Leclair, Natalie

From: McAteer, Julie
Sent: Wednesday, October 17, 2012 10:34 AM
To: Bedor, Tia Leigh
Cc: Leclair, Natalie; Dupuis, Chantal; Baulne, Lucie
Subject: RE: NEW Petition 411-1784 - Lawful Access
Attachments: 411-1784 petition response.doc

Julie McAteer
Senior Advisor, Parliamentary Affairs / Conseillère principale, affaires parlementaires
Public Safety Canada / Sécurité publique Canada
Tel/Tél: (613) 949-9737
Fax:(613) 948-8870
Email/Courriel: julie.mcateer@ps-sp.gc.ca

From: Bedor, Tia Leigh
Sent: October-17-12 10:30 AM
To: McAteer, Julie
Cc: Leclair, Natalie; Dupuis, Chantal; Baulne, Lucie
Subject: RE: NEW Petition 411-1784 - Lawful Access

Can you attach the templates in the email?

Thanks,

Tia Leigh Bedor
Administrative Officer | Agente Administrative
Office of the Senior Assistant Deputy Minister | Cabinet de la Sous-ministre adjointe principale
National Security | Sécurité nationale
Public Safety Canada | Sécurité publique Canada
Tel/Tél: 613-991-2901 | www.publicsafety.gc.ca | www.sécuritépublique.gc.ca

---

From: McAteer, Julie
Sent: Wednesday, October 17, 2012 10:23 AM
To: Bedor, Tia Leigh
Cc: Leclair, Natalie; Dupuis, Chantal; Baulne, Lucie
Subject: RE: NEW Petition 411-1784 - Lawful Access

Good morning,
Further to our conversation last week, please find below the sentence that the MO would like added into the response.

Please also let me know where NS believes that this would fit best – I would assume that it would replace any mention of the future of the legislation...

[redacted]

Should NS agree, we would also need the translation of the addition – before noon tomorrow.

Thank you
Julie

Julie McAteer
Senior Advisor, Parliamentary Affairs / Conseillère principale, affaires parlementaires
Public Safety Canada / Sécurité publique Canada
Tel/Tél: (613) 949-9737
Fax:(613) 948-8870
Email/Courriel: julie.mcateer@ps-sp.gc.ca

From: Bedor, Tia Leigh
Sent: October-12-12 9:59 AM
To: McAteer, Julie
Subject: RE: NEW Petition 411-1784 - Lawful Access

Can you attach the templates in the email?

s.21(1)(a)

Thanks,

Tia Leigh Bedor
Administrative Officer | Agente Administrative
Office of the Senior Assistant Deputy Minister | Cabinet de la Sous-ministre adjointe principale
National Security | Sécurité nationale
Public Safety Canada | Sécurité publique Canada
Tel/Tél: 613-991-2901 | www.publicsafety.gc.ca | www.sécuritépublique.gc.ca

---

From: McAteer, Julie
Sent: Friday, October 12, 2012 9:22 AM
To: Bedor, Tia Leigh; Dupuis, Chantal; Baulne, Lucie
Cc: McAteer, Julie; Leclair, Natalie
Subject: RE: NEW Petition 411-1784 - Lawful Access

[redacted]

Julie McAteer

Senior Advisor, Parliamentary Affairs / Conseillère principale, affaires parlementaires
Public Safety Canada / Sécurité publique Canada
Tel/Tél: (613) 949-9737
Fax:(613) 948-8870
Email/Courriel: julie.mcateer@ps-sp.gc.ca

From: Bedor, Tia Leigh
Sent: October-09-12 10:38 AM
To: Leclair, Natalie; Dupuis, Chantal; Baulne, Lucie
Cc: McAteer, Julie; Issues / Enjeux; Chang, Anna
Subject: RE: NEW Petition 411-1784 - Lawful Access

Nathalie,

s.21(1)(a)

[redacted]

Thanks,

Tia Leigh Bedor
Administrative Officer | Agente Administrative
Office of the Senior Assistant Deputy Minister | Cabinet de la Sous-ministre adjointe principale
National Security | Sécurité nationale
Public Safety Canada | Sécurité publique Canada
Tel/Tél: 613-991-2901 | www.publicsafety.gc.ca | www.sécuritépublique.gc.ca

---

From: Leclair, Natalie
Sent: Thursday, September 27, 2012 10:11 AM
To: Dupuis, Chantal; Bedor, Tia Leigh; Baulne, Lucie
Cc: McAteer, Julie; Issues / Enjeux; Chang, Anna
Subject: NEW Petition 411-1784 - Lawful Access
Importance: High

Good afternoon,

Please find attached a new petition 411-1784 which was presented in the House by Ms. May concerning Telecommunications.

Please note that this petition is similar to previous petitions on this subject. (previous petition 411-1519 attached).

NOTE: Please ensure that the information provided in the response to the petition is accurate and consistent with information or documents already disclosed under the *Access to Information Act* or the *Privacy Act*, or in response to other types of information requests.

Your ADM/ADM equivalent approved bilingual response should sent electronically to me with a CC to Julie McAteer **by COB on October 9, 2012**.

Please do not hesitate to contact me should you have any questions.

Thank you.
Nat

Natalie Leclair
Advisor / Conseillère
Parliamentary Affairs / Affaires parlementaires
Public Safety Canada / Sécurité publique Canada
Tel/Tél: (613) 990-2718
Fax: (613) 954-8774
Email/Courriel: natalie.leclair@ps-sp.gc.ca

RESPONSE TO PETITION
RÉPONSE À LA PÉTITION

PREPARE IN ENGLISH AND FRENCH MARKING "ORIGINAL TEXT" OR "TRANSLATION"
PRÉPARER EN ANGLAIS ET EN FRANÇAIS EN INDIQUANT "TEXTE ORIGINAL" OU "TRADUCTION"

PETITION NO./Nº DE LA PÉTITION	BY / DE	DATE
411-1784	Ms. May (Saanich—Gulf Islands)	September 24, 2012

RESPONSE BY THE MINISTER OF PUBLIC SAFETY
RÉPONSE DU MINISTRE DE LA SÉCURITÉ PUBLIQUE

The Honourable Vic Toews

PRINT NAME OF SIGNATORY
INSCRIRE LE NOM DU SIGNATAIRE

SIGNATURE
MINISTER OR PARLIAMENTARY SECRETARY
MINISTRE OU SECRÉTAIRE PARLEMENTAIRE

SUBJECT / OBJET
Telecommunications

RESPONSE / RÉPONSE

ORIGINAL TEXT / TEXTE ORIGINAL [X] TRANSLATION / TRADUCTION [ ]

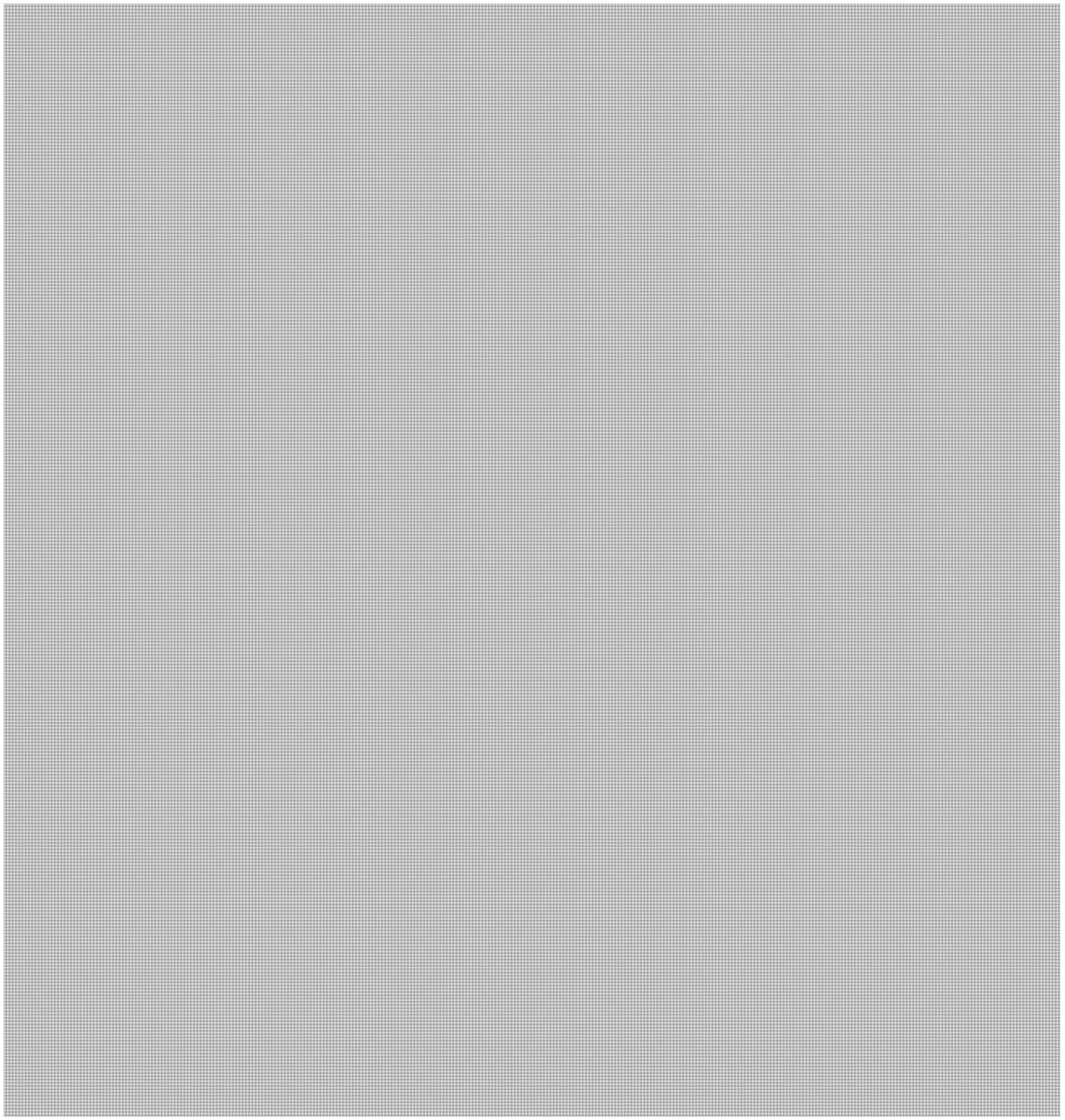
Public Safety Canada

s.21(1)(a)

[redacted]

.../2

s.21(1)(a)



RESPONSE TO PETITION
RÉPONSE À LA PÉTITION

PREPARE IN ENGLISH AND FRENCH MARKING "ORIGINAL TEXT" OR "TRANSLATION"
PRÉPARER EN ANGLAIS ET EN FRANÇAIS EN INDIQUANT "TEXTE ORIGINAL" OU "TRADUCTION"

PETITION NO./Nº DE LA PÉTITION	BY / DE	DATE
411-1784	Mme May (Saanich—Gulf Islands)	24 septembre 2012

RESPONSE BY THE MINISTER OF PUBLIC SAFETY
RÉPONSE DU MINISTRE DE LA SÉCURITÉ PUBLIQUE

L'honorable Vic Toews

PRINT NAME OF SIGNATORY
INSCRIRE LE NOM DU SIGNATAIRE

SIGNATURE
MINISTER OR PARLIAMENTARY SECRETARY
MINISTRE OU SECRÉTAIRE PARLEMENTAIRE

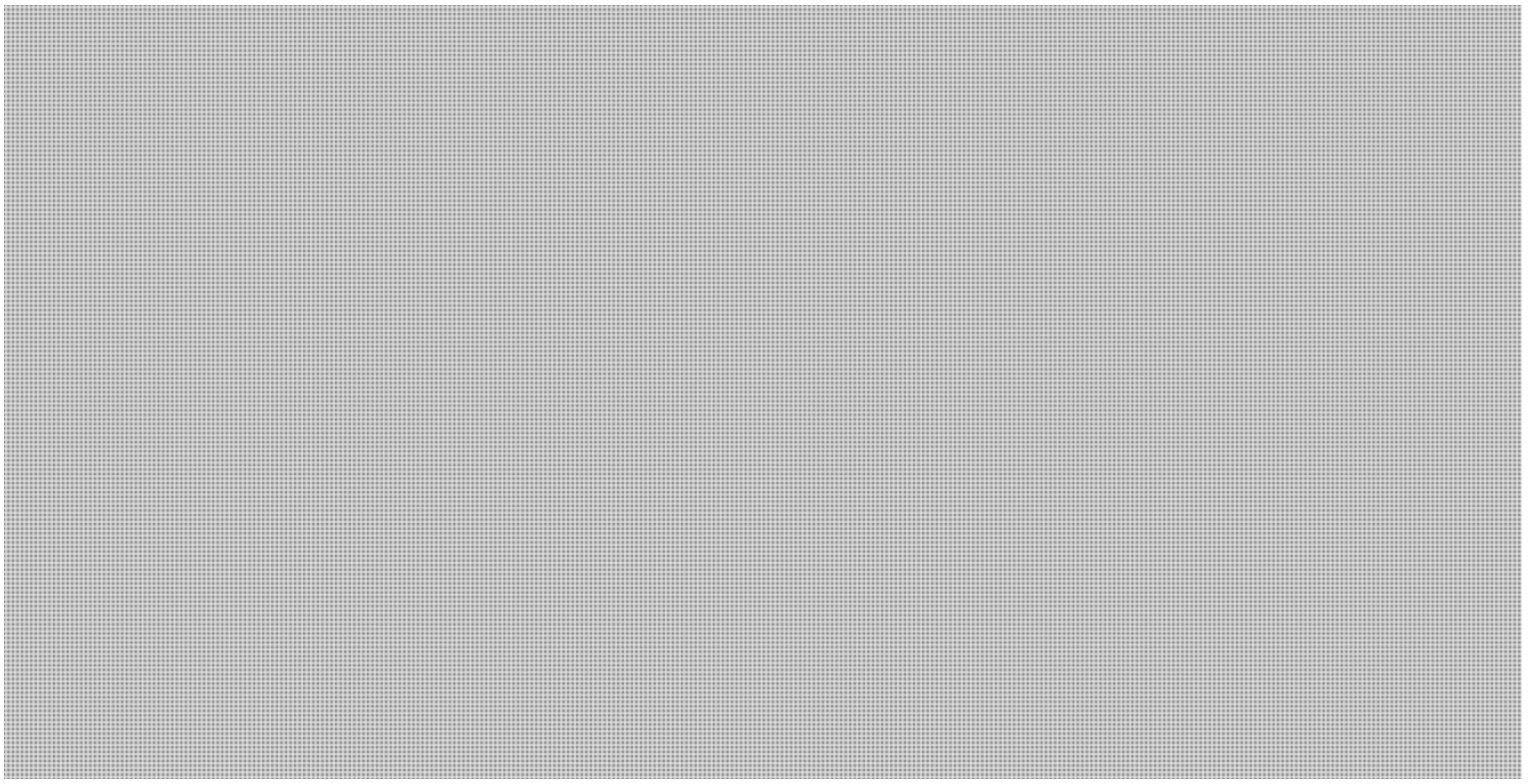
SUBJECT / OBJET
Télécommunications

RESPONSE / RÉPONSE

ORIGINAL TEXT / TEXTE ORIGINAL [ ] TRANSLATION / TRADUCTION [X]

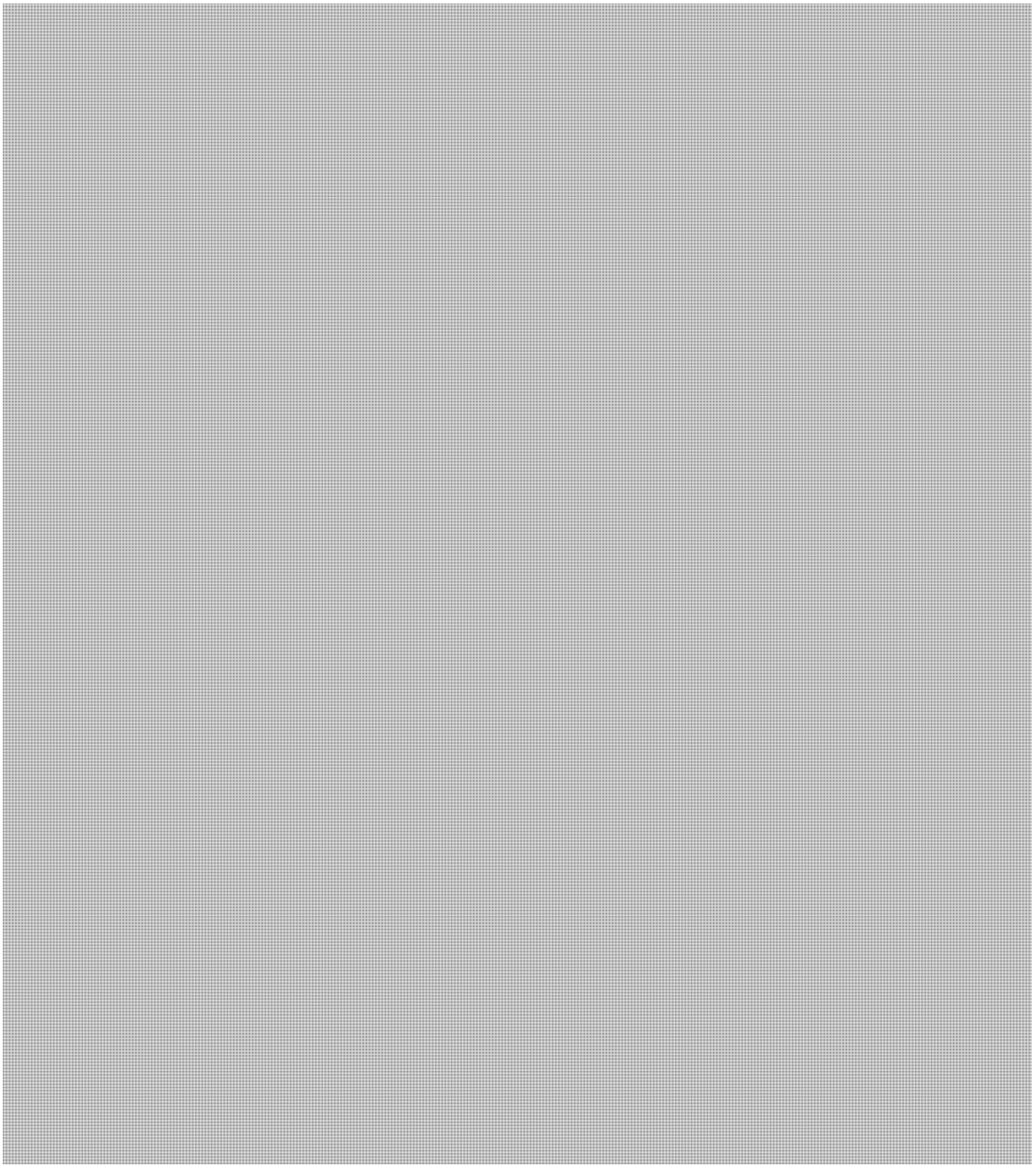
s.21(1)(a)

Sécurité publique Canada

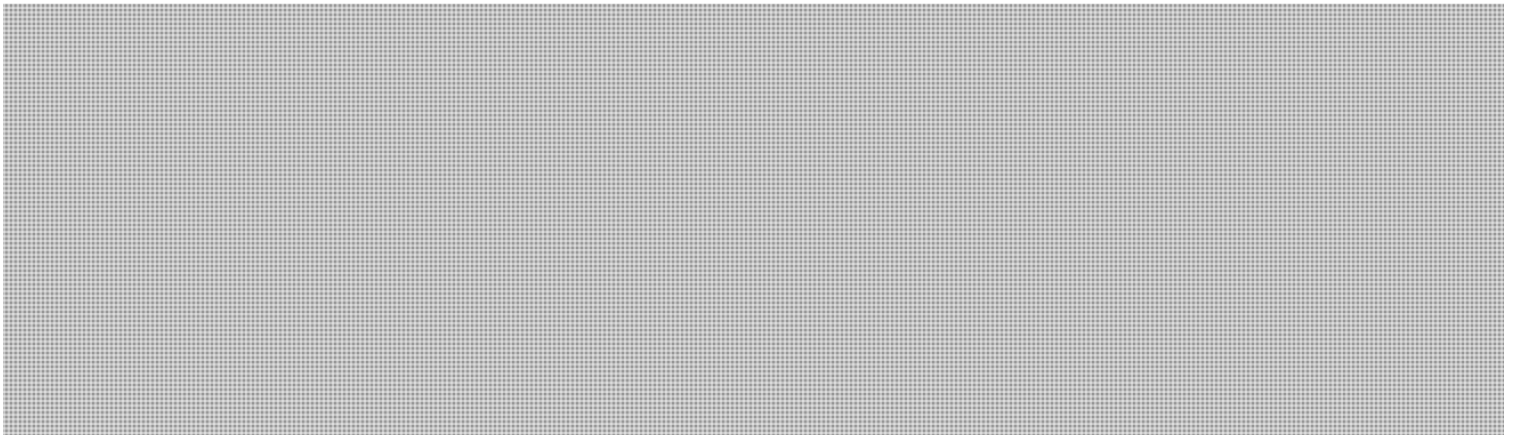


.../2

s.21(1)(a)



.../3



Leclair, Natalie

From: Bedor, Tia Leigh
Sent: Thursday, October 18, 2012 11:22 AM
To: McAteer, Julie; Leclair, Natalie
Cc: Dupuis, Chantal
Subject: FW: NEW Petition 411-1784 - Lawful Access

You should have access now, sorry.

Thanks,

Tia Leigh Bedor
Administrative Officer | Agente Administrative
Office of the Senior Assistant Deputy Minister | Cabinet de la Sous-ministre adjointe principale
National Security | Sécurité nationale
Public Safety Canada | Sécurité publique Canada
Tel/Tél: 613-991-2901 | www.publicsafety.gc.ca | www.sécuritépublique.gc.ca

---

From: Bedor, Tia Leigh
Sent: October 18, 2012 10:58 AM
To: McAteer, Julie
Cc: Leclair, Natalie; Dupuis, Chantal; Baulne, Lucie
Subject: RE: NEW Petition 411-1784 - Lawful Access

Nathalie,

Please find the RDIMS reference to Petition 411-1784 attached.

Thanks,

Tia Leigh Bedor
Administrative Officer | Agente Administrative
Office of the Senior Assistant Deputy Minister | Cabinet de la Sous-ministre adjointe principale
National Security | Sécurité nationale
Public Safety Canada | Sécurité publique Canada
Tel/Tél: 613-991-2901 | www.publicsafety.gc.ca | www.sécuritépublique.gc.ca

---

From: McAteer, Julie
Sent: Wednesday, October 17, 2012 10:23 AM
To: Bedor, Tia Leigh
Cc: Leclair, Natalie; Dupuis, Chantal; Baulne, Lucie
Subject: RE: NEW Petition 411-1784 - Lawful Access

Good morning,
Further to our conversation last week, please find below the sentence that the MO would like added into the response.

Please also let me know where NS believes that this would fit best – I would assume that it would replace any mention of the future of the legislation...

[redacted]

Should NS agree, we would also need the translation of the addition – before noon tomorrow.

Thank you
Julie

Julie McAteer
Senior Advisor, Parliamentary Affairs / Conseillère principale, affaires parlementaires
Public Safety Canada / Sécurité publique Canada
Tel/Tél: (613) 949-9737
Fax:(613) 948-8870
Email/Courriel: julie.mcateer@ps-sp.gc.ca

From: Bedor, Tia Leigh
Sent: October-12-12 9:59 AM
To: McAteer, Julie
Subject: RE: NEW Petition 411-1784 - Lawful Access

Can you attach the templates in the email?

Thanks, s.21(1)(a)

Tia Leigh Bedor
Administrative Officer | Agente Administrative
Office of the Senior Assistant Deputy Minister | Cabinet de la Sous-ministre adjointe principale
National Security | Sécurité nationale
Public Safety Canada | Sécurité publique Canada
Tel/Tél: 613-991-2901 | www.publicsafety.gc.ca | www.sécuritépublique.gc.ca

---

From: McAteer, Julie
Sent: Friday, October 12, 2012 9:22 AM
To: Bedor, Tia Leigh; Dupuis, Chantal; Baulne, Lucie
Cc: McAteer, Julie; Leclair, Natalie
Subject: RE: NEW Petition 411-1784 - Lawful Access

[redacted]

Julie McAteer

Senior Advisor, Parliamentary Affairs / Conseillère principale, affaires parlementaires
Public Safety Canada / Sécurité publique Canada
Tel/Tél: (613) 949-9737
Fax:(613) 948-8870
Email/Courriel: julie.mcateer@ps-sp.gc.ca

From: Bedor, Tia Leigh
Sent: October-09-12 10:38 AM
To: Leclair, Natalie; Dupuis, Chantal; Baulne, Lucie
Cc: McAteer, Julie; Issues / Enjeux; Chang, Anna
Subject: RE: NEW Petition 411-1784 - Lawful Access s.21(1)(a)

Nathalie,

[redacted]

Thanks,

Tia Leigh Bedor
Administrative Officer | Agente Administrative
Office of the Senior Assistant Deputy Minister | Cabinet de la Sous-ministre adjointe principale
National Security | Sécurité nationale
Public Safety Canada | Sécurité publique Canada
Tel/Tél: 613-991-2901 | www.publicsafety.gc.ca | www.sécuritépublique.gc.ca

---

From: Leclair, Natalie
Sent: Thursday, September 27, 2012 10:11 AM
To: Dupuis, Chantal; Bedor, Tia Leigh; Baulne, Lucie
Cc: McAteer, Julie; Issues / Enjeux; Chang, Anna
Subject: NEW Petition 411-1784 - Lawful Access
Importance: High

Good afternoon,

Please find attached a new petition 411-1784 which was presented in the House by Ms. May concerning Telecommunications.

Please note that this petition is similar to previous petitions on this subject. (previous petition 411-1519 attached).

NOTE: Please ensure that the information provided in the response to the petition is accurate and consistent with information or documents already disclosed under the *Access to Information Act* or the *Privacy Act*, or in response to other types of information requests.

Your ADM/ADM equivalent approved bilingual response should sent electronically to me with a CC to Julie McAteer **by COB on October 9, 2012**.

