensure that any measure to do so is consistent with the *Charter*.

An individual accused of a crime has a right to a fair trial, including the right to make full answer and defence. This involves broad access to information that relates to the investigation and charges. The accused also has a right to be present throughout the trial. Finally, the open court principle protected by the *Charter* may come into play when national security information is used in a criminal trial.

Civil Proceedings

National security information may be relevant in a civil proceeding and can sometimes be central to a proceeding. Where national security information is involved, a plaintiff may be unable to make its case, and a defendant may be unable to defend itself, because the information needed to establish the case or defend against a claim needs to be protected. This situation can arise when the federal government is sued for allegedly wrongful conduct, when it is the plaintiff, or in proceedings where the federal government is not at all involved (for example, a dispute between two private companies).

If a judge is unable to take into account the national security information in the civil proceeding, justice may not be served. The lack of relevant information could lead to unwarranted damage to someone's reputation, costly settlements or loss of public confidence in the legal system.

To ensure adequate protection of national security information, the same bifurcated process under the *Canada Evidence Act* described for the criminal process above applies to civil proceedings.

Potential Impacts on *Charter* Rights

Unlike criminal proceedings, civil proceedings do not automatically bring the *Charter* right to liberty into play. However, parties in civil proceedings generally have a right to documents that contain relevant information that either directly or indirectly advances or damages the case of one party or another. The protection of national security information from disclosure in a civil case could make it difficult to successfully pursue, or defend against, *Charter* claims.

Administrative Proceedings

Many federal administrative decision makers might rely on national security information in their work. These decision makers include federal government officials, ministers, boards and administrative tribunals. The decisions involve a wide variety of matters, such as issuing or revoking permits or licences. For example, decisions about issuing passports are considered administrative proceedings.

As in criminal and civil proceedings, national security information must be protected in administrative and related proceedings, while at the same time the proceedings must ensure fairness. Section 38 of the *Canada Evidence Act* provides a general regime for protecting national security

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

information in some of these situations. Challenges similar to those outlined in the criminal and civil contexts exist here as well.

Apart from section 38 of the *Canada Evidence Act*, a number of specific regimes, varying slightly in their procedures, allow for the protection and use of the national security information during proceedings. Immigration proceedings are one example.

Potential Impacts on *Charter* Rights

Procedural fairness requirements vary depending on the nature of the administrative decision. The content of the duty of fairness, which includes the rights to know the case to meet and to respond in a meaningful way, varies depending on the rights and interests at stake. Even when *Charter* rights are significantly impacted, the right to know the case to meet is not absolute.

Proceedings under the *Immigration and Refugee Protection Act* (IRPA)

In making immigration decisions, the Government must sometimes rely on classified information (that is, information that if disclosed would be injurious to national security or endanger the safety of a person) to determine whether foreign nationals and permanent residents may enter or remain in Canada (whether they are "admissible"). Division 9 of the IRPA allows the Government to protect and use this information during immigration proceedings. The best known of these Division 9 proceedings are commonly called security certificate proceedings.

The certificate is a document, signed by the Minister of Public Safety and Emergency Preparedness and the Minister of Immigration, Refugees and Citizenship. It states that there are reasonable grounds to believe that the named person is inadmissible to Canada for reasons of security, violating human or international rights, serious criminality or organized criminality. The certificate is automatically referred to a judge of the Federal Court to determine its reasonableness. The proceedings at the Court have two parts:

(1) public proceedings, where the person named in the certificate, along with their counsel, receive non-classified information and an unclassified summary of the classified information that is the basis for the certificate; and,
(2) closed proceedings, where the public, the person named in the certificate and their counsel are not present and a court-appointed special advocate (a private lawyer with an appropriate security clearance) receives the classified and non-classified information relevant to the certificate and seeks to protect the interests of the named person.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Consider a scenario...

Ms. N is a permanent resident currently in Canada. CSIS has classified information from sources within Canada, as well as from an international partner, that shows Ms. N as part of a terrorist group and a danger to the security of Canada. She has been attending Mr. A's meetings. CSIS provides this information to the Minister of Public Safety and Emergency Preparedness and the Minister of Immigration, Refugees and Citizenship. The ministers decide to sign a security certificate and a warrant for her arrest. The certificate and warrant are filed with the Federal Court. The security certificate process protects the classified information from being disclosed while allowing it to be used by the Federal Court judge, who must determine if the certificate is reasonable.

Potential Impacts on *Charter* Rights

A person's rights under the *Charter* are engaged by security certificate proceedings. These include the right not to be deprived of liberty and security of the person, except in accordance with the principles of fundamental justice. These *Charter* protections include the right to a fair hearing, and the right to know the case to meet and to answer that case.

To protect these rights, the law provides certain safeguards. During closed proceedings, special advocates protect the interests of the person they represent. They can challenge government claims that information cannot be disclosed, as well as the relevance, reliability and sufficiency of the information and evidence in the case. Special advocates can make submissions to the Court, cross-examine witnesses during the closed proceedings, and exercise any other power the judge authorizes.

Also, whenever a person is subject to detention or conditions under a warrant, the Court reviews this detention or these conditions on a regular basis (at least once every six months).

Finally, judges seek to ensure the fairness of these proceedings and decide whether the security certificate is reasonable. The Supreme Court of Canada, in the *Harkat* decision, stated that the "judge is intended to play a gatekeeper role, is vested with broad discretion and must ensure not only that the record supports the reasonableness of the ministers' finding of inadmissibility, but also that the overall process is fair."[31]

The ATA, 2015 changed three aspects of Division 9 of IRPA proceedings (e.g. security certificates):

- The Government can immediately appeal when a judge orders the public disclosure of information that the Government considers must remain classified;
- The information that the ministers must file with the Federal Court is that which is relevant to the ground of inadmissibility on which the certificate is based and which allows the person to be reasonably informed of the case; and,
- The Government may ask the judge for an exemption from providing some classified information to the special advocate (as part of the disclosure of relevant information in closed proceedings). The judge may grant this exemption only if satisfied that the exempted

[31] *Canada (Citizenship and Immigration) v. Harkat*, 2014 SCC 37.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

information would not enable the person to be reasonably informed of the Government's case. The judge is permitted to consult with the special advocates about the information before making this decision.

Continuing the scenario from above...

During the security certificate process for Ms. N, the Federal Court judge decides that some of the classified information should be disclosed publicly. The Government appeals this decision immediately because releasing this information would harm national security. The Federal Court of Appeal reviews the decision to disclose the information. The Federal Court of Appeal decides to protect the information and the case continues without it being disclosed.

What are other countries doing?

Australia, New Zealand, the United Kingdom and the United States face the same challenges of handling intelligence and evidence in their court systems. In criminal matters, for the most part, courts work from legislated roadmaps to protect national security information and maintain an adversarial legal system.

In general, Australia and the United States allow private (non-government) counsel to be security-cleared and have access to national security information in representing their clients. New Zealand and the United Kingdom provide for special counsel to protect the interests of the person involved while not disclosing national security information to that person.

In civil litigation involving the potential disclosure of national security information, some countries differ if national security information is sought to be used as evidence. In the United States, a legal concept known as the common law State Secrets Privilege has evolved. This permits hearings behind closed doors without the affected person or the person's counsel being present which can result in the summary dismissal of claims based on the potential disclosure of state secrets. Elsewhere, including in Australia, procedures established by legislation allow for the substitution of national security information with summaries, admissions of fact or limited disclosure (where possible). Finally, the United Kingdom has legislated closed civil proceedings where the judge may review and rely on national security information tendered in closed proceedings, with the interests of the non-government party represented by a special advocate.

Senior administrative tribunals in Australia, the United Kingdom and New Zealand consider complaints involving security agencies as a part of their broad supervisory roles. Given their mandate, these senior administrative tribunals involve sitting judges.

What do you think?

Do the current section 38 procedures of the *Canada Evidence Act* properly balance fairness with security in legal proceedings?

Could improvements be made to the existing procedures?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Is there a role for security-cleared lawyers in legal proceedings where national security information is involved, to protect the interest of affected persons in closed proceedings? What should that role be?

Are there any non-legislative measures which could improve both the use and protection of national security information in criminal, civil and administrative proceedings?

How could mechanisms to protect national security information be improved to provide for the protection, as well as the reliance on, classified information in all types of legal proceeding? In this context, how can the Government ensure an appropriate balance between protecting national security and respecting the principles of fundamental justice?

Do you think changes made to Division 9 of the IRPA through the ATA, 2015 are appropriately balanced by safeguards, such as special advocates and the role of judges?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

CONCLUSION

Canada, like other countries, faces national security threats. The threat of terrorism, by global and by domestic actors, is real and evolving. More people are radicalizing to violence. Some are leaving Canada to join terrorist groups overseas, while others focus their attention on Canada itself. Canadians expect the Government to keep them safe. At the same time, the Government must comply with the rights enshrined in the *Charter*.

The issues described in this Green Paper relate to major components of our counter-terrorism framework. Some chapters discuss measures already in place. Other chapters highlight current gaps [redacted] while others explain where the Government would like to take action. We hope that this information helps Canadians understand this complex area as we begin consultations with them about how best to respond.

s.21(1)(a)

Government counter-terrorism actions undoubtedly impact rights protected under the *Charter*.

Views will differ on what are justifiable and reasonable impacts. There will also be strong opinions on the tools we should employ and how they should be employed.

[redacted]

Thank you for taking the time to read through this paper and for providing your thoughts.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

ANNEX A – DIAGRAM OF SCENARIO CHARACTERS

The chart below demonstrates Mr. A's links to his followers, and which ones are discussed in various chapters in the document.

Mr. A

Mr. B	Radicalization to violence
Mr. C	Threat reduction
Mr. D	
Mr. F	Domestic national security information sharing
Ms. G	Passenger Protect Program
Mr. I	*Criminal Code* – peace bonds
Ms. J	*Criminal Code* – recognizance with conditions
Ms. K	*Criminal Code* – advocacy or promotion of terrorism offences in general
Ms. K	*Criminal Code* – seizure and forfeiture of terrorist propaganda
Ms. L	Terrorist financing
Mr. M	Investigative capabilities in a digital world
Mr. M	Intelligence and evidence – criminal proceedings
Ms. N	Intelligence and evidence – proceedings under the *Immigration and Refugee Protection Act*

There are also two other individuals, who are not associated to Mr. A, but who appear in some chapters.

Ms. E	Domestic national security information sharing
Mr. H	Passenger Protect Program

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

11 July 2016

EMBARGOED
Do not distribute

INVESTIGATIVE CAPABILITIES IN A DIGITAL WORLD

Commented [AA1]: There are some inconsistency issues WRT some terms (e.g.: email vs e-mail). I have reviewed and replaced using terms from GoC Termium Plus

Evolving technology has changed the way Canadians communicate and live their lives. Canadians are increasingly active online. They may use multiple communications devices and a wide variety of tools such as e-mail, Internet banking, instant messaging and various social media applications. This evolution provides enormous benefits for Canadian society, but criminals and terrorists can use these same technologies to further their activities. Digital communications are now a fundamental tool for terrorism-related activities, including radicalization to violence, facilitation of travel for terrorist purposes, acquisition of funding and equipment, and even training for terrorist ~~actions~~activities. ~~The potential harm of~~ These evolving technologies are often exploited by criminals and threat actors and can be harmful to Canadians. The exploitation of these technologies is not limited to national security, but it also affects criminality more broadly, such as the planning of murders and the commission of frauds. ~~is not limited to national security. Traditional criminal activity – from planning violent crime to committing frauds – also relies on these technologies~~. New public safety challenges continue to appear via the Internet, such as the distribution of terrorist propaganda and child pornography, cyberbullying, and the "Dark Web" and its associated criminal marketplace.

Digital information is sometimes more important than physical evidence or intelligence in investigating national security threats, solving crimes and prosecuting offenders.

To protect Canadians from crime or threats to safety and security, Canada's law enforcement and national ~~intelligence~~ security investigators must be able to work as effectively in the digital world as they do in the physical. ~~They~~ Law enforcement must also have the ability to cooperate effectively with their international partners who seek digital evidence from Canada to further their criminal investigations and prosecutions. The laws governing the collection of information and evidence have not, however, kept pace with the rapid advancements of digital technology in the last 20 years and the role technology plays in the lives of Canadians today. Whether information comes from more traditional sources or from within the increasingly complex digital landscape, investigators need access to that information ~~to~~ when investigating ~~terrorist~~ threats to Canada's national security and criminal activity, and to cooperate with foreign partners in a timely manner.

In the past, the term "lawful access" has been used as an umbrella term to refer to certain legally authorized procedural powers and techniques, as well as criminal laws, that may come into play when national security and law enforcement agencies conduct investigations.[1] The Government has attempted to ensure that investigative tools are adequate to deal with new forms and uses of

[redacted]

s.21(1)(a)

[1] Please note that, as a foreign intelligence and information technology security agency, the Communications Security Establishment (CSE) does not conduct national security or law enforcement investigations. It also does not direct its foreign intelligence or cyber security activities at Canadians or anyone in Canada. As such, the tools discussed in this chapter do not relate to CSE.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

technology. These efforts have included multiple public consultations on "lawful access"[2] and updating cybercrime and cyberbullying laws through the *Protecting Canadians from Online Crime Act.*[3] Canada's digital environment, however, continues to change dramatically. More data has been created in the last five years than ever before. As we move forward, discussions of the investigative capabilities of law enforcement and national security agencies in a digital world must take into account new and emerging technological advances, [redacted] the legal context and the current threat environment.

s.23

Potential Impacts on *Charter* Rights

Access by national security and law enforcement agencies to digital communications, information for investigative or intelligence purposes, or both, it could impact the privacy rights protected by the *Charter*. Some aspects of the issues discussed here could also impact freedom of expression or the right against self-incrimination, also protected under the *Charter*.

These ~~issues~~ challenges discussed in this paper are complex. Each raises specific concerns about its intersection with considerations of security and individual rights, including privacy. International and economic considerations also come into play.

Commented [LO4]: Which issues? The issues mentioned above? The issues discussed in this paper?

Should refer to the issues discussed in this paper.

Also changed it to Challenges, as the next section is about challenges not issues (consistency)

Challenges

In the physical world, law enforcement and national security agencies use a variety of tools to lawfully collect information and evidence to further their investigations and to assist foreign counterparts. The *Criminal Code* and other statutes, such as the *CSIS Act* and *the Mutual Legal Assistance in Criminal Matters Act*, authorize the use of these tools. For example, investigators at a crime scene may look for physical evidence such as DNA, fingerprints, weapons or other items of importance that may relate to the crime. ~~The *Criminal Code* and other statutes, such as the *CSIS Act* and *the Mutual Legal Assistance in Criminal Matters Act*, authorize the use of these tools.~~ In the digital world, [redacted] ~~investigators use other tools to collect digital information and evidence. In the digital world,~~ for example, investigators may be looking for digital information and evidence (data) such as online addresses (website or IP addresses), the types of communication that took place, with whom, and for how long.

Commented [LO5]: Needs to move up, as it causes confusion. Indicate where the tools come from and then go into the examples.

s.23

Law enforcement and national security agencies obtain access to such data as authorized by law. However, the current legislation providing for certain investigative tools ~~may~~ is not, in all cases, ~~be~~

Formatted: Highlight
Formatted: Highlight
Formatted: Highlight
Formatted: Highlight
Formatted: Highlight
Formatted: Highlight
Formatted: Highlight
Formatted: Highlight
Formatted: Not Highlight
Formatted: Not Highlight

[2] These include the 2002-2003 Lawful Access Consultations, details of which can be found at www.justice.gc.ca/eng/cons/la-al/index.html.

[3] Some of the measures introduced by this Act were new production orders that allow for authority to obtain tracking data, tracing communication, and transmission data, new powers for preservation of data, and the creation of a new offence for the non-consensual distribution of intimate images, known as "revenge porn." The Act also introduced measures to adapt some existing investigative tools to current technology and aligned those changes with privacy safeguards and requirements for judicial oversight.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

~~adequate~~ designed to specifically deal with the complexity, diversity, and rapid pace of change in the digital world. Current challenges impacting investigative capabilities include the following:

- lack of consistent and timely access to *basic subscriber information* to help identify the subscriber to a communications service;
- lack of consistent and reliable technical *intercept capability* on domestic telecommunication networks;
- diminished ability to investigate due to the use of *encryption*; and
- inconsistent *retention* of communications data.

Commented [LO7]: It's about design and their specificity

Formatted: Not Highlight

These challenges are discussed in order below.

In addition, cyberspace is not easily bound by domestic borders and laws. Many ~~communication~~ Communication ~~service~~ Service ~~providers~~ Providers (CSPs) have no infrastructure or business presence in Canada, but provide Internet-based communications services. As a result, ~~t~~These providers ~~operate in Canada but~~ may fall beyond the reach of Canadian law. This can cause investigative agencies in Canada significant challenges and delays in acquiring the information necessary to advance investigations. It can also lead to critical intelligence and evidence being unobtainable.

Formatted: Not Highlight

Formatted: Not Highlight

Basic Subscriber Information

Consider a scenario…

There is suspicion that Mr. A. has inspired Mr. M. to begin planning a terrorist attack in Canada with an unidentified person. Much of Mr. M's collaboration happens through exchanges over the Internet, such as through online public forums.

As part of the investigation of this suspicious activity, a police officer wants to request the identity (basic subscriber information) related to a particular Internet Protocol (IP) address that has been involved in these online exchanges. However, to get the information from the Internet ~~service~~ Service ~~provider~~ Provider (ISP), the officer would need a court order. The officer is in the early stages of the investigation and does not have enough information to meet the threshold for obtaining this court order, since getting an order requires more than suspicion that the activities are taking place. As a result, the officer is unable to pursue an investigative lead in a timely and effective manner.

"Basic subscriber information" (BSI) consists of basic identifying information that corresponds to a customer's telecommunications subscription. This can include name, home address, phone number, e-mail address, and/or IP address. BSI does not include the contents of communications. BSI provides law enforcement and national security agencies with key information. This information is particularly useful at the outset of an investigation and may also be used to follow investigative leads ~~further~~. The information allows the police and national security agencies to identify an [redacted] individual.

s.23

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

In 2014, in *R. v. Spencer*, the Supreme Court of Canada decided ~~found~~ that the police could not request the name and address of a person in relation to his or her IP address where it would reveal intimate details of his or her anonymous online activities, except in an emergency situation or pursuant to a reasonable law. The Court ~~recognized~~ concluded that [redacted] interfered with privacy interests protected by the *Charter*.

Without specific legislation designed to permit~~ting~~ access, law enforcement and national security agencies have had difficulty getting timely and effective access to BSI since the *Spencer* decision. As a result, law enforcement agencies have used tools already available in the *Criminal Code*, such as general production orders. These tools are designed for a larger search scope. They are meant for situations such as seeking the complete browsing history, medical records or financial history of an individual. Because of this a high degree of judicial scrutiny is necessary.

The use of these tools for BSI presents the following challenges, especially during early stages of an investigation:

- The information needed to apply for a court order -- for example, a general production order -- may not be available at the beginning of an investigation. The existing information may not attain the threshold required for a court to grant an order.
- The process to obtain a search warrant or a general production order can be slow and involve considerable work and resources. ~~The s~~This process has requirements that may be excessive when the only information investigators are seeking is BSI, even if the requirements are appropriate in other situations involving greater privacy intrusions.

As a result of these challenges, ~~The extensive requirements for attaining the threshold to obtain these warrants or orders can significantly hinder criminal investigations. K~~key evidence may be lost and opportunities to prevent a crime from happening missed. A tool designed to access BSI specifically could, with appropriate safeguards, both enhance investigative capabilities and respect privacy interests.