Please do not hesitate to contact me should you have any questions.

Thank you.
Nat

Natalie Leclair
Advisor / Conseillère
Parliamentary Affairs / Affaires parlementaires
Public Safety Canada / Sécurité publique Canada
Tel/Tél: (613) 990-2718
Fax: (613) 954-8774
Email/Courriel: natalie.leclair@ps-sp.gc.ca

RESPONSE TO PETITION
RÉPONSE À LA PÉTITION

Field Code Changed

PREPARE IN ENGLISH AND FRENCH MARKING "ORIGINAL TEXT" OR "TRANSLATION"
PRÉPARER EN ANGLAIS ET EN FRANÇAIS EN INDIQUANT "TEXTE ORIGINAL" OU "TRADUCTION"

PETITION NO./Nº DE LA PÉTITION	BY / DE	DATE
411-1784	Ms. May (Saanich—Gulf Islands)	September 24, 2012

RESPONSE BY THE MINISTER OF PUBLIC SAFETY
RÉPONSE DU MINISTRE DE LA SÉCURITÉ PUBLIQUE

Field Code Changed

Field Code Changed

The Honourable Vic Toews

PRINT NAME OF SIGNATORY
INSCRIRE LE NOM DU SIGNATAIRE

SIGNATURE
MINISTER OR PARLIAMENTARY SECRETARY
MINISTRE OU SECRÉTAIRE PARLEMENTAIRE

SUBJECT / OBJET
Telecommunications

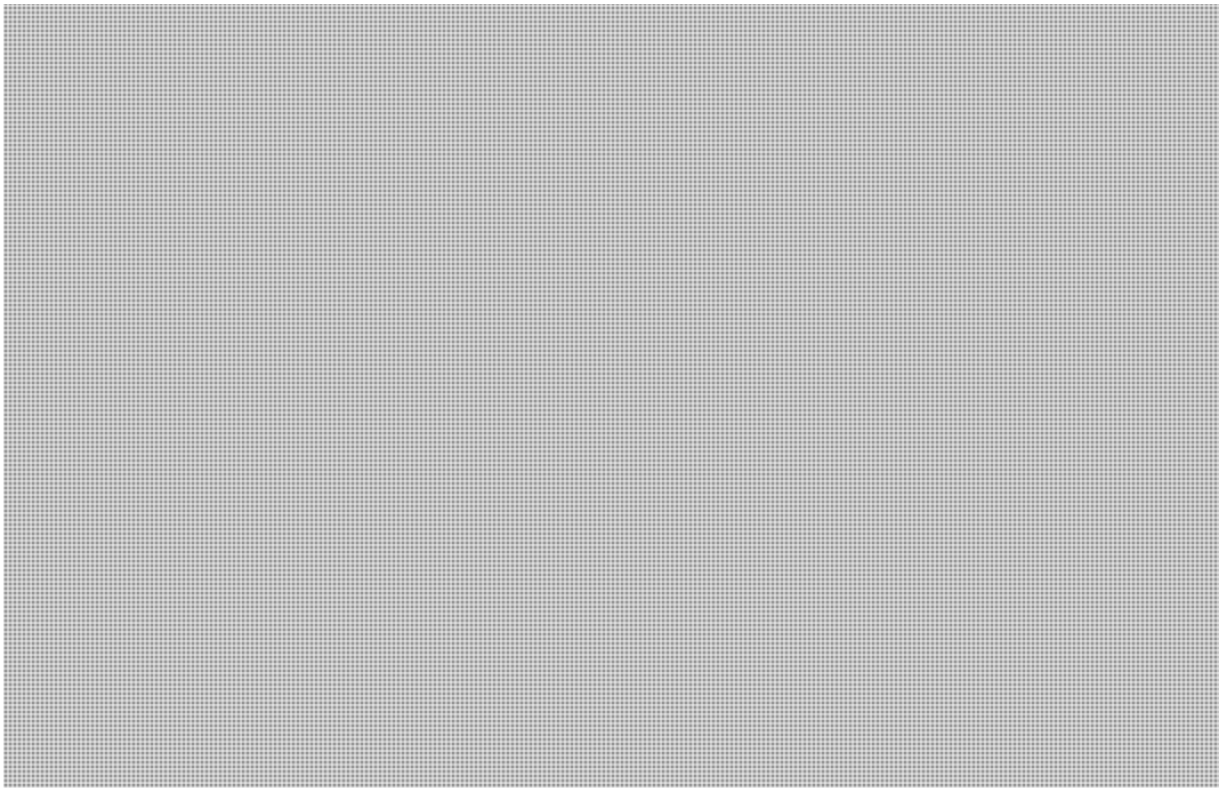
RESPONSE / RÉPONSE

ORIGINAL TEXT / TEXTE ORIGINAL [X]

TRANSLATION / TRADUCTION [ ]

s.21(1)(a)

Public Safety Canada



Page 46

is withheld pursuant to section

est retenue en vertu de l'article

21(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

RESPONSE TO PETITION
RÉPONSE À LA PÉTITION

PREPARE IN ENGLISH AND FRENCH MARKING "ORIGINAL TEXT" OR "TRANSLATION"
PRÉPARER EN ANGLAIS ET EN FRANÇAIS EN INDIQUANT "TEXTE ORIGINAL" OU "TRADUCTION"

PETITION NO./Nº DE LA PÉTITION	BY / DE	DATE
411-1784	Mme May (Saanich—Gulf Islands)	24 septembre 2012

RESPONSE BY THE MINISTER OF PUBLIC SAFETY
RÉPONSE DU MINISTRE DE LA SÉCURITÉ PUBLIQUE

L'honorable Vic Toews

PRINT NAME OF SIGNATORY
INSCRIRE LE NOM DU SIGNATAIRE

SIGNATURE
MINISTER OR PARLIAMENTARY SECRETARY
MINISTRE OU SECRÉTAIRE PARLEMENTAIRE

SUBJECT / OBJET
Télécommunications

RESPONSE / RÉPONSE

ORIGINAL TEXT / TEXTE ORIGINAL [ ]
TRANSLATION / TRADUCTION [X]

Sécurité publique Canada

[redacted]

s.21(1)(a)

Field Code Changed
Field Code Changed
Field Code Changed
Formatted: Pattern: Clear (White)
Formatted: Space After: 0 pt, Line spacing: single
Formatted: Pattern: Clear (White)

Pages 48 to / à 49

are withheld pursuant to section

sont retenues en vertu de l'article

21(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

February 21, 2013

Public Safety Canada / Sécurité publique Canada

UNCLASSIFIED

DATE:

File No.: NS 6652-O3
RDIMS No: 779952

MEMORANDUM FOR THE DIRECTOR ITTP

TRIP REPORT – MEETING WITH [redacted] FEBRUARY 21, 2013

(Information only)

ISSUE

To report on the meeting with [redacted] of the *Solicitor General Enforcement Standards for Lawful Interceptions of Telecommunication* (SGES) and to outline next steps.

SUMMARY

On February 21, 2013, ITTP/Plunkett along with engineers from the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS) met with [redacted] technical and regulatory personnel at the [redacted] The meeting was a constructive exchange that will inform Public Safety Canada's (PS) recommendation to Industry Canada regarding [redacted]

The strategic objective of the meeting was [redacted]

s.16(1)(b)
s.16(2)
s.21(1)(b)

...2

Canada

Specifically, the meeting centred around three topics:

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

This will allow law enforcement and national security agencies to [redacted] The next steps emanating from this meeting are outlined below.

BACKGROUND

The issues surrounding [redacted] According to available documentation, [redacted]

The annotated version of the SGES, which provides additional guidance to Telecommunication Service Providers (TSP) on how to comply with the SGES, [redacted]

NEXT STEPS

Following this meeting, PS will take the following steps to identify a solution to the issue [redacted]

1- Organize a follow-up with meeting participants to thoroughly review and conduct analysis on the information provided [redacted] (week of March 4);

.../3

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

2- ITTP to prepare a memo for decision to the Director General, National Security Operations outlining a recommendation on the issue

3- Prepare a plan for communicating the requirements

Should you require additional information, do not hesitate to contact me at (613) 990-7066.

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

Shawn Plunkett
Senior Policy Advisor
Investigative Technologies and Telecommunications Policy

Emmett, Jamie

From: Plunkett, Shawn
Sent: February-15-13 12:09 PM
To: Covo, Pierre
Subject: RE: Meeting with LSUs on [redacted] (PS LSU #10037-33)

Thanks Pierre. I think we will also need to decide if, from a policy standpoint, it would be better to comment in advance of a revised version.
I'll give you an update if there are any relevant outcomes this afternoon.

From: Covo, Pierre
Sent: February-15-13 10:47 AM
To: Plunkett, Shawn
Subject: RE: Meeting with LSUs on [redacted] (PS LSU #10037-33)

Hi Shawn,

Thanks for the update.

At my end, there was a meeting of counsel from the Public Safety, Defence & Immigration (PSDI) Portfolio this week [redacted] CSIS: S. Alter, RCMP: [redacted] CSEC: M. Gervais, PSDI ADAG's Office). [redacted]

[redacted]

I will let you know as things unfold, but please don't hesitate to contact me in the meantime.

Thanks,

Pierre

Pierre Covo
Counsel | Avocat
Department of Justice | Ministère de la Justice
Public Safety Legal Services | Sécurité publique services juridiques
Tel:/Tél: (613) 990-8418
Email/Courriel: pierre.covo@justice.gc.ca

s.15(1) - Subv
s.16(2)(b)
s.21(1)(a)
s.21(1)(b)

From: Plunkett, Shawn
Sent: February-15-13 9:04 AM
To: Covo, Pierre
Subject: Meeting with LSUs on [redacted]

Hi Pierre,

Did the meeting with PS, RCMP and CSIS LSU take place on the subject of the [redacted] I believe you mentioned that it was scheduled for this week.

We are having a discussion on these issues with policy centres at 1pm today.

s.16(1)(b)

Thanks

Shawn Plunkett
Senior Policy Advisor / Conseiller principal en politiques
Investigative Technologies and Telecommunications Policy (ITTP) /
Technologies d'enquêtes et politiques des télécommunications (TEPT)
National Security Operations Directorate / Direction des opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
Tel: (613) 990-7066
Email: shawn.plunkett@ps.gc.ca

Public Safety Canada | Sécurité publique Canada

Deputy Minister | Sous-ministre

Ottawa, Canada
K1A 0P8

SECRET//CEO

DATE:

File No.: NS 6950-O2 / 393359
RDIMS: Dragon 5410

MEMORANDUM FOR THE MINISTER

THE IMPACT OF INTERNATIONAL LAWFUL INTERCEPTION LEGISLATION ON TELECOMMUNICATIONS EQUIPMENT IN CANADA

(For information)

ISSUE

To provide information on the impact that other countries' interception legislation has on the interception capability of Canadian telecommunications service providers (TSPs).

BACKGROUND

Most developed countries have legislation compelling TSPs to build and maintain intercept capable networks. For example, the United States (U.S.) introduced the *Communications Assistance for Law Enforcement Act* (CALEA) in 1994. In fact, all of Canada's closest allies have similar legislation in place.

In light of this, leading telecommunications equipment vendors began to develop basic interception capability functions as part of the products they offer to TSPs. Today, each of the top five equipment manufacturers, Cisco (US), Alcatel-Lucent (France), Huawei (China), Juniper (US), and ZTE (China), offer TSPs the option to purchase telecommunications equipment with some interception capability built in for a small additional cost.

Canadian TSPs have suggested that the proliferation of interception capability legislation and standards, and the resulting growth in the marketplace of "built in" interception capability, eliminates the need for Canada to have a specific interception capability law. Indeed, Canadian TSPs argue that the telecommunications market will soon shift to a point where interception capability will simply become a standard component of available equipment, and that technical changes in the way communications actually travel on telecommunications networks will make it even easier to intercept communications.

s.15(1) - Int'l
s.16(2)
s.21(1)(a)
s.21(1)(b)

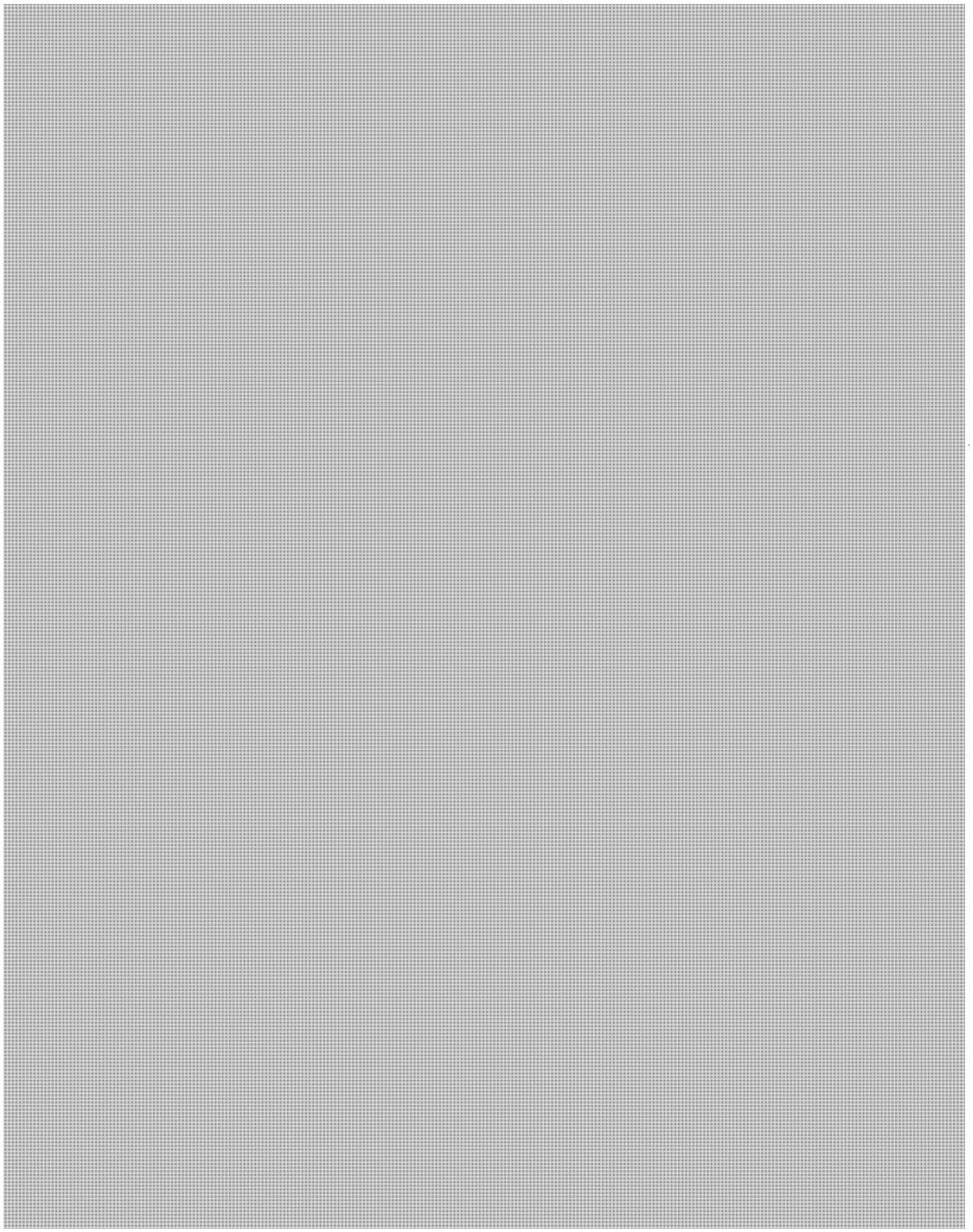
CONSIDERATIONS

[redacted]

.../3

s.15(1) - Int'l
s.16(2)
s.21(1)(a)
s.21(1)(b)

International legislation and standards (e.g. CALEA)



.../3

CONCLUSION

The claim that the telecommunications market will eventually evolve to a point where all service provider networks and equipment will naturally become intercept capable is not supportable. Canadian TSPs can purchase built in interception capability for their telecommunications equipment, but interception is a complex process that requires specific equipment or software, technical expertise and ongoing operational management.

As a result, other countries' legislative requirements and standards have no direct impact on the interception capability of Canadian TSPs. In the absence of a legislated requirement for TSPs operating in Canada to build, maintain and manage interception capability, the ability of law enforcement and national security agencies to investigate serious crimes and gather intelligence on threats through the interception of communications will continue to decrease year after year.

Should you require additional information, please do not hesitate to contact me or Ms. Lynda Clairmont, Senior Assistant Deputy Minister, National Security, at 613-990-4976.

François Guimont

Prepared by: Maciek Hawrylak

s.19(1)

Hawrylak, Maciek

From: Plunkett, Shawn
Sent: January-16-13 8:01 AM
To: Hawrylak, Maciek
Cc: Thompson, Julie
Subject: Fw: lawful interception of traffic on the PSMBN
Attachments: RE: lawful interception of traffic on the PSMBN

I can't read the attachment on BB, but from what I gather below, the folks putting together the 1st responders network are looking for some guidance on LI requirements.
They proposed a meeting on Friday from 2-2:30pm, are you available then?
I can give you the backstory on this when I'm back.
Shawn Plunkett
[redacted]
PS/SP Canada

From: Brown, Émilie
Sent: Tuesday, January 15, 2013 04:17 PM
To: Plunkett, Shawn
Subject: FW: lawful interception of traffic on the PSMBN

FYI : discussions from the Tech WG on lawful interceptions below and in attachment. I recommended you be kept in the loop and organized a quick meeting on the 18th with you to discuss this.

PS: Happy New Year!

Émilie Brown
Senior Policy Analyst / Analyste de politiques principale
Emergency Management Planning Division (EMPD)/Division Planification de la gestion des mesures d'urgences (DPGMU)
Public Safety Canada / Sécurité publique Canada
Tel : 613-949-3995
cell: [redacted]
Email/Courriel : emilie.brown@ps-sp.gc.ca

From: Claudio Lucente [mailto:clucente@fiorel.com]
Sent: Tuesday, January 15, 2013 3:09 PM
To: Brown, Émilie
Subject: Re: lawful interception of traffic on the PSMBN

Hi Emilie,

I haven't yet...too much going on right now and this is lower priority.

I think your suggestion to set up a meeting is a great idea. I'll be at 269 Laurier on the 18th. Do you want to set up a short meeting after the CRTC meeting?

Best regards,
Claudio Lucente, M.Eng, P.Eng
Senior Technical Advisor – 700MHz Public Safety Mobile Broadband Network
Centre for Security Science (CSS)

On Tue, Jan 15, 2013 at 2:54 PM, Brown, Émilie <Emilie.Brown@ps-sp.gc.ca> wrote:

Hi Claudio,

Did you get in touch with Shawn Plunkett? Seeing as they are the lead at PS on lawful intercepts, I think it would be important to include them. If you want me to set something up with them, next time you're here, maybe that simpler.

Emilie

Émilie Brown

Senior Policy Analyst / Analyste de politiques principale

Emergency Management Planning Division (EMPD)/Division Planification de la gestion des mesures d'urgences (DPGMU)

Public Safety Canada / Sécurité publique Canada

Tel : 613-949-3995

s.19(1)

cell:

Email/Courriel : emilie.brown@ps-sp.gc.ca

From: Claudio Lucente [mailto:clucente@fiorel.com]
Sent: Tuesday, January 08, 2013 5:31 PM
To:
Cc: St-Laurent, Bernard; Brown, Émilie;
Subject: Re: lawful interception of traffic on the PSMBN

Hi

Thanks for this. Please upload the 3GPP TS doc to SharePoint under the WG1 folder. I think the others are already on SP in various folders.

A couple of points...

a) The PS response to IC's consultation in Oct.2012 stated that public safety would consider leasing

the ps spectrum to commercial operators for use by consumers under suitable conditions for priority, etc. The doc is on SharePoint.

b) I met with IC today to discuss several items including next consulation on licensing conditions. On the subject of lawful intercept, [redacted] It was in the news today that the govt will want to bring the bill back in some manner. http://www.cbc.ca/news/politics/story/2013/01/08/pol-cp-privacy-watchdog-online-surveillance.html

Based on (a) and [redacted] we should plan to include this in our scope. I presume we need to show a connection to a Law Enforcement Network that is specific for this purpose.

Assuming that these conections are at the MME, SGW, and PGW, why would the warrant impact all of these NEs in the country rather than the NEs in the region where the subject of interest is served?

Best regards,

Claudio Lucente, M.Eng, P.Eng
Senior Technical Advisor – 700MHz Public Safety Mobile Broadband Network
Centre for Security Science (CSS)
http://www.css.drdc-rddc.gc.ca
[redacted]

On Tue, Jan 8, 2013 at 9:54 AM, [redacted] wrote:

Hi all,

I scanned through some of the NPSTC documents (and others): the bottom line is they are also unsure if there is any lawful intercept requirement on the PSMBN (how can one dare to potentially intercept intercepters ;-)) and are hoping for clarifications from FCC on this. But for sure, accepting commercial users on the PSMBN will mandate lawful intercept capabilities. The reference to the 3GPP spec is the right one.

As a side note, if the lawful requirement applies, having regional entities managing the MME, the SGW and/or the PGW will mean that one intercept warrant will translate into 10+ warrants to implement.

s.16(1)(c)
s.19(1)
s.21(1)(a)

[redacted]

A - Public Safety Broadband High-Level Statement of Requirements for FirstNet Consideration -

Draft Rev C, July 25, 2012

Section 4.1.6 Page 64

Today, the Communications Assistance for Law Enforcement Act (CALEA) is a regulatory requirement supported by commercial carriers to facilitate the capture of user content (including telephony sessions) when a warrant has been issued. The evidence-gathering CALEA capability requires additional equipment and resources in the carrier's network. It is anticipated that FirstNet will have to work with governing officials to determine the applicability of CALEA to the FirstNet network and its subscribers. Therefore, specific user needs are not captured in this document.

B - Public Safety Broadband High-Level Launch Requirements Statement of Requirements for FirstNet Consideration

December 7, 2012

Section 4.1.5.0 Page 25

Today, the Communications Assistance for Law Enforcement Act (CALEA) is a regulatory requirement supported by commercial carriers to facilitate the capture of user content (including telephony sessions) when a warrant has been issued. The evidence-gathering CALEA capability requires additional equipment and resources in the carrier's network. It is anticipated that FirstNet will have to work with governing officials to determine the applicability of CALEA to the FirstNet network and its subscribers. While compliance with CALEA for public safety users on a private network is not generally required, NPSTC believes that warrant-triggered collection of a secondary user's content will be necessary if FirstNet supports secondary users. However, specific user needs regarding CALEA are not captured in this document.

C - NPSTC 700 MHZ BROADBAND NETWORK REQUIREMENTS TASK - FORCE (TASK FORCE) - Technical Working Group - 700 MHz LTE Network Interoperability

Page 11

Pending the outcome of the waiver requests and the potential addition of voice capability or if the FCC requires this by rule, the implementation of lawful intercept (CALEA) may be required on the public safety LTE network. The MME, PGW and SGW have the necessary interfaces to support this functionality and public safety LTE networks should use 3GPP TS 33.107 v8.8 (or later) as a reference on how to support this functionality.

***D - Local Control in the Nationwide Public Safety Broadband Network* - Rev F - March 2012**

No specific reference

E - Priority and QoS in the Nationwide Public Safety Broadband Network -

Rev 1.0 - April 17, 2012

No specific reference

F - Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network - *Prepared by: Technical Advisory Board for First Responder Interoperability - Final Report - May 22, 2012*

No specific reference

----- Original Message -----

From: Claudio Lucente

To: Bernard St-Laurent

Cc: Brown, Émilie ; [redacted] s.19(1)

Sent: Friday, January 04, 2013 2:17 PM

Subject: lawful interception of traffic on the PSMBN

Bonjour Bernard,

Bonne Année!

The WG is asking if there is, or will be, a requirement for the operator(s) of the PSMBN to provide the means to carry out a warrant for lawful interception of traffic. Do you know where I can find this answer?

Best regards,

Claudio Lucente, M.Eng, P.Eng
Senior Technical Advisor – 700MHz Public Safety Mobile Broadband Network
Centre for Security Science (CSS)
http://www.css.drdc-rddc.gc.ca
[redacted]

Hawrylak, Maciek

From: [redacted]
Sent: January-09-13 10:28 AM
To: [redacted]
Cc: Brown, Émilie; [redacted] St-Laurent, Bernard; Claudio Lucente
Subject: RE: lawful interception of traffic on the PSMBN

Hi [redacted]
Thanks for your response and additional probing thoughts. Please see my responses embedded below ...

From: [redacted]
Sent: Tuesday, January 08, 2013 7:30 PM
To: [redacted]
Cc: Brown, Émilie; [redacted] Bernard St-Laurent; Claudio Lucente
Subject: Re: lawful interception of traffic on the PSMBN

Hi [redacted]

thanks for your insights.

Hum.... Would the 10+ work orders carry the same legal weight as the single warrant?
[redacted] ***Unfortunately I can't offer a legal opinion on this question. However, I think it is reasonable to assume that all operating entities would be responsible for compliance with Canadian laws.***

The PSMBN governing entity you mention, is it the national entity?
[redacted] ***From my limited visibility into the process, it appears that the PSMBN governing entity would be the national entity. However, I am not certain of this, so in attempt to avoid a faux pas, I elected to describe the function rather than the level of ownership.***

If so, does that mean that the national entity carries some legal obligations and potentially liabilities for the errors and omissions of the regional entities?
[redacted] ***Again, I cannot offer a legal opinion, but this seems like a reasonable assumption.***

Legal intercept is only one such instance, but others exit, not the least 911 (even if 911 calls remain within a region, your statement seems to imply there is only one operator responsible and liable). Do we need a lawyer? (just kidding)! I assume governance addresses those legal aspects.

All of this (and we came across a few other instances) calls for clear SLAs between all entities managing the single network, as roles and responsibilities do cross management domains : LI, 911, customer support, overall end-to-end network performance, network availability & reliability, network survivability...
[redacted] ***I do agree – SLA's will likely be needed for many functions & responsibilities which cross management domains. I suppose this is the crux of my point – LI is just one example, among many, that will require implementation of processes and establish a chain of accountability for functions which cross administrative domains.***

Thanks again.