Laws in many foreign jurisdictions ~~specifically permit~~include specific provisions that permit law enforcement and national security agencies to obtain BSI in a timely and effective manner. In many cases, this can occur without prior judicial authorization (generally, obtaining BSI without prior judicial authorization is called administrative access). These foreign jurisdictions that have provisions for BSI include the United States, the United Kingdom, Australia, Germany, Sweden, Ireland, Denmark, Spain, Finland, the Netherlands and Norway.

The laws and regulations in these jurisdictions vary in how they limit and safeguard administrative access to BSI. Some jurisdictions give certain agencies access to BSI administratively but require other agencies to obtain judicial authorization first. In some cases, a general administrative scheme for obtaining BSI operates, but an order from a judge may be required under certain conditions. These conditions requiring a court order may include when BSI is stored as part of a data retention

Formatted: Not Highlight
Formatted: Highlight
Formatted: Not Highlight
Formatted: Not Highlight
s.21(1)(a)
Formatted: Not Highlight
Formatted: Not Highlight

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

requirement, or when certain categories of BSI are sought, such as an IP address or other data unique to mobile cellular devices, such as an International Mobile Subscriber Identity (IMSI) number. Other limitations in getting administrative access to BSI include requirements for senior police officers to approve requests and limiting BSI access to certain types of crime, or including prosecutors in the process to obtain some types of BSI.

Commented [AA9]: This sentence is out of place – suggest either removing or moving.

Any measures to address the need for consistent and timely access to BSI would have to take into account the investigative needs of law enforcement and national security agencies and the impact of those measures on the communications industry, and potentially other industry sectors where BSI is involved. The measures would also have to protect privacy rights in accordance with the *Spencer* decision.

Interception Capability for Communications Services

Law enforcement and national security agencies intercept private communications under the *Criminal Code* and the *Canadian Security Intelligence Service Act* to obtain communications when investigating certain crimes (as listed in the *Criminal Code*) or threats to national security. Each Act sets out procedures to obtain judicial authorization to use interception techniques. These procedures are designed to uphold privacy rights.

s.21(1)(a)

Formatted: Not Highlight

[redacted]aw enforcement and national security agencies obtain the necessary court orders to intercept communications. However, in some cases, ~~communications service providers~~ (CSPs) may not be able to perform the interception because the technical capability to intercept communications has not been built into ~~the CSP's~~ their infrastructure. This hinders investigations that are being pursued under judicial authorization. In turn, this can prevent~~s~~ law enforcement and national security agencies from: fulfilling their mandates~~:~~ (e.g.: carrying out court orders; and obtaining critical evidence and intelligence).

Commented [LO10]: They always seek the necessary court orders to do intercept.

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Canada does not impose a general legal requirement for CSPs to have interception capabilities on their networks. Many other countries do. Australia, the United States, the United Kingdom and many other European nations require CSPs to have an interception capability. In the U.S., for example, the *Communications Assistance for Law Enforcement Act*, usually referred to as CALEA, imposes this obligation. The U.S. Federal Communications Commission (FCC) website explains CALEA.[4] Because of CALEA, traditional voice switches in the U.S. today include an intercept feature.

Formatted: Not Highlight

[4] https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Continuing the scenario from above...

The investigation has now proceeded to a point well beyond suspicion and the police have received an authorization from a judge to intercept the communications of Mr. M.

However, when the police contact the telecommunications service provider, they learn that the service provider has not built a capability to intercept communications into its infrastructure. The service provider cannot complete the work required to develop and implement this intercept capability before the authorization expires. As a result, the police miss out on obtaining key evidence, even though they had court authority to intercept the communications.

Several issues ~~need to~~must be taken into account when discussing whether to require CSPs to introduce intercept capabilities. These include the impact on privacy, the investigative needs of law enforcement and national security agencies, and how introducing requirements for intercept capabilities may affect~~s~~ the costs and competitiveness of the communications industry.

Encryption

Encryption converts a readable electronic message into an unreadable message. To decrypt the message (make it readable again), the reader must use one or more specific decryption "keys." Encryption is widely regarded as a best practice to enhance security and protect privacy online. It is commonly used to protect individual messages, personal devices and transmission channels. Secure encryption is also vital to cybersecurity, e-commerce, data and intellectual property protection, and the commercial interests of the communications industry. Canada's policy on cryptography ([redacted] established in 1998) underlines the importance of encryption to the viability, stability and growth of the economy and e-marketplace and encourages the use of encryption to protect privacy, personal information and data. Today, free encryption technologies and services are widely available. These include encryption that often operates without the users' knowledge or need to activate it. Encryption technologies may be built in to a user's communication service.

However, encryption technology also helps criminals and terrorists to avoid discovery, investigation and prosecution by making their communications unreadable to outsiders. The international availability of encryption tools and the complexities of encryption make law enforcement and national security investigations more difficult. This also poses challenges for law enforcement working with foreign partners in fighting serious international crimes, ~~including those involving foreign partners against serious international crimes~~.

It is difficult to address~~limit~~ the problematic use of encryption without also impairing ~~reducing~~ its use and benefits. As a result, very few countries have proceeded to limit encryption through the law in the interests of protecting law enforcement and national security agency capabilities. This is despite the challenges posed by encryption for law enforcement and national security agencies being well known. Encryption has been the subject of concern and discussion in many jurisdictions since the 1990s.

Formatted: Highlight
Formatted: Highlight
Formatted: Highlight
Formatted: Highlight

The United Kingdom is among the few countries to impose limits on encryption through law – in this case, the *Regulation of Investigatory Powers Act, 2000*. The Act gives legally authorized persons (such

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

as law enforcement~~, security and intelligence~~ and national security agencies) the authority to serve notices on individuals or bodies requiring the disclosure of protected (for example, encrypted) information in an intelligible form. This can be done through decryption or disclosure of encryption keys that the person is believed to hold. These provisions have attracted controversy.

s.21(1)(a)

In the 1990s, a series of legislative initiatives (sometimes referred to as "Clipper Chip" proposals) were suggested in the U.S. to impose built-in decryption capabilities. These proposals were highly controversial and attracted vigorous opposition from privacy and civil liberties groups [redacted] groups [redacted] concerned about the potential damage to industry.

None of these proposals became law. However, vigorous debate about encryption continues in the U.S., as do concerns of law enforcement about encryption. This was seen most recently in the controversy that arose when the U.S. government asked Apple to help it obtain information contained on a phone associated with the San Bernardino terrorist incident.

Continuing the scenario from above...

The police were finally able to develop intercept capability and obtain court authority again to intercept the communications of Mr. M.

To avoid having his plans discovered, however, Mr. M had encrypted his communications, which were unreadable to the police as a result. In addition, the service provider advised the police that it could not help decrypt the communications. After months of investigative delays and despite court authority to intercept the communications of Mr. M, the police cannot read them to obtain potential evidence. As a result, Mr. M's communications remain protected from law enforcement.

Even when law enforcement or national security agencies can intercept a communication, with assistance from a service provider under a court order, the data that is obtained is often unreadable due to the layers of encryption that cannot be decrypted or otherwise removed. Encryption challenges also apply to the court-ordered production of historical data, such as e-mail, text messages, photos and videos from lawfully seized smartphones, computer hard drives and other digital devices. Since encryption can be used by anyone, a private sector organization may not be able to help law enforcement and national security agencies decrypt communications because the organization might not have the technical ability to decrypt material encrypted by someone else.

No provisions specifically designed to compel decryption are found in the *Criminal Code,* the *Canadian Security Intelligence Service Act* or in other Canadian laws. In other words, there is no law in Canada designed to ~~can~~ ~~forced~~ require a person or organization to decrypt their communications.

The d~~D~~iscussion about encryption and decryption must ~~involve~~ also take into account the potential impact on the following:

- human rights, including privacy rights, freedom of expression, and the right against self-incrimination;
- the investigative needs of law enforcement and national security agencies;

s.23

Formatted: Highlight

Formatted: Highlight

Formatted: Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Commented [AA13]: Would suggest replacing "force" with "require"

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- commercial interests, such as competitiveness and the protection of intellectual property;
- how compelling decryption could weaken existing IT infrastructure models and systems;
- cybersecurity; and
- e-commerce.

Data Retention

"Data retention" refers to the general requirements to store certain elements of subscribers' telecommunications data, such as telephone numbers dialed, call length, time of call, and Internet equivalents. ~~This is done to~~ for the purpose of supporting law enforcement and national security investigations. ~~These~~ This type of data can provide key pieces of intelligence and evidence. Data retention ensures that this information will be kept for a specified period so that law enforcement and national security agencies ~~might be able to~~can obtain this information with a warrant, if required for an investigation. To date, Canada has not pursued a telecommunications data retention requirement for law enforcement and national security purposes.

Commented [LO14]: These two sentence need to be bridged together as this section isn't about data retention at large, it is about specific data retention issues related to law enforcement and national security investigations.

Continuing the scenario from above...

As part of its ongoing investigation, the police learn that Mr. M had used his mobile phone over three weeks in July 2015 to communicate with individuals linked to terrorist groups. The police seek a court order to obtain telecommunications data associated with Mr. M's mobile phone account. However, the company keeps records for business purposes only for nine months. As a result, the company has already deleted data from July 2015 and the data are not available to the police.

Parliament recently introduced *preservation* powers into the *Criminal Code* when it enacted the *Protecting Canadians from Online Crime Act*. These powers allow law enforcement agencies to seek a court order or demand the preservation of specific computer data belonging to specific persons for a brief time to assist in investigations.

However, some business practices are changing and companies are deleting data more quickly than before, sometimes before law enforcement can seek a court order for or demand preservation. This poses a new challenge. In addition, the length of time data is held varies from company to company. General data retention requirements would provide for companies to keep data for a standardized period. However, these new requirements ~~this~~ might mean that companies ~~might~~ have to store data for longer than they require ~~strictly~~ for their business purposes. Requiring data retention for a given period could also increase risks to personal information held by companies. The longer personal information is kept, the longer it is vulnerable to attack.

General requirements for data retention already exist in some foreign jurisdictions or have been proposed or debated there. In the U.S., some data retention bills have been introduced in Congress,

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

but none have been enacted. Australia recently enacted data retention requirements. On March 15, 2006, the European Union (EU) issued a Data Retention Directive (DRD) to impose data retention requirements for telecommunications data on its member states.

The DRD required that data retention be implemented through legislation enacted by EU member states at the national level. The manner of the implementation varied significantly among member states, in part because of controversy over these requirements in some states. On April 8, 2014, the Court of Justice of the European Union struck down the DRD, calling it inconsistent with privacy rights in Europe.

EU member states are now looking at their respective national laws to determine if and how their national laws on data retention need adjustment after the court decision. Some countries, such as Germany, have already introduced changes. The Federal Constitutional Court of Germany declared the country's own domestic legislation unconstitutional in March 2010. A new data retention law came into effect in Germany on January 4, 2016. The law introduced many safeguards, such as reducing the obligation to retain data from six months to ten weeks and restricting access to such data to cases involving "serious crimes" only.

Formatted: Not Highlight

Formatted: Not Highlight

The discussion of telecommunications data retention requirements ~~should~~ must also take into account several issues, including the following: the investigative needs of law enforcement and national security agencies, the impact on privacy interests and the impact on the costs and competitiveness of companies resulting from ~~by~~ data retention requirements.

What do you think?

How can the Government address challenges to law enforcement and national security investigations posed by the evolving technological landscape in a manner that is consistent with Canadian values, including respect for privacy, provision of security and the protection of economic interests?

In the physical world, if the police obtain a search warrant from a judge to enter your home to conduct an investigation, you must allow them access. Should investigative agencies operate any differently in the digital world?

Currently, investigative agencies have tools in the digital world similar to those in the physical world. As this document shows, there is concern that these tools may not be as effective in the digital world as in the physical world. Should the government update these tools to better support digital/online investigations?

Is your expectation of privacy different in the digital world than in the physical world?

Basic Subscriber Information (BSI)

Since the *Spencer* decision, police and national security agencies have had difficulty obtaining BSI in a timely and efficient manner. This has limited their ability to carry out their mandates, including law

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

enforcements's investigation of crimes. If the Government developed legislation to respond to this problem, under what circumstances should BSI (such as name, address, telephone number and e-mail address) be available to these agencies? [redacted] s.21(1)(a)

[redacted] to further an investigative lead, or in other specific situations, including clarifying emergency situations such as helping find a missing person?

Do you consider your basic identifying information identified through BSI (such as name, home address, phone number and e-mail address) to be as private as the contents of your e-mails? your personal diary? your financial records? your medical records? Why or why not?

Do you see a difference between the police having access to your name, home address and phone number, and the police having access to your Internet address, such as your IP address or e-mail address?

s.23

Interception Capability

The Government has made previous attempts to enact interception capability legislation. This legislation would have required ~~attempted to compel~~ domestic communications service providers to create and maintain networks that would be technically capable of intercepting communications if a court order authorized the interception. These ~~attempts to enact law~~ legislative proposals were controversial with Canadians. Some were concerned about privacy intrusions. As well, the Canadian communications industry was concerned about how such laws might affect it.

[redacted]

Should Canada's laws help to ensure that consistent interception capabilities are available through domestic ~~telecommunications~~ communications service provider networks when a court order authorizing the intercepting is granted by the courts?

Encryption

If the Government were to consider options to address the challenges encryption poses in ~~police~~ law enforcement and national security investigations, in what circumstances, if any, should investigators have the ability to compel individuals or companies to assist with [redacted]

Formatted: Highlight

How can law enforcement and national security agencies reduce the effectiveness of encryption for individuals and organizations involved in crime or ~~terrorist activities~~threats to Canada's security, yet not limit the beneficial uses of encryption by those not involved in illegal activities?

[redacted]

Data Retention

s.21(1)(a)

Should the law require Canadian service providers to keep telecommunications data for a certain period to ensure that it is available if ~~police~~ law enforcement and national security agencies need it for their investigations and a court authorizes access?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

If the Government ~~of Canada~~ were to enact a general data retention requirement, what type of data should be included or excluded? How long should this information be kept?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

9 August 2016

UNDER EMBARGO
Do not distribute

Our Security, Our Rights: National Security Green Paper, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

9 August 2016

UNDER EMBARGO
Do not distribute

MESSAGE FROM THE MINISTERS

A fundamental obligation of the Government of Canada is the responsibility to protect our safety and security at home and abroad. Equally fundamental is the responsibility to uphold the Constitution of Canada, and to ensure all laws respect the rights and freedoms we enjoy as people living in a free and democratic country.

When former Bill C-51, the *Anti-terrorism Act, 2015* (ATA, 2015), was tabled in the House of Commons, many Canadians voiced concern with the Government's approach to these responsibilities and whether the proposed legislation appropriately safeguards both security and rights. Those concerns have not diminished since the passage of the ATA, 2015.

The Government is committed to openness, transparency, and accountability. An early demonstration of this commitment was making public the Prime Minister's mandate letters to Ministers, so that Canadians could see our full list of priorities. Reflecting the seriousness with which the Government regards the concerns about the ATA, 2015, our mandate letters direct us to work together to repeal its problematic elements and introduce new legislation that strengthens accountability and national security. In this respect, we have made commitments to:

- guarantee that all Canadian Security Intelligence Service (CSIS) warrants comply with the *Canadian Charter of Rights and Freedoms* (the *Charter*);
- ensure all Canadians are not limited from legitimate protest and advocacy;
- enhance the redress process related to the Passenger Protect Program and address the issue of false positive matches to the list;
- narrow overly broad definitions, such as defining "terrorist propaganda" more clearly; and
- require a statutory review of the ATA, 2015 after three years.

In addition, we are establishing a statutory national security and intelligence committee of parliamentarians with broad access to classified information to examine how national security institutions are working. Further, we are also launching the Office of the community outreach and counter-radicalization coordinator to provide national coordination on preventing radicalization to violence; work with partners across communities, provinces, stakeholders and experts to ensure community resiliency; and, to develop a national strategy involving programming, policy and research.

These are our commitments thus far, but we know more can be done. We do not view this as a simple exercise of repealing some legislative provisions and enacting new ones. Our aim is to ensure that the right tools are available to law enforcement and security officials, that they are appropriate, and that they are in keeping with Canadian values.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

We consider this as an opportunity to engage you and your fellow Canadians in a discussion about certain aspects of our country's national security framework. This discussion is necessary if Canadians are to be appropriately informed about national security matters and empowered to contribute to – and influence - elements of that framework.

This Green Paper has been prepared to facilitate the process of providing us with your views. It will also serve as the foundation for the consultation that will take place in the coming months.

We sincerely hope that you will take the time to read this material and join in this discussion. We look forward to your contributions to what, we are sure you will agree, is a timely and truly important national initiative. Together we can ensure that the Government appropriately achieves a framework that upholds both security and rights.

Hon. Ralph Goodale, P.C., M.P.
Minister of Public Safety and Emergency Preparedness

Hon. Jody Wilson-Raybould, P.C., M.P.
Minister of Justice and Attorney General of Canada

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

INTRODUCTION

In Canada, we are not isolated from the terrorist threat. Since the 2001 *Anti-terrorism Act*, threats to our domestic and international security have continued to evolve.

New terrorist groups – including the so-called Islamic State of Iraq and the Levant (ISIL) – have emerged and engineered chaos and destruction in many parts of the world. Increasing numbers of Canadians have travelled to the Middle East to join terrorist organizations, including ISIL. And extremist narratives have motivated a number of Canadians to plot and pursue attacks against domestic targets.

Indeed, the principal terrorist threat to Canada remains the possibility of violent extremists carrying out attacks within our borders.

Our national security institutions share a duty to keep Canadians safe – and they do so daily. At the same time, these agencies are themselves subject to measures to keep them accountable to Canadians and ensure that the rule of law is respected.

In a world of uncertainty, risk and rapid change, do we have the tools necessary to keep people safe – and are we using all our tools in ways that also safeguard our values?

The Government urges Canadians to use this consultation process to be active partners in revamping our national security framework. We want policies that are more informed and better reflect the nature of the country we share.

Counter-terrorism efforts represent a complex and deeply charged area of public policy. People have strong perspectives and clear opinions, as they should on matters of such importance.

Each of the following chapters briefly outlines the issues at hand and gives a sense of the relevant challenges. Other documents available online – including an expanded background document – provide more detailed, technical information on issues.

You are invited and encouraged to respond online and share your views on this Green Paper and the associated documents. Your input will be welcomed until November 1, 2016 – at which point the government will begin the process of crafting new legislation, policy options and / or programs.

We have before us the opportunity to build the national security framework we want for our country – a framework that reflects Canadian values and priorities, and the nature and character of who we are and how we want to live in the world. Let us begin.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

ACCOUNTABILITY

To protect our national security, a number of government agencies are given the power to collect intelligence and enforce laws. Much of this work is very sensitive and confidential.

We must make certain that a system is in place to ensure the accountability of these agencies. That is how Canadians will know that our intelligence and law enforcement powers are being exercised with great care, in a way that respects the *Charter*.

Ministerial Oversight

In addition to the Prime Minister, two ministers in particular have important responsibilities related to national security and intelligence gathering:

The Minister of Public Safety and Emergency Preparedness is responsible for the Canada Border Services Agency (CBSA), the Canadian Security Intelligence Service (CSIS), the Royal Canadian Mounted Police (RCMP), and Public Safety Canada.

The Minister of National Defence is responsible for the Communications Security Establishment (CSE), the Department of National Defence and the Canadian Armed Forces.

All Ministers are directly accountable to Parliament for the activities of their agencies.

The Judiciary

Courts play an important role in national security.

For example, they rule on whether a warrant will be issued to allow the use of intrusive powers to investigate a threat. That is one way of ensuring that our security efforts respect the *Charter*.