[redacted]

PS: your statement "...then deliver the resulting information to the PSMBN governing entity, who would then deliver the information to the designated receiving entity.." sounds easy, but this may actually impose additional requirements, as I don't believe this is a standard procedure.

s.19(1)

Good point; I completely agree. Just to clarify my intentions; I did not mean to imply that this would be easy, but rather I was trying to think-through a plausible process which could support LI within the stated context.

----- Original Message -----
From:
To:
Cc: Brown, Émilie ; ; Bernard St-Laurent ; Claudio Lucente
Sent: Tuesday, January 08, 2013 6:54 PM
Subject: RE: lawful interception of traffic on the PSMBN

s.19(1)

Hi
You have some good thoughts here. Regarding the side note if Lawful Intercept is required, it is unclear to me if having regional entities managing the MME, the SGW and/or the PGW will mean that one intercept warrant will translate into 10+ warrants to implement.

For sure, one intercept warrant will need to be implemented in 10+ (or whatever the number greater than one) locations, but would this really imply 10+ *different* warrants? I would think that the warrant process should be unencumbered by physical topology of the LI devices comprising the target operator network. Even in commercial carrier networks, surely there are more than one location for each MME, SGW, and PGW.

I don't know much about this, but I would imagine that a warrant instructs an operator to implement LI for one or more users for a certain period of time. Then it is up to the operator to implement that warrant and deliver the resulting information to the designated receiving entity. The operator in this case should be the entity responsible for operating the PSMBN, and typically would be identified by the organizational entity which has been issued the PLMN ID(s) corresponding to the PSMBN. The PSMBN governing entity should then be responsible for insuring that the warrant is executed, and could do so by distributing the warrant information to the 10+ (or whatever number) regional entities managing the MME, SGW, and/or PGW. Those regional entities would then execute the LI for the prescribed amount of time, and then deliver the resulting information to the PSMBN governing entity, who would then deliver the information to the designated receiving entity. I would think that a similar process would need to be instituted in any case where the LI nodes are distributed in multiple locations.

Hope this helps,

From:
Sent: Tuesday, January 08, 2013 8:55 AM
To: Claudio Lucente; Bernard St-Laurent
Cc: Brown, Émilie;
Subject: Re: lawful interception of traffic on the PSMBN

Hi all,

I scanned through some of the NPSTC documents (and others): the bottom line is they are also unsure if there is any lawful intercept requirement on the PSMBN (how can one dare to potentially intercept intercepters ;-)) and are hoping for clarifications from FCC on this. But for sure, accepting commercial users on the PSMBN will mandate lawful intercept capabilities. The reference to the 3GPP spec is the right one.

As a side note, if the lawful requirement applies, having regional entities managing the MME, the SGW and/or the PGW will mean that one intercept warrant will translate into 10+ warrants to implement.

A - Public Safety Broadband High-Level Statement of Requirements for FirstNet Consideration - Draft Rev C, July 25, 2012

Section 4.1.6 Page 64

Today, the Communications Assistance for Law Enforcement Act (CALEA) is a regulatory requirement supported by commercial carriers to facilitate the capture of user content (including telephony sessions) when a warrant has been issued. The evidence-gathering CALEA capability requires additional equipment and resources in the carrier's network. It is anticipated that FirstNet will have to work with governing officials to determine the applicability of CALEA to the FirstNet network and its subscribers. Therefore, specific user needs are not captured in this document.

B - Public Safety Broadband High-Level Launch Requirements Statement of Requirements for FirstNet Consideration December 7, 2012

Section 4.1.5.0 Page 25

Today, the Communications Assistance for Law Enforcement Act (CALEA) is a regulatory requirement supported by commercial carriers to facilitate the capture of user content (including telephony sessions) when a warrant has been issued. The evidence-gathering CALEA capability requires additional equipment and resources in the carrier's network. It is anticipated that FirstNet will have to work with governing officials to determine the applicability of CALEA to the FirstNet network and its subscribers. While compliance with CALEA for public safety users on a private network is not generally required, NPSTC believes that warrant-triggered collection of a secondary user's content will be necessary if FirstNet supports secondary users. However, specific user needs regarding CALEA are not captured in this document.

C - NPSTC 700 MHZ BROADBAND NETWORK REQUIREMENTS TASK - FORCE (TASK FORCE) - Technical Working Group - 700 MHz LTE Network Interoperability

Page 11

Pending the outcome of the waiver requests and the potential addition of voice capability or if the FCC requires this by rule, the implementation of lawful intercept (CALEA) may be required on the public safety LTE network. The MME, PGW and SGW have the necessary interfaces to support this functionality and public safety LTE networks should use 3GPP TS 33.107 v8.8 (or later) as a reference on how to support this functionality.

***D - Local Control in the Nationwide Public Safety Broadband Network* - Rev F - March 2012**

No specific reference

***E - Priority and QoS in the Nationwide Public Safety Broadband Network* - Rev 1.0 - April 17, 2012**

No specific reference

F - Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network - *Prepared by: Technical Advisory Board for First Responder Interoperability - Final Report - May 22, 2012*

No specific reference

----- Original Message -----
From: Claudio Lucente
To: Bernard St-Laurent
Cc: Brown, Émilie ; [redacted] s.19(1)
Sent: Friday, January 04, 2013 2:17 PM
Subject: lawful interception of traffic on the PSMBN

Bonjour Bernard,

Bonne Année!

The WG is asking if there is, or will be, a requirement for the operator(s) of the PSMBN to provide the means to carry out a warrant for lawful interception of traffic. Do you know where I can find this answer?

Best regards,

Claudio Lucente, M.Eng, P.Eng
Senior Technical Advisor – 700MHz Public Safety Mobile Broadband Network
Centre for Security Science (CSS)
http://www.css.drdc-rddc.gc.ca

s.19(1)

Plunkett, Shawn

From: Plunkett, Shawn
Sent: December-06-12 11:23 AM
To: Kousha, Hasti
Cc: Chayer, Marie-Helene
Subject: Opinion Rquest -
Attachments: PS-SP-SEC-#4498-v2-NOTES_-
2012-12-05.doc

Hi Hasti,
Hope things are well.

Please find enclosed a series of questions related to the paper circulated by CLP regarding the
we would also be interested in knowing the views of the Portfolio agencies (RCMP and CSIS) and CSEC.

Prior to commencing work, we would be grateful if you could provide us with an estimated time to provide a preliminary assessment of our questions. As you may have seen, CLP has requested a meeting for December 19th. Ideally, we would like to have, at least some initial thinking on these issues prior to this meeting, if possible.

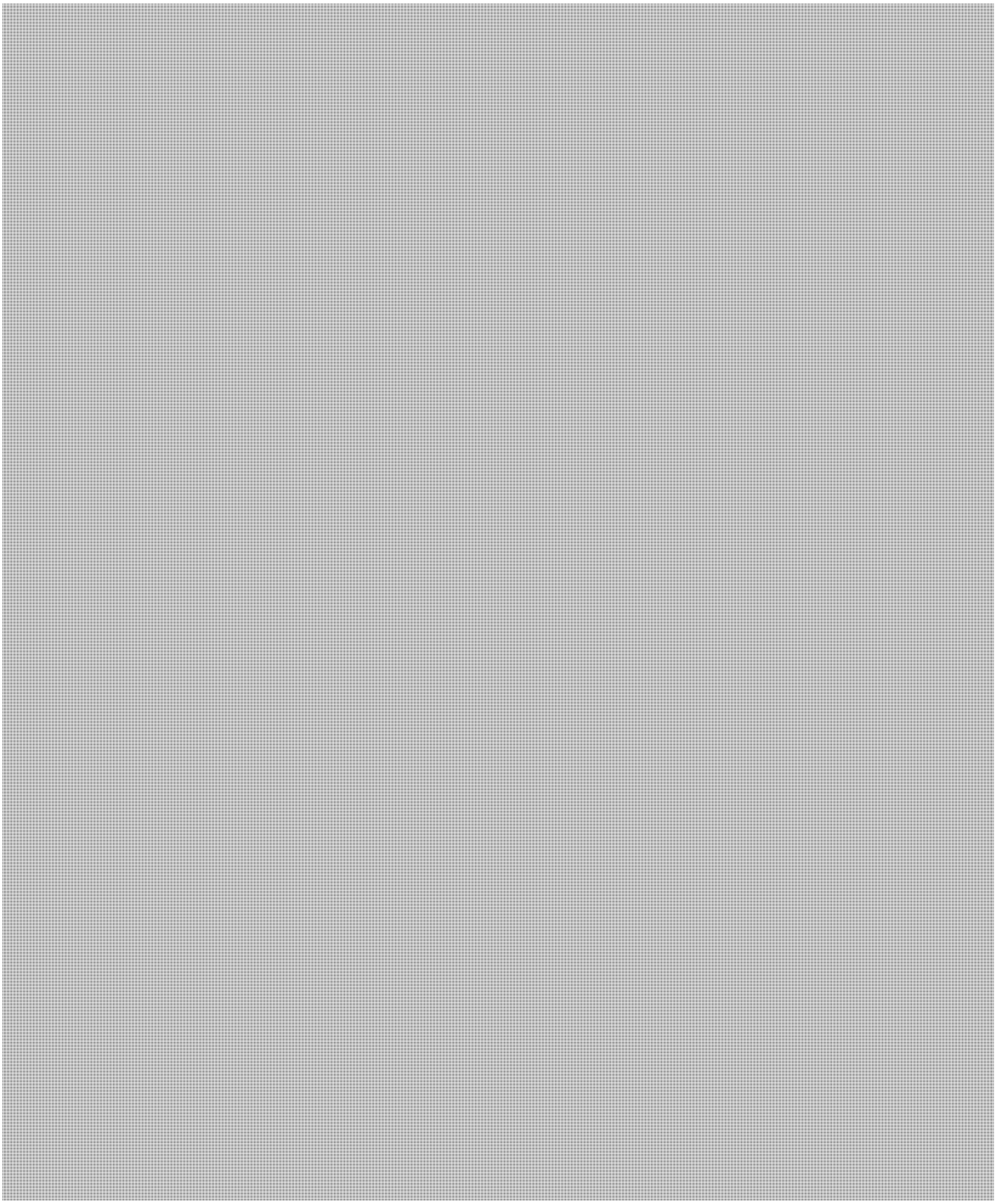
Should you have any questions, please do not hesitate to contact me.

Thanks very much.

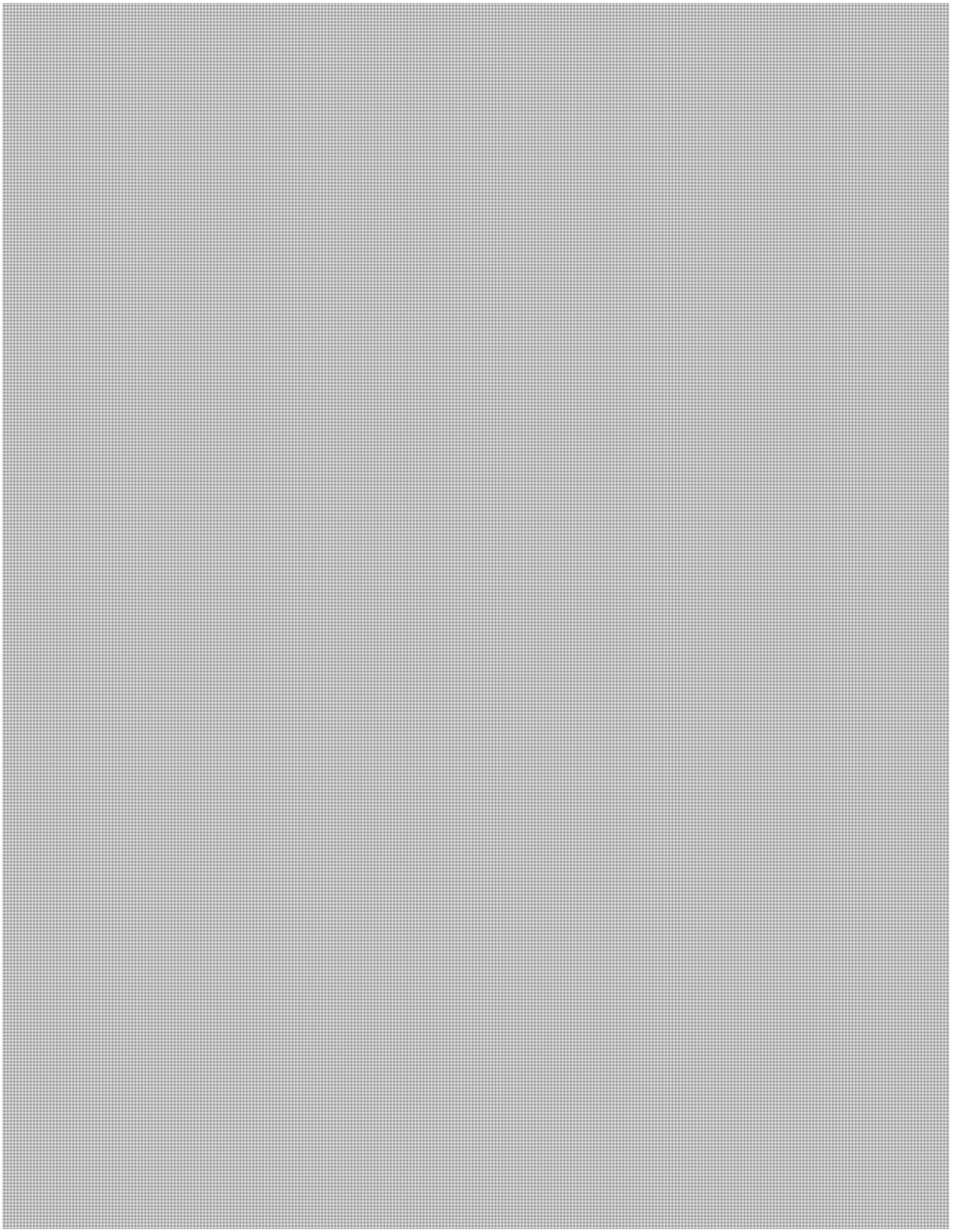
Shawn

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

Solicitor-Client Privilege



s.23



s.23

Thompson, Julie

From: Plunkett, Shawn
Sent: Friday, November 30, 2012 10:39 AM
To: Chayer, Marie-Helene
Cc: Thompson, Julie
Subject: Public Comments on Lawful Intercept Condition of Licence - 2500 MHz Consultation

Marie-Hélène,

Last week Industry Canada posted the public comments received regarding the rules and conditions of licences relating to the 2500 MHz spectrum auction.
Comments Received on Gazette Notice DGSO-004-12 Consultation on a Licensing Framework for Broadband Radio Service (BRS) — 2500 MHz Band

The vast majority of the replies mirror the comments made under the 700 MHz band consultation (see report far below). Below are some of the major comments received:

1) Near unanimous opposition to change in condition of licence (Bell, CWTA, Eastlink, WIND, MTS Allstream, Public Mobile, Quebecor, Rogers, Sasktel, Telus). Only Mobilicity stated no comment, while several small or independent organizations were silent.

2) C-30: All major carriers and CWTA argued that changes of this magnitude are more appropriately done with legislation and not that the condition of licence.

3) 'Substantial new obligations' to carriers. Most major carriers and Bell in particular noted that as standard 1 requires access to the entire telecommunication transmitted removing circuit-switched would open up to Internet and Broadcasting services and thus place 'substantial new obligations' on carriers.

4) SGES Revisions: Major carriers noted that changes to the SGES should be done through an accredited standards body and that the lawful intercept obligations should be limited to circumstances where commercially-available, standards-based technology is available. Non-standard based solutions should be funded by the government (Bell).

5) Auction Proceeds: Bell re-iterated its previous comment that spectrum auction proceeds should be used to fund lawful access initiatives.

We are now in the 'reply comment' phase, where the public can reply to the comments posted on IC's website. Parties have until December 17, 2012 to make 'reply comments'. The reply comments for the 700 MHz auction were essentially re-iterating support for the opposition to the condition of licence (See Report on reply comments– RDIMS 705722)

In sum, there is no new information, nor any surprises with the responses for this consultation.

Please let me know if you have any further questions.

Merci

Shawn

From: Plunkett, Shawn
Sent: June-29-12 11:17 AM
To: Kingsley, Michèle
Cc: Kwavnick, Andrea; Hawrylak, Maciek
Subject: Overview - Public Comments on Lawful Intercept Condition of Licence

Michèle,

Yesterday afternoon, Industry Canada posted the public comments received regarding the rules and conditions of licence relating to the 700 MHz spectrum auction.
Comments Received on Gazette Notice DGSO-002-12 — Consultation on a Licensing Framework for Mobile Broadband Services (MBS) — 700 MHz Band

Several respondents provided comments on the lawful intercept condition of licence. (Bell, the Canadian Wireless Telecommunications Association, Globalive, MTS Allstream, SSi Group of Companies, Rogers, TbayTel and Telus.) The responses were similar in nature, using similar language, thus implying a concerted effort. It should also be noted that several commenters referenced CWTA`s comments in their response on lawful interception.

I am currently undertaking a more rigorous review, but after a preliminary look, some themes have appeared:

1) *Majority Opposed to LI Changes*: With the exception of the Ssi Group (an Internet Service Provider based in Yellowknife), all commenters were opposed to changes to the Lawful Interception Condition of Licences The primary reason indicated was that changes would introduce new and significant obligations on licence holders.

2) *Legislation should be vehicle for LI changes*: There was a general consensus that the condition of licence should not be changed and that the appropriate venue for making significant changes of this nature is through the legislation. It was argued that the CoL should be unchanged until Parliament passes the legislation, at which time the CoL can be updated (if needed). It was also noted that the lawful intercept condition of licence should reflect existing legislative requirements and should not anticipate future legislative requirements.

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

3) *SolGen Standards.* Two main points were raised regarding the SGES:
   a. Changes to the Solicitor General Standards should be part of a separate consultation.
   b. Any changes to the standards should be done in accredited standard-setting bodies and should only require standard-based and commercially available solutions.

Potential Options:

If you have time either today or early next week to discuss, that would be best given that there is a very short turnaround for Reply Comments and it would likely take time to receive the necessary consultations and approvals.

Thanks.

Shawn Plunkett
Senior Policy Advisor / Conseiller principal en politiques
Investigative Technologies and Telecommunications Policy (ITTP) /
Technologies d'enquêtes et politiques des télécommunications (TEPT)
National Security Operations Directorate / Direction des opérations de sécurité nationale

Public Safety Canada / Sécurité Publique Canada
Tel: (613) 990-7066
Email: shawn.plunkett@ps.gc.ca

Spectrum Management and Telecommunications

Comments Received on Gazette Notice DGSO-004-12

Information from external sources, not subject to the *Official Languages Act* has been provided as a courtesy and is available only in the language in which it was provided.

Some of the information on this Web page has been provided by external sources. The Government of Canada is not responsible for the accuracy, reliability or currency of the information supplied by external sources. Users wishing to rely upon this information should consult directly with the source of the information. Content provided by external sources is not subject to official languages, privacy and accessibility requirements.

PDF Readers

Posted on Industry Canada website: November 22, 2012

Comments Received

Companies and Organizations

Provincial and Municipal Governments

Private Individuals

Related Documents

Gazette Notice DGSO-004-12 — Consultation on a Licensing Framework for Broadband Radio Service (BRS) — 2500 MHz Band

Consultation on a Licensing Framework for Broadband Radio Service (BRS) — 2500 MHz Band

Reply Comments

Companies and Organizations

- **Bell Mobility Inc.**
  - Letter (PDF, 15 KB, 1 page)
  - Submission (PDF, 140 KB, 45 pages)
- **British Columbia Broadband Association (BCBA)**
  - Submission (PDF, 673 KB, 3 pages)
- **Canadian Wireless Telecommunications Association (CWTA)**
  - Submission (PDF, 201 KB, 5 pages)
- **Eastlink**
  - Submission (PDF, 426 KB, 15 pages)
- **Globalive Wireless Management Corp.**
  - Letter (PDF, 43 KB, 1 page)
  - Submission (PDF, 371 KB, 16 pages)
- **Mobilicity**
  - Submission (PDF, 491 KB, 37 pages)

Print RSS

- **MTS Allstream**
  - Submission (PDF, 80 KB, 14 pages)

- **Public Mobile Inc.**
  - Submission (PDF, 6172 KB, 19 pages)

- **Quebecor Media Inc. and Videotron G.P.**
  - Letter (PDF, 25 KB, 1 page)
  - Submission (PDF, 85 KB, 20 pages)

- **Rogers Communications Partnership**
  - Submission (PDF, 286 KB, 52 pages)

- **SaskTel**
  - Letter (PDF, 25 KB, 1 page)
  - Submission (PDF, 33 KB, 7 pages)

- **TELUS Communications Company**
  - Submission (PDF, 354 KB, 46 pages)

- **Xplornet**
  - Submission (PDF, 234 KB, 18 pages)

Provincial and Municipal Governments

- **Kativik Regional Government**
  - Submission (PDF, 148 KB, 9 pages)

Private Individuals

- **Taylor, Dr. Gregory and Middleton, Dr. Catherine (Ryerson University)**
  - Submission (PDF, 20 KB, 6 pages)

Government of Canada / Gouvernement du Canada

Canada

Industry Canada

Spectrum Management and Telecommunications

Comments Received on Gazette Notice DGSO-002-12 — Consultation on a Licensing Framework for Mobile Broadband Services (MBS) — 700 MHz Band

Some of the information on this Web page has been provided by external sources. The Government of Canada is not responsible for the accuracy, reliability or currency of the information supplied by external sources. Users wishing to rely upon this information should consult directly with the source of the information. Content provided by external sources is not subject to official languages, privacy and accessibility requirements.

Information from external sources, not subject to the *Official Languages Act* has been provided as a courtesy and is available only in the language in which it was provided.

Companies and Organizations

Bell Mobility Inc.
- Letter (PDF, 17 KB, 1 page)
- Submission (PDF, 169 KB, 43 pages)

British Columbia Broadband Association (BCBA)
- Submission (PDF, 352 KB, 6 pages)

Canadian Wireless Telecommunications Association (CWTA)
- Submission (PDF, 119 KB, 5 pages)

Cogeco Cable Inc.
- Submission (PDF, 130 KB, 8 pages)

Eastern Ontario Regional Network
- Submission (PDF, 347 KB, 8 pages)

Eastlink
- Submission (PDF, 487 KB, 23 pages)

Globalive Wireless Management Corp.
- Letter (PDF, 67 KB, 1 page)
- Submission (PDF, 414 KB, 16 pages)

Ice Wireless
- Submission (PDF, 79 KB, 1 page)

Mobilicity
- Submission (PDF, 283 KB, 47 pages)

MTS Allstream

Related Documents

Gazette Notice DGSO-002-12 — Consultation on a Licensing Framework for Mobile Broadband Services (MBS) - 700 MHz Band

Consultation on a Licensing Framework for Mobile Broadband Services (MBS) - 700 MHz Band

Reply Comments

Applicants and Status of Applications for the Auction of Spectrum Licences for Mobile Broadband Services (MBS) in the 700 MHz Band

- Submission (PDF, 100 KB, 15 pages)

Public Interest Advocacy Centre (PIAC)
- Submission (PDF, 543 KB, 7 pages)

Public Mobile Inc.
- Submission (PDF, 527 KB, 16 pages)

Quebecor Media Inc. and Videotron G.P.
- Letter (PDF, 25 KB, 1 page)
- Submission 1 (PDF, 98 KB, 25 pages)
- Submission 2 (PDF, 91 KB, 28 pages)

Rogers Communications Partnership
- Submission (PDF, 355 KB, 60 pages)

SaskTel
- Letter (PDF, 26 KB, 1 page)
- Submission (PDF, 78 KB, 18 pages)

Sogetel Mobilité
- Letter (PDF, 299 KB, 1 page)
- Submission 1 (PDF, 291 KB, 5 pages)
- Submission 2 (PDF, 779 KB, 31 pages)

SSi Group of Companies
- Letter (PDF, 146 KB, 1 page)
- Submission (PDF, 273 KB, 13 pages)

Tbaytel
- Submission (PDF, 651 KB, 14 pages)

TELUS Communications Company
- Submission (PDF, 267 KB, 43 pages)

Xplornet
- Submission (PDF, 319 KB, 19 pages)

Provincial and Municipal Governments

Ontario Ministry of Agriculture, Food and Rural Affairs
- Submission (PDF, 68 KB, 3 pages)

Private Individuals

Hambly Odame, Dr. Helen (University of Guelph)
- Submission (PDF, 227 KB, 2 pages)

Taylor, Dr. Gregory and Middleton, Dr. Catherine (Ryerson University)
- Submission (PDF, 130 KB, 5 pages)

Thompson, Julie

From: Plunkett, Shawn
Sent: Tuesday, July 31, 2012 1:27 PM
To: Kingsley, Michèle
Cc: Kwavnick, Andrea; Hawrylak, Maciek
Subject: Overview - Reply Comments on LI Condition of Licence - 700 MHz Spectrum Auction

Michèle,

The Reply Comments as part of the 700 MHz consultation are now publicly available on the Industry Canada website. These reply comments are an opportunity for commentators to review and respond to comments put forth during the initial consultation period. I spoke with IC yesterday and they stated that the next step will be for IC to review all the comments and reply comments. These comments may inform their decision paper outlining the rules and conditions for the auction. They did not yet have a timeline for the release of this paper (which will include a decision on the LI CoL).

Most of the replies reiterate or indicate support for the comments made during the initial round, notably with respect to the following:

1) All those who provided reply comments on the LI CoL were opposed to the proposed wording removing 'circuit-switched' (Bell, CWTA, Rogers, Telus, Eastlink, Public Mobile and Shaw). It should be noted that Bell stated that the unanimous view based on initial comments is that the LI CoL should not be changed at this time. (*This is incorrect as a small TSP 'SSi Group' agreed with proposed wording.).*The CWTA refers to the 'overwhelming majority'.

2) Most explicitly indicated that the proposed wording would result in new and significant obligations on licence holders.

3) Several noted it was inappropriate to make these changes while Parliament is reviewing related legislation.

4) Changes to SGES should be done through a separate consultation.

5) All LI requirements(including SGES) should be linked to commercially-available technology and industry standards.