The courts also examine and judge whether the methods used to secure arrests and prosecutions were justifiable and proper. And they have the authority to provide remedies in appropriate cases in relation to law enforcement misconduct.

Independent Review

There are independent, non-partisan review bodies that scrutinize the activities of certain government agencies. Their task is straightforward: to ensure that our national security and intelligence agencies operate:

- within the law; and
- in compliance with the directions set out by their Ministers.

There are three such review bodies:

- The Civilian Review and Complaints Commission (CRCC), which is responsible for reviewing the RCMP;

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- The Security Intelligence Review Committee (SIRC), which reviews CSIS;
- The Office of the Communications Security Establishment Commissioner (OCSEC), which reviews the CSE.

All three review bodies have a mandate to review activities and hear complaints. Each produces an annual public report that summarizes its activities.

Parliament

Parliament holds Ministers to account for the actions of the agencies they oversee. It also considers, debates and votes on legislation relating to national security matters.

House of Commons and Senate committees can also examine policy issues related to national security, and conduct studies of government activities and existing or proposed legislation.

Currently, most Parliamentarians do not have access to classified information, which limits their ability to fully examine national security issues. The Government has therefore committed to creating a new national security and intelligence committee made up of Parliamentarians who will be given broad access to classified material.

Agents of Parliament

Certain "agents of Parliament" have the authority to scrutinize national security activities.

The Privacy Commissioner, for instance, can examine how personal information is handled. The Information Commissioner can investigate complaints regarding access to information requests. And the Auditor General can conduct "value-for-money" audits on national security programs.

Commissions of Inquiry

Commissions can be established to impartially investigate issues of national importance. Over the past decade, three separate Commissions of Inquiry have examined certain national security agencies. The three Commissions of Inquiry are:

- The Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar;
- The Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin; and,
- The Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

PREVENTION

In recent years, we have all become familiar with the concept of "radicalization to violence." It is a process whereby a person or group of people adopts a belief or ideological position that moves them toward extremism, violence and, ultimately, to terrorist activity.

It is not a crime to be a radical, nor to have radical thoughts or ideas. But as a society, our goal must be to prevent violence of all kinds, including violence committed in the name of radical ideologies or beliefs, and activities that support such violence such as facilitation and financing.

To do this, we must better understand how and why violent radicalization typically takes root. And we must ask ourselves: What more can we do to prevent people from becoming radicalized to violence?

Here is what we know:

- Family members and friends are often the first ones aware of an individual's first steps down the path of radicalization to violence – and may be in the best position to steer them away.
- Radicalization to violence is often driven by "narratives" that reduce global events to a few simplistic ideas.
- It frequently takes place within networks and communities, both physical and virtual (the Internet often plays a critical role).
- Radicalization to violence can be incited by friends, mentors or other influential individuals.
- Association with radicalized people can influence others to adopt a similar perspective.

What Are We Currently Doing?

In the Government of Canada, a number of agencies play a role in addressing radicalization to violence:

- The RCMP trains officers on how to recognize early warning signs of radicalization. It also leads interventions in an effort to divert those on the path to violence.
- Correctional Service Canada conducts tailored interventions for individuals in prison who have radicalized to violence, or are at risk of doing so.

What More Can We Do?

The Government is dedicating $35 million over five years to create an office for community outreach and countering radicalization to violence.

Activities to be supported by this office could include:

- *Working with Communities.* Empowering local leaders to strengthen community resilience and develop early intervention programs can be an effective way of preventing radicalization to violence.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- *Youth Engagement.* Radicalization to violence is, in Canada, disproportionately common among young people - it is important to reach out and support youth in ways that are meaningful to them.
- *Alternative Narratives.* Promoting positive alternative narratives through credible voices is one way to diminish the influence of violent, radical messages.
- *Emerging Research.* By engaging academics, think tanks and other Canadians, we can collect best practices and ensure the most effective means are being used to counter radicalization to violence. Knowing what works will help inform future policy in this area.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

THREAT REDUCTION

Here is how our system has worked for the past 30 years:

- CSIS collects information on suspected threats to the security of Canada and Canadians, at home and abroad.
- CSIS advises other agencies of government – law enforcement, for example – about the threats.
- These other agencies act on the information.

When Bill C-51 (the *Anti-terrorism Act, 2015*) was passed, CSIS was given a new mandate to take direct action to reduce threats to the security of Canada. This is known as "threat reduction," or "disruption." These threats are defined in the *CSIS Act* and have remained unchanged over the past 30 years.

To be clear: CSIS cannot arrest people. But it now has the authority to take timely action to reduce a threat – disrupting financial transactions, for instance, or interfering with terrorist communications.

To investigate, CSIS needs to have reasonable grounds to *suspect* that an activity is a threat. For threat reduction measures, CSIS has a higher threshold – it must have reasonable grounds to *believe* that an activity is a threat.

All threat reduction measures must be reasonable and proportional in the circumstances, and are subject to explicit restrictions. According to direction from the Minister of Public Safety and Emergency Preparedness, CSIS must also perform a risk assessment – and consult law enforcement and other agencies, as appropriate – for each threat reduction measure.

Depending on the actions it plans to take, the law requires that CSIS might have to get a warrant to proceed, especially if the measures would potentially affect the rights of Canadians as enshrined in the *Charter*.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

9 August 2016

UNDER EMBARGO
Do not distribute

DOMESTIC NATIONAL SECURITY INFORMATION SHARING

National security threats can emerge and evolve quickly. Information must be gathered and shared among government agencies to ensure a full understanding of a potential threat, as various agencies can have different pieces of the full picture.

There are rules in place that affect the Government's authority to share information, especially information that may impact on individuals' privacy rights.

However, these rules are complex. It is sometimes difficult for one agency to know whether it can share information with another agency, and in some cases, there is no authority to share. This can affect our awareness of, and response to, an emerging national security threat.

Here is some important background: The *Privacy Act* governs the Government's management of personal information, including its collection, use and disclosure. Disclosure is not permitted without the consent of the individual to whom the information relates, other than in certain circumstances, some of which may apply to national security information sharing.

For example, the Department of Immigration, Refugees and Citizenship Canada will share with CSIS some personal information of applicants for permanent resident status in our country. This allows for more efficient and effective security screening.

The *Security of Canada Information Sharing Act*

Bill C-51 (the *Anti-terrorism Act, 2015*) created the *Security of Canada Information Sharing Act* (SCISA), which established an additional authority for national security information sharing. It provides all federal government institutions with a new, explicit authority to disclose information related to an "activity that undermines the security of Canada" to certain designated federal institutions with national security responsibilities.

Importantly, this does not include activities of protest, advocacy, dissent or artistic expression. Information about these activities cannot be disclosed under the SCISA.

000716

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

9 August 2016

UNDER EMBARGO
Do not distribute

THE PASSENGER PROTECT PROGRAM

Protecting air travellers is a key responsibility of the Government of Canada. We must also confront the threat posed by individuals who travel abroad – to countries such as Syria and Iraq – to engage in acts of terrorism.

These individuals can be involved in training, fundraising and other activities on behalf of terrorist groups such as the so-called Islamic State in Iraq and the Levant (ISIL). There is also the risk that, upon returning to Canada, these people may launch or inspire attacks here.

Under the new *Secure Air Travel Act* (SATA), which came into being with the passage of Bill C-51, the Government can use the Passenger Protect Program (PPP) – an air passenger identity screening program – to identify individuals who pose a threat to transportation security or are seeking to travel to commit certain terrorism offences.

These people are placed on what is known within the Government as "the SATA list" (casually referred to as a "No Fly List").

Individuals on this list may be subjected to a range of measures to mitigate the threat that they pose, including being denied boarding of an aircraft – or having to undergo additional screening measures.

The list must be reviewed every 90 days to ensure there are still reasonable grounds to suspect an individual poses a threat.

Anyone who is denied boarding of an aircraft has the right to apply to the Minister of Public Safety and Emergency Preparedness to be removed from the SATA list and, if unsuccessful, to appeal the decision to the Federal Court.

False positive matches sometimes occur. This can result in air travel delays. The Government has made a commitment to introduce a new, more efficient and effective redress program to address the issue of false positive name matches to the SATA list.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

9 August 2016

UNDER EMBARGO
Do not distribute

CRIMINAL CODE TERRORISM MEASURES

Since 2001, a number of people have been convicted of terrorism offences in Canada. Some have received life sentences. Our *Criminal Code* sets out a range of anti-terrorism powers for law enforcement and lists a range of terrorism-related offences.

With the *Anti-terrorism Act, 2015*, the *Criminal Code* was amended to:

- make it easier to prevent the carrying out of terrorist activity or terrorism offences;
- make it a crime to advocate or promote terrorism offences;
- give courts the power to order the seizure and forfeiture or removal of terrorist propaganda;
- give additional protection to witnesses and other participants in national security proceedings.

Let us look at each of these amendments, one by one.

Reasonable Conditions

Generally, Canadian criminal law focuses on the prosecution of offences that have already taken place. But courts can also impose reasonable conditions on an individual in an effort to reduce the risk of that person committing an offence.

When it comes to potential terrorism, law enforcement has two tools at its disposal that it may use with the approval of a judge:

- **Recognizance with conditions**, which allows police to intervene and seek to have the court impose conditions on an individual who is suspected of being connected in some way to terrorist activity.
- A **terrorism peace bond**, which is used to prevent an individual from committing a specific terrorism offence, such as leaving Canada to commit an offence for a terrorist group.

With the passage of Bill C-51, it became easier for police to apply for, and use, these two tools.

For example, the thresholds to obtain a **recognizance with conditions** was lowered to apply to instances in which law enforcement officials believe terrorist activity "may be carried out" and suspect that the recognizance "is likely to prevent" it – rather than the previous thresholds of "will be carried out" and "is necessary to prevent".

And a **terrorism peace bond** can now be issued where law enforcement believes an individual "may commit"- rather than "will commit" - a terrorism offence.

People who are subject to a **recognizance with conditions** or a **terrorism peace bond** face the possibility of detention and other restrictions on their liberty, without having been charged with, or convicted of, an offence.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Promotion of Terrorism Offences

It is now a criminal offence for a person to knowingly advocate the commission of terrorism offences in general. The individual *must know* that an offence will be committed or *be reckless* as to whether an offence may be committed as a result of what they say or write.

Seizure and Forfeiture of Terrorist Propaganda

There are two new warrants in the *Criminal Code* that allow police to seize terrorist propaganda. This is material that encourages the commission of a specific terrorism offence, or terrorism offences in general. This material can be in printed, audio or video form, or it can be in electronic form on the Internet.

Related amendments to the *Customs Tariff* also allow CBSA border services officers to seize terrorist propaganda being imported into Canada without a warrant, as they would other contraband.

Protection of Witnesses and Other Participants in the Justice System

Under the *Anti-terrorism Act, 2015*, enhanced measures are now available to protect witnesses and other participants in national security-related proceedings.

For example, judges can now order that witnesses testify behind a screen to conceal their identity, or use a pseudonym, or wear a disguise. And there is a broader range of instances under which charges can be laid against those who attempt to intimidate justice system participants.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

9 August 2016

UNDER EMBARGO
Do not distribute

PROCEDURES FOR LISTING TERRORIST ENTITIES

Formally listing an individual or group as a "terrorist entity" is a way of curtailing their support and publicizing their involvement with terrorism.

The most common method of listing is available through the *Criminal Code*. An individual or group listed as a terrorist entity under the *Criminal Code* has its funds immediately frozen, and potentially seized and forfeited.

There are currently more than 50 terrorist entities which have been listed in this way. They include al-Qaida, the Taliban, ISIL, Boko Haram and more.

How Does a Group Get Listed?

It begins with an investigation by the RCMP or CSIS. The Minister of Public Safety and Emergency Preparedness may then recommend to Cabinet that the entity be listed, so long as there are reasonable grounds to believe that the entity:

- knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity; or
- is knowingly acting on behalf of, at the direction of, or in association with an entity that has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity.

Many of Canada's closest allies keep similar lists of terrorist entities.

000720

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

9 August 2016

UNDER EMBARGO
Do not distribute

TERRORIST FINANCING

Terrorist entities raise, collect and transfer funds all over the world to finance their attacks and support their day-to-day operations. They make use of everything from the formal banking system to money service businesses, to the physical transfer of gold.

Funds are vital to these organizations – and to the violence they perpetrate. It is therefore important that we deprive them of the money they need to plan and conduct their activities.

Canada's approach to cutting off funds to terrorist groups involves 11 departments and agencies. Additionally, financial service providers – such as banks – have an obligation to know their customers, keep records and report certain transactions to help identify money laundering and terrorist financing.

Law enforcement and intelligence agencies can use some of the information from these reports to assist in their efforts to identify and disrupt terrorist activities.

A challenge faced by Canada and other advanced nations is the pace of evolution within the financial sector. It can be difficult to keep up to date as financial technology advances and new platforms emerge that could be exploited for terrorist financing.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

9 August 2016

UNDER EMBARGO
Do not distribute

INVESTIGATIVE CAPABILITIES IN A DIGITAL WORLD

We live in a digitized and highly networked world in which technological innovation is always forging ahead, advancing our quality of life, but also bringing new threats to our security.

The same technologies we enjoy and rely on everyday - smartphones, laptops and the like - can also be exploited by terrorists and other criminals to coordinate, finance and carry out their attacks or criminal activities.

[redacted]

s.21(1)(a)

[redacted]

We treasure our privacy, and rightly so, but we also expect law enforcement and national security investigators to be as effective in keeping us safe and secure in the digital world as they are in the physical world.

But our laws on how information can be properly collected and then used in court as evidence were mostly written before the rapid pace of new technology became a consideration. In the face of evolving threats, investigators worry about four main problems:

- slow and inconsistent access to basic subscriber information to help identify who was using a particular communications service at a particular time;
- the lack of a general requirement that ~~technical inability of~~ domestic telecommunications networks maintain the technical ability to intercept messages;
- the use of advanced encryption techniques ~~to~~ that can ~~"go dark" and~~ render ~~all~~ messages unreadable; and
- unreliable and inconsistent retention of communications data.

s.23

[redacted]

Let's look at each of these challenges in turn:

Basic Subscriber Information

Like looking up an address in a phone book or checking out a ~~licence~~license-plate number, ~~examining~~ access to basic subscriber information is one way for law enforcement and national security investigators to identify an individual. But Canadian court rulings,

[redacted]

Some other countries allow police and intelligence agencies to obtain basic subscriber information without going to court.

Intercept Capability

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

With legal authorization, the ability to intercept communications is a valuable tool in national security and criminal investigations. However, some communications providers are unable to comply with court orders to cooperate because they [redacted]

s.23

[redacted]

Encryption

Encryption technology is ~~another~~ tool that can be used ~~by~~ [redacted] to avoid detection, investigation and prosecution. After investigators get the proper legal authorizations and make a successful interception or seizure, the ~~messages~~ information obtained may be indecipherable due to encryption. And there is currently no legal procedure [redacted] require a person or an organization to decrypt their material [redacted]

Data Retention

"Data retention" means the storage of telecommunications information - keeping track of which telephone numbers a person dials, for example, or how long calls last. Phone and Internet records of this kind can be critical to effective investigations. But there is no general requirement for communications providers to retain this information. Some delete it almost immediately. Some use it for their own commercial purposes, and then destroy it.

These and other challenges are amplified by the fact that data moves instantaneously across national boundaries. Communications providers may offer their services in Canada, but may have no business presence here, and thus operate beyond the reach of Canadian law.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

INTELLIGENCE AND EVIDENCE

We all want to ensure that Canada's national security information is protected. Indeed, the Government has an obligation to protect sensitive sources, capabilities and techniques. At the same time, there are instances in which this information may be required for a legal proceeding.

There are existing frameworks that govern the protection and use of national security information in a range of legal proceedings. For the most part, a Federal Court judge must decide whether disclosure of the information would hurt our international relations, national security or national defence. If so, the judge must then consider whether the public interest in disclosing the information outweighs the public interest in keeping it protected.

Sometimes, this means that a criminal court may be unable to hear the national security information – and may need to rely on an unclassified summary instead. Or it could be the case that, in a civil proceeding, a plaintiff may not have full access to the information required to make their case – or a defendant may be unable to mount a full defence. This raises the question of whether justice can truly be served in these examples.

There are also implications relating to immigration proceedings, where classified information is sometimes used. A good example is what is known as a "security certificate proceeding," in which the Government makes the case that a non-citizen is inadmissible to Canada for reasons of security, violation of human or international rights, serious criminality or organized criminality.

In this case, a Federal Court judge rules on whether the certificate is reasonable. Former Bill C-51 made changes to immigration proceedings relying on classified information to shield that type of information.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

CONCLUSION

We invite all Canadians to consider the questions raised in this Green Paper – and to read the longer and more comprehensive background document, which includes greater detail and a number of scenarios that help to illustrate what is at stake as we work to improve our security and intelligence framework.

Most of all, we encourage Canadians to let their opinions, ideas and potential solutions be heard.

As a starting point, here are a few questions to consider:

1. What steps should the Government take to strengthen the accountability of Canada's national security institutions?
2. Preventing radicalization to violence helps keep our communities safe. Are there particular prevention efforts that the Government should pursue?
3. In an era in which the terrorist threat is evolving, does the Government have what it needs to protect Canadians' safety while safeguarding rights and freedoms?
4. Do you have additional ideas or comments on the topics raised in this Green Paper and in the background document?

These are just suggestions to begin the dialogue as we seek the broad and meaningful contributions of Canadians.

Invariably, views will differ. Not all of us will share the same perspective on what is justified and what is reasonable. There will be strong opinions on which tools should be made available to the Government and its security and intelligence agencies, and which should not.

But that is what we want. We want to hear your views, and the views of your fellow Canadians.

Be mindful of our two-fold objective:

- To be effective in keeping Canadians safe;
- To safeguard our values, our rights and freedoms, and the open, inclusive and democratic character of our country.

We want to carefully consider the results of the consultations as we work to make meaningful improvements to Canada's national security laws and procedures.

Respond to the Consultation Questions Online at [website].

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

9 August 2016

UNDER EMBARGO
Do not distribute

Our Security, Our Rights: National Security Green Paper, 2016

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

9 August 2016

UNDER EMBARGO
Do not distribute

MESSAGE FROM THE MINISTERS

A fundamental obligation of the Government of Canada is the responsibility to protect our safety and security at home and abroad. Equally fundamental is the responsibility to uphold the Constitution of Canada, and to ensure all laws respect the rights and freedoms we enjoy as people living in a free and democratic country.

When former Bill C-51, the *Anti-terrorism Act, 2015* (ATA, 2015), was tabled in the House of Commons, many Canadians voiced concern with the Government's approach to these responsibilities and whether the proposed legislation appropriately ~~balanced security with rights and freedoms~~safeguards both security and rights. Those concerns have not diminished since the passage of the ATA, 2015.

The Government is committed to openness, transparency, and accountability. An early demonstration of this commitment was making public the Prime Minister's mandate letters to Ministers, so that Canadians could see our full list of priorities. Reflecting the seriousness with which the Government regards the concerns about the ATA, 2015, our mandate letters direct us to work together to repeal its problematic elements and introduce new legislation that strengthens accountability and national security. In this respect, we have made commitments to:

- guarantee that all Canadian Security Intelligence Service (CSIS) warrants comply with the *Canadian Charter of Rights and Freedoms* (the *Charter*);
- ensure all Canadians are not limited from ~~lawful~~ legitimate protest and advocacy;
- enhance the redress process related to the Passenger Protect Program and address the issue of false positive matches to the list;
- narrow overly broad definitions, such as defining "terrorist propaganda" more clearly; and
- require a statutory review of the ATA, 2015 after three years.