[redacted] Unsure what IC's response to this would be.

2500MHz Auction

On a related note, IC indicated that they have an initial draft of the 2500 MHz consultation paper that is being reviewed by their legal staff. Once they have a more 'polished' working draft, I was promised to receive a copy of the LI paragraph. IC [redacted]

Shawn Plunkett
Senior Policy Advisor / Conseiller principal en politiques
Investigative Technologies and Telecommunications Policy (ITTP) /
Technologies d'enquêtes et politiques des télécommunications (TEPT)
National Security Operations Directorate / Direction des opérations de sécurité nationale

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

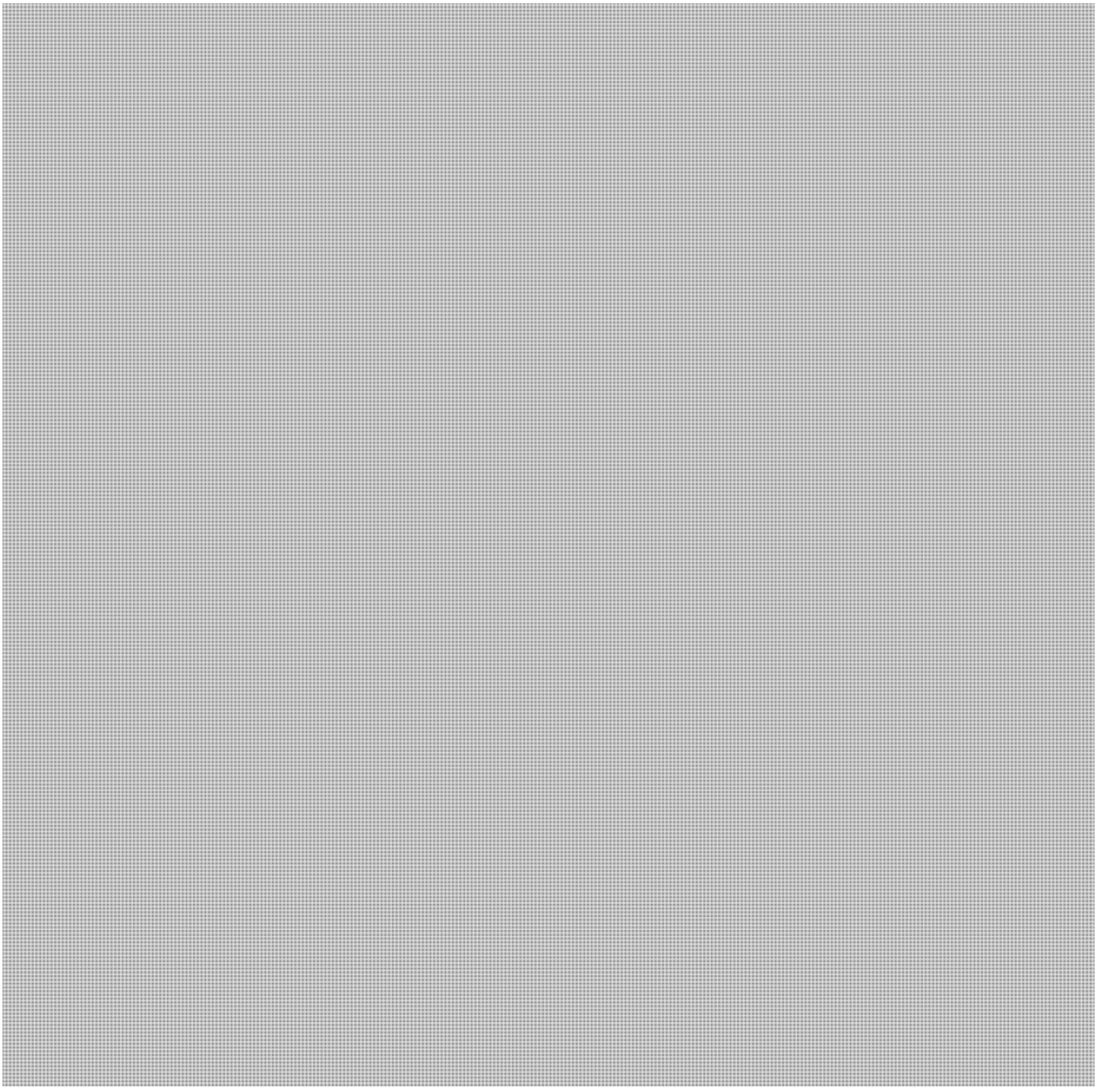
Public Safety Canada / Sécurité Publique Canada
Tel: (613) 990-7066
Email: shawn.plunkett@ps.gc.ca

s.21(1)(a)

Internal use only
29 November 2012

Lawful Access Regulations Working Group
Proposal for look-up compensation scheme (IPCECA s.21)

The Lawful Access Regulations Working Group, which is chaired by Public Safety and whose members include the RCMP, CSIS, the Competition Bureau, Industry Canada, and Justice Canada, has developed the following compensation scheme for the provision of basic subscriber information, pursuant to section 21 of the *Investigating and Preventing Criminal Electronic Communications Act*.



Pages 131 to / à 134

are withheld pursuant to section

sont retenues en vertu de l'article

21(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

CONFIDENTIAL

DATE:

File No.: NS 6950
RDIMS: Dragon 4184

MEMORANDUM FOR THE SENIOR ASSISTANT DEPUTY MINISTER

REPORT FROM THE BRIGHTON

(For information)

ISSUE

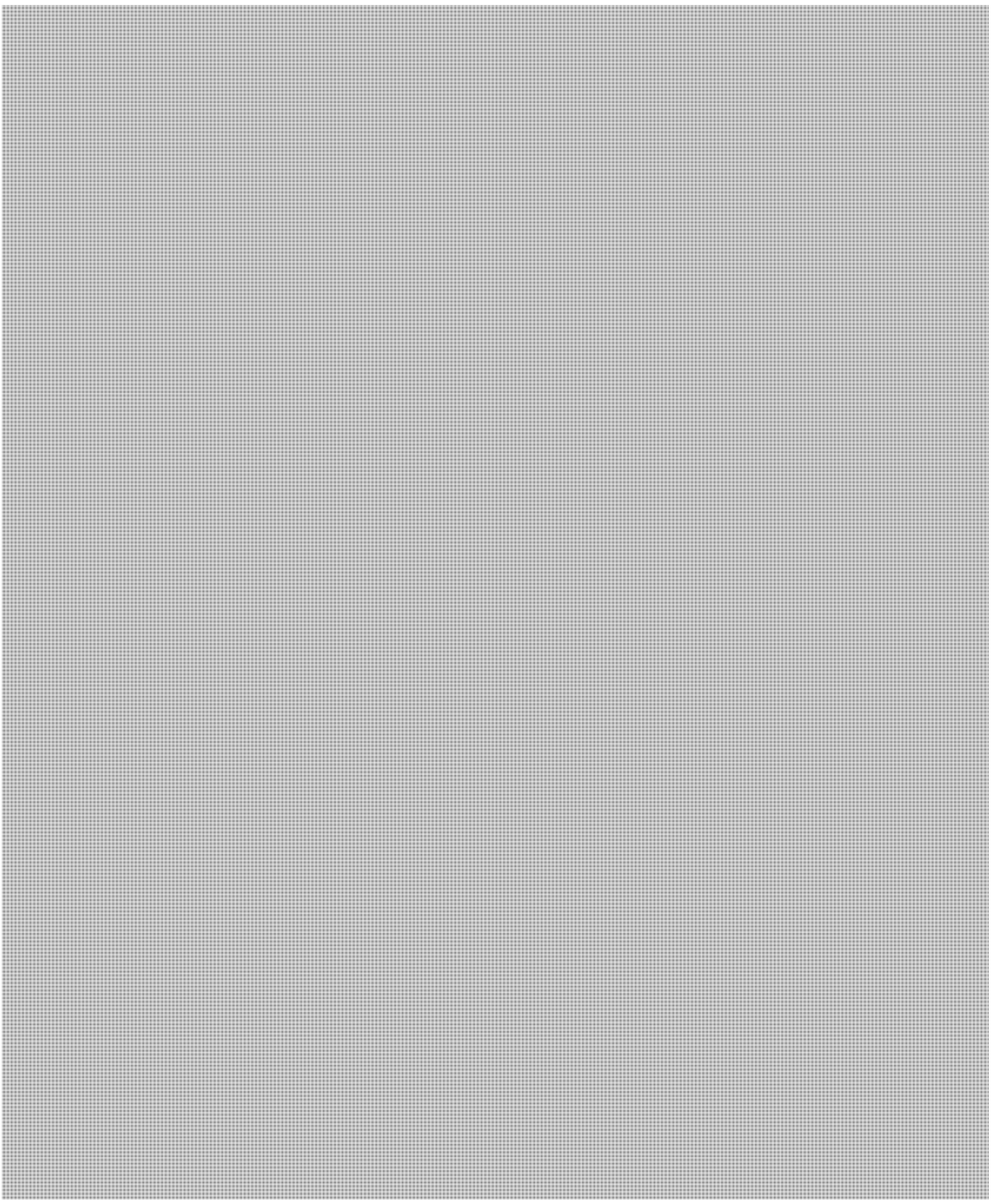
Maciek Hawrylak, Senior Policy Advisor, Investigative Technology and Telecommunications Policy Division, attended the in Brighton, United Kingdom, from November 12-16, 2012.

BACKGROUND

In addition to the Public Safety representative, Canada's delegation included two CSIS employees.

s.15(1) - Int'l

.../2



s.15(1) - Int'l

…/3

CONSIDERATIONS

[redacted]

Should you require additional information, please do not hesitate to contact me at 613-993-4595 or Marie-Hélène Chayer, Director, Investigative Technologies and Telecommunications Policy, at 613-949-3181.

Michael MacDonald
Director General
National Security Operations Directorate

Prepared by: Maciek Hawrylak

Emmett, Jamie s.21(1)(b)

From: Plunkett, Shawn
Sent: November-16-12 2:17 PM
To: Chayer, Marie-Helene
Cc: Kousha, Hasti
Subject: REPORT- [redacted] Meeint (Nov 16)

Marie,

As discussed, this morning I attended a meeting called by Criminal Law Policy to discuss the meaning of [redacted] RCMP legal and CSIS legal attended. Counsel from PPSC and several members of CLP were also in attendance. The meeting's objective was to provide CLP's thinking (in the form of a discussion paper) regarding [redacted] While the meeting included quite a bit of legal musings [redacted]

1) [redacted]

2) [redacted]

3) There was some discussion as to whether to the statement made at the top of page 41 (beginning with "These considerations…") represented a categorical position. [redacted]

4) While the paper did a thorough job mapping the various components surrounding this issue, it was noted by the RCMP that 2 years have been spent examining the issue, without any real substantive work done on developing practical solutions. While there was no actual discussion on this issue (as it was made at the very end of the meeting) it appears to be a valid point and one that will likely be raised by operational folks, as well as P/T partners.

Please let me know should you have any questions.

Shawn

Emmett, Jamie

From: Plunkett, Shawn
Sent: November-19-12 9:22 AM
To: Yves Desjardins (Yves.Desjardins@rcmp-grc.gc.ca); [redacted]
Cc: Chayer, Marie-Helene
Subject: REPORT- [redacted] Meeting (Nov 16)

Colleagues, FYI

Friday morning I attended a meeting called by Criminal Law Policy to discuss the meaning [redacted] RCMP legal and CSIS legal attended. Counsel from PPSC and several members of CLP were also in attendance. The meeting's objective was to provide CLP's thinking (in the form of a discussion paper) regarding [redacted] While the meeting included quite a bit of legal musings [redacted]

1) [redacted]

2) [redacted]

3) There was some discussion as to whether the following statement, made at the top of page 41, represented a categorical position [redacted]

4) While the paper did a thorough job mapping the various components surrounding this issue, it was noted by the RCMP that 2 years have been spent examining the issue, without any real substantive work done on developing practical solutions. While there was no actual discussion on this issue (as it was made at the very end of the meeting) it appears to be a valid point and one that will likely be raised by operational folks, as well as P/T partners.

Please let me know should you have any questions.

Shawn

s.15(1) - Subv
s.21(1)(b)

SECRET

Preliminary Options for Addressing Challenges with Decryption of Lawfully Accessed Communications

ISSUE

Decryption is a growing challenge for law enforcement and national security authorities. Encryption programs are becoming increasingly sophisticated and difficult to crack, thereby rendering it difficult for authorities to access the content of lawfully intercepted communications.

ENCRYPTION IN CANADA

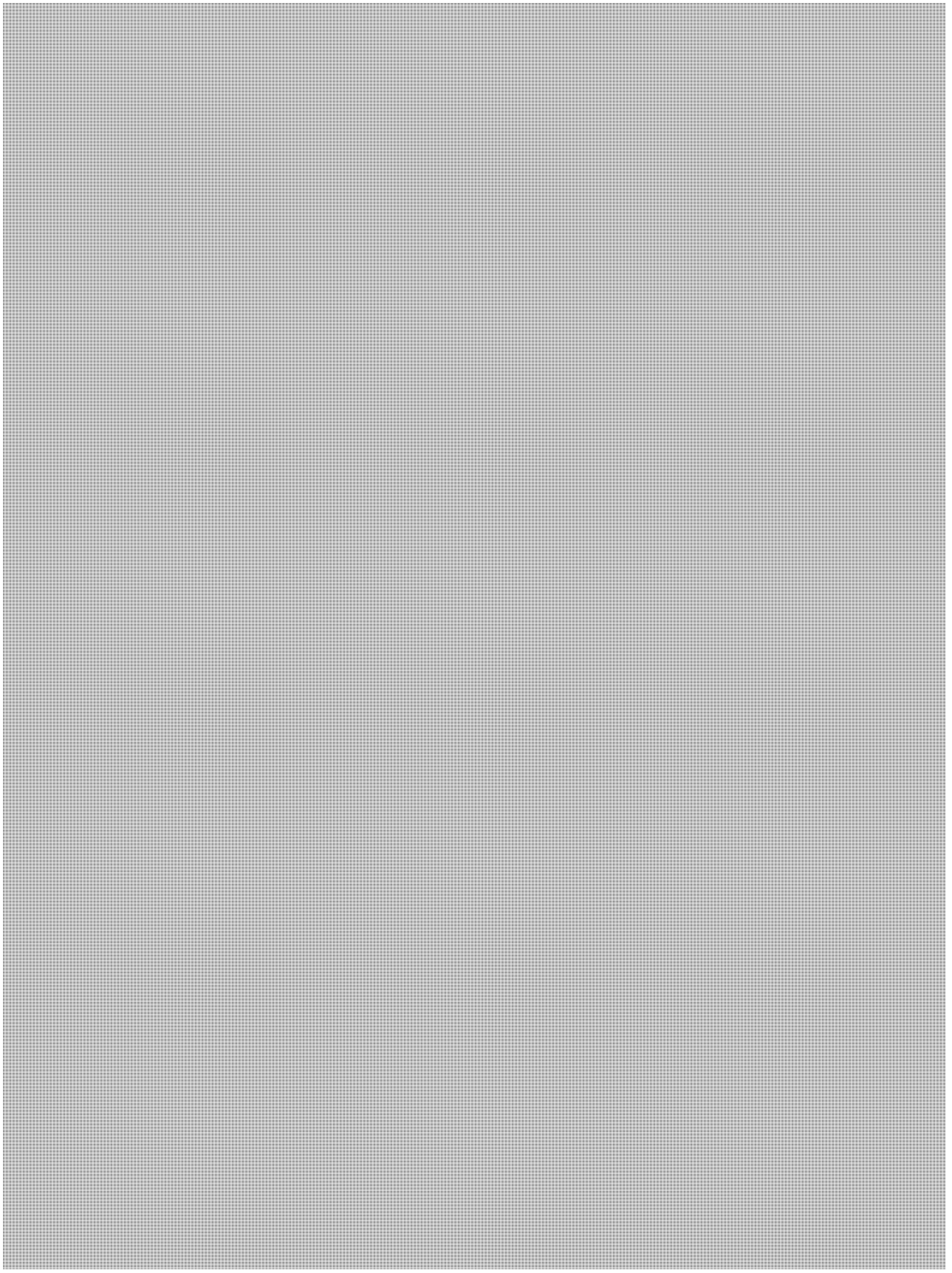
The Government of Canada has recognized encryption as an essential component of protecting government, businesses and consumer information. In 1998, the Government committed to implementing a cryptography policy based on a consultative paper titled "A Cryptography Policy Framework for Electronic Commerce". The policy allows Canadians to freely develop, import and use whatever cryptology products they wish, without being subject to mandatory key recovery requirements or licensing regimes. It takes into consideration international export agreements[1].

In recognition that law enforcement and national security agencies have a legitimate need to access decrypted data to ensure public safety, the policy also proposed "amendments to the *Criminal Code* and other statutes as necessary" to criminalize the wrongful disclosure of keys, deter the use of encryption in the commission of a crime, and apply existing interception, search and seizure and assistance procedures to cryptographic situations and circumstances. Consideration of proposed amendments took place at a number of forums including by the Federal/Provincial/Territorial Cybercrime Working Group, the Canadian Association of Chiefs of Police eCrime Committee and the National Tech Crime Advisory Group. To date, specific amendments to existing legislation have not been proposed; however, the introductions of anti-spam and lawful access legislation were a result of some of these discussions.

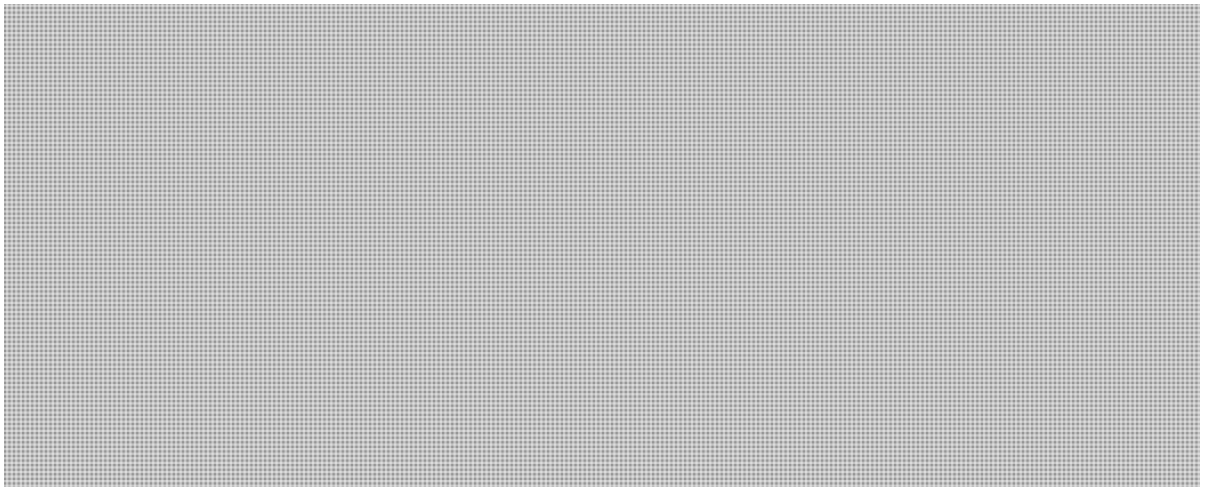
As the use of the internet has grown in popularity, so too has the use of encryption. Faster computer systems, current programming languages, and the availability of open source codes make encryption applications easier, faster and cheaper for anyone to develop and use. Encryption can be applied to communications by any number of entities, including telecommunications service providers (TSPs) providing an Internet service ("the access-providing TSP"), a webmail or application service provider (i.e. gmail.com, Skype), or by individuals or businesses themselves using software. The ease

---

[1] Canada is part of the *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*, along with 32 other signatories, all of whom have agreed to place export restrictions on items which could be used for the development of enhancement of military capabilities that undermine the goal of regional and international stability.



s.15(1) - Int'l
s.16(2)



INTERNATIONAL APPROACHES

The following are samples of some international approaches taken to provide lawful access to decrypted communications. All are limited by jurisdictional boundaries.

Russia

Through a Presidential Decree, Russia has outlawed any encryption software or hardware device not approved by the Government from being used within its borders. It is unclear how and when this Presidential directive is enforced if a service or software provider is based outside the country.

India

Under the *Information Technology Act*, last updated in 2000, anyone that is in charge of a "computer resource" to which encryption has been applied must "extend all facilities and technical assistance to decrypt the information" when requested to do so. Failure to assist could result in a jail term of up to 7 years.

Finland

Under the "*Coercive Measures Act*", last updated in 2007, an information system owner, administrator or other person is required to provide law enforcement with any passwords or other similar information. This excludes the suspect in a case for which the request is being made, to address issues related to self-incrimination.

Australia

In July 2012, Australian officials put forward a discussion paper to the Parliamentary Joint Committee on Intelligence and Security expressly seeking their views on amending the *Telecommunications (Intercept and Access) Act 1979* to make it an offence for service providers not to assist in decryption. Discussions are ongoing.

United Kingdom

Part III of the *Regulatory Investigative Powers Act* (RIPA) requires persons or organizations to supply decrypted information or keys to the government when requested to do so. There are jail terms associated with non-compliance, and to date it appears that at least three individuals have been convicted under the legislation.

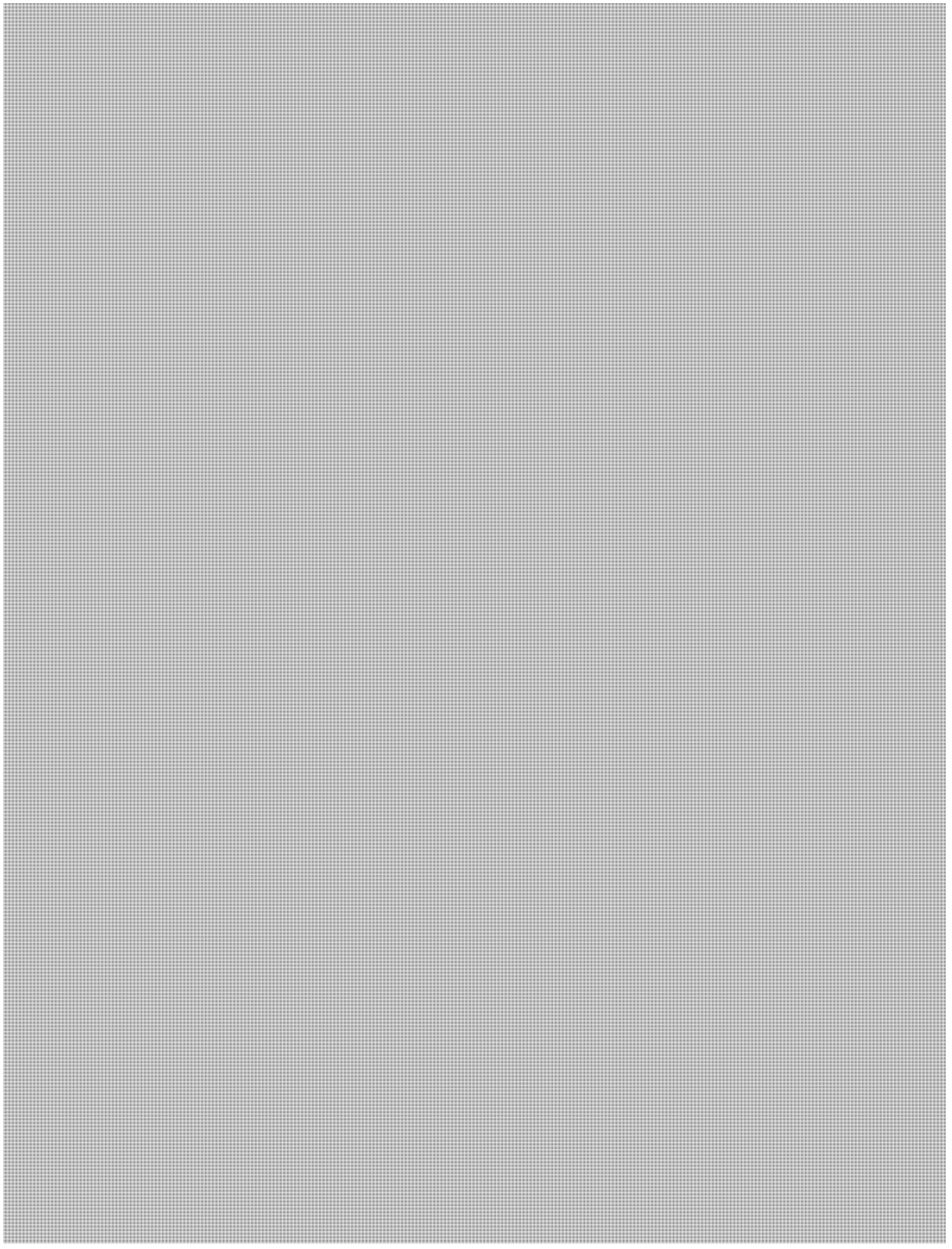
United States

Under the *Communications Assistance for Law Enforcement Act*, carriers who encrypt data must apply the decryption, but do not need to decrypt any communication encrypted by a subscriber or customer. This is similar to what is proposed in current lawful access legislation in Canada.

OPTIONS TO ADDRESS CHALLENGES

The options below reflect a range of responses

s.21(1)(a)



s.21(1)(a)

Plunkett, Shawn

From: Plunkett, Shawn
Sent: November-14-12 3:01 PM
To: Thompson, Julie
Subject: FW: Lawful Interception Condition of Licence - 700MHz Spectrum

FYI

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

From: Chayer, Marie-Helene
Sent: November-14-12 2:55 PM
To: david.bosquet@ic.gc.ca
Cc: MacDonald, Michael; Plunkett, Shawn
Subject: Lawful Interception Condition of Licence - 700MHz Spectrum

David,

It was nice talking to you last Thursday. We very much appreciate your consulting us on the lawful interception condition of licence for the 700 MHz spectrum auction.

I would like to note that Industry Canada and Public Safety Canada worked together diligently on the specific language of the lawful interception condition of licence prior to the launch of the second phase of the 700 MHz public consultation. It was in this spirit of cooperation that we collectively determined that removing 'circuit-switched voice telephony' would be the best approach for moving forward on the lawful interception condition of licence. We were very grateful to see that this was reflected in Industry Canada's public consultation.

[redacted] As licences on the 700 MHz are being proposed for 20 years, we feel that the wording of the condition should be as broad as possible. [redacted]

[redacted] Should the TSP not believe they are in a reasonable position to comply with any portion of the lawful interception condition of licence, they could still apply for forbearance. [redacted] The forbearance process allows us (PS and Portfolio agencies) to develop stronger partnerships with the TSPs and to have discussions that lead to mutually beneficial arrangements.

However, while we strongly believe that [redacted] is the best way forward, we would offer the following as a possible alternative. (Please note that this language would need further consultation with the Public Safety Portfolio before being assigned to licences.)

[redacted]

This condition would be technology and service neutral and retain the forbearance regime as is now for [redacted]

I am happy to discuss further at your convenience and I'm looking forward to continuing to work with you on developing a condition of licence that supports a strong and safe telecommunications sector in Canada. With that in mind, I would be grateful if you could share your thoughts on our proposal as well as the next steps.

Thanks again for consulting us.

Marie-Hélène

s.21(1)(a)

Marie-Hélène Chayer
Director – Investigative Technology and Telecommunications Policy /
Directrice – Politique sur les technologies d'enquêtes et les télécommunications
National Security Operations Division / Division des Opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
(613)949-3181

31 octobre 2012

Public Safety Canada / Sécurité publique Canada

SECRET

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

DATE: 31 October 2012

File No.: NS 6950-03 / 391118
RDIMS No.: Dragon 3779

MEMORANDUM FOR THE DIRECTOR GENERAL

FORBEARANCE QUARTERLY REPORT, FY 2012-2013, Q2

(Information only)

ISSUE

To provide an update on issues related to forbearance from the lawful interception condition of licence (LIC) for the second quarter of FY 2012-2013; from July 1, 2012 to September 30, 2012. The next report is due January 31, 2012. A copy of the *Solicitor General Enforcement Standards for Lawful Interception of Telecommunications* (SGES) is attached at **TAB A.**

STATUS OF FORBEARANCE REQUESTS

[redacted]

Status: [redacted]

Report: [redacted]

Canada

.../2

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

Next Steps: [redacted] Agreed

Forbearance expiry date: [redacted]

[redacted]

Status: [redacted]

Report: [redacted]

Forbearance expiry date: [redacted]

Next Steps: [redacted] Agreed

[redacted]

Status: [redacted]

Report: [redacted]

…/3

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

[redacted]

Forbearance expiry date: [redacted]

Next Steps: [redacted] or earlier Agreed

[redacted]

Status: [redacted]

Report: [redacted]

Forbearance expiry date: [redacted]

Next Steps: [redacted] Agreed

[redacted]

Status: [redacted]

Report: [redacted]

Next Steps: [redacted] Agreed

Forbearance expiry date: [redacted]

.../4

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

MEETINGS WITH PORTFOLIO

[redacted]

Do we need a Dem meeting at some point?

LOOK AHEAD

- October 2012
  - Recommendation to IC on [redacted] Forbearance (October 3)
  - Cross-Border Interception Meeting with DoJ (October 18)

- November 2012
  - Meeting with the RCMP and CSIS on the Forbearance Regime (November 7)
  - Forbearance Expiry – [redacted] (November 30)
  - Forbearance Expiry – [redacted] (November 30)

- December 2012
  - Forbearance Expiry – [redacted] (December 30)
  - Forbearance Expiry – [redacted] (December 30)

Should you require additional information, please do not hesitate to contact me at 613-949-3181 or Shawn Plunkett, Senior Policy Advisor, Investigative Technologies and Telecommunications Policy at 613-990-7066.

Marie-Hélène Chayer
Director, Investigative Technologies and Telecommunications Policy
National Security Operations

Prepared by: Julie Thompson

Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table

Solicitor Generals Standards

Standard 1: Law enforcement agencies require access to the entire telecommunications transmitted, or caused to be transmitted, to and from the number or other identifier of the target service used by the interception subject. Law enforcement agencies also require access to the call-associated data that is generated to process the call.

Standard 2: Law enforcement agencies require access to all mobile interception subjects operating temporarily or permanently within a telecommunications system.

Standard 3: Law enforcement agencies require access in cases where the interception subject may be using features to divert calls to other telecommunications service or terminal equipment, including calls that traverse more than one network or are processed by more than one network operator/service provider before completing.

Standard 4: Law enforcement agencies require that the telecommunications to and from a target service be provided to the exclusion of any telecommunications that do not fall within the scope of the interception authorization.

Standard 5: Law enforcement agencies require access to available call associated data such as:

A) Signaling of access ready status

B) Called party number for outgoing connections even if there is no successful connection established

C) Calling party number for incoming connections even if there is no successful connection established

D) All digits dialed by the target, including post-connection dialed digits used to activate features such as conference calling and call transfer

E) Beginning, end, and duration of the connection

F) Actual destination and intermediate directory numbers if call has been diverted.

Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table

Standard 6: Law enforcement agencies require information on the most accurate geographical location known to the network for mobile subscribers.

Standard 7: Law enforcement agencies require data on the specific service used by the interception subject and the technical parameters for that type of communication.

Standard 8: Law enforcement agencies require a real- time, full-time monitoring capability for the interception of telecommunications. Call associated data should also be provided in real-time. If call associated data cannot be made available in real time, law enforcement agencies require the data to be available as soon as possible upon call termination.

Standard 9: Law enforcement agencies require network operators/service providers to provide one or more interfaces from which the intercepted communications can be transmitted to the law enforcement monitoring facility. These interfaces have to be commonly agreed on by the interception authorities and the network operators/service providers. Other issues associated with these interfaces will be handled according to generally accepted practices.

Standard 10: Law enforcement agencies require network operators/service providers to provide call associated data and call content from the target service in a way that allows for the accurate correlation of call associated data with call content.

Standard 11: Law enforcement agencies require that the format for transmitting the intercepted communications to the monitoring facility be a generally available format.

Standard 12: If network operators/service providers initiate encoding, compression or encryption of telecommunications traffic, law enforcement agencies require the network operators/service providers to provide intercepted communications en clair.

Standard 13: Law enforcement agencies require network operators/service providers to be able to transmit the intercepted communications to the law enforcement monitoring facility via fixed or switched connections.

Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table

Standard 14: Law enforcement agencies require that the transmission of the intercepted communications to the monitoring facility meet applicable Government of Canada security requirements.

Standard 15: Law enforcement agencies require interceptions to be implemented so that neither the interception target nor any other unauthorized person is aware of any changes made to fulfill the interception order. In particular, the operation of the target service must appear unchanged to the interception subject.

Standard 16: Law enforcement agencies require the interception to be designed and implemented to preclude unauthorized or improper use and to safeguard the information related to the interception.

Standard 17: Law enforcement agencies require network operators/service providers to protect information on which and how many interceptions are being or have been performed, and not disclose information on how interceptions are carried out.

Standard 18: Law enforcement agencies require network operators/service providers to ensure that intercepted communications are only transmitted to the monitoring agency specified in the interception authorization.

Standard 19: Based on a lawful inquiry and before implementation of the interception, law enforcement agencies require **(1)** the interception subject's identity service number or other distinctive identifier, **(2)** information on the services and features of the telecommunications system used by the interception subject and delivered by network operators/service providers, and **(3)** information on the technical parameters of the transmission to the law enforcement monitoring facility.

Standard 20: During the interception law enforcement agencies may require information and/or assistance from the network operators/service providers to ensure that the communications acquired at the interception interface are those communications associated with the target service.

Standard 21: Law enforcement agencies require network operators/service providers to make provisions for implementing a number of simultaneous intercepts. Multiple interceptions may be required for a single target service to allow monitoring by more than one law enforcement agency. In this case,

network operators/service providers should take precautions to safeguard the identities of the monitoring agencies and ensure the confidentiality of the investigations.

Standard 22: Law enforcement agencies require network operators/service providers to implement interceptions as quickly as possible (in urgent cases within a few hours or minutes). The response requirements of law enforcement agencies will vary by the type of target service to be intercepted.

Standard 23: For the duration of the interception, law enforcement agencies require that the reliability of the services supporting the interception at least equals the reliability of the target services provided to the interception subject. Law enforcement agencies require the quality of service of the intercepted transmissions forwarded to the monitoring facility to comply with the performance standards of the network operators/service providers.

OCTOBER 22, 2012

Public Safety Canada / Sécurité publique Canada

s.16(1)(c)
s.16(2)
s.20(1)(b)

SECRET

DATE:

File No.: 6652-O3 / 390664

MEMORANDUM FOR THE SENIOR ASSISTANT DEPUTY MINISTER

[redacted]

(Signature required)

ISSUE

To seek approval for an approach with respect to [redacted] forbearance from the lawful interception condition of licence.

BACKGROUND

[redacted] This will further the necessity to have the capacity to conduct lawful interceptions on these systems.

[redacted]

.../2

Canada

s.15(1) - Int'l
s.16(1)(c)
s.16(2)
s.20(1)(b)
s.21(1)(a)
s.21(1)(b)

[redacted]

CONSIDERATIONS

[redacted]

.../3

s.15(1) - Int'l
s.16(1)(c)
s.16(2)
s.20(1)(c)
s.21(1)(a)
s.21(1)(b)

[redacted]

RECOMMENDATION

It is recommended that you support National Security Operations (NSOD) in pursuing the second (recommended) option with respect to [redacted]
Legal services were consulted and did not raise any concern with the recommended approach, which they see as being in line with past decisions. NSOD will continue to update you on this issue as it moves forward.

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Marie-Hélène Chayer, Director of Investigative Technologies and Telecommunications Policy at 613-949-3181.

Michael MacDonald

Prepared by: Shawn Plunkett

Emmett, Jamie

From: Hawrylak, Maciek
Sent: October-30-12 3:29 PM
To: Scott, Marcie
Subject: FW: RESUME TASKING: NEW Petition 411-1784 - Lawful Access

As discussed.

Maciek

From: Chayer, Marie-Helene
Sent: October-17-12 10:47 AM
To: Hawrylak, Maciek
Cc: Haeck, Kimberly
Subject: RE: RESUME TASKING: NEW Petition 411-1784 - Lawful Access

Maciek,

Please action.

thanks

Marie-Hélène Chayer
Director – Investigative Technology and Telecommunications Policy /
Directrice – Politique sur les technologies d'enquêtes et les télécommunications
National Security Operations Division / Division des Opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
(613)949-3181

From: Haeck, Kimberly
Sent: October-17-12 10:40 AM
To: Chayer, Marie-Helene
Subject: FW: RESUME TASKING: NEW Petition 411-1784 - Lawful Access
Importance: High

FYI

From: Bedor, Tia Leigh
Sent: Wednesday, October 17, 2012 10:38 AM
To: MacDonald, Michael
Cc: Johnston, Shannon; Haeck, Kimberly; Jacquard, Christina; Baulne, Lucie; Dupuis, Chantal; Larose, Nathalie; Bedor, Tia Leigh
Subject: RESUME TASKING: NEW Petition 411-1784 - Lawful Access
Importance: High

(For action)

Good morning,

Further to our conversation last week, please find below the sentence that the MO would like added into the response.

Please also let me know where you believe that this would fit best – I would assume that it would replace any mention of the future of the legislation…

"With Regards to C-30, our Government is thoroughly reviewing this legislation. At all times we will strike an appropriate balance between privacy and giving police the tools they need to do their job".

Should you agree, we would also need the translation of the addition – **before 11:00a.m. tomorrow, October 18, 2012.**

Please advise.

Thanks,

Tia Leigh Bedor
Administrative Officer | Agente Administrative
Office of the Senior Assistant Deputy Minister | Cabinet de la Sous-ministre adjointe principale
National Security | Sécurité nationale
Public Safety Canada | Sécurité publique Canada
Tel/Tél: 613-991-2901 | www.publicsafety.gc.ca | www.sécuritépublique.gc.ca

From: Bedor, Tia Leigh
Sent: Friday, October 12, 2012 12:18 PM
To: 'Johnston, Shannon'
Subject: RE: TASKING: NEW Petition 411-1784 - Lawful Access

We are to hold on this – MO is currently reviewing this first.

Thanks,

Tia Leigh Bedor
Administrative Officer | Agente Administrative
Office of the Senior Assistant Deputy Minister | Cabinet de la Sous-ministre adjointe principale
National Security | Sécurité nationale
Public Safety Canada | Sécurité publique Canada
Tel/Tél: 613-991-2901 | www.publicsafety.gc.ca | www.sécuritépublique.gc.ca

From: Johnston, Shannon
Sent: Friday, October 12, 2012 10:22 AM
To: Bedor, Tia Leigh
Subject: FW: TASKING: NEW Petition 411-1784 - Lawful Access
Importance: High

Hey Tia – please see below

Shannon Johnston
EA to DG
PSC - NSOD
Tel: 613-949-4623

From: Chayer, Marie-Helene
Sent: Friday, October 12, 2012 10:17 AM
To: Hawrylak, Maciek; Johnston, Shannon
Cc: Haeck, Kimberly

Subject: FW: TASKING: NEW Petition 411-1784 - Lawful Access
Importance: High

Maciek – As discussed. Thanks

Shannon - the template you sent is not related to Lawful Access. (you sent 411-1837 instead of 411-1784) Could you please send Maciek the right document. Many thanks

MH

Marie-Hélène Chayer
Director – Investigative Technology and Telecommunications Policy /
Directrice – Politique sur les technologies d'enquêtes et les télécommunications
National Security Operations Division / Division des Opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
(613)949-3181

From: Haeck, Kimberly
Sent: October-12-12 9:51 AM
To: Chayer, Marie-Helene
Subject: FW: TASKING: NEW Petition 411-1784 - Lawful Access
Importance: High

FYI

Kimberly Haeck
Administrative Assistant / Adjointe Administrative
National Security Technologies/Technologies de Sécurité Nationale
National Security Operations Directorate / Direction des Operations de Sécurité Nationale
Public Safety Canada / Sécurité Publique Canada
Tel: (613) 990-7575
Kimberly.Haeck@ps-sp.gc.ca

From: Bedor, Tia Leigh
Sent: October-12-12 9:44 AM
To: MacDonald, Michael
Cc: Johnston, Shannon; Haeck, Kimberly; Jacquard, Christina; Baulne, Lucie; Dupuis, Chantal
Subject: TASKING: NEW Petition 411-1784 - Lawful Access

(For action)

Is it possible to update the current wording of the petition to better reflect the new situation concerning this bill and its future?
For example, please see the two lines below used by MO yesterday in the media

- **With respect to Bill C-30, the *Protecting Children from Internet Predators Act*, our government is thoroughly reviewing this legislation.**
- **At all times we will strike an appropriate balance between protecting privacy and giving police the tools they need to do their job.**

Thanks,

Tia Leigh Bedor
Administrative Officer | Agente Administrative
Office of the Senior Assistant Deputy Minister | Cabinet de la Sous-ministre adjointe principale
National Security | Sécurité nationale

Public Safety Canada | Sécurité publique Canada
Tel/Tél: 613-991-2901 | www.publicsafety.gc.ca | www.sécuritépublique.gc.ca

From: Leclair, Natalie
Sent: Thursday, September 27, 2012 10:11 AM
To: Dupuis, Chantal; Bedor, Tia Leigh; Baulne, Lucie
Cc: McAteer, Julie; Issues / Enjeux; Chang, Anna
Subject: NEW Petition 411-1784 - Lawful Access
Importance: High

Good afternoon,

Please find attached a new petition 411-1784 which was presented in the House by Ms. May concerning Telecommunications.

Please note that this petition is similar to previous petitions on this subject. (previous petition 411-1519 attached).

NOTE: Please ensure that the information provided in the response to the petition is accurate and consistent with information or documents already disclosed under the *Access to Information Act* or the *Privacy Act*, or in response to other types of information requests.

Your ADM/ADM equivalent approved bilingual response should sent electronically to me with a CC to Julie McAteer **by COB on October 9, 2012**.

Please do not hesitate to contact me should you have any questions.

Thank you.
Nat

Natalie Leclair
Advisor / Conseillère
Parliamentary Affairs / Affaires parlementaires
Public Safety Canada / Sécurité publique Canada
Tel/Tél: (613) 990-2718
Fax: (613) 954-8774
Email/Courriel: natalie.leclair@ps-sp.gc.ca

Public Safety Canada / Sécurité publique Canada

s.16(1)(c)
s.21(1)(b)

SECRET

Thanks
Mike

DATE:

File No.: 6652-O3 / 390663

MEMORANDUM FOR THE SENIOR ASSISTANT DEPUTY MINISTER

[redacted]

(For information)

ISSUE

To provide information on the challenges associated with [redacted] and on ongoing work to develop potential solutions.

BACKGROUND

[redacted]

.../2

Canada

s.14(a)
s.15(1) - Int'l
s.16(1)(c)
s.21(1)(a)

[redacted]

CONSIDERATIONS

Challenges will increase: [redacted] As well, a 2009 Criminal Intelligence Service Canada (CISC) *National Threat Assessment on Organized and Serious Crime in Canada* indicated [redacted]

Ongoing domestic work: The justice and public safety community in Canada is aware of the domestic and international challenges and through the Federal-Provincial-Territorial Coordinating Committee of Senior Officials (CCSO) Cybercrime Working Group (CWG) is developing potential solutions [redacted] The CWG has put forward a recommendation to deal with the issue [redacted]

.../3

s.14(a)
s.15(1) - Int'l
s.16(1)(c)
s.21(1)(a)
s.21(1)(b)

[redacted] The Department of Justice (DoJ) is drafting a paper examining these issues to present at the next CWG meeting in November 2012.

[redacted]

While PS and Portfolio agencies continue to pursue potential technical solutions, a more effective course of action [redacted]

NEXT STEPS

National Security Operations Directorate (NSOD) will continue to work with DoJ, the CWG and [redacted] ensuring that it does not negatively impact other national security activities. [redacted]

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Marie-Hélène Chayer, Investigative Technologies and Telecommunications Policy at 613-949-3181.

Michael MacDonald

Prepared by: Shawn Plunkett

Public Safety Canada / Sécurité publique Canada

s.16(1)(c)
s.16(2)
s.20(1)(b)

SECRET

DATE:

File No.: 6652-O3 / 390664

MEMORANDUM FOR THE SENIOR ASSISTANT DEPUTY MINISTER

[redacted]

(Signature required)

ISSUE

To seek approval for an approach with respect to [redacted] forbearance from the lawful interception condition of licence.

BACKGROUND

[redacted] This will further the necessity to have the capacity to conduct lawful interceptions on these systems.

[redacted]

.../2

Canada

s.15(1) - Int'l
s.16(1)(c)
s.16(2)
s.20(1)(b)
s.21(1)(a)
s.21(1)(b)

[redacted]

CONSIDERATIONS

[redacted]

…/3

s.15(1) - Int'l
s.16(1)(c)
s.16(2)
s.20(1)(c)
s.21(1)(a)
s.21(1)(b)

[redacted]

RECOMMENDATION

It is recommended that you support National Security Operations (NSOD) in pursuing the second (recommended) option with respect to [redacted]
Legal services were consulted and did not raise any concern with the recommended approach, which they see as being in line with past decisions. NSOD will continue to update you on this issue as it moves forward.

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Marie-Hélène Chayer, Director of Investigative Technologies and Telecommunications Policy at 613-949-3181.

Michael MacDonald

Prepared by: Shawn Plunkett

Emmett, Jamie

From: Chayer, Marie-Helene
Sent: October-19-12 8:56 AM
To: Hawrylak, Maciek; Scott, Marcie; Maillé, Marie Anick
Subject: Fw: [redacted]-016: INTERCEPTION POWERS / AUSTRALIA: ASIO Chief Publicly Defends Need for Modernized Interception Regime (20121019)

From: MacDonald, Michael
Sent: Friday, October 19, 2012 08:18 AM
To: Gordon, Robert
Cc: Chayer, Marie-Helene
Subject: Re: [redacted]-016: INTERCEPTION POWERS / AUSTRALIA: ASIO Chief Publicly Defends Need for Modernized Interception Regime (20121019)

Thanks

From: Gordon, Robert
Sent: Friday, October 19, 2012 07:50 AM
To: MacDonald, Michael; Shuttle, Paul
Cc: Matz, Mark; Hatfield, Adam; Baulne, Lucie
Subject: FW: [redacted]-016: INTERCEPTION POWERS / AUSTRALIA: ASIO Chief Publicly Defends Need for Modernized Interception Regime (20121019)

Not certain whether you have already received this; sorry if it's duplication.
Bob

Robert W. (Bob) Gordon
Special Advisor, Cyber Security / Conseiller spécial, cybersécurité
Public Safety Canada / Sécurité publique Canada
340 Laurier Avenue West / 340 avenue Laurier Quest
Ottawa, Ontario K1A 0P9 / Ottawa (Ontario) K1A 0P8
613 949-7380 Fax/Téléc.: 613 990-3287
E-Mail / Courriel: Robert.Gordon@ps-sp.gc.ca

s.15(1) - Int'l
s.15(1) - Subv
s.17

From: [redacted]@international.gc.ca [mailto:[redacted]@international.gc.ca]
Sent: October-18-12 11:02 PM
To: rennie.marcoux@pco-bcp.gc.ca; Clairmont, Lynda; [redacted]; Dick, Robert; Gordon, Robert; Mark.Glauser@international.gc.ca
Cc: Banerjee, Ritu; Davies, John; [redacted] Gwen.Beauchemin@international.gc.ca; James.Galt@international.gc.ca; [redacted]@international.gc.ca; [redacted]@international.gc.ca; [redacted]@international.gc.ca; [redacted]@international.gc.ca; Artur.Wilczynski@international.gc.ca; Evelyn.Puxley@international.gc.ca; David.Nelson@international.gc.ca; Colin.Shonk@international.gc.ca; Tricia.Geddes@pco-bcp.gc.ca; brigitte.diogo@pco-bcp.gc.ca; Christopher.Blain@pco-bcp.gc.ca; christopher.lynam@pco-bcp.gc.ca; erin.dorgan@bcp-pco.gc.ca; Michael.Small@international.gc.ca; David.McKinnon@international.gc.ca; Stephen.Burridge@international.gc.ca; Mark.Berman@international.gc.ca; Kent.Vachon@international.gc.ca; Michael.Walma@international.gc.ca; Roland.Legault@international.gc.ca; Linder, Glen; [redacted]; Robert.Sinclair@international.gc.ca; Mike.Elliott@international.gc.ca; Michael.Blackmore@international.gc.ca; Wendell.Sanford@international.gc.ca; Roland.Legault@international.gc.ca; [redacted]

Subject: [redacted]016: INTERCEPTION POWERS/AUSTRALIA: ASIO Chief Publicly Defends Need for Modernized Interception Regime (20121019)

I draw your attention to today's report of an interview given by the Director-General of the Australian Security Intelligence Organisation (ASIO) David Irvine concerning the modernization of the interception regime for law enforcement and national security purposes in Australia. The Australian Parliament's Joint Committee on Intelligence and Security has started the pre-bill review of a national security legislation package, aiming in particular to modernize the interception regime, streamline intercept warrants, and create legal obligations for telcos concerning their network security. [Parliamentary Committee review's own webpage: http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/index.htm]

[redacted]

[redacted] will continue to monitor and report on developments related to the parliamentary review.

s.15(1) - Int'l

ANNEX:

Transcript of interview (found at http://www.abc.net.au/am/content/2012/s3613972.htm) (emphases added):

> TONY EASTLEY (PRESENTER): Australia's domestic spy agency has revealed there's been intelligence failures in recent years because of changing technology. In his first interview in a year, ASIO (Australian Security Intelligence Organisation) head David Irvine says new ways of communicating electronically are white-anting his agency's surveillance powers. Di Martin has this report for AM.
>
> DI MARTIN (REPORTER): Australia's domestic spy agency says it's just trying to stay up to date but critics say ASIO's request for new laws is a blatant power grab. ASIO has put several proposals to the Federal Government, including allowing its officers to commit crimes and not be charged. It also wants to hack computers of people who haven't committed a crime. And most controversially, it wants telcos to store our phone and internet data for up to two years so it can be searched without a warrant. ASIO director-general of Security David Irvine bristles at the suggestion that he is empire building.
>
> **DAVID IRVINE (ASIO DG): Di, we are talking about the modernisation of an interception regime. It does not mean extensive new powers, it means the ability to do what we could do 15 years ago and even 10 years ago and even five years ago that we are gradually losing the ability to do unless the law better accommodates the interception capability with the march of modern technology.**
>
> DI MARTIN: Top lawyers and privacy advocates say the domestic spy agency already has unprecedented powers accumulated post-9/11 and it doesn't need any more. But David Irvine reveals here for the first time that there've been intelligence failures because of changing technology.
>
> **DAVID IRVINE: We've had not near misses, we've had misses. In recent years there have been instances where devices have been used or devices have been used that we didn't know about and we have missed information.**
>
> DI MARTIN: Can you tell us about some of the forms of communication that were used which are of particular difficulty for you?
>
> DAVID IRVINE: No, I'm not going to go into that sort of operational detail but the fact is that when people have lots of telephones you have a requirement to go on a warrant by device, when people are using various different

forms of internet protocol type communications, it becomes more difficult. s

DI MARTIN: David Irvine says interception is critically important to ASIO but new ways to communicate electronically have white-anted ASIO's interception powers - like making phone calls over the internet. Some don't use a phone number that can be tapped. The conversation is rendered into packets of encrypted data whizzing from one computer to another.

DAVID IRVINE: What's changed is that once upon a time, interception was very easy - one telephone to another telephone. Today there are hundreds of different ways of communicating electronically and the law does not cater for those ways in the way it should.

DI MARTIN: David Irvine says that ASIO already has access to phone and internet records without a warrant but many telcos no longer need to keep that data for billing purposes. **So ASIO wants the Government to force companies to keep up to two years of our phone and internet records. He says the proposals are about properly equipping ASIO to do its job, like introducing a single warrant system to intercept whatever device a suspect uses.**

DAVID IRVINE: Based on the fact that a person will use several different devices at any one time, will swap SIM cards day in, day out.

DI MARTIN: And this is not covered by the current warrants?

DAVID IRVINE: Not in any convenient way at all, no.