In addition, we are establishing a statutory national security and intelligence committee of parliamentarians with broad access to classified information to examine how national security institutions are working. Further, we are also launching the Office of the community outreach and counter-radicalization coordinator to provide national coordination on preventing radicalization to violence; work with partners across communities, provinces, stakeholders and experts to ensure community resiliency; and, to develop a national strategy involving programming, policy and research.

These are our commitments thus far, but we know more can be done. We do not view this as a simple exercise of repealing some legislative provisions and enacting new ones. Our aim is to ensure that the right tools are available to law enforcement and security officials, that they are appropriate, and that they are in keeping with Canadian values.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

We consider this as an opportunity to engage you and your fellow Canadians in a discussion about certain aspects of our country's national security framework. This discussion is necessary if Canadians are to be appropriately informed about national security matters and empowered to contribute to – and influence - elements of that framework.

This Green Paper has been prepared to facilitate the process of providing us with your views. It will also serve as the foundation for the consultation that will take place in the coming months.

We sincerely hope that you will take the time to read this material and join in this discussion. We look forward to your contributions to what, we are sure you will agree, is a timely and truly important national initiative. Together we can ensure that the Government appropriately achieves a framework that upholds both security and rights.

Hon. Ralph Goodale, P.C., M.P.
Minister of Public Safety and Emergency Preparedness

Hon. Jody Wilson-Raybould, P.C., M.P.
Minister of Justice and Attorney General of Canada

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

9 August 2016

UNDER EMBARGO
Do not distribute

INTRODUCTION

In Canada, we are not isolated from the terrorist threat. Since the 2001 *Anti-terrorism Act*, threats to our domestic and international security have continued to evolve.

New terrorist groups – including the so-called Islamic State of Iraq and the Levant (ISIL) – have emerged and engineered chaos and destruction in many parts of the world. Increasing numbers of Canadians have travelled to the Middle East to join terrorist organizations, including ISIL. And extremist narratives have motivated a number of Canadians to plot and pursue attacks against domestic targets.

Indeed, the principal terrorist threat to Canada remains the possibility of violent extremists carrying out attacks within our borders.

Our national security institutions share a duty to keep Canadians safe – and they do so daily. At the same time, these agencies are themselves subject to measures to keep them accountable to Canadians and ensure that the rule of law is respected.

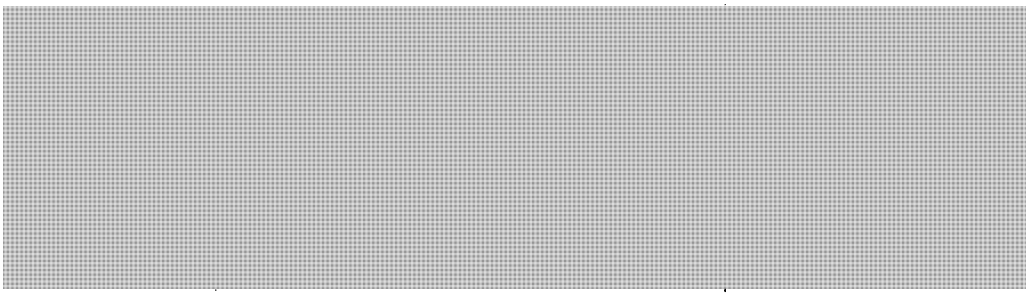
In a world of uncertainty, risk and rapid change, do we have the tools necessary to keep people safe – and are we using all our tools in ways that also safeguard our values?

The Government urges Canadians to use this consultation process to be active partners in revamping our national security framework. We want policies that are more informed and better reflect the nature of the country we share.

Counter-terrorism efforts represent a complex and deeply charged area of public policy. People have strong perspectives and clear opinions, as they should on matters of such importance.

Each of the following chapters briefly outlines the issues at hand and gives a sense of the relevant challenges. Other documents available online – including an expanded background document – provide more detailed, technical information on issues.

You are invited and encouraged to respond online and share your views on this Green Paper and the associated documents. Your input will be welcomed until November 1, 2016 – at which point the government will begin the process of crafting new legislation, policy options and / or programs.



s.21(1)(a)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

We have before us the opportunity to build the national security framework we want for our country – a framework that reflects Canadian values and priorities, and the nature and character of who we are and how we want to live in the world. Let us begin.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

ACCOUNTABILITY

To protect our national security, a number of government agencies are given the power to collect intelligence and enforce laws. Much of this work [redacted] is very sensitive and confidential.

[redacted] We must make certain that a system is in place to ensure the accountability of these agencies. That is how Canadians will know that our intelligence and law enforcement powers are being exercised with great care, in a way that respects the *Charter*.

Ministerial Oversight

In addition to the Prime Minister, Two ministers in particular have important responsibilities related to national security and intelligence gathering:

The Minister of Public Safety and Emergency Preparedness is responsible for the Canada Border Services Agency (CBSA), the Canadian Security Intelligence Service (CSIS), the Royal Canadian Mounted Police (RCMP), and Public Safety Canada.

The Minister of National Defence is responsible for the Communications Security Establishment (CSE), the Department of National Defence and the Canadian Armed Forces.

All Ministers are directly accountable to Parliament for the activities of their agencies.

The Judiciary

Courts play an important role in national security.

For example, they rule on whether a warrant will be issued to allow the use of intrusive powers to investigate a threat. That is one way of ensuring that our security efforts respect the *Charter*.

The courts also examine and judge whether the methods used to secure arrests and prosecutions were justifiable and proper. And they have the authority to provide remedies in appropriate cases in relation to law enforcement misconduct.

Independent Review

There are independent, non-partisan review bodies that scrutinize the activities of certain government agencies. Their task is straightforward: to ensure that our national security and intelligence agencies operate:

- within the law; and
- respecting in compliance with the directions set out by their Ministers.

There are three such review bodies:

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- The Civilian Review and Complaints Commission (CRCC), which is responsible for reviewing the RCMP;
- The Security Intelligence Review Committee (SIRC), which reviews CSIS;
- The Office of the Communications Security Establishment Commissioner (OCSEC), which reviews the CSE.

All three review bodies have a mandate to review activities and hear complaints. Each produces an annual public report that summarizes its activities.

Parliament

Parliament holds Ministers to account for the actions of the agencies they oversee. It also considers, debates and votes on legislation relating to national security matters.

House of Commons and Senate committees can also examine policy issues related to national security, and conduct studies of government activities and existing or proposed legislation.

Currently, most Parliamentarians do not have access to classified information, which limits their ability to fully examine national security issues. The Government has therefore committed to creating a new national security and intelligence committee made up of Parliamentarians who will be given broad access to classified material.

Agents of Parliament

Certain "agents of Parliament" have the authority to scrutinize national security activities.

The Privacy Commissioner, for instance, can examine how personal information is handled. The Information Commissioner can investigate complaints regarding access to information requests. And the Auditor General can conduct "value-for-money" audits on national security programs.

Commissions of Inquiry

Commissions can be established to impartially investigate issues of national importance. Over the past decade, three separate Commissions of Inquiry have examined certain national security agencies. The three Commissions of Inquiry are:

- The Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar;
- The Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin; and,
- The Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

PREVENTION

In recent years, we have all become familiar with the concept of "radicalization to violence." It is a process whereby a person or group of people adopts a belief or ideological position that moves them toward extremism, violence and, ultimately, to terrorist activity.

It is not a crime to be a radical, nor to have radical thoughts or ideas. But as a society, our goal must be to prevent violence of all kinds, including violence committed in the name of radical ideologies or beliefs, and activities that support such violence such as facilitation and financing.

To do this, we must better understand how and why violent radicalization typically takes root. And we must ask ourselves: What more can we do to prevent people from becoming radicalized to violence?

Here is what we know:

- Family members and friends are often the first ones aware of an individual's first steps down the path of radicalization to violence – and may be in the best position to steer them away.
- Radicalization to violence is often driven by "narratives" that reduce global events to a few simplistic ideas.
- It frequently takes place within networks and communities, both physical and virtual (the Internet often plays a critical role).
- Radicalization to violence can be incited by friends, mentors or other influential individuals.
- Association with radicalized people can influence others to adopt a similar perspective.

What Are We Currently Doing?

In the Government of Canada, a number of agencies play a role in addressing radicalization to violence:

- The RCMP trains officers on how to recognize early warning signs of radicalization. It also leads interventions in an effort to divert those on the path to violence.
- Correctional Service Canada conducts tailored interventions for individuals in prison who have radicalized to violence, or are at risk of doing so.

What More Can We Do?

The Government is dedicating $35 million over five years to create an office for community outreach and countering radicalization to violence.

Activities to be supported by this office could include:

- *Working with Communities.* Empowering local leaders to strengthen community resilience and develop early intervention programs can be an effective way of preventing radicalization to violence.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- *Youth Engagement.* Radicalization to violence is, in Canada, disproportionately common among young people - it is important to reach out and support youth in ways that are meaningful to them.
- *Alternative Narratives.* Promoting positive alternative narratives through credible voices is one way to diminish the influence of violent, radical messages.
- *Emerging Research.* By engaging academics, think tanks and other Canadians, we can collect best practices and ensure the most effective means are being used to counter radicalization to violence. Knowing what works will help inform future policy in this area.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

THREAT REDUCTION

Here is how our system has worked for the past 30 years:

- CSIS collects information on suspected threats to the security of Canada and Canadians, at home and abroad.
- CSIS advises other agencies of government – law enforcement, for example – about the threats.
- These other agencies act on the information.

When Bill C-51 (the *Anti-terrorism Act, 2015*) was passed, CSIS was given a new mandate to take direct action to reduce threats to the security of Canada. This is known as "threat reduction," or "disruption." These threats are defined in the *CSIS Act* and have remained unchanged over the past 30 years.

To be clear: CSIS cannot arrest people. But it now has the authority to take timely action to reduce a threat – disrupting financial transactions, for instance, or interfering with terrorist communications.

To investigate, CSIS needs to have reasonable grounds to *suspect* that an activity is a threat. For threat reduction measures, CSIS has a higher threshold – it must have reasonable grounds to *believe* that an activity is a threat.

All threat reduction measures must be reasonable and proportional in the circumstances, and are subject to explicit restrictions. According to direction from the Minister of Public Safety and Emergency Preparedness, CSIS must also perform a risk assessment – and consult law enforcement and other agencies, as appropriate – for each threat reduction measure.

Depending on the actions it plans to take, the law requires that CSIS might have to get ~~CSIS may require a~~ warrant to proceed, especially if the measures would potentially affect the rights of Canadians as enshrined in the *Charter*.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

9 August 2016

UNDER EMBARGO
Do not distribute

DOMESTIC NATIONAL SECURITY INFORMATION SHARING

National security threats can emerge and evolve quickly. Information must be gathered and shared among government agencies to ensure a full understanding of a potential threat, as various agencies can have different pieces of the full picture.

There are rules in place that affect the Government's authority to share information, especially information that may impact on individuals' privacy rights.

However, these rules are complex. It is sometimes difficult for one agency to know whether it can share information with another agency, and in some cases, there is no authority to share. This can affect our awareness of, and response to, an emerging national security threat.

Here is some important background: The *Privacy Act* governs the Government's management of personal information, including its collection, use and disclosure. Disclosure is not permitted without the consent of the individual to whom the information relates, other than in certain circumstances, some of which may apply to national security information sharing.

For example, the Department of Immigration, Refugees and Citizenship Canada will share with CSIS some personal information of applicants for permanent resident status in our country. This allows for more efficient and effective security screening.

The *Security of Canada Information Sharing Act*

Bill C-51 (the *Anti-terrorism Act, 2015*) created the *Security of Canada Information Sharing Act* (SCISA), which established an additional authority for national security information sharing. It provides all federal government institutions with a new, explicit authority to disclose information related to an "activity that undermines the security of Canada" to certain designated federal institutions with national security responsibilities.

Importantly, this does not include activities of protest, advocacy, dissent or artistic expression. Information about these activities cannot be disclosed under the SCISA.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

9 August 2016

UNDER EMBARGO
Do not distribute

THE PASSENGER PROTECT PROGRAM

Protecting air travellers is a key responsibility of the Government of Canada. We must also confront the threat posed by individuals who travel abroad – to countries such as Syria and Iraq – to engage in acts of terrorism.

These individuals can be involved in training, fundraising and other activities on behalf of terrorist groups such as the so-called Islamic State in Iraq and the Levant (ISIL). There is also the risk that, upon returning to Canada, these people may launch or inspire attacks here.

Under the new *Secure Air Travel Act* (SATA), which came into being with the passage of Bill C-51, the Government can use the Passenger Protect Program (PPP) – an air passenger identity screening program – to identify individuals who pose a threat to transportation security or are seeking to travel to commit certain terrorism offences.

These people are placed on what is known within the Government as "the SATA list" (~~sometimes mistakenly~~ casually referred to as a "No Fly List").

Individuals on this list may be subjected to a range of measures to mitigate the threat that they pose, including being denied boarding of an aircraft – or having to undergo additional screening measures.

The list must be reviewed every 90 days to ensure there are still reasonable grounds to suspect an individual poses a threat.

Anyone who is denied boarding of an aircraft has the right to apply to the Minister of Public Safety and Emergency Preparedness to be removed from the SATA list and, if unsuccessful, to appeal the decision to the Federal Court.

False positive matches sometimes occur. This can result in air travel delays. The Government has made a commitment to introduce a new, more ~~an~~ efficient and effective redress program to address the issue of false positive name matches to the SATA list.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

9 August 2016

UNDER EMBARGO
Do not distribute

CRIMINAL CODE TERRORISM MEASURES

Since 2001, a number of people have been convicted of terrorism offences in Canada. Some have received life sentences. Our *Criminal Code* sets out a range of anti-terrorism powers for law enforcement and lists a range of terrorism-related offences.

With the *Anti-terrorism Act, 2015*, the *Criminal Code* was amended to:

- make it easier to prevent the carrying out of terrorist activity or terrorism offences;
- make it a crime to advocate or promote terrorism offences;
- give courts the power to order the seizure and forfeiture or removal of terrorist propaganda;
- give additional protection to witnesses and other participants in national security proceedings.

Let us look at each of these amendments, one by one.

Reasonable Conditions

Generally, Canadian criminal law focuses on the prosecution of offences that have already taken place. But courts can also impose reasonable conditions on an individual in an effort to reduce the risk ~~order to prevent~~ of that person ~~from~~ committing an offence.

When it comes to potential terrorism, law enforcement has two tools at its disposal~~, upon application to the courts~~ that it may use with the approval of a judge:

- **Recognizance with conditions**, which allows police to intervene and seek to have the court impose conditions on an individual who is suspected of being connected in some way to terrorist activity.
- A **terrorism peace bond**, which is used to prevent an individual from committing a specific terrorism offence, such as leaving Canada to commit an offence for a terrorist group.

With the passage of Bill C-51, it became easier for police to apply for, and use, these two tools.

For example, the thresholds to obtain a **recognizance with conditions** was lowered to apply to instances in which law enforcement officials believe terrorist activity "may be carried out" and suspect that the recognizance "is likely to prevent" it – rather than the previous thresholds of "will be carried out" and "is necessary to prevent".

And a **terrorism peace bond** can now be issued where law enforcement believes an individual "may commit"- rather than "will commit" - a terrorism offence.

People who are subject to a **recognizance with conditions** or a **terrorism peace bond** face the possibility of detention and other restrictions on their liberty, without having been charged with, or convicted of, an offence.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Promotion of Terrorism Offences

It is now a criminal offence for a person to knowingly advocate the commission of terrorism offences in general. The individual *must know* that an offence will be committed or *be reckless* as to whether an offence may be committed as a result of what they say or write.

Seizure and Forfeiture of Terrorist Propaganda

There are two new warrants in the *Criminal Code* that allow police to seize terrorist propaganda. This is material that encourages the commission of a specific terrorism offence, or terrorism offences in general. This material can be in printed, audio or video form, or it can be in electronic form on the Internet.

Related amendments to the *Customs Tariff* also allow CBSA border services officers to seize terrorist propaganda being imported into Canada without a warrant, as they would other contraband.

Protection of Witnesses and Other Participants in the Justice System

Under the *Anti-terrorism Act, 2015*, enhanced measures are now available to protect witnesses and other participants in national security-related proceedings.

For example, judges can now order that witnesses testify behind a screen to conceal their identity, or use a pseudonym, or wear a disguise. And there is a broader range of instances under which charges can be laid against those who attempt to intimidate justice system participants.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

9 August 2016

UNDER EMBARGO
Do not distribute

PROCEDURES FOR LISTING TERRORIST ENTITIES

Formally listing an individual or group as a "terrorist entity" is a way of curtailing their support and publicizing their involvement with terrorism.

s.21(1)(a)

[redacted]-The most common method of listing is available through the *Criminal Code*. An individual or group listed as a terrorist entity under the *Criminal Code* has its funds immediately frozen, and potentially seized and forfeited.

There are currently more than 50 terrorist entities which have been listed in this way. They include al-Qaida, the Taliban, ISIL, Boko Haram and more.

How Does a Group Get Listed?

It begins with an investigation by the RCMP or CSIS. The Minister of Public Safety and Emergency Preparedness may then recommend to Cabinet that the entity be listed, so long as there are reasonable grounds to believe that the entity:

- knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity; or
- is knowingly acting on behalf of, at the direction of, or in association with an entity that has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity.

Many of Canada's closest allies keep similar lists of terrorist entities.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

9 August 2016

UNDER EMBARGO
Do not distribute

TERRORIST FINANCING

Terrorist entities raise, collect and transfer funds all over the world to finance their attacks and support their day-to-day operations. They make use of everything from the formal banking system to money service businesses, to the physical transfer of gold.

Funds are vital to these organizations – and to the violence they perpetrate. It is therefore important that we deprive them of the money they need to plan and conduct their activities.

Canada's approach to cutting off funds to terrorist groups involves 11 departments and agencies. Additionally, financial service providers – such as banks – have an obligation to know their customers, keep records and report certain transactions to help identify money laundering and terrorist financing.

Law enforcement and intelligence agencies can use some of the information from these reports to assist in their efforts to identify and disrupt terrorist activities.

A challenge faced by Canada and other advanced nations is the pace of evolution within the financial sector. It can be difficult to keep up to date as financial technology advances and new platforms emerge that could be exploited for terrorist financing ~~emerge~~.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

9 August 2016

UNDER EMBARGO
Do not distribute

INVESTIGATIVE CAPABILITIES IN A DIGITAL WORLD

We live in a digitized and highly networked world in which technological innovation is always forging ahead, advancing our quality of life, but also bringing new threats to our security.

The same technologies we enjoy and rely on everyday - smartphones, laptops and the like - can also be exploited by terrorists and other criminals to coordinate, finance and carry out their attacks or criminal activities.

[redacted]

We treasure our privacy, and rightly so, but we also expect law enforcement and national security investigators to be as effective in keeping us safe and secure in the digital world as they are in the physical world.

But our laws on how information can be properly collected and then used in court as evidence were mostly written before the rapid pace of new technology became a consideration. In the face of evolving threats, investigators worry about [redacted] four main problems:

- slow and inconsistent access to basic subscriber information to help identify who was using a particular communications service at a particular time;
- the absence of a general requirement on telecommunications service providers to have a reliable technical ~~in~~ability on~~f~~ domestic telecommunications networks to intercept messages;
- the use of advanced encryption techniques which can ~~to "go dark" and~~ render communications and information ~~all messages~~ unreadable; and
- unreliable and inconsistent retention of communications data.

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.63 cm + Indent at: 1.27 cm

s.23

[redacted]

s.21(1)(a)

[redacted]

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- ~~lack of consistent and timely access to basic subscriber information, to help identify the subscriber of a communications service;~~
- ~~lack of reliable technical intercept capability on domestic telecommunications networks;~~
- ~~diminished ability to investigate due to the use of advanced encryption;~~
- ~~lack of consistent retention of communication data.~~

~~Let us look more closely at each of these four challenges:~~

Basic Subscriber Information

Like looking up an address in a phone book or checking out a licence-plate number, access to~~examining~~ basic subscriber information is one way for law enforcement and national security investigators to identify an individual. ~~But Canadian courts~~

s.23

[redacted]

Some other countries allow police and intelligence agencies to obtain basic subscriber information without going to court.

[redacted]

Formatted: Highlight

Intercept Capability

s.23

With legal authorization, the ability to intercept communications is a valuable tool in national security and criminal investigations. However, some communications providers are unable to comply with court orders to cooperate because they

[redacted]

~~The ability to intercept communication is an essential tool in national security and criminal investigations. However, some communications providers are unable to comply with court orders because they lack the technical ability to intercept communications. Investigators can therefore miss out on key intelligence and evidence.~~

Encryption

Encryption technology is a~~nother~~ tool that can be used [redacted] to avoid detection, investigation and prosecution. After investigators get the proper legal authorizations and make a successful interception or a seizure, the information obtained~~messages~~ may be indecipherable due to

[redacted]

s.21(1)(a)

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

[redacted]

[redacted]

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

Data Retention

"Data retention" means the storage of telecommunications information - keeping track of which telephone numbers a person dials, for example, or how long calls last. Phone and Internet records of this kind can be critical to effective investigations. But there is no general requirement for communications providers to retain this information. Some delete it almost immediately. Some use it for their own commercial purposes, and then destroy it.

[redacted]

These and other challenges are amplified by the fact that data moves instantaneously across national boundaries. Communications providers may offer their services in Canada, but may have no business presence here, and thus operate beyond the reach of Canadian law.

~~These and other challenges can be amplified by the fact that data can move instantly across national borders. Communications service providers may offer services in Canada – but may have no business presence here, and therefore may fall beyond the reach of Canadian law.~~

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

INTELLIGENCE AND EVIDENCE

We all want to ensure that Canada's national security information is protected. Indeed, the Government has an obligation to protect sensitive sources, capabilities and techniques. At the same time, there are instances in which this information may be required for a legal proceeding.

There are existing frameworks that govern the protection and use of national security information in a range of legal proceedings. For the most part, a Federal Court judge must decide whether disclosure of the information would hurt our international relations, national security or national defence. If so, the judge must then consider whether the public interest in disclosing the information outweighs the public interest in keeping it protected.

Sometimes, this means that a criminal court may be unable to hear the national security information – and may need to rely on an unclassified summary instead. Or it could be the case that, in a civil proceeding, a plaintiff may not have full access to the information required to make their case – or a defendant may be unable to mount a full defence. This raises the question of whether justice can truly be served in these examples.

There are also implications relating to immigration proceedings, where classified information is sometimes used. A good example is what is known as a "security certificate proceeding," in which the Government makes the case that a non-citizen is inadmissible to Canada for reasons of security, violation of human or international rights, serious criminality or organized criminality.

In this case, a Federal Court judge rules on whether the certificate is reasonable. Former Bill C-51 made changes to immigration proceedings relying on classified information to ~~better protect~~shield that type of information.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

CONCLUSION

We invite all Canadians to consider the questions raised in this Green Paper – and to read the longer and more comprehensive background document, which includes greater detail and a number of scenarios that help to illustrate what is at stake as we work to improve our security and intelligence framework.

Most of all, we encourage Canadians to let their opinions, ideas and potential solutions be heard.

As a starting point, here are a few questions to consider:

1. What steps should the Government take to strengthen the accountability of Canada's national security institutions?
2. Preventing radicalization to violence helps keep our communities safe. Are there particular prevention efforts that the Government should pursue?
3. In an era in which the terrorist threat is evolving, does the Government have what it needs to protect Canadians' safety while safeguarding rights and freedoms?
4. Do you have additional ideas or comments on the topics raised in this Green Paper and in the background document?

These are just suggestions to begin the dialogue as we seek the broad and meaningful contributions of Canadians.

Invariably, views will differ. Not all of us will share the same perspective on what is justified and what is reasonable. There will be strong opinions on which tools should be made available to the Government and its security and intelligence agencies, and which should not.

But that is what we want. We want to hear your views, and the views of your fellow Canadians.

Be mindful of our two-fold objective:

- To be effective in keeping Canadians safe;
- To safeguard our values, our rights and freedoms, and the open, inclusive and democratic character of our country.

We want to carefully consider the results of the consultations as we work to make meaningful improvements to Canada's national security ~~efforts~~laws and procedures.

Respond to the Consultation Questions Online at [website].

000746

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Audcent, Karen

From: Potter, Jay
Sent: 2016-Aug-23 11:16 AM
To: Audcent, Karen; Belanger, Pierre-Gilles; Wong, Normand; Angers, Lucie; Sansom, Gareth
Subject: Toronto Star Op-Ed on Encryption & Self-Incrimination

In case you missed it, an op-ed piece is in today's Toronto Star that responds (unfavourably) to the recent CACP resolution on encryption.

https://www.thestar.com/opinion/commentary/2016/08/23/password-protection-a-crucial-charter-right.html

Jay

From: Audcent, Karen
Sent: August-19-16 2:51 PM
To: Belanger, Pierre-Gilles <Pierre-Gilles.Belanger@justice.gc.ca>; Wong, Normand <Normand.Wong@justice.gc.ca>; Potter, Jay <Jay.Potter@justice.gc.ca>; Thérien, Michelle <Michelle.Therien@justice.gc.ca>
Cc: Angers, Lucie <Lucie.Angers@justice.gc.ca>; Sansom, Gareth <Gareth.Sansom@justice.gc.ca>
Subject: Monday Vacation

s.19(1)

[redacted] dialling into an early AM teleconference meeting which I will [redacted] Pierre-Gilles has agreed to be acting team leader (merci Pierre-Gilles!). You can call me [redacted] if you need me. Karen

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

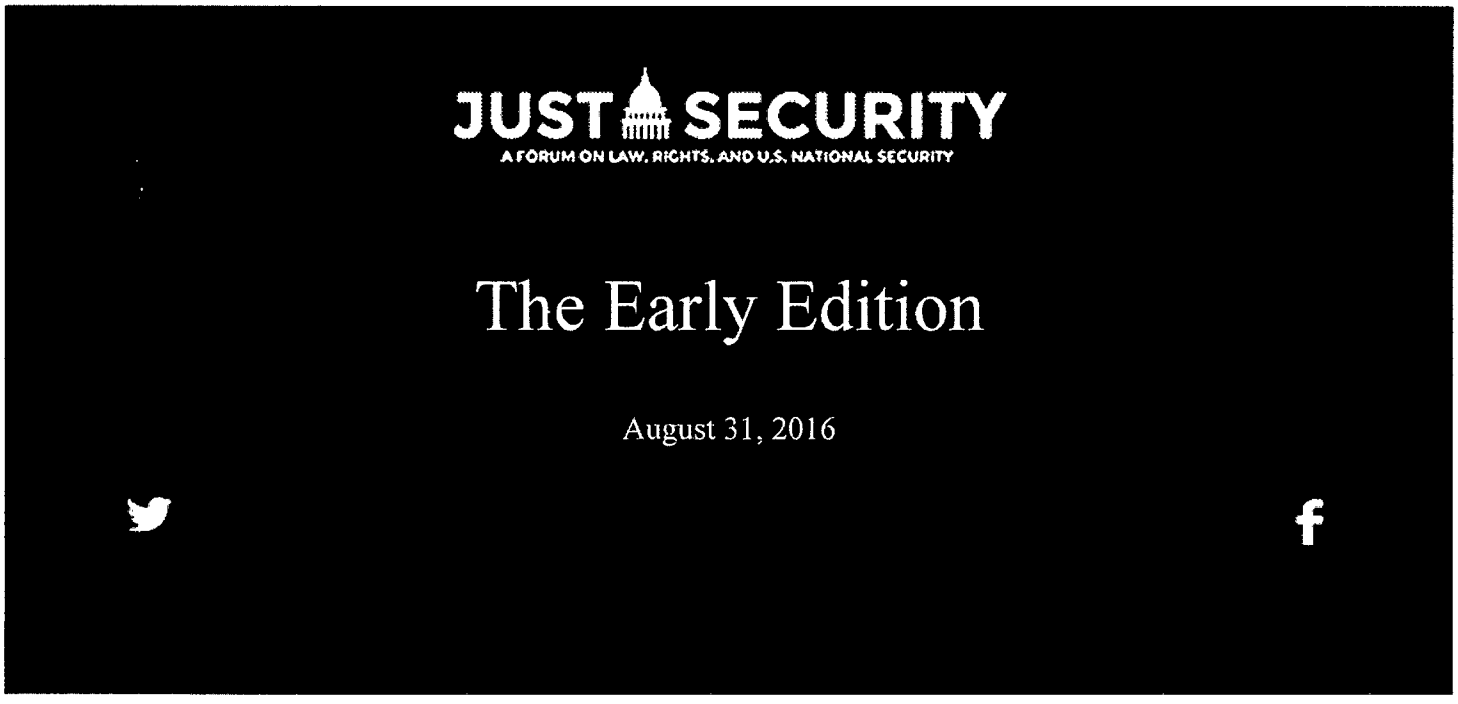
Audcent, Karen

From: Holthuis, Annemieke
Sent: 2016-Aug-31 1:16 PM
To: Audcent, Karen; Sansom, Gareth; Wong, Normand; Potter, Jay; Ram, Christopher; McKey, Erin
Cc: Angers, Lucie
Subject: "adult conversation" about encryption..

FYI - Funny choice of words but here is the article:

FBI investigators want an "adult conversation" about encryption with manufacturers of digital devices, director James Comey told a cybersecurity symposium yesterday, as legal questions over FBI access to devices such as smartphones remain unanswered following the court case earlier this year over the iPhone of one of the San Bernadino shooters, dropped when the FBI got into the phone with the help of a third party. [The Guardian]

From: Just Security [mailto:no-reply=justsecurity.org@mail96.atl11.rsgsv.net] **On Behalf Of** Just Security
Sent: Wednesday, August 31, 2016 5:02 AM
To: Holthuis, Annemieke <Annemieke.Holthuis@justice.gc.ca>
Subject: Early Edition for August 31, 2016



NEWS ROUNDUP AND NOTES :

Be sure to visit www.justsecurity.org throughout the day for the latest analysis from the Just Security *team. And now with the news:*

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

IRAQ and SYRIA

Syrian rebels and Kurdish forces have reached a "loose agreement" to cease fire, according to US officials, though Turkey's foreign ministry has insisted that Operation Euphrates Shield will continue "until the calamity of terror is not disturbing Turkish citizens." [Al Jazeera]

The US Ambassador to Ankara John Bass was reportedly summoned to Ankara by the Turkish government over Washington's statements that a loose agreement has been reached, a spokesperson for the Foreign Ministry saying the statements were "by no means acceptable" and did not "comply with the alliance relationship." [Hürriyet Daily News] State Department spokesperson John Kirby was unable to comment on this report yesterday.

The State Department denied the US is mediating the "period of calm," but said it was aware that Turkish forces had moved to the west, while Kurdish forces had moved east of the Eurphrates River, as per the insistence of Turkey and the US. Sarah El Deeb and Dusan Stojanovic report at the AP.

The Turkey-Kurdish fight may delay the US military campaign to seize Raqqa, the Islamic State's de-facto capital in Syria, suggests David Ignatius at the Washington Post. US strategy in Syria is built on the "treacherous fault line of Turkish-Kurdish enmity," and although Turkey has allowed the US to launch missions from its Incirlik airbase in support of the Kurds, its patience has frayed following its July 15 coup attempt.

The absence of US leadership in Syria has debilitating consequences even for the immediate aim of ousting the Islamic State, as well as for devising a political settlement, says the Washington Post editorial board.

Senior Islamic State strategist and spokesperson Abu Muhammad al-Adnani was killed in a US "precision strike" near Al Bab, northern Syria, Pentagon press secretary Peter Cook has confirmed. [New York Times' Eric Schmitt and Anne Barnard]

Killing leaders of terrorist organizations like the Islamic State makes little difference, scholars have found, because of two features: popular support and bureaucracy. Max Fisher reports at the New York Times.

The UN Security Council failed to agree on whether to sanction Syria for its use of chemical weapons yesterday following inspectors' determination that Assad regime forces had deployed them on at least two occasions over the past two years, reports Michael Astor at the AP. Russian Ambassador Vitaly Churkin questioned the evidence, insisting it was too soon to implement a September 2013 council resolution authorizing sanctions that can be militarily enforced for any use of chemical weapons in Syria.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The UN Security Council-mandated Joint Investigative Mechanism released its report Tuesday, finding what the panel described as "sufficient evidence" of three cases of chemical weapons use, including one by the Islamic State. Investigation head Virgina Gamba said she fears the number of parties in Syria today with the ability to make and use chemical weapons is growing.

The UN is under pressure to launch an inquiry into its Syria aid program following a Guardian investigation that revealed that millions of dollars had been awarded to people close to President Assad, report Nick Hopkins and Emma Beals.

The growing use of remote-controlled weaponry by insurgents and terrorist groups in places like Syria and Iraq has been identified in a new US Army report released last week by its Foreign Military Studies Office. Thomas Gibbons-Neff discusses the history of tele-operated weaponry at the Washington Post.

The US has offered a reward of $3 million for information on an Islamic State leader who underwent US special forces training before joining the Islamist group, reports Rebecca Kheel at the Hill.

US-led airstrikes continue. US and coalition forces carried out nine airstrikes against Islamic State targets in Syria on August 29. Separately, partner forces conducted seven strikes against targets in Iraq. [Central Command]

IRAN

The US will protect itself if a "situation" arises from "harassment" by Iranian naval ships in the Persian Gulf, the top US commander in the Middle East Army Gen. Joseph Votel warned at a press briefing yesterday. [The Hill's Kristina Wong]

President Obama's "infinite patience with global rogues" will buy him a legacy of spreading nuclear threat, writes the Wall Street Journal editorial board, berating Obama for refusing to sanction Moscow over its transfer of S-300 surface-to-air missiles to Iran, which on Sunday moved them to its Fordow nuclear facility.

CYBERSECURITY, PRIVACY and TECHNOLOGY

FBI investigators want an "adult conversation" about encryption with manufacturers of digital devices, director James Comey told a cybersecurity symposium yesterday, as legal questions over FBI access to devices such as smartphones remain unanswered following the court

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

case earlier this year over the iPhone of one of the San Bernadino shooters, dropped when the FBI got into the phone with the help of a third party. [The Guardian]

Around 30 emails related to the 2012 Benghazi attacks have been found among the 15,000 recovered by the FBI from Hillary Clinton's private account as part of its investigation into whether she or her aides mishandled classified information, the State Department confirmed yesterday. Byron Tau reports at the Wall Street Journal.

Dozens of notes from Hillary Clinton's voluntary interview during the investigation are expected to be released in the coming days, as well as the FBI's report to the Justice Department recommending no criminal charges against Clinton, reports CNN's Evan Perez and Laura Koran.

GUANTANAMO BAY

Ex-Guantánamo Bay detainee Abu Wa-el Dhiab has been deported back to Uruguay after going missing for weeks, later resurfacing in Venezuela, authorities said yesterday. [AP]

A federal appeals court has refused to halt the Guantánamo-based military commission trial of Saudi Abd al Rahim al Nashiri after he sought to challenge the commission's authority to hear his case. Nashiri, accused of orchestrating the 2000 attack on the USS Cole, argued that military commissions only have authority over offenses that took place during armed conflict. The court ordered that Nashiri must wait until the proceedings are over before raising the challenge, Sam Hananel reports at the Miami Herald.

OTHER DEVELOPMENTS

The US and India signed a landmark defense agreement yesterday that will increase military cooperation between the two nations, reports Rama Lakshmi at the Washington Post.

A video released by the Afghan Taliban depicting a US woman and her Canadian husband warning that their Taliban captors will kill them and their children unless the Kabul government halts its executions of Taliban prisoners is being evaluated by the State Department, Amir Shah reports at the AP.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

German police are interrogating a suspect following a bomb threat at Frankfurt airport this morning, they have confirmed. No suspicious items were found in the departure area following the evacuation that took place, reports Reuters.

Violations of the ceasefire agreement between Lebanon and Israel may lead to a new conflict "that none of the parties or the region can afford," the UN Security Council warned yesterday. [AP's Edith M. Lederer]

Turkey has banned 52,075 people from entering Turkey and detained 5,803 in its "fight against terrorism," Turkey's interior minister has said. [Reuters]

Nigeria's army expects to take Boko Haram's remaining strongholds in the northeast over the coming few weeks, the commander in charge of combating the jihadist group and its seven-year insurgency said today. [Reuters]

Clashes between the Philippine military and the militant group Abu Sayyaf have killed fifteen Philippine soldiers this week. The government plans to deploy thousands more soldiers to Abu Sayyaf's stronghold in the south of the country, reports Felipe Villamore at the New York Times.

Tunisian police killed two people and seized arms and an explosive belt in a dawn raid on suspected al-Qaeda-linked hideouts in the central Kasserine province this morning, reports Reuters.

Three suspected Islamic State members have been arrested for planning to attack entertainment venues and a Hindu temple outside Kuala Lumpur, according to Malaysian police. [Wall Street Journal's James Hookway]

Secretary of State John Kerry urged Pakistan to push harder against extremism within its borders today, during his second day of a visit to India, reports Reuters.

Japan's government has requested another increase in military spending, with plans to extend missile defenses that would put pressure on the nation's commitment to pacifism and on the regional arms race with China and North Korea, reports Motoko Rich at the New York Times.

China has charged US consultant Sandy Phan-Gillis with espionage after detaining her for over a year, a move that could complicate US-China ties ahead of the G-20 summit, suggests Emily Rauhala at the Washington Post.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

ICYMI: YESTERDAY ON *JUST SECURITY*

Foreign Governments, Tech Companies, and Your Data: A Response to Jennifer Daskal and Andrew Woods
by Ross Schulman and Greg Nojeim

The ICRC Updated Commentaries: Reconciling Form and Substance, Part II
by Kenneth Watkin

Copyright © 2012-2013 Just Security

Follow Just Security on Twitter or Facebook

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

This email was sent to annemieke.holthuis@justice.gc.ca

why did I get this? unsubscribe from this list update subscription preferences

Just Security · NYU School of Law; Wilf Hall · 139 MacDougal Street (5th Floor) · New York, NY 10012 · USA

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

MESSAGE FROM THE MINISTERS

When it comes to national security, the dual responsibilities of government are clear:

- We must keep Canadians safe, at home and abroad.
- In so doing, we must preserve our rights and freedoms, which help to shape the character of our open, generous and inclusive country.

We cannot enjoy our individual freedoms without effective collective security. But we must achieve that security in a manner that does not undermine the essence of that which we seek to protect – in short, the very qualities that define the country we love.

The former Bill C-51 – the *Anti-Terrorism Act, 2015* – was an important piece of legislation. It addressed certain gaps in Canada's counter-terrorism framework. But the legislation contained a number of problematic elements. Many Canadians were concerned, and remain so.

Now is the opportunity to get it right – to bring forward new initiatives and introduce new legislation that strengthens accountability, bolsters our security and further protects the rights of Canadians.

As a government, we have already pledged to deliver legislative changes and new initiatives that will:

- protect the right of Canadians to protest, demonstrate and advocate;
- ensure that security and intelligence efforts comply with the *Canadian Charter of ~~Canadian~~ Rights and Freedoms*;
- more precisely define "terrorist propaganda" to make certain we focus on genuine threats to Canadians;
- draw a clear distinction between security services and police forces;
- create a new national security committee of parliamentarians to review and scrutinize security and intelligence activities;
- launch a new national office and centere of excellence for community outreach and engagement – to better understand and prevent radicalization to violence;
- correct shortcomings in our No Fly List, while continuing to ensure air

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

travel is safe and would-be terrorists are kept from travelling to become foreign fighters.