DI MARTIN: ASIO also wants to be able to vary that warrant itself without going back to the Attorney-General. But critics say laws should not be changed for the sake of convenience, that there must be strong justification to allow any change to national security laws. **Top law agencies are worried about several ASIO proposals, including the request to allow officers to break the law without penalty. David Irvine explains why ASIO wants this power.**

DAVID IRVINE: If an ASIO source were to penetrate a terrorist group that wishes to do harm to Australia and our only source of information about that terrorist group was that penetration, and that group was proscribed under Australian law, then technically by being part of that group the ASIO officer or source could be breaking the law. And what I would like to see is a removal of that ambiguity.

DI MARTIN: But ASIO was accused of blurring the line between spying and policing. Police officers are allowed to break the law in limited circumstances but any resulting prosecution will end up in court and so be open to public scrutiny. This safeguard won't apply to an ASIO officer because their job is to collect intelligence. They don't bring cases to court. David Irvine says there is still accountability.

DAVID IRVINE: And that is exactly why we have the independent Inspector-General of Intelligence and Security, to monitor and ensure that ASIO acts in accordance with the law and with the utmost probity and reports to Parliament if that is not the case.

[redacted]@international.gc.ca
Telephone | Téléphone : [redacted]
Facsimile | Télécopieur : [redacted]
Commonwealth Avenue, Canberra ACT 2600
Canadian High Commission | Haut-commissariat du Canada
Government of Canada | Gouvernement du Canada

s.15(1) - Subv
s.17

PARLIAMENT of AUSTRALIA

House of Representatives Committees

Joint Parliamentary Committee on Intelligence and Security

Committee activities (inquiries and reports)

Inquiry into potential reforms of National Security Legislation

The Parliamentary Joint Committee on Intelligence and Security has commenced an inquiry into potential reforms of national security legislation. The inquiry was referred to the Committee by the Attorney-General.

The Committee has been asked to examine a package of national security ideas comprising proposals for telecommunications interception reform, telecommunications sector security reform and Australian intelligence community legislation reform. The reform proposals relate to the *Telecommunications (Interception and Access) Act 1979*, the *Telecommunications Act 1997*, the *Australian Security Intelligence Organisation Act 1979* and the *Intelligence Services Act 2001*.

The Committee has extended the date for lodgement of submissions by two weeks. Interested persons and organisations are now invited to make submissions addressing the terms of reference by **Monday, 20 August 2012**. Please refer to our brochure called preparing a submission for more information.

A discussion paper, which accompanies the terms of reference and describes the reform proposals, has been published on the Committee's web site and is available by clicking on the link below. *Interested parties are strongly encouraged to have regard to the discussion paper in the preparation of submissions.*

On 19 September 2012, the Committee received a letter from the Attorney-General clarifying the data retention aspects of the terms of reference.

In order to facilitate electronic publishing of submissions, the Committee would prefer them to be emailed to pjcis@aph.gov.au or sent on disk or CD-ROM to the Committee Secretariat in Microsoft Word® or Portable Document Format (PDF).

Terms of reference

Discussion paper

Submissions

Hearings

Media releases

Report

AM with Tony Eastley

Monday to Saturday from 8:00 am on ABC Local Radio and 7:10 am on Radio National.

ASIO head defends proposed changes to national security law

Di Martin reported this story on Friday, October 19, 2012 08:09:00

TONY EASTLEY: Australia's domestic spy agency has revealed there's been intelligence failures in recent years because of changing technology.

In his first interview in a year, ASIO (Australian Security Intelligence Organisation) head David Irvine says new ways of communicating electronically are white-anting his agency's surveillance powers.

David Irvine spoke exclusively to RN's Background Briefing program to defend ASIO's proposed and controversial changes to national security laws.

Di Martin has this report for AM.

DI MARTIN: Australia's domestic spy agency says it's just trying to stay up to date but critics say ASIO's request for new laws is a blatant power grab.

ASIO has put several proposals to the Federal Government, including allowing its officers to commit crimes and not be charged.

It also wants to hack computers of people who haven't committed a crime.

And most controversially, it wants telcos to store our phone and internet data for up to two years so it can be searched without a warrant.

ASIO director-general of Security David Irvine bristles at the suggestion that he is empire building.

DAVID IRVINE: Di, we are talking about the modernisation of an interception regime. It does not mean extensive new powers, it means the ability to do what we could do 15 years ago and even 10 years ago and even five years ago that we are gradually losing the ability to do unless the law better accommodates the interception capability with the march of modern technology.

DI MARTIN: Top lawyers and privacy advocates say the domestic spy agency already has unprecedented powers accumulated post-9/11 and it doesn't need any more.

But David Irvine reveals here for the first time that there've been intelligence failures because of changing technology.

DAVID IRVINE: We've had not near misses, we've had misses. In recent years there have been instances where devices have been used or devices have been used that we didn't know about and we have missed information.

DI MARTIN: Can you tell us about some of the forms of communication that were used which are of particular difficulty for you?

DAVID IRVINE: No, I'm not going to go into that sort of operational detail but the fact is that when people have lots of telephones you have a requirement to go on a warrant by device, when people are using various different forms of internet protocol type communications, it becomes more difficult. s

DI MARTIN: David Irvine says interception is critically important to ASIO but new ways to communicate electronically have white-anted ASIO's interception powers - like making phone calls over the internet.
Some don't use a phone number that can be tapped. The conversation is rendered into packets of encrypted data whizzing from one computer to another.

DAVID IRVINE: What's changed is that once upon a time, interception was very easy - one telephone to another telephone. Today there are hundreds of different ways of communicating electronically and the law does not cater for those ways in the way it should.

DI MARTIN: David Irvine says that ASIO already has access to phone and internet records without a warrant but many telcos no longer need to keep that data for billing purposes. So ASIO wants the Government to force companies to keep up to two years of our phone and internet records.

He says the proposals are about properly equipping ASIO to do its job, like introducing a single warrant system to intercept whatever device a suspect uses.

DAVID IRVINE: Based on the fact that a person will use several different devices at any one time, will swap SIM cards day in, day out.

DI MARTIN: And this is not covered by the current warrants?

DAVID IRVINE: Not in any convenient way at all, no.

DI MARTIN: ASIO also wants to be able to vary that warrant itself without going back to the Attorney-General.

But critics say laws should not be changed for the sake of convenience, that there must be strong justification to allow any change to national security laws. Top law agencies are worried about several ASIO proposals, including the request to allow officers to break the law without penalty.

David Irvine explains why ASIO wants this power.

DAVID IRVINE: If an ASIO source were to penetrate a terrorist group that wishes to do harm to Australia and our only source of information about that terrorist group was that penetration, and that group was proscribed under Australian law, then technically by being part of that group the ASIO officer or source could be breaking the law. And what I would like to see is a removal of that ambiguity.

DI MARTIN: But ASIO was accused of blurring the line between spying and policing. Police officers are allowed to break the law in limited circumstances but any resulting prosecution will end up in court and so be open to public scrutiny.

This safeguard won't apply to an ASIO officer because their job is to collect intelligence. They don't bring cases to court.

David Irvine says there is still accountability.

DAVID IRVINE: And that is exactly why we have the independent Inspector-General of Intelligence and Security, to monitor and ensure that ASIO acts in accordance with the law and with the utmost probity and reports to Parliament if that is not the case.

TONY EASTLEY: The head of ASIO David Irvine, Di Martin with that report and you can hear more this Sunday on RN's Background Briefing program after the 8 o'clock news.

Hawrylak, Maciek

From: Bedor, Tia Leigh
Sent: October-18-12 10:57 AM
To: Hawrylak, Maciek
Cc: Haeck, Kimberly
Subject: RE: RESUME TASKING: NEW Petition 411-1784 - Lawful Access

Please give Parliamentary affairs full access as soon as possible.

Thanks,

Tia Leigh Bedor
Administrative Officer | Agente Administrative
Office of the Senior Assistant Deputy Minister | Cabinet de la Sous-ministre adjointe principale
National Security | Sécurité nationale
Public Safety Canada | Sécurité publique Canada
Tel/Tél: 613-991-2901 | www.publicsafety.gc.ca | www.sécuritépublique.gc.ca

From: Hawrylak, Maciek
Sent: Thursday, October 18, 2012 10:44 AM
To: Bedor, Tia Leigh
Cc: Haeck, Kimberly
Subject: FW: RESUME TASKING: NEW Petition 411-1784 - Lawful Access

Tia,

Please find the RDIMS reference to Petition 411-1784 attached. SADMO staff already have Normal Access rights.

Best,
Maciek

Maciek Hawrylak
National Security Operations Directorate | Direction des Operations de Sécurité Nationale
Public Safety Canada | Sécurité Publique Canada
Tel | Tél : 613-991-6036
Fax | Téléc : 613-991-4669
Maciek.Hawrylak@ps-sp.gc.ca

From: Haeck, Kimberly
Sent: October-18-12 10:39 AM
To: Hawrylak, Maciek
Cc: Chayer, Marie-Helene; Jacquard, Christina; Johnston, Shannon
Subject: FW: RESUME TASKING: NEW Petition 411-1784 - Lawful Access

Hi Maciek,

We delivered the document to SADM/O this morning. They have asked us to receive an electronic copy. Can you send it over please and ensure everyone has the proper access rights?

Thank you.

From: Chayer, Marie-Helene
Sent: Wednesday, October 17, 2012 10:47 AM

To: Hawrylak, Maciek
Cc: Haeck, Kimberly
Subject: RE: RESUME TASKING: NEW Petition 411-1784 - Lawful Access

Maciek,

Please action.

thanks

Marie-Hélène Chayer
Director – Investigative Technology and Telecommunications Policy /
Directrice – **Politique sur les technologies d'enquêtes et les télécommunications**
National Security Operations Division / Division des Opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
(613)949-3181

From: Haeck, Kimberly
Sent: October-17-12 10:40 AM
To: Chayer, Marie-Helene
Subject: FW: RESUME TASKING: NEW Petition 411-1784 - Lawful Access
Importance: High

FYI

From: Bedor, Tia Leigh
Sent: Wednesday, October 17, 2012 10:38 AM
To: MacDonald, Michael
Cc: Johnston, Shannon; Haeck, Kimberly; Jacquard, Christina; Baulne, Lucie; Dupuis, Chantal; Larose, Nathalie; Bedor, Tia Leigh
Subject: RESUME TASKING: NEW Petition 411-1784 - Lawful Access
Importance: High

(For action)

Good morning, s.21(1)(a)

Further to our conversation last week, please find below the sentence that the MO would like added into the response.

Please also let me know where you believe that this would fit best – I would assume that it would replace any mention of the future of the legislation…

Should you agree, we would also need the translation of the addition – **before 11:00a.m. tomorrow, October 18, 2012.**

Please advise.

Thanks,

Tia Leigh Bedor
Administrative Officer | Agente Administrative
Office of the Senior Assistant Deputy Minister | Cabinet de la Sous-ministre adjointe principale

National Security | Sécurité nationale
Public Safety Canada | Sécurité publique Canada
Tel/Tél: 613-991-2901 | www.publicsafety.gc.ca | www.sécuritépublique.gc.ca

From: Bedor, Tia Leigh
Sent: Friday, October 12, 2012 12:18 PM
To: 'Johnston, Shannon'
Subject: RE: TASKING: NEW Petition 411-1784 - Lawful Access

We are to hold on this – MO is currently reviewing this first.

Thanks,

Tia Leigh Bedor
Administrative Officer | Agente Administrative
Office of the Senior Assistant Deputy Minister | Cabinet de la Sous-ministre adjointe principale
National Security | Sécurité nationale
Public Safety Canada | Sécurité publique Canada
Tel/Tél: 613-991-2901 | www.publicsafety.gc.ca | www.sécuritépublique.gc.ca

From: Johnston, Shannon
Sent: Friday, October 12, 2012 10:22 AM
To: Bedor, Tia Leigh
Subject: FW: TASKING: NEW Petition 411-1784 - Lawful Access
Importance: High

Hey Tia – please see below

Shannon Johnston
EA to DG
PSC - NSOD
Tel: 613-949-4623

From: Chayer, Marie-Helene
Sent: Friday, October 12, 2012 10:17 AM
To: Hawrylak, Maciek; Johnston, Shannon
Cc: Haeck, Kimberly
Subject: FW: TASKING: NEW Petition 411-1784 - Lawful Access
Importance: High

Maciek – As discussed. Thanks

Shannon - the template you sent is not related to Lawful Access. (you sent 411-1837 instead of 411-1784) Could you please send Maciek the right document. Many thanks

MH

Marie-Hélène Chayer
Director – Investigative Technology and Telecommunications Policy /
Directrice – **Politique sur les technologies d'enquêtes et les télécommunications**
National Security Operations Division / Division des Opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
(613)949-3181

From: Haeck, Kimberly
Sent: October-12-12 9:51 AM

To: Chayer, Marie-Helene
Subject: FW: TASKING: NEW Petition 411-1784 - Lawful Access
Importance: High

FYI

Kimberly Haeck
Administrative Assistant / Adjointe Administrative
National Security Technologies/Technologies de Sécurité Nationale
National Security Operations Directorate / Direction des Operations de Sécurité Nationale
Public Safety Canada / Sécurité Publique Canada
Tel: (613) 990-7575
Kimberly.Haeck@ps-sp.gc.ca

From: Bedor, Tia Leigh
Sent: October-12-12 9:44 AM
To: MacDonald, Michael
Cc: Johnston, Shannon; Haeck, Kimberly; Jacquard, Christina; Baulne, Lucie; Dupuis, Chantal
Subject: TASKING: NEW Petition 411-1784 - Lawful Access

(For action)

Is it possible to update the current wording of the petition to better reflect the new situation concerning this bill and its future?
For example, please see the two lines below used by MO yesterday in the media

- **With respect to Bill C-30, the *Protecting Children from Internet Predators Act*, our government is thoroughly reviewing this legislation.**
- **At all times we will strike an appropriate balance between protecting privacy and giving police the tools they need to do their job.**

Thanks,

Tia Leigh Bedor
Administrative Officer | Agente Administrative
Office of the Senior Assistant Deputy Minister | Cabinet de la Sous-ministre adjointe principale
National Security | Sécurité nationale
Public Safety Canada | Sécurité publique Canada
Tel/Tél: 613-991-2901 | www.publicsafety.gc.ca | www.sécuritépublique.gc.ca

From: Leclair, Natalie
Sent: Thursday, September 27, 2012 10:11 AM
To: Dupuis, Chantal; Bedor, Tia Leigh; Baulne, Lucie
Cc: McAteer, Julie; Issues / Enjeux; Chang, Anna
Subject: NEW Petition 411-1784 - Lawful Access
Importance: High

Good afternoon,

Please find attached a new petition 411-1784 which was presented in the House by Ms. May concerning Telecommunications.

Please note that this petition is similar to previous petitions on this subject. (previous petition 411-1519 attached).

NOTE: Please ensure that the information provided in the response to the petition is accurate and consistent with information or documents already disclosed under the *Access to Information Act* or the *Privacy Act*, or in response to other types of information requests.

Your ADM/ADM equivalent approved bilingual response should sent electronically to me with a CC to Julie McAteer **by COB on October 9, 2012**.

Please do not hesitate to contact me should you have any questions.

Thank you.
Nat

Natalie Leclair
Advisor / Conseillère
Parliamentary Affairs / Affaires parlementaires
Public Safety Canada / Sécurité publique Canada
Tel/Tél: (613) 990-2718
Fax: (613) 954-8774
Email/Courriel: natalie.leclair@ps-sp.gc.ca

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

Centralized models of interception

Australia, the United Kingdom, and the United States have all centralized or are in the process of centralizing some lawful interception (LI) functions in order to achieve economies of scale and improve LI effectiveness. Functions being centralized run from basic knowledge exchange to implementing lawful interceptions on behalf of law enforcement and national security agencies. A brief review of the models used or proposed by the three states is found below,

The UK's National Technical Assistance Centre (NTAC)

The UK's NTAC was established in 2002 to support the UK's *Regulation of Investigatory Powers Act* (RIPA, 2000). NTAC's role in supporting RIPA is two-fold: first, it actually implements interceptions on behalf of law enforcement and intelligence agencies, and decrypts any encrypted communications; and, second, it is the approval body that law enforcement and intelligence agencies must consult prior to issuing a decryption order under Part III of RIPA (which permits authorities to force someone to reveal a password, encryption algorithm, or any other means of protection).

NTAC undertakes all the necessary work to implement the interception and provide its decrypted contents (if necessary) to the requesting agency, but does not analyze the content of the interception. That remains a function of the agency which submitted the request. All costs are borne by the central government.

NTAC is also the lead national agency for the application of Part III of RIPA, which permits public authorities to serve notice to a person or TSP to provide decryption keys. All agencies must consult with and receive the approval of NTAC when considering the use of Part III.

NTAC is subject to statutory oversight by the Interception of Communications Commissioner, the Intelligence Services Commissioner and the Surveillance Commissioners, as well as court scrutiny in respect of its handling of lawfully seized material. NTAC is a 24-hour centre housed at the Government Communications Headquarters (GCHQ) in Cheltenham.

The US' National Domestic Communications Assistance Center (NDCAC)

As opposed to the NTAC, the US' NDCAC does not actually conduct interceptions. It was established in 2011 with a more limited function: to leverage and share the collective technical knowledge and resources of the law enforcement community on LI issues, and liaise more effectively with industry. The NDCAC has three main function:

1. Technology sharing: this involves maintaining a resource centre for sharing technical solutions, providing training on LI solutions, identifying and sharing best practices, and modifying existing solutions for use across the over 18,000 LEAs in the US.
2. CALEA implementation: this involves developing and evaluating standards and facilitating evaluation of industry-developed solutions.
3. Industry relations: this involves being the principal communications link with industry, and organizing periodic government-industry forums.

NDCAC will provide a one stop shop for the various types of LI assistance, and minimize duplication of efforts. All costs are assumed by the federal government.

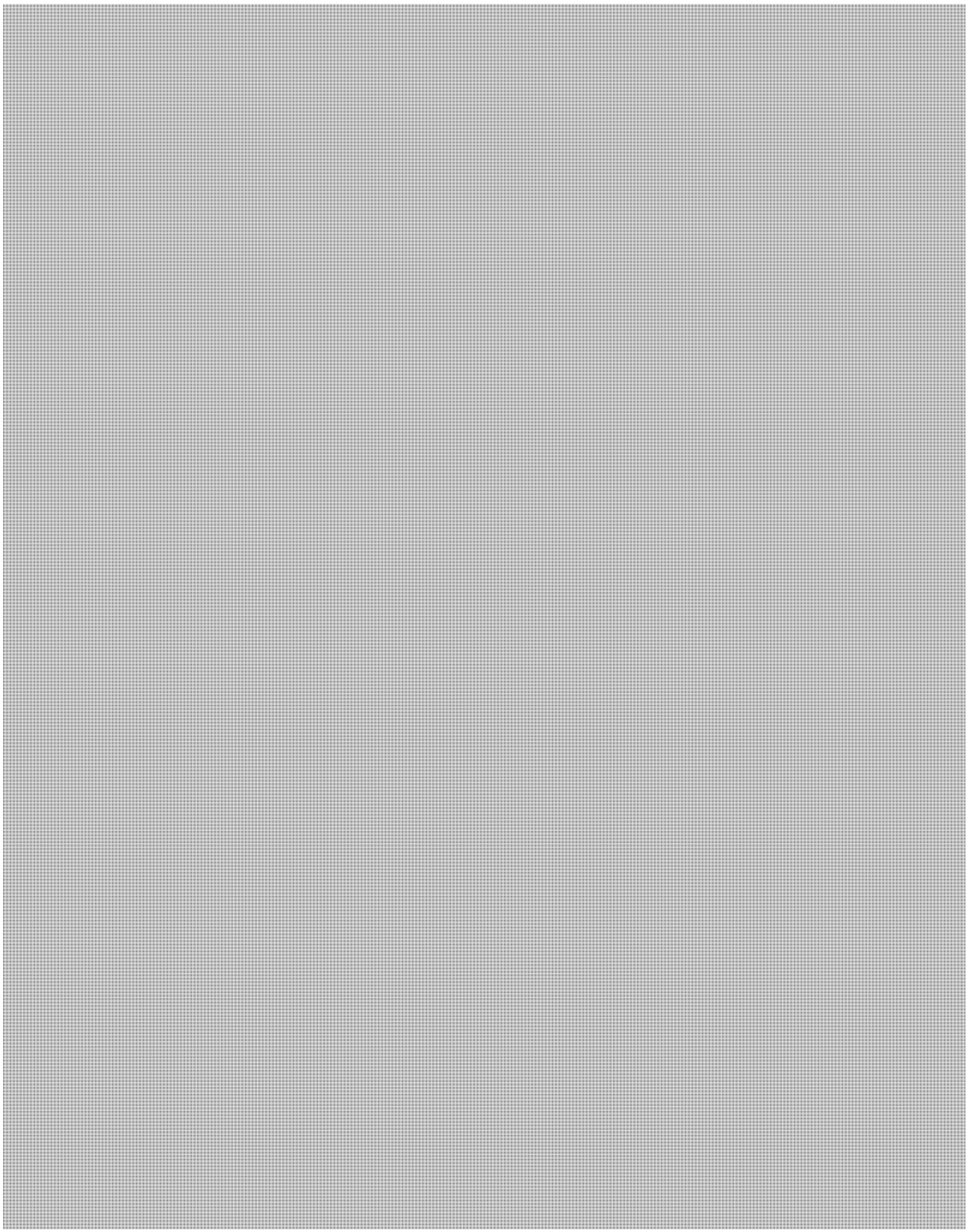
Australia's National Interception Technical Assistance Centre (NITAC)

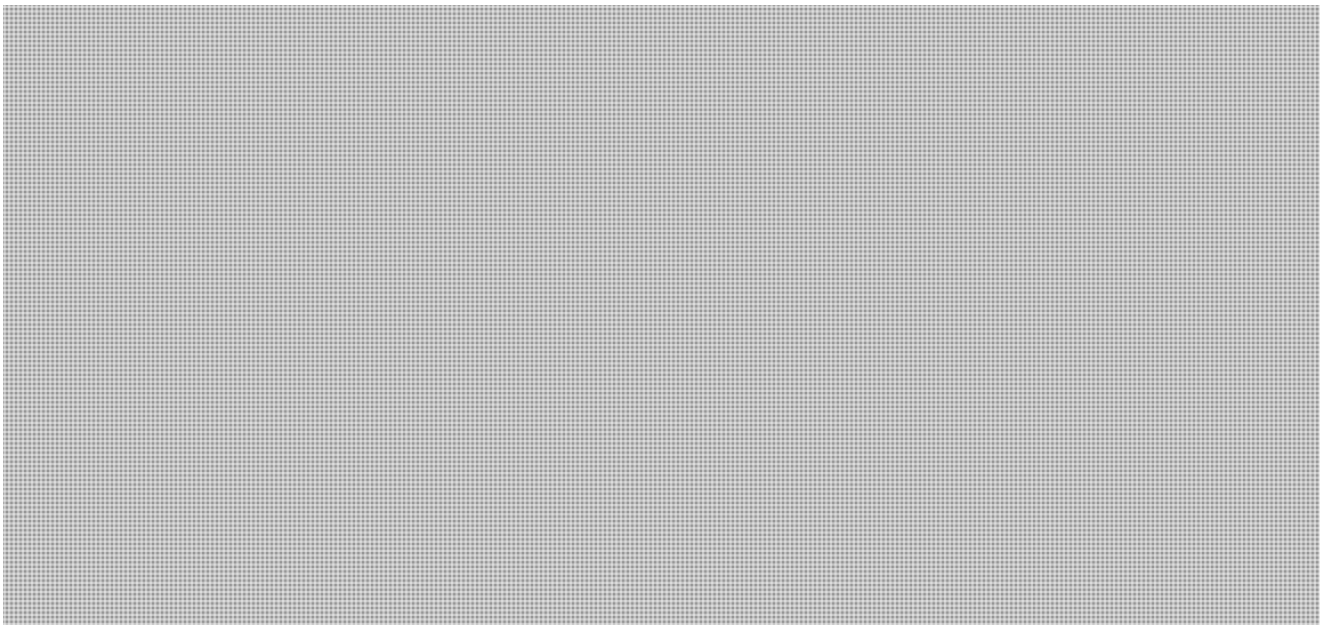
Similar to the US' NDCAC, Australia's NITAC was piloted in 2010-11 to be a central LI technical assistance agency. It performs training, proposes solutions to LI problems, and performs knowledge exchange functions. The two-year pilot project ends at the end of 2012.

s.13(1)(a)

s.21(1)(a)

NITAC is housed within the Australian Security Intelligence Organization, with costs shared between all the agencies that use it.





s.21(1)(a)

Pages 318 to / à 319

are withheld pursuant to section

sont retenues en vertu de l'article

14(a)

of the Access to Information

de la Loi sur l'accès à l'information

SECRET

MEMORANDUM FOR THE ACTING DEPUTY MINISTER

OPTION FOR THE LAWFUL INTERCEPTION OF COMMUNICATIONS

ISSUE

To provide information on a potential option to increase lawful interception capabilities.

BACKGROUND

The ability to lawfully intercept communications is vital for law enforcement and national security agencies to conduct investigations. CSIS annually prevents terrorist attacks on Canadian soil by using intelligence gathered from lawful interceptions. Evidence obtained through the interception of communications is equally indispensable for law enforcement to respond to serious offences, such as drug trafficking and child exploitation. However, the current legal framework governing the interception of communications does not reflect the complexity of today's telecommunications environment. The rapidly growing number of telecommunications service providers (TSPs) in Canada (now over 1000), technological advancements and the use of technology in almost every aspect of modern life have outpaced lawful access capabilities.

Indeed, although the *Criminal Code* allows for the lawful interception of private communications, there is no legislation compelling TSPs to make their networks – wireline (traditional phone), wireless (cellular networks), and internet – intercept capable.

At present, the only means to compel some TSPs to have and maintain lawful interception capability is through the Minister of Industry's power under the *Radiocommunication Act* (RA) to include lawful interception as a condition of their spectrum and radio licence.