This is only a beginning. More can be done to keep Canadians safe and to protect our democratic way of life.

This discussion paper serves as an invitation to Canadians to participate in, and contribute to, the next stage of our counter-terrorism efforts.

We want your opinions and your ideas as we work to ensure that the appropriate tools are available to our law enforcement and security officials – tools that are in keeping with Canadian values and respectful of the *Charter*.

Please read this discussion paper and the other relevant documents available online. Let us know what you think. Working together, we can better protect both our national security and the fundamental rights of all Canadians.

Hon. Ralph Goodale, P.C., M.P.
Minister of Public Safety and Emergency Preparedness

Hon. Jody Wilson-Raybould, P.C., M.P
Minister of Justice and Attorney General of Canada

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

INTRODUCTION

In Canada, we are not isolated from the terrorist threat. We are not immune to menace and tragedy. Since 2001, when Canada passed into law the *Anti-terrorism Act*, threats to our domestic and international security have continued to evolve.

New terrorist groups – including the Islamic State of Iraq and the Levant (ISIL) – have emerged and engineered chaos and destruction in many parts of the world. Increasing numbers of Canadians have traveled to the Middle East to join ISIL. And extremist narratives have inspired a number of Canadians to plot and pursue attacks against domestic targets.

Indeed, the principal terrorist threat to Canada remains the possibility of violent extremists carrying out attacks within our borders.

Our national security institutions share a duty to keep Canadians safe – and they do so daily. At the same time, these agencies are themselves subject to measures that keep them accountable to Canadians and ensure the rule of law is respected.

In a world of uncertainty, risk and rapid change, do we have the tools necessary to keep people safe – and are we using all our tools in ways that also safeguard our values?

The government urges Canadians to use this consultation process to be active partners in revamping our counter-terrorism framework. We want policies that are more informed and that better reflect the nature of the country we share.

Counter-terrorism efforts represent a complex and deeply charged area of public policy. People have strong perspectives and clear opinions, as they should on matters of such importance.

Each of the following chapters briefly outlines the issues at hand and gives a sense of the relevant challenges. Other documents available online – including an expanded version of this discussion paper – provide more detailed, technical information on issues.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.21(1)(a)

As a Canadian, you are invited and encouraged to respond online and share your views on this discussion paper and the associated documents. Your input will be welcomed until [Xxxxx, xx] – at which point the government will begin the process of crafting new legislation relating to counter-terrorism measures.

We have before us the opportunity to build the security and intelligence framework we want for our country – a framework that reflects Canadian values and priorities, and the nature and character of who we are and how we want to live in the world. Let's begin.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

ACCOUNTABILTY

To protect our national security, a number of government agencies are given the power to collect intelligence and enforce laws. Much of this work must be done in secret. That's just common sense.

But even as we preserve this secrecy, we must make certain that a system is in place to ensure the accountability of these agencies. That's how Canadians will know that our intelligence and enforcement powers are being exercised with great care, in a way that respects the *Canadian Charter of Rights and Freedoms.*

Ministerial Oversight

s.21(1)(a)

Two ministers in particular have important responsibilities related to national security and intelligence gathering:

- The Minister of Public Safety and Emergency Preparedness is responsible for a number of agencies including the Canadian Border Services Agency (CBSA), the Canadian Security Intelligence Service (CSIS), the Royal Canadian Mounted Police (RCMP) and Public Safety Canada.

- The Minister of National Defence is responsible for a number of agencies including the Communications Security Establishment (CSE), the Department of National Defence and the Canadian Armed Forces.

The Ministers are directly accountable to Parliament for the activities of their agencies.

The Judiciary

Courts play an important role in our national security.

For example, they rule on whether a warrant will be issued to allow the use of intrusive powers to investigate a threat. That's one way of ensuring that our security efforts respect the *Charter.*

The courts also examine and judge whether the methods used to secure arrests and prosecutions were justifiable and proper. And they have the

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

authority to provide remedies ~~to~~ when any citizen ~~who~~ complains of law enforcement misconduct.

Independent Review

There are independent, non-partisan review bodies that scrutinize the activities of certain government agencies. Their task is straightforward: to ensure that our national security and intelligence agencies operate:

- within the law; and
- respecting the directions set out by their Ministers.

There are three such review bodies:

- The Civilian Review and Complaints Commission (CRCC), which is responsible for reviewing the RCMP;
- The Security Intelligence Review Committee (SIRC), which reviews CSIS;
- The Office of the Communications Security Establishment Commissioner (OCSEC), which reviews the CSE.

All three review bodies have a mandate to review activities and hear complaints. Each produces an annual public report that summarizes its activities.

Parliament

Parliament holds Ministers to account for the actions of the agencies they oversee. It also considers and debates legislation on national security matters.

House of Commons and Senate committees can also examine policy issues related to national security, and conduct studies of government activities and existing legislation.

Currently, most Parliamentarians do not have access to classified information, which limits their ability to fully examine national security issues. The government has therefore committed to creating a new national security and

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

intelligence committee made up of Parliamentarians who will be given broad access to classified material.

Agents of Parliament

Certain so-called "agents of Parliament" have the authority to scrutinize national security activities.

The Privacy Commissioner, for instance, can examine how personal information is handled. The Information Commissioner can investigate complaints regarding access to information requests. And the Auditor General can conduct "value-for-money" audits on national security programs.

Commissions of Inquiry

Commissions can be established to impartially investigate issues of national importance. Over the past decade, three separate Commissions of Inquiry have examined certain national security agencies and offered recommendations in the public interest.

What Do You Think?

Should review bodies have even greater powers?

Should agencies such as the CBSA be subjected to this kind of independent review?

Does the establishment of a committee of Parliamentarians – with access to classified material – mean there is no need to create an independent review body to examine national security activities across government (an idea currently under consideration)?

These questions are a starting point. We want to know your thoughts on how best to ensure our national security agencies remain accountable.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

PREVENTION

In recent years, we have all become familiar with the concept of "radicalization to violence." It's a process whereby a person or group of people adopt a belief or ideological position that moves them toward extremism and, ultimately, to terrorist activity.

It is not a crime to be a radical, nor to have radical thoughts or ideas. But as a society, our goal must be to prevent violence committed in the name of radical ideologies or beliefs.

To do this, we must better understand how and why the terrorist impulse takes root. And we must ask ourselves: What more can we do to prevent people from becoming radicalized to violence?

What plays a role?

Here's what we know:

- Radicalization to violence is often driven by "narratives" that reduce global events to a few simplistic ideas.
- It frequently takes place within networks and communities, both physical and virtual (the Internet often plays an critical role).
- Radicalization can be incited by friends, mentors or other influential individuals.
- Association with radicalized people can influence others to adopt a similar perspective.

What are we currently doing?

There is a role to be played by a number of people and agencies in identifying and steering at-risk individuals off the path to radicalization:

- The RCMP trains officers on how to recognize early warning signs of radicalization. It also leads interventions in an effort to divert those on the path to violence.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

- Correctional Services Canada conducts tailored interventions for individuals in prison who have radicalized to violence, or are at risk of doing so.

- Family members and friends of at-risk individuals are often the first ones aware of radicalization to violence – and may be in the best position to steer these individuals off the path of potential terrorist activity.

What more can we do?

The Government is dedicating $35 million over five years to create an office for community outreach and countering radicalization to violence.

Activities to be supported by this office could include:

- *Working with Communities.* Early intervention programs run by local leaders can be an effective way of preventing radicalization to violence.

- *Youth Engagement.* Given that radicalization to violence is disproportionately common among young people, it is important to provide tailored outreach that can steer at-risk youth off the path that could lead to terrorist activity.

- *Alternative Narratives.* Promoting positive narratives through credible voices is one way to counter the influence of violent, radical messages.

- *Emerging Research.* By engaging academics, think tanks and other Canadians, we can collect best practices and ensure the most effective tactics are being used to counter radicalization to violence. Knowing what works will help inform future policy in this area.

What do you think?

What role should the government play in actively countering radicalization to violence?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

How should the government engage with communities as we work to protect security and improve prevention efforts?

How should we prioritize funding for efforts to counter radicalization to violence?

What are the most effective ways to counteract the negative ideologies?

These questions are a starting point. We want to know your thoughts on how best to prevent the radicalization to violence in Canada – and which programs the new office should pursue.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

THREAT REDUCTION

Here's how our system has worked for the past 30 years:

- The Canadian Security Intelligence Service collects intelligence on potential threats to the security of Canada and Canadians, at home and abroad.
- CSIS advises other agencies of government – law enforcement, for example – about the threats.
- These agencies act on the information.

When Bill C-51 (the *Anti-terrorism Act, 2015*) was passed, CSIS was given a new mandate to reduce threats to the security of Canada.

CSIS can now do more than simply share information about a threat – it can take direct action to reduce the danger. This is known as "threat reduction," or "disruption."

CSIS can't arrest people. But it now has the authority to take timely action to reduce a threat – disrupting financial transactions, for instance, or interfering with terrorist communications.

Depending on the actions it plans to take, CSIS may require a warrant to proceed, especially if the measures would potentially affect the rights of Canadians as enshrined in the *Charter*.

It is important to recognize that the *Charter* itself declares that our rights and freedoms are not absolute and may at times be justifiably limited. [redacted] s.23

That said, threat reduction warrants can limit the full range of *Charter* rights, not just privacy rights.

What do you think?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

What scope should CSIS have to limit or reduce the threats it identifies through intelligence gathering?

Should additional safeguards be put in place to ensure that CSIS makes responsible use of its threat reduction powers?

These questions are a starting point. We want to know your thoughts on CSIS's new mandate for threat reduction.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

DOMESTIC NATIONAL SECURITY INFORMATION SHARING

National security threats can emerge and evolve quickly. Intelligence must be gathered and shared among government agencies to ensure a full understanding of a potential threat.

There are rules in place that affect government's ability to share information, especially information about individuals. This is to ensure that privacy rights are protected.

However, these rules are complex. It is sometimes difficult for one agency to know whether it can share information with another agency. This can affect our awareness of, and response to, an emerging national security threat.

Here's some important background: Under the *Privacy Act*, the personal information of Canadians is protected. Government must follow rules on how to collect, retain and disclose this information. But there are some exceptions that allow government to share information in certain instances, especially as it relates to national security.

For example, the Department of Immigration, Refugees and Citizenship Canada will share with CSIS some personal information of applicants for permanent resident status in our country. This allows for a more efficient and effective method of security screening.

The *Security of Canada Information Sharing Act*

Formatted: Font: Italic

When Bill C-51(the *Anti-terrorism Act, 2015*) was passed, a new process was established for national security information sharing. It provides greater clarity about when information can be disclosed.

The *Security of Canada Information Sharing Act* (SCISA) gives all federal institutions the power to disclose information related to "activities that undermine the security of Canada." Importantly, this does not include activities such as lawful protest, advocacy or dissent. Information about these activities cannot be disclosed under the SCISA.

Formatted: Font: Italic

Another important fact: Information sharing practices under the SCISA can be reviewed. For instance, the Privacy Commissioner can examine the handling

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

of personal information to hold institutions accountable and ensure *Charter* rights have been respected.

What do you think?

Is there more the government can do to reinforce the fact that lawful protest and advocacy is permitted and that these activities do not fall with the definition of "activity that undermines the security of Canada?"

Should the Privacy Commissioner be mandated to deliver an annual public report on information disclosed under the SCISA?

These questions are a starting point. We want to know your thoughts on how information is shared under the *Security of Canada Information Sharing Act.*

Formatted: Font: Italic

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

THE PASSENGER PROTECT PROGRAM

Protecting air travelers is a key responsibility of government. We must also confront the threat posed by individuals who travel abroad – to countries such as Syria and Iraq – to engage in acts of terrorism.

These individuals can be involved in training, fundraising and other activities on behalf of terrorist groups such as the Islamic State in Iraq and the Levant (ISIL). There is also the risk that, upon returning to Canada, these people may launch or inspire attacks here.

Under the new *Secure Air Travel Act* (SATA), which came into being with the passage of Bill C-51, government can use the Passenger Protect Program (PPP) – an air passenger identity screening program – to identify individuals who pose a threat to transportation security or are seeking to travel to commit terrorism offences.

Formatted: Font: Italic

These people are placed on what's known within government as "the SATA list" – but is perhaps better understood as a "No Fly List."

Individuals on this list are denied the right to board an aircraft – or forced to undergo additional screening. The listing process is conducted confidentially and is based on intelligence and other information from investigations. The list is reviewed every 90 days to ensure there are still reasonable grounds to suspect an individual.

Anyone who is denied the right to board an aircraft has the right to apply to be removed from the No Fly List and, if unsuccessful, to appeal the decision to the Federal Court.

False positive matches sometimes occur. This can result in air travel delays. The government has made a commitment to enhance the current redress process and make it more reliable and efficient.

What do you think?

We want to know your thoughts on how the No Fly List list is managed, and what more can be done to mitigate the impact of false matches.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

CRIMINAL CODE TERRORISM MEASURES

Since 2001, a number of people have been convicted of terrorism offences in Canada. Some have received life sentences. Our *Criminal Code* sets out a range of anti-terrorism powers for law enforcement and lists a range of terrorism-related offences.

With the *Anti-terrorism Act, 2015*, the *Criminal Code* was amended to:

- make it easier to temporarily detain an individual to prevent the carrying out of terrorist activity;
- make it a crime to advocate or promote a terrorist act;
- give courts the power to order the seizure and forfeiture of terrorist propaganda;
- give additional protection to witnesses and other participants in national security proceedings.

Let's look at each of these amendments, one by one.

Temporary Detention

Generally, Canadian criminal law focuses on the prosecution of offences that have already taken place. But courts can also impose what are known as "preventative conditions" on an individual, so long as there is evidence that the person is likely to commit an offence.

When it comes to potential terrorism, courts have two tools at their disposal:

- **Recognizance with conditions**, which allows police to intervene when an individual is suspected of being connected in some way to terrorist activity.
- A **terrorism peace bond**, which is used to prevent an individual from committing a specific terrorism offence, such as leaving Canada to commit an offence for a terrorist group.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

With the passage of Bill C-51, it became easier for police to apply for, and use, these two tools.

For example, the threshold to obtain a **recognizance with conditions** was lowered to apply to instances in which law enforcement officials believe terrorist activity "may be carried out" – rather than the previous "will be carried out."

And a **terrorism peace bond** can now be issued where law enforcement believes an individual "may commit" a terrorism offence – rather than "will commit."

People who are subject to **recognizance with conditions** or a **terrorism peace bond** face the possibility of detention and other restrictions on their liberty, without having been charged with, or convicted of, an offence.

Promotion of Terrorism

It is now a criminal offence for a person to knowingly advocate the commission of terrorist acts in general. The individual *must know* that an offence will be committed or *be reckless* as to whether an offence may be committed as a result of what they say or write.

The maximum penalty is five years' imprisonment.

It is important to note that this offence is directed exclusively at prohibiting the *active encouragement* of the *commission of terrorism offences*. It's not about mere expressions of opinion regarding the acceptability of terrorism.

Seizure and forfeiture of terrorist propaganda

There are two new warrants in the *Criminal Code* that allow police to seize terrorist propaganda. Terrorist propaganda ~~his~~ is material that encourages the commission of a specific terrorist act, or terrorist offences in general. This allows for the seizure of material ~~can be~~ in printed or audio form, or in ~~it can be in~~ electronic form that is made available to the public through a Canadian service provider on the Internet.

Protection of witnesses and other participants in the justice system

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Under the *Anti-terrorism Act, 2015*, enhanced measures are now available to protect witnesses and other participants in terrorism-related proceedings.

For example, judges can now order that witnesses testify behind a screen to conceal their identity, or use a pseudonym, or wear a disguise. And there are broader instances under which charges can be laid against those who attempt to intimidate justice system participants.

What do you think?

Should it be harder or easier to obtain **recognizance with conditions** or a **terrorism peace bond**?

Should those who use propaganda to promote terrorism offences in general be charged with a crime?

These questions are a starting point. We want to know your thoughts on anti-terrorism measures as included in the *Criminal Code*.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

TERRORIST ENTITY LISTING PROCEDURES

Formally listing an individual or group as a "terrorist entity" is a way of curtailing their support and publicizing their involvement with terrorism.

Right now, there are three ways a terrorist entry may be listed in Canada. The most common method is available through the *Criminal Code*. A group listed as a terrorist entity under the *Criminal Code* has its funds immediately frozen, and potentially seized and forfeited.

There are currently more than 50 terrorist entities who have been listed in this way. They include al-Qaida, the Taliban, ISIL, Boko Haram and more.

How does a group get listed?

It begins with an investigation by RCMP or CSIS. The Minister of Public Safety and Emergency Preparedness may then recommend to Cabinet that the entity be listed, so long as there are reasonable grounds to believe that the group:

- knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity; or

- is knowingly acting on behalf of, at the direction of, or in association with an entity that has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity.

Many of Canada's closest allies keep similar lists of terrorist entities.

What do you think?

How does the current process of listing terrorist entities help Canada meet its domestic needs and international obligations?

Most listed entities are groups that originated overseas. How should Canada focus its listing activities in the future?

These questions are a starting point. We want to know your thoughts on the formal listing of terrorist groups and individuals.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

TERRORIST FINANCING

Terrorist entities raise, collect and transfer funds all over the world to finance their attacks and support their day-to-day operations. They make use of everything from the formal banking system to money service outlets to the physical transfer of gold.

Individuals also finance terrorist activities by raising money on their own behalf to travel abroad for terrorist purposes, or to purchase materials for an attack.

Funds are vital to these organizations. It is therefore important that we deprive them of the money they need to plan and conduct their activities.

This is a goal shared by countries around the world. For example, one of the five priorities of the Global Coalition against ISIL is to diminish the group's capabilities by cutting off its funding.

Canada's approach to cutting off funds to terrorist groups involves 11 departments and agencies. Additionally, financial service providers – such as banks – have an obligation to know their customers and report transactions over $10,000 to help identify money laundering and terrorist financing.

Law enforcement and intelligence agencies can use this information to assist in their efforts to identify and disrupt terrorist activities.

Looking beyond our borders, Canada is an active member of the Financial Action Task Force, an international organization that sets standards in the fight against money laundering and terrorist financing. We also support developing regions that are at a high risk for terrorist financing, helping countries in the Middle East and North Africa maintain the integrity of their financial systems.

A challenge faced by Canada and other advanced nations is the pace of evolution within the financial sector. It can be difficult to keep up to date as financial technology advances and new platforms for terrorist financing emerge.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Another challenge: Terrorist supporters often transfer funds below the $10,000 threshold, which means the financing goes unreported.

This is one of the ways in which terrorists exploit gaps to avoid detection.

What do you think?

What changes could be made to ensure counter-terrorist financing measures are more effective?

What additional measures could the government undertake to improve its ability to cut off terrorist financing?

These questions are a starting point. We want to know your thoughts on how terrorist financing should be further curtailed.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

INVESTIGATIVE CAPABILITIES IN A DIGITAL WORLD

We live in a highly networked world where technological innovation is always forging ahead, bringing great advancements to our quality of life but also evolving threats to our security.

The same technologies we enjoy and rely on everyday – smartphones, laptop computers and the like – can be exploited by terrorists to coordinate, finance and conduct their attacks.

Digital devices allow terrorists to buy equipment, send encrypted messages and radicalize individuals to violence.

Our national intelligence investigators must therefore be able to work as effectively in the digital world as they do in the physical world.