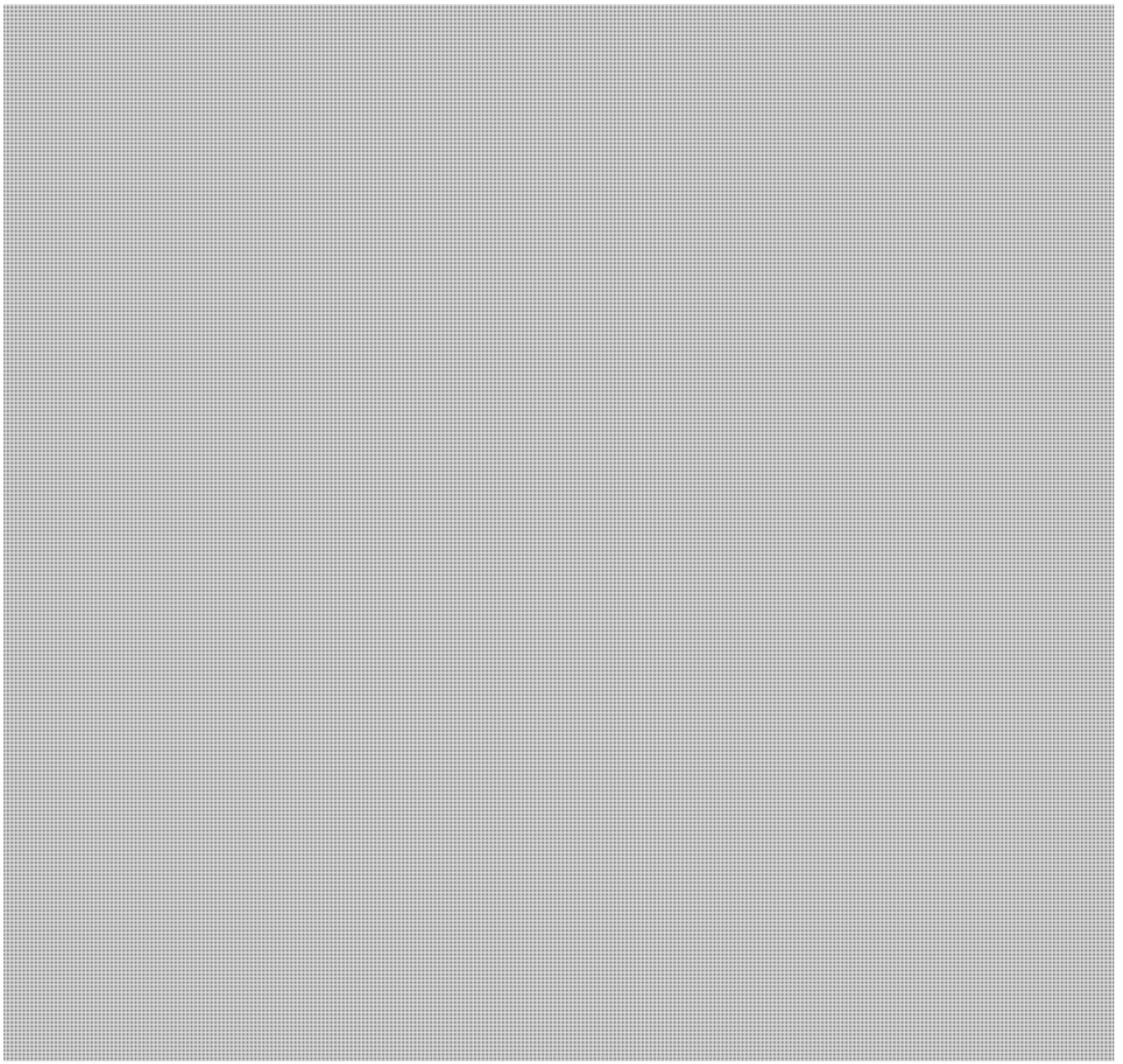
[redacted]

s.16(1)(c)
s.16(2)

[redacted]

To address this challenge, the Minister of Public Safety introduced Bill C-30, the *Protecting Children from Internet Predators Act*, on February 14, 2012. Bill C-30 contains a suite of legislative measures, including the *Investigating and Preventing Criminal Electronic Communications Act* (IPCECA), which would require TSPs to implement and maintain systems that are capable of lawfully intercepting communications. It would also require TSPs to provide basic subscriber information to designated police, CSIS and Competition Bureau officials upon request. In addition, it would amend elements of the *Criminal Code*, the *Competition Act* and the *Mutual Legal Assistance in Criminal Matters Act*. The provisions contained in Bill C-30 are similar to what can be found in lawful interception legislation of like-minded countries.

Bill C-30 was heavily criticized, in particular with regards to the requirement to provide basic subscriber information to authorities upon request. Minister Toews announced in late February 2012 that the Bill would go directly to Committee for study before second reading. [redacted]



Thompson, Julie

From: Plunkett, Shawn
Sent: Thursday, September 27, 2012 3:17 PM
To: Thompson, Julie
Subject: RE: PS-SP-#695448-v1-QP_Note_-_Lawful_Interception_Condition_of_Licence

When you have a moment can you swing by?

From: Thompson, Julie
Sent: September-27-12 12:25 PM
To: Plunkett, Shawn
Subject: PS-SP-#695448-v1-QP_Note_-_Lawful_Interception_Condition_of_Licence

Hi Shawn
Here is the QP notes on the lawful interception – condition of licence.
Please make changes as you see fit. If there is anything I forgot to include, let me know and I can add it.

Julie

Date: December 2011
Classification: UNCLASSIFIED
Branch / Agency: PS/ NSOD

Question Period Note

LAWFUL INTERCEPTION – CONDITION OF SPECTRUM LICENCE

ISSUE: The lawful interception as a condition of spectrum licence to replace lawful access legislation.

BACKGROUND:

Law enforcement and national security agencies require telecommunications companies to maintain lawful interception capability in order to investigate crimes and threats to Canadian security. Until the passage of the lawful access legislation, the primary instrument for public safety agencies to compel telecommunications companies to provide court authorized intercepts is through including a requirement for lawful interception in their spectrum licence. Part of the requirements of the lawful interception condition of licence is for licensees to abide by the Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications (Solicitor General Standards) - a set of 23 standards that indicate the technical requirements needed by law enforcement and national security agencies for lawful interception.

Since introducing the Solicitor General Standards in the mid 1990's, most telecommunications companies have As a result, the condition In order to address this issue, Public Safety Canada and Industry Canada have examining ways to revise the lawful interception condition.

Indeed, in early 2012, in anticipation of the upcoming public consultation on the conditions of spectrum licence for the 700 MHz and 2500 MHz spectrum licence auction, PS recommended to Industry Canada that a lawful interception condition be applied on those specific bands and be amended in order to bring the wording in line with current technologies. PS also proposed amendments to the current Solicitor General Standards. Industry Canada publicly consulted on PS's proposed lawful interception condition.

The majority of reply comments from telecommunications companies on the licensing framework for the 700 MHz, opposed the new language for lawful intercept condition of licence and maintained that any changes to the Solicitor General Standards should be the subject of a separate consultation. Industry Canada has not yet conveyed its final decision on the outcome of the consultation process.

The lawful interception condition of spectrum licence and the Solicitor General Standards While a stronger lawful interception condition of spectrum licence, while beneficial to law enforcement and national security agencies, it may pose additional requirements on spectrum licence holders.

To minimize the lawful interception impact on telecommunications companies, the licensee may request the Minister of Industry, following consultation with PS, to forbear from enforcing certain or all Solicitor General Standards for a limited period, if the requirements are considered not achievable.

s.16(1)(c)

LAWFUL INTERCEPTION – CONDITION OF SPECTRUM LICENCE

PROPOSED RESPONSE:

- **Lawful interception of communications is an essential tool for investigating serious offences such as online child sexual exploitation, organized crime, and threats to national security.**

- **The authority to intercept communications is already well entrenched in Canadian law. However, new technologies have undermined the effectiveness of existing interception tools.**

- **The purpose of updating the lawful interception condition of licence and the Solicitor General Standards is to bring these requirements up to speed with the technological realities of our times.**

- **I have been working with the Minister of Industry to minimize the impacts of lawful interception requirements on telecommunications companies. Indeed, telecommunications companies who are unable to meet interceptions standards may request the Minister of Industry to forbear from enforcing certain lawful intercept requirements for a determined period.**

- **Until full implementation of this Government's proposed lawful access legislation, the lawful interception condition and the Solicitor General standards are important tools for law enforcement and national security agencies in the fight against criminal and terrorist-related activity.**

CONTACTS:			
Prepared by Shawn Plunkett Senior Policy Advisor	Tel. no. 613.990-7066 (office) [redacted] (BB)	Approved by (DG level only) Michael MacDonald Director General	Tel. no. 613.990-4976 (office) [redacted] (BB)

s.19(1)

Emmett, Jamie

From: Chayer, Marie-Helene
Sent: September-27-12 11:34 AM
To: Maillé, Marie Anick
Subject: FW: TASKING: NEW Petition 411-1784 - Lawful Access
Attachments: 411-1519 - Signed response.pdf; 411-1784-notice.doc; 411-1784 petition response.doc

Importance: High

Marie Anick,

Peux-tu t'en occuper?

merci

Marie-Hélène Chayer
Director – Investigative Technology and Telecommunications Policy /
Directrice – **Politique sur les technologies d'enquêtes et les télécommunications**
National Security Operations Division / Division des Opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
(613)949-3181

From: Johnston, Shannon
Sent: September-27-12 11:04 AM
To: Chayer, Marie-Helene
Cc: MacDonald, Michael
Subject: FW: TASKING: NEW Petition 411-1784 - Lawful Access
Importance: High

Good morning,

Please find attached a new petition 411-1784 - you will notice that it is similar to the previous petitions on the subject.

Please advise if you agree the language from the previous petitions would apply to this one. If not, you must provide the new language in both official languages to DGO by 4pm, Oct. 4.

Thank you

Shannon Johnston
EA to DG
PSC - NSOD
Tel: 613-949-4623

From: Bedor, Tia Leigh
Sent: Thursday, September 27, 2012 10:48 AM
To: Johnston, Shannon; Haeck, Kimberly; Jacquard, Christina
Cc: MacDonald, Michael; Baulne, Lucie; Dupuis, Chantal
Subject: TASKING: NEW Petition 411-1784 - Lawful Access
Importance: High

(For action)

Good afternoon,

Please find attached a new petition 411-1784 which was presented in the House by Ms. May concerning Telecommunications.

Please note that this petition is similar to previous petitions on this subject. (previous petition 411-1519 attached).

NOTE: Please ensure that the information provided in the response to the petition is accurate and consistent with information or documents already disclosed under the *Access to Information Act* or the *Privacy Act*, or in response to other types of information requests.

Your DG/DG equivalent approved bilingual response should sent electronically to Chantal Dupuis with a CC to me **by 16:00 on October 5, 2012**.

Thanks,

Tia Leigh Bedor
Administrative Officer | Agente Administrative
Office of the Senior Assistant Deputy Minister | Cabinet de la Sous-ministre adjointe principale
National Security | Sécurité nationale
Public Safety Canada | Sécurité publique Canada
Tel/Tél: 613-991-2901 | www.publicsafety.gc.ca | www.sécuritépublique.gc.ca

RESPONSE TO PETITION
RÉPONSE À LA PÉTITION

PREPARE IN ENGLISH AND FRENCH MARKING "ORIGINAL TEXT" OR "TRANSLATION"
PRÉPARER EN ANGLAIS ET EN FRANÇAIS EN INDIQUANT "TEXTE ORIGINAL" OU "TRADUCTION"

PETITION NO./Nº DE LA PÉTITION	BY / DE	DATE
411-1519	Ms. Savoie (Victoria)	June 21, 2012

RESPONSE BY THE MINISTER OF PUBLIC SAFETY
RÉPONSE DU MINISTRE DE LA SÉCURITÉ PUBLIQUE

The Honourable Vic Toews

PRINT NAME OF SIGNATORY
INSCRIRE LE NOM DU SIGNATAIRE

SIGNATURE
MINISTER OR PARLIAMENTARY SECRETARY
MINISTRE OU SECRÉTAIRE PARLEMENTAIRE

SUBJECT / OBJET
Telecommunications

RESPONSE / RÉPONSE

ORIGINAL TEXT / TEXTE ORIGINAL [X] TRANSLATION / TRADUCTION [ ]

Public Safety Canada

Canadians are concerned about crime, particularly crime involving children.

Reported child pornography offences were up 36% in 2010 in Canada (Statistics Canada, Police-reported crime statistics in Canada, 2010).

Inspector Scott Naylor, manager of the Ontario Provincial Police child exploitation unit, said that our current system for obtaining Internet Protocol (IP) addresses of suspected child pornographers isn't effective. "It's still like putting a cup under Niagara Falls. That's all we are catching".

That is why our Government has introduced the *Protecting Children from Internet Predators Act*.

We want to fix our laws while striking the right balance when it comes to protecting privacy.

Bill C-30 creates no new powers to access the content of e-mails or phone calls beyond that which already exists in Canadian law.

We will send this legislation directly to Committee for a full examination of potential amendments to achieve the best protection for our children.

Today, telecommunications service providers (TSP) may provide authorities, without a warrant, with basic subscriber information under the *Personal Information Protection and Electronic Documents Act*. The problem is that there is no consistency across the country in how service providers respond to these requests: sometimes they respond in a timely manner, but often they respond only after considerable delays, if at all.

.../2

Specifically:

I. According to the Royal Canadian Mounted Police's (RCMP) National Child Exploitation Coordination Centre in Ottawa, in 2010, the average response time for a basic subscriber information (BSI) request was 13 days, and only 72.5% of requests were fulfilled.

II. One TSP only responds to BSI requests on Fridays, regardless of when the requests are submitted.

III. Another TSP only accepts BSI requests via email, which can be problematic in emergencies.

IV. In December 2010, New Brunswick RCMP began to investigate the distribution of child pornography. Police suspected an individual who was using a TSP who had historically not shared information with police. As a result, local police applied for a court order. There was a substantial delay and by this time the case had gone cold as the suspect had stopped his activities. Due to this delay, abuse could have been prevented at an earlier date as it was later discovered that this suspect was abusing two young boys to create child pornography. Several months later, the suspect resumed his online activity. This time the TSP was cooperative with police requests. The suspect was charged with possession and distribution of child pornography.

V. In 2007, the RCMP assisted with an international investigation in which suspects located in Canada were attempting to defraud American corporations of approximately $100 million. The investigation required police to find the individuals who were committing these fraudulent activities. The suspects were constantly on the move and police needed the immediate support of the TSPs to determine the location of these networks. However, the service providers would not provide police with the basic subscriber information they needed. Because of the lack of cooperation from the TSPs, it took eight full-time technical investigators five days to finally locate and arrest the suspects. The suspects successfully defrauded victims of $15 million. Had police been provided the information when it was requested, the value of the fraud would have been reduced considerably and police resources would have been used more effectively.

VI. A child was abducted in British Columbia in 2011. An amber alert was broadcast and, fortunately, the suspect returned the child. However, the suspect was not apprehended and his location remained unknown. Through further investigation, police obtained an IP address associated with the suspect. Police contacted the TSP directly and were advised that it was against policy to provide subscriber information related to an IP address without a Production Order. Police advised the TSP that the suspect had already abducted one child and that other children could possibly be at risk. The TSP decided to provide the information and the suspect was located and apprehended less than 24 hours after police received the information.

RESPONSE TO PETITION
RÉPONSE À LA PÉTITION

PREPARE IN ENGLISH AND FRENCH MARKING "ORIGINAL TEXT" OR "TRANSLATION"
PRÉPARER EN ANGLAIS ET EN FRANÇAIS EN INDIQUANT "TEXTE ORIGINAL" OU "TRADUCTION"

PETITION NO./Nº DE LA PÉTITION	BY / DE	DATE
411-1519	Mme. Savoie (Victoria)	21 juin 2012

RESPONSE BY THE MINISTER OF PUBLIC SAFETY
RÉPONSE DU MINISTRE DE LA SÉCURITÉ PUBLIQUE

L'honorable Vic Toews

PRINT NAME OF SIGNATORY
INSCRIRE LE NOM DU SIGNATAIRE

SIGNATURE
MINISTER OR PARLIAMENTARY SECRETARY
MINISTRE OU SECRÉTAIRE PARLEMENTAIRE

SUBJECT / OBJET
Télécommunications

RESPONSE / RÉPONSE

ORIGINAL TEXT / TEXTE ORIGINAL [ ] TRANSLATION / TRADUCTION [X]

Sécurité publique Canada

Les Canadiens sont préoccupés par le crime, particulièrement lorsque cela implique des enfants.

Les infractions de pornographie juvéniles déclarées par la police ont augmentées de 36% en 2010. (Statistiques Canada, Statistiques sur les crimes déclarés par la police au Canada, 2010)

L'inspecteur Scott Naylor, gestionnaire de la Section de la pornographie juvénile à la Police provinciale de l'Ontario, affirme que notre système pour obtenir les adresses protocole Internet (IP) des pornographes juvéniles présumés est inefficace. « C'est comme mettre une tasse sous les chutes Niagara. C'est tout ce qui est pris. »

C'est pourquoi nous avons introduit la *Loi sur la protection des enfants contre les cyberprédateurs*.

Nous voulons modifier nos lois tout en établissant un juste équilibre avec la protection de la vie privée.

Le projet de loi C-30 ne créerait aucun nouveau pouvoir d'accéder au contenu des courriels ou à des appels téléphoniques qui iraient au-delà des pouvoirs qui existent déjà dans la loi canadienne.

Nous enverrons ce projet de loi directement au comité pour un examen complet d'amendements potentiels afin d'atteindre la meilleure protection pour nos enfants.

.../2

En vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques*, les télécommunicateurs peuvent, sans qu'un mandat soit nécessaire, transmettre aux autorités des renseignements de base sur les abonnés. Or, le problème est qu'il n'y a aucune uniformité à l'échelle du pays dans la façon dont les télécommunicateurs répondent à ces demandes. Parfois, ils y donnent suite rapidement, mais parfois, ils y répondent qu'après un long délai ou n'y répondent pas du tout.

Ainsi :

I. En 2010, selon le Centre national de coordination contre l'exploitation des enfants de la Gendarmerie royale du Canada (GRC) à Ottawa, le temps de réponse moyen à une demande de renseignements de base sur les abonnés était de 13 jours et seulement 72,5% des demandes ont été exécuté.

II. Un certain télécommunicateur répond seulement le vendredi aux demandes de renseignements de base sur les abonnés, et ce, peu importe le moment où la requête est soumise.

III. Un autre télécommunicateur accepte seulement les demandes de renseignements de base sur les abonnés soumises par courrier électronique. Il va sans dire que cela peut s'avérer problématique lors de situations d'urgence.

IV. En décembre 2010, la GRC du Nouveau-Brunswick a commencé à enquêter sur un cas de distribution de pornographie juvénile. Les policiers soupçonnaient un individu qui utilisait un télécommunicateur reconnu pour ne pas fournir l'information demandée aux policiers. Sachant cela, le policier local a fait une demande d'autorisation. En raison de ce délai, des abus envers des personnes mineures n'ont pas pu être prévenus plus rapidement. De fait, il s'est avéré que ce suspect abusait de deux jeunes garçons afin de produire de la pornographie juvénile. Cependant, le suspect a arrêté ses activités en ligne durant la période d'obtention du mandat et l'enquête a été suspendue. Quelques mois plus tard, le suspect a repris ses activités en ligne et, cette fois, le télécommunicateur a accepté de fournir les renseignements demandés. Le suspect a été accusé de possession et de distribution de pornographie juvénile.

V. En 2007, la GRC a pris part à une enquête internationale visant des suspects qui se trouvaient au Canada et qui essayaient d'obtenir frauduleusement environ 100 millions de dollars de sociétés américaines. Au cours de l'enquête, les policiers devaient identifier les personnes commettant ces activités frauduleuses. Les suspects se déplaçaient constamment et les policiers avaient besoin de l'aide immédiate des télécommunicateurs pour déterminer où se trouvaient les réseaux. Cependant, les télécommunicateurs refusaient de fournir les *renseignements de base sur les abonnés nécessaires*. En raison du manque de collaboration des télécommunicateurs, il a fallu cinq jours à huit enquêteurs spécialisés travaillant à temps plein pour enfin trouver et arrêter les suspects, qui avaient alors déjà escroqué 15 millions de dollars à leurs victimes. Si les policiers avaient obtenu les renseignements dont ils avaient besoin lorsqu'ils les ont demandés, on aurait pu limiter considérablement le montant de la fraude et les ressources policières auraient pu être utilisées plus efficacement.

.../3

VI. Un enfant a été enlevé en Colombie-Britannique en 2011. Une alerte Amber a été diffusée et, heureusement, le suspect a libéré l'enfant. Toutefois, le suspect n'a pas alors été appréhendé, et on ignorait où il se trouvait. En effectuant une enquête plus approfondie, les policiers ont obtenu une adresse IP associée au suspect. Ils ont donc communiqué directement avec le télécommunicateur, et on leur a répondu que, sans une ordonnance de communication, il était contraire à leur politique de fournir des renseignements sur les abonnés liés à une adresse IP. Les policiers ont avisé le télécommunicateur que le suspect avait déjà enlevé un enfant et que d'autres enfants pourraient être à risque. Le télécommunicateur a alors accepté de fournir les renseignements demandés, et le suspect a été localisé et appréhendé moins de 24 heures après que les policiers ont obtenu les renseignements.

Government of Canada
Privy Council Office

Gouvernement du Canada
Bureau du Conseil privé

PETITION - PÉTITION

To / À **PUBLIC SAFETY**

Date **September 27, 2012**

SUBJECT: Petition No. / Pétition N° **411-1784**

SUJET: Member / Député **MS. MAY (SAANICH-GULF ISLANDS)**

Date of Petition / Date de la pétition **September 24, 2012**

FOR PRIORITY ATTENTION

Section 36 (8) of the Standing Orders:

(a) Every petition presented pursuant to this Standing Order shall forthwith be transmitted to the Ministry, which shall, within forty-five days, respond to every petition referred to it; provided that the said response may be tabled pursuant to S.O. 32(1).

(b) If such a petition remains without a response at the expiration of the said period of forty-five days, the matter of the failure of the Ministry to respond shall be deemed referred to the appropriate Standing Committee. Within five sitting days of such a referral the Chair of the committee shall convene a meeting of the committee to consider the matter of the failure of the Ministry to respond.

Would you please respond to this petition before

November 2, 2012

The response should be prepared on a "Response to Petition" form in both official languages.

If you have no information on this subject or you consider that another department should be contacted, please advise us without delay.

POUR EXAMEN PRIORITAIRE

Paragraphe 36 (8) du Règlement:

a) Toute pétition présentée conformément au présent article est transmise sur-le-champ au gouvernement, qui répond dans les quarante-cinq jours à toutes les pétitions qui lui sont renvoyées. La réponse peut être déposée conformément à l'article 32(1) du Règlement.

b) Dans le cas où une pétition reste sans réponse à l'expiration de ce délai de quarante-cinq jours, cette absence de réponse de la part du gouvernement est réputée renvoyée au comité permanent concerné. Dans les cinq jours de séance suivants ce renvoi, le président du comité convoque une réunion pour se pencher sur l'absence de réponse de la part du gouvernement.

Veuillez répondre à cette pétition avant le

La réponse doit être présentée dans les deux langues officielles sur le formulaire "Réponse à la pétition".

Si vous ne possédez aucun renseignement sur ce sujet ou si vous jugez qu'un autre ministère devrait être contacté, veuillez nous aviser sans délai.

Nicole Baker

Nicole Baker
Coordinator of Parliamentary Returns
Coordonnatrice des documents parlementaires

Canada

ASSIGNMENT: **PUBLIC SAFETY**
ASSIGNATION:

SUBJECT/SUJET

— by Ms. May (Saanich—Gulf Islands), one concerning **environmental assessment and review** (No. 411-1783) and one concerning **telecommunications** (No. 411-1784).	— par M[me] May (Saanich—Gulf Islands), une au sujet de **l'examen et des évaluations environnementales** (n° 411-1783) et une au sujet au sujet des **télécommunications** (n° 411-1784).

REPEAT OF / RÉPÉTITION DE LA : 411-1519

NOTE:

The subject to be typed on the form Response to Petition should be the same as the one in the Journals. (See Subject/Sujet above)

Le sujet à dactylographier sur le formulaire Réponse à la Pétition doit être le même que celui des Journaux. (Voir Subject/Sujet ci-haut)

Canada

411-1784

PETITION TO THE HOUSE OF COMMONS

We, the undersigned residents of Canada, draw the attention of the House of Commons to the following:

THAT Canadians do not wish to allow warrantless surveillance by a range of government authorities, including access to financial and personal information, through internet and mobile devices.

THAT Federal and Provincial/Territorial Commissioners to Privacy have voiced concern that Bill C-30 will allow unacceptable intrusions into privacy rights.

THAT requiring internet and service providers to provide the information to authorities will lead to costs that will be passed on to the purchaser of the internet and mobile services, rather than borne by the authorities requesting the information.

THAT Canadians do not need a level of surveillance that is typically associated with totalitarian regimes.

THAT Canadians need privacy protection that reflects the present state of communication technology and the rights and freedoms they enjoy under the Constitution.

THEREFORE, your petitioners call upon the Government of Canada to reject those aspects of the proposed lawful access that expand surveillance, allow authorities unrestricted and warrantless access to personal information and violate the privacy of Canadians. Bill C-30 must be amended sufficiently that it is supported by federal and provincial/territorial privacy commissioners.