To make that possible, we need to ensure that our laws for the collection of intelligence and evidence keep up with the pace of technology. For instance, our current investigative capability can be impeded by:

- lack of consistent and timely access to basic subscriber information, to help identify the subscriber to a communications service;
- lack of reliable technical intercept capability on domestic telecommunications networks;
- diminished ability to investigate due to the use of advanced encryption;
- lack of consistent retention of communication data.

Let's look more closely at each of these four challenges:

Basic subscriber information. This is a way for law enforcement officials to use a communications subscription (to an Internet provider, for instance) to identify an ~~otherwise anonymous~~ individual. ~~But court rulings have made i~~It has become increasingly difficult to access this information in a timely and effective manner, in part as a result of privacy concerns arising from some court rulings. Many countries allow police and intelligence agencies to access basic subscriber information without going to court.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Intercept capability. Investigations into national security threats can be strengthened by the interception of private communications (with court approval). However, police may be unable to execute authorizations from the court as some communications providers ~~are unable to comply with these court orders because they~~ lack the technical ability to intercept communications. Investigators can therefore miss out on key evidence.

Encryption. Encryption technology gives terrorists an additional way to avoid discovery, investigation and prosecution. Often, even when law enforcement is able to intercept communications, the messages are protected and unreadable. Currently, there is no legal mechanism designed~~way~~ to force a person or organization to decrypt their communications.

Data retention. This term refers to the storage of telecommunication information – keeping track of which telephone numbers a person dialed, for instance, or how long the calls lasted. Phone and Internet data of this kind can be useful in intelligence and evidence gathering.

However, there is currently no ~~widespread~~ requirement for communications providers to retain this information for law enforcement and national security purposes. Some delete it very quickly.

The government recently enacted what's known as "preservation" powers in the *Criminal Code*. This gives law enforcement the power ~~to seek a court order~~ to preserve specific computer data belonging to a specific person, in essence a "do not delete" order, for a brief period of time to help with an investigation, and the length of time could be extended with a court order.

These and other challenges can be amplified by the fact that cyberspace is not easily bound by national borders. Communications service providers may offer services in Canada – but may have no business presence here, and therefore may fall beyond the reach of Canadian law.

What do you think?

How can Canada address the challenges posed by the rapidly evolving technological landscape in a manner that respects privacy rights and is consistent with Canadian values?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

s.23

Should our expectation of privacy be different in the digital world?

Should investigators have the ability to identify suspects in a timely and effective manner?

Should Canada compel communications providers to have interception capability on their networks, as is the case in the United States, United Kingdom, Australia and other countries?

Should investigators have the power to compel individuals or companies to assist in decrypting messages?

Should service providers be required by law to keep phone and Internet data for a fixed period of time to potentially aid in criminal and terrorism investigations?

These questions are a starting point. We want to know your thoughts on how best to enhance our digital investigative capabilities.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

INTELLIGENCE AND EVIDENCE

We all want to ensure that Canada's national security information is protected. Indeed, the government has an obligation to protect sensitive sources, capabilities and techniques. At the same time, there are instances in which this information may be required for a legal proceeding.

There is an existing framework that governs the use of national security information in a range of legal proceedings. In essence, a federal judge must decide whether disclosure of the information would hurt our international relations, national security or national defence. If so, the judge must then consider whether the public interest in disclosing the information outweighs the public interest in keeping it protected.

Sometimes, this means that a criminal court may be unable to hear the national security information – and may need to rely on an unclassified summary instead. Or it could be the case that, in a civil proceeding, a plaintiff may not have full access to the information required to make its case – or a defendant may be unable to fully defend itself. This raises the question of whether justice can truly be served in these examples.

There are also implications relating to immigration decisions, which are sometimes made based on classified information. A good example is the so-called "security certificate proceeding," in which government makes the case that a person is inadmissible to Canada for reasons of security, violation of human or international rights, serious criminality or organized criminality.

In this case, a federal judge rules on whether the certificate is reasonable.

What do you think?

How can the government ensure an appropriate balance between protecting national security and respecting the principles of justice?

How do we properly balance the need for secrecy with the accused's right to know the source of the case against him?

Commented [KA5]: Need to fix this sentence so it refers to a balance between two things – this is one possible way to frame the missing idea.

Are we currently assuring both fairness and security in legal proceedings that involve classified material?

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

Are there any non-legislative measures that could improve both the use and protection of national security information in legal proceedings?

These questions are simply a starting point. We want to know your thoughts on how to navigate the challenging terrain of intelligence and evidence.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

CONCLUSION

We invite all Canadians to consider the questions raised in this discussion paper – and to read the longer and more comprehensive version of the Counter-Terrorism Green Paper, which includes greater detail and a number of scenarios that help to illustrate what's at stake as we work to improve our security and intelligence framework.

Most of all, we encourage Canadians to let their opinions, ideas and potential solutions be heard.

Invariably, views will differ. Not all of us will share the same perspective on what is justified and what is reasonable. There will be strong opinions on which tools should be made available to government and its security and intelligence agencies.

But that's what we want. We want to hear your views, and the views of your fellow Canadians.

We want to carefully consider the impact of each potential measure as we work to make meaningful and long-lasting improvements to Canada's counter-terrorism efforts.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

For BSI

To be inserted at page 46 of 60, under the second last paragraph beginning "As a result, criminal investigations..." and ending "...and respect privacy interests." The following text would replace the last para on page 46 of 60, which begins "Many foreign jurisdictions..." and ends "...obtained and how it is to be provided."

Many foreign jurisdictions have provision in law that specifically permit law enforcement and national security agencies access to BSI, in many cases without prior judicial authorization. These jurisdictions include, but are not limited to, the United States, the United Kingdom, Australia, Germany, Sweden, Ireland, Denmark, Spain, Finland, the Netherlands and Norway. The laws in these jurisdictions may however place certain limits on the type of BSI that can be obtained and how it can be obtained. For example, in the United States and in the Netherlands, prosecutors are involved in the process to obtain some types of BSI. An order from a judge for access to BSI is required in some situations such as for BSI when it is stored as part of a data retention requirement in Finland or when access is needed by intelligence agencies in Spain. While BSI is available administratively, without prior judicial authorization, in Australia, Ireland, the Netherlands, the United Kingdom, Norway and the United States, an order from a judge is needed for certain BSI identifiers in some places, such as for IP addresses in Germany and Denmark and for a certain cell phone identifier (IMEI) in Sweden. Other limitations on access seen in other countries' laws include requirements for senior police officers to approve some requests, seen in Ireland and in Finland, and limiting access to certain types of crime, which is done in Ireland, and in Finland and Sweden in some cases (for certain cell phone identifiers).

For Intercept Capability

To be inserted on page 47 of 60, after the first para after the box that begins "In some cases, where..." and ends "...built into the infrastructure." It will replace the second para after the box, that begins "This means that investigations..." and ends "...on their networks."

This means that investigations that are being pursued under judicial authorization are being impacted, which is affecting law enforcement and national security agencies' ability to achieve their individual mandates. Canada does not have a general requirement for CSPs to have interception capability on their networks. These requirements are in place in many other countries. Australia, the United States, the United Kingdom and other European nations require that CSPs have an interception capability.

An example of these requirements can be seen in the United States legislation entitled the *Communications Assistance for Law Enforcement Act*, usually referred to as CALEA. The US Federal Communications Commission (FCC) website provides the following information to describe CALEA:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

> In response to concerns that emerging technologies such as digital and wireless communications were making it increasingly difficult for law enforcement agencies to execute authorized surveillance, Congress enacted CALEA on October 25, 1994. CALEA requires a "telecommunications carrier," as defined by the CALEA statute, to ensure that equipment, facilities, or services that allow a customer or subscriber to "originate, terminate, or direct communications," enable law enforcement officials to conduct electronic surveillance pursuant to court order or other lawful authorization. CALEA is intended to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment design and modify their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities as communications network technologies evolve. Communications services utilizing Circuit Mode equipment and facilities, and communications services utilizing packet mode are all subject to CALEA. In May 2006, the FCC issued a Second Report and Order also requiring facilities-based broadband Internet access providers and providers of interconnected Voice over Internet Protocol (VoIP) service to come into compliance with CALEA obligations no later than May 14, 2007.
>
> ....
>
> A telecommunications carrier may comply with CALEA in different ways. First, the carrier may develop its own compliance solution for its unique network. Second, the carrier may purchase a compliance solution from vendors, including the manufacturers of the equipment it is using to provide service. Third, the carrier may purchase a compliance solution from a trusted third party (TPP). See CALEA Second Report and Order at para. 26.

As a result of this legislation, in the US today, traditional voice switches have an intercept feature included.

For Encryption

Text to be added at page 48 of 60, following the para beginning "Encryption technology does, however..." and ending "...availability of encryption tools."

Given the challenges inherent in limiting problematic use without negatively impacting its benefits, very few countries around the world have imposed limitations on the use of encryption through the law in the interests of protecting law enforcement and national security agency capabilities. This is despite the fact that the challenges posed by encryption for law enforcement and national security agencies are well known and have been the subject of concern and discussion in many jurisdictions since the 1990s. The United Kingdom is one of the few countries that has imposed some limitations in legislation in relation to the use of encryption to assist law enforcement, and these requirements have attracted controversy since their enactment. In the 1990s, the United States put forward a series of legislative initiatives (sometimes referred to as "Clipper Chip" proposals) designed to impose built-in decryption capabilities. These proposals were highly controversial and attracted vigorous opposition and criticism from the perspective of privacy and civil liberties as well as from the perspective of the potential

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

negative impact on industry given the protection provided by encryption. None of these legislative proposals were enacted; however, concerns of law enforcement in relation to encryption and the vigorous debate around these issues in the United States continues to take place, most recently seen in the controversy arising from the request by the US government to Apple for assistance with a phone associated with the San Bernardino terrorist incident.

For Data Retention

To be added to the text of the third paragraph after the box on page 49 of 60, which is only one sentence as present that reads "General requirements for data retention currently exist in some foreign jurisdictions, or have been proposed or debated." The paragraph would be expanded to include the following:

In the United States, some bills to enact data retention have been brought forward for consideration by federal legislators, but these requirements have never been enacted. Australia recently enacted data retention requirements. On March 15, 2006, the European Union imposed data retention requirements with respect to telecommunications data on all its member states, through a Data Retention Directive (DRD). The DRD required that data retention be implemented through legislation enacted by European Union member states at the national level. The manner of the implementation varied significantly between jurisdictions, in part in response to controversy in relation to these requirements at the national level in some jurisdictions. The DRD was struck down on April 8, 2014 by the Court of Justice of the European Union as being inconsistent with privacy rights in Europe. European Union member states are now looking at their respective national laws to determine if and how their national laws on data retention should be amended to respond to this decision to strike down the DRD. Some countries, such as Germany, have already introduced changes. The Federal Constitutional Court of Germany declared their own domestic legislation unconstitutional in March 2010. A new data retention law came into effect in Germany on January 4, 2016 which introduced many safeguards such as reducing retention from six months to ten weeks and restricting access to such data to "serious crimes" only.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

For BSI

To be inserted at page 46 of 60, under the second last paragraph beginning "As a result, criminal investigations..." and ending "...and respect privacy interests." The following text would replace the last para on page 46 of 60, which begins "Many foreign jurisdictions..." and ends "...obtained and how it is to be provided."

Many foreign jurisdictions have provision in law that specifically permit law enforcement and national security agencies access to BSI, in many cases without prior judicial authorization. These jurisdictions include, but are not limited to, the United States, the United Kingdom, Australia, Germany, Sweden, Ireland, Denmark, Spain, Finland, the Netherlands and Norway. The laws in these jurisdictions may however place certain limits on the type of BSI that can be obtained and how it can be obtained. For example, in the United States and in the Netherlands, prosecutors are involved in the process to obtain some types of BSI. An order from ~~an~~ judge for access to BSI is required in some situations such as for BSI when it is stored as part of a data retention requirement in Finland or when access is needed by intelligence agencies in Spain. While BSI is available administratively, without prior judicial authorization, in Australia, Ireland, the Netherlands, the United Kingdom, Norway and the United States, an order from a judge is needed for certain BSI identifiers in some places, such as for IP addresses in Germany and Denmark and for a certain cell phone identifier (IMEI) in Sweden. Other limitations on access seen in other countries' laws include requirements for senior police officers to approve some requests, seen in Ireland and in Finland, and limiting access to certain types of crime, which is done in Ireland, and in Finland and Sweden in some cases (for certain cell phone identifiers).

For Intercept Capability

To be inserted on page 47 of 60, after the first para after the box, that begins "In some cases, where..." and ends "...built into the infrastructure." It will replace the second para after the box, that begins "This means that investigations..." and ends "...on their networks."

This means that investigations that are being pursued under judicial authorization are being impacted, which is affecting law enforcement and national security agencies' ability to achieve their individual mandates. Canada does not have a general requirement for CSPs to have interception capability on their networks. These requirements are in place in many other countries. Australia, the United States, the United Kingdom and other European nations require that CSPs have an interception capability.

An example of these requirements can be seen in the United States legislation entitled the *Communications Assistance for Law Enforcement Act*, usually referred to as CALEA. The US Federal Communications Commission (FCC) website provides the following information to describe CALEA:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

> In response to concerns that emerging technologies such as digital and wireless communications were making it increasingly difficult for law enforcement agencies to execute authorized surveillance, Congress enacted CALEA on October 25, 1994. CALEA requires a "telecommunications carrier," as defined by the CALEA statute, to ensure that equipment, facilities, or services that allow a customer or subscriber to "originate, terminate, or direct communications," enable law enforcement officials to conduct electronic surveillance pursuant to court order or other lawful authorization. CALEA is intended to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment design and modify their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities as communications network technologies evolve. Communications services utilizing Circuit Mode equipment and facilities, and communications services utilizing packet mode are all subject to CALEA. In May 2006, the FCC issued a Second Report and Order also requiring facilities-based broadband Internet access providers and providers of interconnected Voice over Internet Protocol (VoIP) service to come into compliance with CALEA obligations no later than May 14, 2007.
>
> ....
>
> A telecommunications carrier may comply with CALEA in different ways. First, the carrier may develop its own compliance solution for its unique network. Second, the carrier may purchase a compliance solution from vendors, including the manufacturers of the equipment it is using to provide service. Third, the carrier may purchase a compliance solution from a trusted third party (TPP). See CALEA Second Report and Order at para. 26.

As a result of this legislation, in the US today, traditional voice switches have an intercept feature included.

For Encryption

Text to be added at page 48 of 60, following the para beginning "Encryption technology does, however..." and ending "...availability of encryption tools."

Given the challenges inherent in limiting problematic use without negatively impacting its benefits, very few countries around the world have imposed limitations on the use of encryption through the law in the interests of protecting law enforcement and national security agency capabilities~~,~~. This is despite the fact that ~~although~~ the challenges posed by encryption for law enforcement and national security agencies are well known and have been the subject of concern and discussion in many jurisdictions since the 1990s. The United Kingdom is one of the few countries that has imposed some limitations in legislation in relation to the use of encryption to assist law enforcement, and these requirements have attracted controversy since their enactment. In the 1990s, t~~T~~he United States put forward ~~in the 1990s~~ a series of legislative initiatives (sometimes referred to as "Clipper Chip" proposals) designed to impose built-in decryption capabilities. These proposals were highly controversial and attracted vigorous opposition and criticism from the perspective of privacy and civil liberties as well as from the perspective of the

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

potential ~~for a~~ negative impact on industry ~~and~~ given the protection provided by encryption. None of these legislative proposals were enacted~~,~~; however, concerns of law enforcement in relation to encryption and the vigorous debate around these issues in the United States continues to take place, most recently seen in the controversy arising from the request by the US government to Apple for assistance with a phone associated with the San Bernardino terrorist incident.

For Data Retention

To be added to the text of the third paragraph after the box on page 49 of 60, which is only one sentence as present that reads "General requirements for data retention currently exist in some foreign jurisdictions, or have been proposed or debated." The paragraph would be expanded to include the following:

In the United States, some bills to enact data retention have been brought forward for consideration by federal legislators, but these requirements have never been enacted. Australia recently enacted data retention requirements. ~~The~~ On March 15, 2006, the European Union ~~had, until recently,~~ imposed data retention requirements with respect to telecommunications data on all its member states, through a Data Retention Directive (DRD). The DRD required that data retention be implemented through legislation enacted by European Union member states at the national level. The manner of the implementation varied significantly between jurisdictions, in part in response to controversy in relation to these requirements at the national level in some jurisdictions. The DRD was ~~recently~~ struck down on April 8, 2014 by ~~a European court~~the Court of Justice of the European Union as being inconsistent with ~~European privacy requirements~~"fundamental rights to respect for private life". European Union member states are now looking at their respective national laws to determine if and how their national laws on data retention should be amended to respond to this decision to strike down the DRD. Some countries, such as Germany, have already introduced changes. The Federal Constituitional Court of Germany declared their own domestic legislation unconstitutional in March 2010. A new data retention law came into effect on January 4, 2016 which introduced many safe guards such as reducing retention from six months to ten weeks and restricting access to such data to "serious crimes" only.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

For BSI

To be inserted at page 46 of 60, under the second last paragraph beginning "As a result, criminal investigations..." and ending "...and respect privacy interests." The following text would replace the last para on page 46 of 60, which begins "Many foreign jurisdictions..." and ends "...obtained and how it is to be provided."

Many foreign jurisdictions have provision in law that specifically permit law enforcement and national security agencies access to BSI, in many cases without prior judicial authorization. These jurisdictions include, but are not limited to, the United States, the United Kingdom, Australia, Germany, Sweden, Ireland, Denmark, Spain, Finland, the Netherlands and Norway. The laws in these jurisdictions may however place certain limits on the type of BSI that can be obtained and how it can be obtained. For example, in the United States and in the Netherlands, prosecutors are involved in the process to obtain some types of BSI. An order from an judge for access to BSI is required in some situations such as for BSI when it is stored as part of a data retention requirement in Finland or when access is needed by intelligence agencies in Spain. While BSI is available administratively, without prior judicial authorization, in Australia, Ireland, the Netherlands, the United Kingdom, Norway and the United States, an order from a judge is needed for certain BSI identifiers in some places, such as for IP addresses in Germany and Denmark and for a certain cell phone identifier (IMEI) in Sweden. Other limitations on access seen in other countries' laws include requirements for senior police officers to approve some requests, seen in Ireland and in Finland, and limiting access to certain types of crime, which is done in Ireland, and in Finland and Sweden in some cases (for certain cell phone identifiers).

For Intercept Capability

To be inserted on page 47 of 60, after the first para after the box, that begins "In some cases, where..." and ends "...built into the infrastructure." It will replace the second para after the box, that begins "This means that investigations..." and ends "...on their networks."

This means that investigations that are being pursued under judicial authorization are being impacted, which is affecting law enforcement and national security agencies' ability to achieve their individual mandates. Canada does not have a general requirement for CSPs to have interception capability on their networks. These requirements are in place in many other countries. Australia, the United States, the United Kingdom and other European nations require that CSPs have an interception capability.

An example of these requirements can be seen in the United States legislation entitled the *Communications Assistance for Law Enforcement Act*, usually referred to as CALEA. The US Federal Communications Commission (FCC) website provides the following information to describe CALEA:

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

> In response to concerns that emerging technologies such as digital and wireless communications were making it increasingly difficult for law enforcement agencies to execute authorized surveillance, Congress enacted CALEA on October 25, 1994. CALEA requires a "telecommunications carrier," as defined by the CALEA statute, to ensure that equipment, facilities, or services that allow a customer or subscriber to "originate, terminate, or direct communications," enable law enforcement officials to conduct electronic surveillance pursuant to court order or other lawful authorization. CALEA is intended to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment design and modify their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities as communications network technologies evolve. Communications services utilizing Circuit Mode equipment and facilities, and communications services utilizing packet mode are all subject to CALEA. In May 2006, the FCC issued a Second Report and Order also requiring facilities-based broadband Internet access providers and providers of interconnected Voice over Internet Protocol (VoIP) service to come into compliance with CALEA obligations no later than May 14, 2007.
>
> ....
>
> A telecommunications carrier may comply with CALEA in different ways. First, the carrier may develop its own compliance solution for its unique network. Second, the carrier may purchase a compliance solution from vendors, including the manufacturers of the equipment it is using to provide service. Third, the carrier may purchase a compliance solution from a trusted third party (TPP). See CALEA Second Report and Order at para. 26.

As a result of this legislation, the US today, traditional voice switches have an intercept feature included.

<u>For Encryption</u>

Text to be added at page 48 of 60, following the para beginning "Encryption technology does, however..." and ending "...availability of encryption tools."

Given the challenges inherent in limiting problematic use without negatively impacting its benefits, very few countries around the world have imposed limitations on the use of encryption through the law in the interests of protecting law enforcement and national security agency capabilities, although the challenges posed by encryption for law enforcement and national security agencies are well known and have been the subject of concern and discussion in many jurisdictions since the 1990s. The United Kingdom is one of the few countries that has imposed some limitations in legislation in relation to the use of encryption to assist law enforcement, and these requirements have attracted controversy since their enactment. The United States put forward in the 1990s a series of legislative initiatives (sometimes referred to as "Clipper Chip" proposals) designed to impose built-in decryption capabilities. These proposals were highly controversial and attracted vigorous opposition and criticism from the perspective of privacy and civil liberties as well as from the perspective of potential for a negative impact on industry and

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

protection provided by encryption. None of these legislative proposals were enacted, however concerns of law enforcement in relation to encryption and the vigorous debate around these issues in the United States continues to take place, most recently seen in the controversy arising from the request by the US government to Apple for assistance with a phone associated with the San Bernardino terrorist incident.

For Data Retention

To be added to the text of the third paragraph after the box on page 49 of 60, which is only one sentence as present that reads "General requirements for data retention currently exist in some foreign jurisdictions, or have been proposed or debated." The paragraph would be expanded to include the following:

In the United States, some bills to enact data retention have been brought forward for consideration by federal legislators, but these requirements have never been enacted. Australia recently enacted data retention requirements. The European Union had, until recently, imposed data retention requirements on all its members, through a Data Retention Directive (DRD). The DRD required that data retention be implemented through legislation enacted by European Union member states at the national level. The manner of the implementation varied significantly between jurisdictions, in part in response to controversy in relation to these requirements at the national level in some jurisdictions. The DRD was recently struck down by a European court as being inconsistent with European privacy requirements. European Union member states are now looking at their respective national laws to determine if and how their national laws on data retention should be amended to respond to this decision to strike down the DRD.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

For BSI

To be inserted at page 46 of 60, under the second last paragraph beginning "As a result, criminal investigations..." and ending "...and respect privacy interests." The following text would replace the last para on page 46 of 60, which begins "Many foreign jurisdictions..." and ends "...obtained and how it is to be provided."

Many foreign jurisdictions have provision in law that specifically permit law enforcement and national security agencies access to BSI, in many cases without prior judicial authorization. These jurisdictions include, but are not limited to, the United States, the United Kingdom, Australia, Germany, Sweden, Ireland, Denmark, Spain, Finland, the Netherlands and Norway. The laws in these jurisdictions may however place certain limits on the type of BSI that can be obtained and how it can be obtained. For example, in the United States and in the Netherlands, prosecutors are involved in the process to obtain some types of BSI. An order from a judge for access to BSI is required in some situations such as for BSI when it is stored as part of a data retention requirement in Finland or when access is needed by intelligence agencies in Spain. While BSI is available administratively, without prior judicial authorization, in Australia, Ireland, the Netherlands, the United Kingdom, Norway and the United States, an order from a judge is needed for certain BSI identifiers in some places, such as for IP addresses in Germany and Denmark and for a certain cell phone identifier (IMEI) in Sweden. Other limitations on access seen in other countries' laws include requirements for senior police officers to approve some requests, seen in Ireland and in Finland, and limiting access to certain types of crime, which is done in Ireland, and in Finland and Sweden in some cases (for certain cell phone identifiers).

For Intercept Capability

To be inserted on page 47 of 60, after the first para after the box that begins "In some cases, where..." and ends "...built into the infrastructure." It will replace the second para after the box, that begins "This means that investigations..." and ends "...on their networks."

This means that investigations that are being pursued under judicial authorization are being impacted, which is affecting law enforcement and national security agencies' ability to achieve their individual mandates. Canada does not have a general requirement for CSPs to have interception capability on their networks. These requirements are in place in many other countries. Australia, the United States, the United Kingdom and other European nations require that CSPs have an interception capability.

An example of these requirements can be seen in the United States legislation entitled the *Communications Assistance for Law Enforcement Act*, usually referred to as CALEA.

Released under the Access to Information Act / Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The US Federal Communications Commission (FCC) website provides~~es the following~~ information to describe CALEA[1]:

Commented [LO1]: Karen, could you confirm that this is the right link?

~~In response to concerns that emerging technologies such as digital and wireless communications were making it increasingly difficult for law enforcement agencies to execute authorized surveillance, Congress enacted CALEA on October 25, 1994. CALEA requires a "telecommunications carrier," as defined by the CALEA statute, to ensure that equipment, facilities, or services that allow a customer or subscriber to "originate, terminate, or direct communications," enable law enforcement officials to conduct electronic surveillance pursuant to court order or other lawful authorization. CALEA is intended to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment design and modify their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities as communications network technologies evolve. Communications services utilizing Circuit Mode equipment and facilities, and communications services utilizing packet mode are all subject to CALEA. In May 2006, the FCC issued a Second Report and Order also requiring facilities based broadband Internet access providers and providers of interconnected Voice over Internet Protocol (VoIP) service to come into compliance with CALEA obligations no later than May 14, 2007.~~

~~....~~

~~A telecommunications carrier may comply with CALEA in different ways. First, the carrier may develop its own compliance solution for its unique network. Second, the carrier may purchase a compliance solution from vendors, including the manufacturers of the equipment it is using to provide service. Third, the carrier may purchase a compliance solution from a trusted third party (TPP). See CALEA Second Report and Order at para. 26.~~

As a result of this legislation, in the US today, traditional voice switches have an intercept feature included.

For Encryption

Text to be added at page 48 of 60, following the para beginning "Encryption technology does, however..." and ending "...availability of encryption tools."

Given the challenges inherent in limiting problematic use without negatively impacting its benefits, very few countries around the world have imposed limitations on the use of encryption through the law in the interests of protecting law enforcement and national security agency capabilities. This is despite the fact that the challenges posed by encryption for law enforcement and national security agencies are well known and have been the subject of concern and discussion in many jurisdictions since the 1990s. The

[1] https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance#CCSBI

~~[2] https://apps.fcc.gov/mwg-internal/de5fs23hu73ds/progress?id=Hf1ZRlslxuKReCPk8M3Cbp99-aN4Z1O_d2g-BMGB-wQ,&dl~~

Formatted: Default Paragraph Font

Formatted: Default Paragraph Font

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

United Kingdom is one of the few countries that has imposed some limitations in legislation, through the *Regulation of Investigatory Powers Act, 2000*, ~~in relatio~~to assist law enforcement when dealing with encrypted data.~~n to the use of encryption to assist law enforcement. and~~ These requirements, which provide legally authorized persons (such as law enforcement, security and intelligence agencies) the authority to serve notices on individuals or bodies requiring the disclosure of protected (e.g. encrypted) information in an intelligible form through decryption or disclosure of encryption keys the person is believed to have in their possession,~~which they lawfully hold, or are likely to hold, in an intelligible form,~~ have attracted controversy since their enactment. In the 1990s, the United States put forward a series of legislative initiatives (sometimes referred to as "Clipper Chip" proposals) designed to impose built-in decryption capabilities. These proposals were highly controversial and attracted vigorous opposition and criticism from the perspective of privacy and civil liberties as well as from the perspective of the potential negative impact on industry given the protection provided by encryption. None of these legislative proposals were enacted; however, concerns of law enforcement in relation to encryption and the vigorous debate around these issues in the United States continues to take place, most recently seen in the controversy arising from the request by the US government to Apple for assistance with a phone associated with the San Bernardino terrorist incident.

Formatted: Font: Italic

For Data Retention

To be added to the text of the third paragraph after the box on page 49 of 60, which is only one sentence as present that reads "General requirements for data retention currently exist in some foreign jurisdictions, or have been proposed or debated." The paragraph would be expanded to include the following:

In the United States, some bills to enact data retention have been brought forward for consideration by federal legislators, but these requirements have never been enacted. Australia recently enacted data retention requirements. On March 15, 2006, the European Union imposed data retention requirements with respect to telecommunications data on all its member states, through a Data Retention Directive (DRD). The DRD required that data retention be implemented through legislation enacted by European Union member states at the national level. The manner of the implementation varied significantly between jurisdictions, in part in response to controversy in relation to these requirements at the national level in some jurisdictions. The DRD was struck down on April 8, 2014 by the Court of Justice of the European Union as being inconsistent with privacy rights in Europe. European Union member states are now looking at their respective national laws to determine if and how their national laws on data retention should be amended to respond to this decision to strike down the DRD. Some countries, such as Germany, have already introduced changes. The Federal Constitutional Court of Germany declared their own domestic legislation unconstitutional in March 2010. A new data retention law came into effect in Germany on January 4, 2016 which introduced many safeguards such as reducing retention from six months to ten weeks and restricting access to such data to "serious crimes" only.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

For BSI

To be inserted at page 46 of 60, under the second last paragraph beginning "As a result, criminal investigations..." and ending "...and respect privacy interests." The following text would replace the last para on page 46 of 60, which begins "Many foreign jurisdictions..." and ends "...obtained and how it is to be provided."

Many foreign jurisdictions have provisions in law that specifically permit law enforcement and national security agencies access to BSI, in many cases without prior judicial authorization. These jurisdictions include, but are not limited to, the United States, the United Kingdom, Australia, Germany, Sweden, Ireland, Denmark, Spain, Finland, the Netherlands and Norway. The laws in these jurisdictions may however place certain limits on the type of BSI that can be obtained and how it can be obtained.

For example, prosecutors are involved in the process to obtain some types of BSI in some places. An order from a judge for access to BSI is required in some countries in certain types of situations such as for example for BSI when it is stored as part of a data retention requirement. Or in some places an order from a judge may be needed for access by certain agencies, while other agencies can access it administratively. While BSI is available administratively, without prior judicial authorization, in many countries, an order from a judge may be needed for certain BSI identifiers in some places, for example a court order may be needed for an IP address or for a certain type of cell phone identifier, such as an IMEI. Other limitations on access seen in other countries' laws include requirements for senior police officers to approve some requests and limiting access to certain types of crime. Most jurisdictions have some of these limitations in their laws in relation to access to BSI.

For Intercept Capability

To be inserted on page 47 of 60, after the first para after the box that begins "In some cases, where..." and ends "...built into the infrastructure." It will replace the second para after the box, that begins "This means that investigations..." and ends "...on their networks."

This means that investigations that are being pursued under judicial authorization are being impacted, which is affecting law enforcement and national security agencies' ability to achieve their individual mandates. Canada does not have a general requirement for CSPs to have interception capability on their networks. These requirements are in place in many other countries. Australia, the United States, the United Kingdom and other European nations require that CSPs have an interception capability.

An example of these requirements can be seen in the United States legislation entitled the *Communications Assistance for Law Enforcement Act*, usually referred to as CALEA.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The US Federal Communications Commission (FCC) website provides information to describe CALEA[1] .

As a result of this legislation, in the US today, traditional voice switches have an intercept feature included.

For Encryption

Text to be added at page 48 of 60, following the para beginning "Encryption technology does, however..." and ending "...availability of encryption tools."

Given the challenges inherent in limiting problematic use without negatively impacting its benefits, very few countries around the world have imposed limitations on the use of encryption through the law in the interests of protecting law enforcement and national security agency capabilities. This is despite the fact that the challenges posed by encryption for law enforcement and national security agencies are well known and have been the subject of concern and discussion in many jurisdictions since the 1990s.

The United Kingdom is one of the few countries that has imposed some limitations in legislation, through the *Regulation of Investigatory Powers Act, 2000*, to assist law enforcement when dealing with encrypted data. These requirements, which provide legally authorized persons (such as law enforcement, security and intelligence agencies) the authority to serve notices on individuals or bodies requiring the disclosure of protected (e.g. encrypted) information in an intelligible form through decryption or disclosure of encryption keys the person is believed to have in their possession, have attracted controversy since their enactment.

In the 1990s, the United States put forward a series of legislative initiatives (sometimes referred to as "Clipper Chip" proposals) designed to impose built-in decryption capabilities. These proposals were highly controversial and attracted vigorous opposition and criticism from the perspective of privacy and civil liberties as well as from the perspective of the potential negative impact on industry given the protection provided by encryption. None of these legislative proposals were enacted; however, concerns of law enforcement in relation to encryption and the vigorous debate around these issues in the United States continues to take place, most recently seen in the controversy arising from the request by the US government to Apple for assistance with a phone associated with the San Bernardino terrorist incident.

For Data Retention

To be added to the text of the third paragraph after the box on page 49 of 60, which is only one sentence as present that reads "General requirements for data retention

[1] https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

currently exist in some foreign jurisdictions, or have been proposed or debated." The paragraph would be expanded to include the following:

In the United States, some bills to enact data retention have been brought forward for consideration by federal legislators, but these requirements have never been enacted. Australia recently enacted data retention requirements. On March 15, 2006, the European Union imposed data retention requirements with respect to telecommunications data on all its member states, through a Data Retention Directive (DRD).

The DRD required that data retention be implemented through legislation enacted by European Union member states at the national level. The manner of the implementation varied significantly between jurisdictions, in part in response to controversy in relation to these requirements at the national level in some jurisdictions. The DRD was struck down on April 8, 2014 by the Court of Justice of the European Union as being inconsistent with privacy rights in Europe.

European Union member states are now looking at their respective national laws to determine if and how their national laws on data retention should be amended to respond to this decision to strike down the DRD. Some countries, such as Germany, have already introduced changes. The Federal Constitutional Court of Germany declared their own domestic legislation unconstitutional in March 2010. A new data retention law came into effect in Germany on January 4, 2016 which introduced many safeguards such as reducing retention from six months to ten weeks and restricting access to such data to "serious crimes" only.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

For BSI

To be inserted at page 46 of 60, under the second last paragraph beginning "As a result, criminal investigations..." and ending "...and respect privacy interests." The following text would replace the last para on page 46 of 60, which begins "Many foreign jurisdictions..." and ends "...obtained and how it is to be provided."

Many foreign jurisdictions have provision in law that specifically permit law enforcement and national security agencies access to BSI, in many cases without prior judicial authorization. These jurisdictions include, but are not limited to, the United States, the United Kingdom, Australia, Germany, Sweden, Ireland, Denmark, Spain, Finland, the Netherlands and Norway. The laws in these jurisdictions may however place certain limits on the type of BSI that can be obtained and how it can be obtained.

For example, in the United States and in the Netherlands, prosecutors are involved in the process to obtain some types of BSI. An order from a judge for access to BSI is required in some situations such as for BSI when it is stored as part of a data retention requirement in Finland or when access is needed by intelligence agencies in Spain.

While BSI is available administratively, without prior judicial authorization, in Australia, Ireland, the Netherlands, the United Kingdom, Norway and the United States, an order from a judge is needed for certain BSI identifiers in some places, such as for IP addresses in Germany and Denmark and for a certain cell phone identifier (IMEI) in Sweden. Other limitations on access seen in other countries' laws include requirements for senior police officers to approve some requests, seen in Ireland and in Finland, and limiting access to certain types of crime, which is done in Ireland, and in Finland and Sweden in some cases (for certain cell phone identifiers).

For Intercept Capability

To be inserted on page 47 of 60, after the first para after the box that begins "In some cases, where..." and ends "...built into the infrastructure." It will replace the second para after the box, that begins "This means that investigations..." and ends "...on their networks."

This means that investigations that are being pursued under judicial authorization are being impacted, which is affecting law enforcement and national security agencies' ability to achieve their individual mandates. Canada does not have a general requirement for CSPs to have interception capability on their networks. These requirements are in place in many other countries. Australia, the United States, the United Kingdom and other European nations require that CSPs have an interception capability.

An example of these requirements can be seen in the United States legislation entitled the *Communications Assistance for Law Enforcement Act*, usually referred to as CALEA.

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

The US Federal Communications Commission (FCC) website provides information to describe CALEA[1] .

As a result of this legislation, in the US today, traditional voice switches have an intercept feature included.

For Encryption

Text to be added at page 48 of 60, following the para beginning "Encryption technology does, however..." and ending "...availability of encryption tools."

Given the challenges inherent in limiting problematic use without negatively impacting its benefits, very few countries around the world have imposed limitations on the use of encryption through the law in the interests of protecting law enforcement and national security agency capabilities. This is despite the fact that the challenges posed by encryption for law enforcement and national security agencies are well known and have been the subject of concern and discussion in many jurisdictions since the 1990s.

The United Kingdom is one of the few countries that has imposed some limitations in legislation, through the *Regulation of Investigatory Powers Act, 2000*, to assist law enforcement when dealing with encrypted data. These requirements, which provide legally authorized persons (such as law enforcement, security and intelligence agencies) the authority to serve notices on individuals or bodies requiring the disclosure of protected (e.g. encrypted) information in an intelligible form through decryption or disclosure of encryption keys the person is believed to have in their possession, have attracted controversy since their enactment.

In the 1990s, the United States put forward a series of legislative initiatives (sometimes referred to as "Clipper Chip" proposals) designed to impose built-in decryption capabilities. These proposals were highly controversial and attracted vigorous opposition and criticism from the perspective of privacy and civil liberties as well as from the perspective of the potential negative impact on industry given the protection provided by encryption. None of these legislative proposals were enacted; however, concerns of law enforcement in relation to encryption and the vigorous debate around these issues in the United States continues to take place, most recently seen in the controversy arising from the request by the US government to Apple for assistance with a phone associated with the San Bernardino terrorist incident.

For Data Retention

To be added to the text of the third paragraph after the box on page 49 of 60, which is only one sentence as present that reads "General requirements for data retention

[1] https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance

Released under the Access to Information Act /
Divulgé(s) en vertu de la Loi sur l'accès à l'information.

currently exist in some foreign jurisdictions, or have been proposed or debated." The paragraph would be expanded to include the following:

In the United States, some bills to enact data retention have been brought forward for consideration by federal legislators, but these requirements have never been enacted. Australia recently enacted data retention requirements. On March 15, 2006, the European Union imposed data retention requirements with respect to telecommunications data on all its member states, through a Data Retention Directive (DRD).

The DRD required that data retention be implemented through legislation enacted by European Union member states at the national level. The manner of the implementation varied significantly between jurisdictions, in part in response to controversy in relation to these requirements at the national level in some jurisdictions. The DRD was struck down on April 8, 2014 by the Court of Justice of the European Union as being inconsistent with privacy rights in Europe.

European Union member states are now looking at their respective national laws to determine if and how their national laws on data retention should be amended to respond to this decision to strike down the DRD. Some countries, such as Germany, have already introduced changes. The Federal Constitutional Court of Germany declared their own domestic legislation unconstitutional in March 2010. A new data retention law came into effect in Germany on January 4, 2016 which introduced many safeguards such as reducing retention from six months to ten weeks and restricting access to such data to "serious crimes" only.