RESPONSE TO PETITION
RÉPONSE À LA PÉTITION

PREPARE IN ENGLISH AND FRENCH MARKING "ORIGINAL TEXT" OR "TRANSLATION"
PRÉPARER EN ANGLAIS ET EN FRANÇAIS EN INDIQUANT "TEXTE ORIGINAL" OU "TRADUCTION"

PETITION NO./Nº DE LA PÉTITION	BY / DE	DATE
411-1784	Ms. May (Saanich—Gulf Islands)	September 24, 2012

RESPONSE BY THE MINISTER OF PUBLIC SAFETY
RÉPONSE DU MINISTRE DE LA SÉCURITÉ PUBLIQUE

The Honourable Vic Toews

PRINT NAME OF SIGNATORY
INSCRIRE LE NOM DU SIGNATAIRE

SIGNATURE
MINISTER OR PARLIAMENTARY SECRETARY
MINISTRE OU SECRÉTAIRE PARLEMENTAIRE

SUBJECT / OBJET
Telecommunications

RESPONSE / RÉPONSE

ORIGINAL TEXT / TEXTE ORIGINAL [X]

TRANSLATION / TRADUCTION [ ]

Public Safety Canada

RESPONSE TO PETITION
RÉPONSE À LA PÉTITION

PREPARE IN ENGLISH AND FRENCH MARKING "ORIGINAL TEXT" OR "TRANSLATION"
PRÉPARER EN ANGLAIS ET EN FRANÇAIS EN INDIQUANT "TEXTE ORIGINAL" OU "TRADUCTION"

PETITION NO./Nº DE LA PÉTITION	BY / DE	DATE
411-1784	Mme May (Saanich—Gulf Islands)	24 septembre 2012

RESPONSE BY THE MINISTER OF PUBLIC SAFETY
RÉPONSE DU MINISTRE DE LA SÉCURITÉ PUBLIQUE

L'honorable Vic Toews

PRINT NAME OF SIGNATORY
INSCRIRE LE NOM DU SIGNATAIRE

SIGNATURE
MINISTER OR PARLIAMENTARY SECRETARY
MINISTRE OU SECRÉTAIRE PARLEMENTAIRE

SUBJECT / OBJET
Télécommunications

RESPONSE / RÉPONSE

ORIGINAL TEXT / TEXTE ORIGINAL [ ]
TRANSLATION / TRADUCTION [X]

Sécurité publique Canada

Emmett, Jamie

From: Chayer, Marie-Helene
Sent: September-27-12 3:06 PM
To: Maillé, Marie Anick
Subject: FW: Teleconference re. Lawful Access - CACP Up-date
Attachments: IPCECA Request from PO to to Designated Person.doc; ATT00001.htm; IPCECA Exigent Request to Provider by Officer.doc; ATT00002.htm; IPCECA Request from Designated Person to Service Providers.doc; ATT00003.htm

Importance: High

s.19(1)

Marie-Hélène Chayer
Director – Investigative Technology and Telecommunications Policy
Directrice – Politique sur les technologies d'enquêtes et les télécommunications
National Security Operations Division / Division des Opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
(613)949-3181

From: Timothy Smith [mailto:timsmith2000@rogers.com]
Sent: September-19-12 2:25 PM
To: Chayer, Marie-Helene
Cc: Johnston, Shannon; Haeck, Kimberly; MacDonald, Michael; [redacted]
Timothy M. Smith
Subject: Teleconference re. Lawful Access - CACP Up-date
Importance: High

Had not yet heard back from you Marie-Helene but I wanted to pass on some information which assumes we will be going ahead with the teleconference. Would appreciate if you could confirm back that the timing works.

Teleconference re. Lawful Access - CACP Up-date:

- Friday, Sept. 21 at 11:00 a.m.

From the CACP:

- [redacted]
- [redacted]
- Tim Smith (CACP - Government Relations)

[redacted] will forward call-in instructions shortly.

I am attaching three documents for discussion during the teleconference.

Pages 445 to / à 451

are withheld pursuant to sections

sont retenues en vertu des articles

21(1)(a), 21(1)(c)

of the Access to Information

de la Loi sur l'accès à l'information

We look forward to having this brief discussion which should not last more than 45 minutes.

Timothy M. Smith
Government Relations and Strategic Communications,
Canadian Association of Chiefs of Police
www.CACP.ca
613-601-0692
timsmith2000@rogers.com

On 2012-09-18, at 9:01 AM, "Chayer, Marie-Helene" <Marie-Helene.Chayer@ps-sp.gc.ca> wrote:

> Good morning,
>
> I will confirm with Mike and get back to you as soon as possible.
>
> I look forward to working with you,
>
> Marie-Hélène
>
> Marie-Hélène Chayer
>
> Director – Investigative Technology and Telecommunications Policy /
>
> Directrice – Politique sur les technologies d'enquêtes et les télécommunications
>
> National Security Operations Division / Division des Opérations de sécurité nationale
>
> Public Safety Canada / Sécurité Publique Canada
>
> (613)949-3181
>
> -----Original Message-----
> From: Tim Smith [mailto:timsmith2000@rogers.com]
> Sent: September-18-12 8:54 AM
> To: Johnston, Shannon
> Cc: Chayer, Marie-Helene; Haeck, Kimberly; MacDonald, Michael
> Subject: Re: Teleconference re. lawful access
>
> That sounds great. Do you want to confirm that now or talk to Mike first?
>
> On 2012-09-18, at 8:50 AM, "Johnston, Shannon" <Shannon.Johnston@ps-sp.gc.ca> wrote:
>
> > Good morning,

s.19(1)

Mike is away at a presentation this A.M. (with no access to his BB until lunch) but after looking at both his and Marie-Helene's calendars, Friday morning at 11am would work best.

Thank you

Shannon Johnston
Executive Assistant / Adjointe administrative éxecutive National Security Operations Directorate / Direction des operations de sécurité nationale
Tel: (613) 949-4623

-----Original Message-----
From: Tim Smith [mailto:timsmith2000@rogers.com]
Sent: September-18-12 8:37 AM
To: MacDonald, Michael
Cc: Chayer, Marie-Helene; Johnston, Shannon; Haeck, Kimberly
Subject: Re: Teleconference re. lawful access

Mike, would you have time for this call this Thursday afternoon (Sept. 20) or any time on Friday (Sept 21). Once confirmed, we will send you some background documentation and call in instructions. [redacted] potentially [redacted] and myself will be on from our end.

Thanks,

Timothy M. Smith
Government Relations and Strategic Communications Canadian Association of Chiefs of Police

On 2012-09-13, at 12:36 PM, "MacDonald, Michael" <Michael.MacDonald@ps-sp.gc.ca> wrote:

> Hi Tim,
>
> This is great - thanks. Please note that Marie-Helene [redacted] has resumed her duties as Director of this area.
>
> Michele is still with us, but has taken on a new Director role in my area.
>
> Look forward to chatting. Mike
>
> -----Original Message-----
> From: Timothy Smith [mailto:timsmith2000@rogers.com]
> Sent: September-13-12 10:48 AM
> To: MacDonald, Michael
> Cc: Kingsley, Michèle; Timothy M. Smith
> Subject: Teleconference re. lawful access

Michael and Michele - Our Law Amendments committee wanted to keep you both in the loop re. discussions we have had with the Office of the Privacy Commissioner and any further information we can share on this issue. We are hoping to set-up a teleconf to discuss with you. [redacted] and myself). WIll let you know possible times but just wanted to give you a heads-up. I hope that is agreeable with you.

Tim

s.19(1)

SECRET

Interception and wireless providers' lawful access condition of licence

Under the *Radiocommunication Act*, telecommunications service providers (TSPs) are subject to certain conditions of licence, which can include lawful interception. While the current licencing regime is an important tool in the investigative toolbox, [redacted]
Specifically, key challenges include:

[redacted]

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

[redacted]

Comprehensive legislation would cover all of the following subscribers, while a lawful intercept condition of licence would cover only some of those in the "Wireless" column below:

Subscribers to Telecom Services (figure range from 2010 to 2012)			
TSP	**Wireless**	**Wireline/Cable Phone**	**Wireline Internet**
Rogers	9,400,000	1,052,000	1,793,000
Bell	7,500,000	8,730,000	2,975,000
Telus	7,400,000	3,593,000	1,286,000
SaskTel	600,000	514,000	235,000
MTS	491,000	Unknown	190,000
Shaw	N/A	1,233,000	1,877,000
Wind	457,000	N/A	N/A
Videotron	348,000	1,205,000	1,333,000
Cogeco	N/A	418,000	601,000
Mobilicity	250,000 (estimated)	N/A	N/A
Public Mobile	199,000 (estimated)	N/A	N/A
Eastlink	N/A	457,000	457,000
All Others	Unknown	Unknown	Unknown
TOTAL	**26,644,000**	**17,202,000**	**10,747,000*** **

*** There are many more independent ISPs than there are wireless/wireline phone companies, so the entry "All Others" under Wireline Internet is likely to be significant.

s.21(1)(a)

Cost of lawful interception solutions

1. Open source:

s.15(1) - Int'l
s.16(1)(c)
s.16(2)

- In the US, initial industry estimates was that CALEA would cost between $3-5B, while the FBI estimated $500M to $1B.
- Industry lowered its estimates to $1.3B in 1998/99.

Source: US Department of Justice, Office of the Inspector General, "Implementation of the Communications Assistance for Law Enforcement Act by the Federal Bureau of Investigation", Report No. 04-19, April 2004, http://www.justice.gov/oig/reports/FBI/a0419/

2. From the Agencies:

[redacted]

Source: [redacted] phone discussion May 2012

3. From LI Vendors:

[redacted]

s.21(1)(a)

SECRET

Drafted: NSOD/Hawrylak
Date: 21 September 2012

s.23

Plunkett, Shawn

From: Ted.Murphy@justice.gc.ca
Sent: September-14-12 2:26 PM
To: Natacha.Guilbault@ic.gc.ca
Cc: Edward.Livingstone@justice.gc.ca
Subject: RE: Urgent request - Lawful Intercept Conditions of Licence

Thanks for the billing info.

In case it might prove useful going forward, the following is a very brief recap of the preliminary thoughts that I tried to communicate yesterday.

[redacted]

-----Original Message-----
From: Natacha.Guilbault@ic.gc.ca [mailto:Natacha.Guilbault@ic.gc.ca] s.21(1)(a)
Sent: 2012-Sep-13 4:36 PM s.23
To: Murphy, Ted
Subject: RE: Urgent request - Lawful Intercept Conditions of Licence

Ted,

Thanks again for taking the time to consider our question in such a short timeframe. We will certainly be in touch should our client decide [redacted]

For billing purposes, the client is Helen McDonald, Senior Assistant Deputy Minister, Spectrum, Information Technologies and Telecommunications, Industry Canada.

Best regards,

Natacha Guilbault

Legal Counsel | Avocate

Department of Justice Canada | Ministère de la Justice Canada

Industrie Canada Legal Services | Services juridiques d'Industrie Canada

235 Queen, 8th Floor East | 235 Queen, 8e étage

Ottawa, ON K1A 0H5

Natacha.Guilbault@ic.gc.ca

Telephone | Téléphone 613-957-8122

Facsimile | Télécopieur 613-954-5356

Teletypewriter | Téléimprimeur 1-866-694-8389

Government of Canada | Gouvernement du Canada

utiliser ou de les divulguer. Si vous recevez le présent message par erreur, veuillez nous en aviser immédiatement et le détruire, ainsi que les documents qui y sont joints. Merci.

-----Original Message-----

From: Murphy, Ted [mailto:Ted.Murphy@justice.gc.ca]

Sent: Thursday, September 13, 2012 1:34 PM

To: Guilbault, Natacha: LEG-DROIT

Cc: Fournier, Véronique

Subject: RE: Urgent request - Lawful Intercept Conditions of Licence

Thanks. Could you pls confirm once successfully sent, so that we can have the doc picked up immediately.

-----Original Message-----

From: Natacha.Guilbault@ic.gc.ca [mailto:Natacha.Guilbault@ic.gc.ca]

Sent: 2012-Sep-13 1:04 PM

To: Murphy, Ted

Cc: Fournier, Véronique

Subject: RE: Urgent request - Lawful Intercept Conditions of Licence

I'm having it sent right now. Apologies for the delay.

-----Original Message-----

s.15(1) - Subv
s.23

From: Murphy, Ted [mailto:Ted.Murphy@justice.gc.ca]

Sent: Thursday, September 13, 2012 12:26 PM

To: Guilbault, Natacha: LEG-DROIT

Cc: Fournier, Véronique

Subject: RE: Urgent request - Lawful Intercept Conditions of Licence

Importance: High

Also, [redacted] may not be located on LOPORS/Justipedia, presumably because it was characterized as SECRET. The fastest way for me to access it is to have you send it to me. Could you pls fax to our secure fax asap? The # is [redacted]

Vero -- pls watch for this incoming fax for me.

Thank you.

-----Original Message-----

From: Murphy, Ted

Sent: 2012-Sep-13 12:20 PM

To: 'Natacha.Guilbault@ic.gc.ca'

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

Subject: FW: Urgent request - Lawful Intercept Conditions of Licence

Hello Natacha.

[redacted]

However, it occurs to us that, if you have not already, it would be advisable for you simultaneously [redacted]

Ted J. Murphy

Counsel

Constitutional, Administrative and International Law Section

Department of Justice Canada

284 Wellington Street, Office #3073

Ottawa, ON K1A 0H8

613.952.1232

613.941.1937 (fax)

ted.murphy@justice.gc.ca

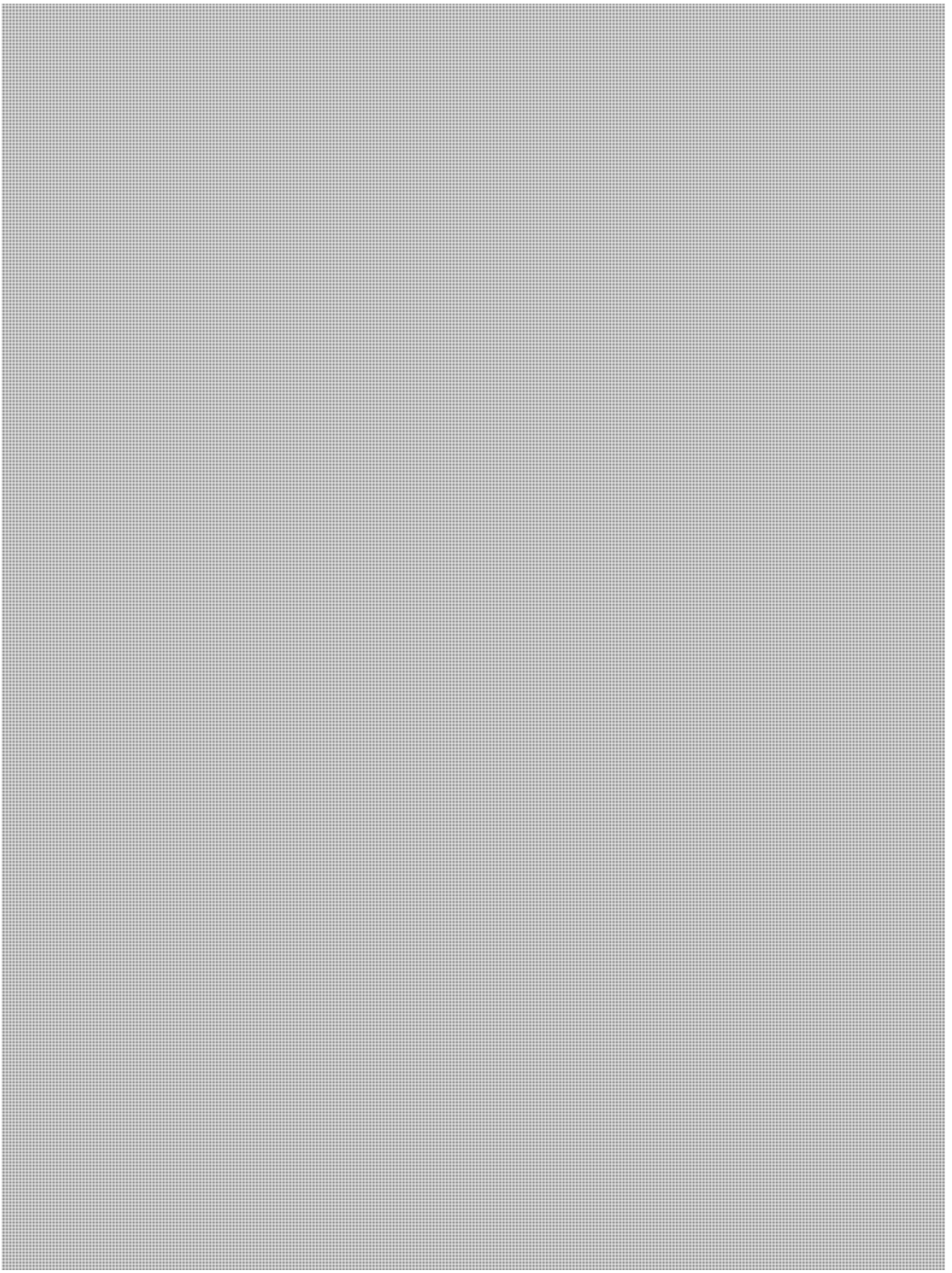
-----Original Message-----

From: Guilbault, Natacha: LEG-DROIT

Sent: 2012 Sep 13 11:23 AM

To: Wright, Laurie

Entire document subject to ATIP exemption 16(1)(b)



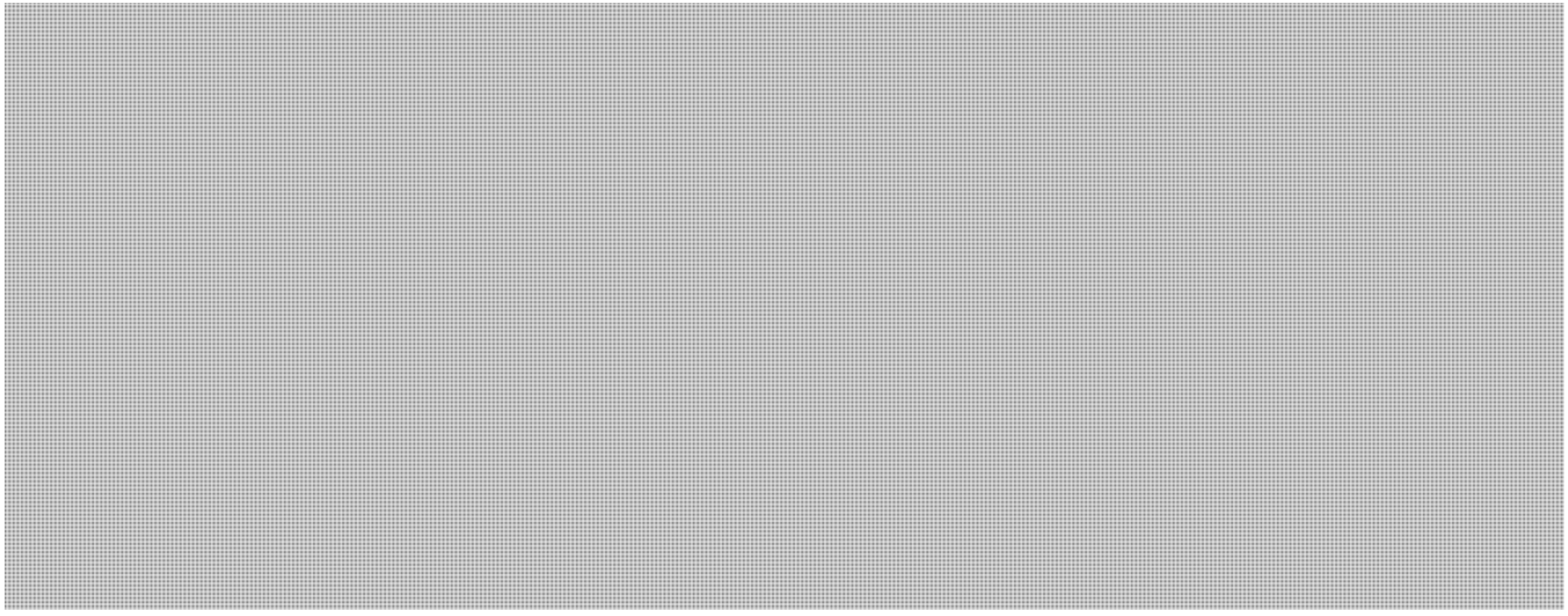
s.20(1)(b)

August 27, 2012

Bell

s.20(1)(b)

Objective

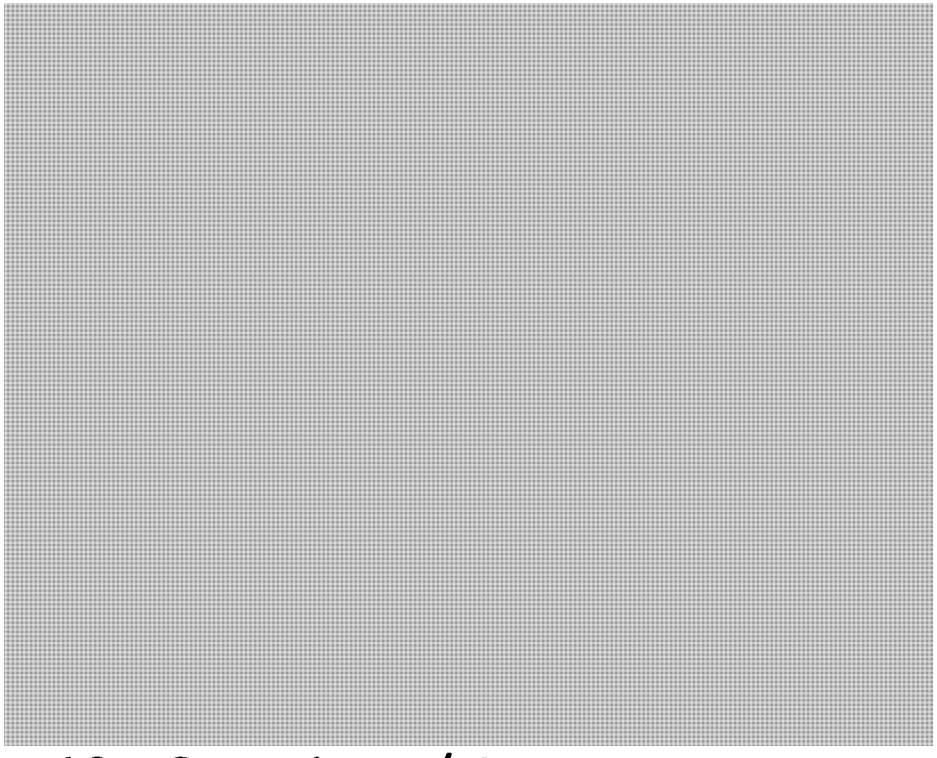


Bell

s.20(1)(b)

[redacted] Agenda

1. Objective



12. Questions / Answers

Bell

Page 467

is withheld pursuant to section

est retenue en vertu de l'article

21(1)(b)

of the Access to Information

de la Loi sur l'accès à l'information

Page 468

is withheld pursuant to section

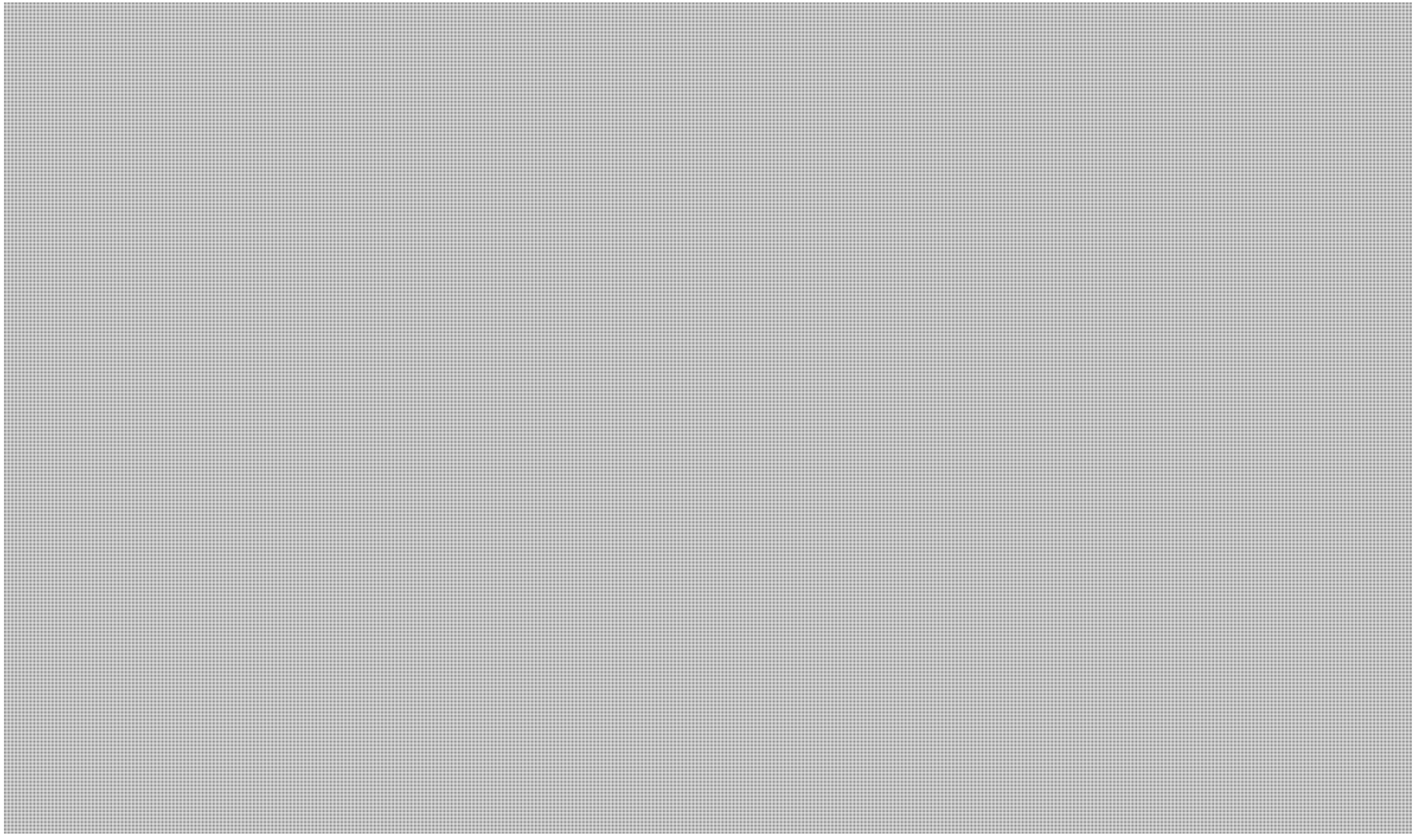
est retenue en vertu de l'article

20(1)(b)

of the Access to Information

de la Loi sur l'accès à l'information

s.20(1)(b)



s.20(1)(b)

s.20(1)(b)

s.20(1)(b)

s.20(1)(b)

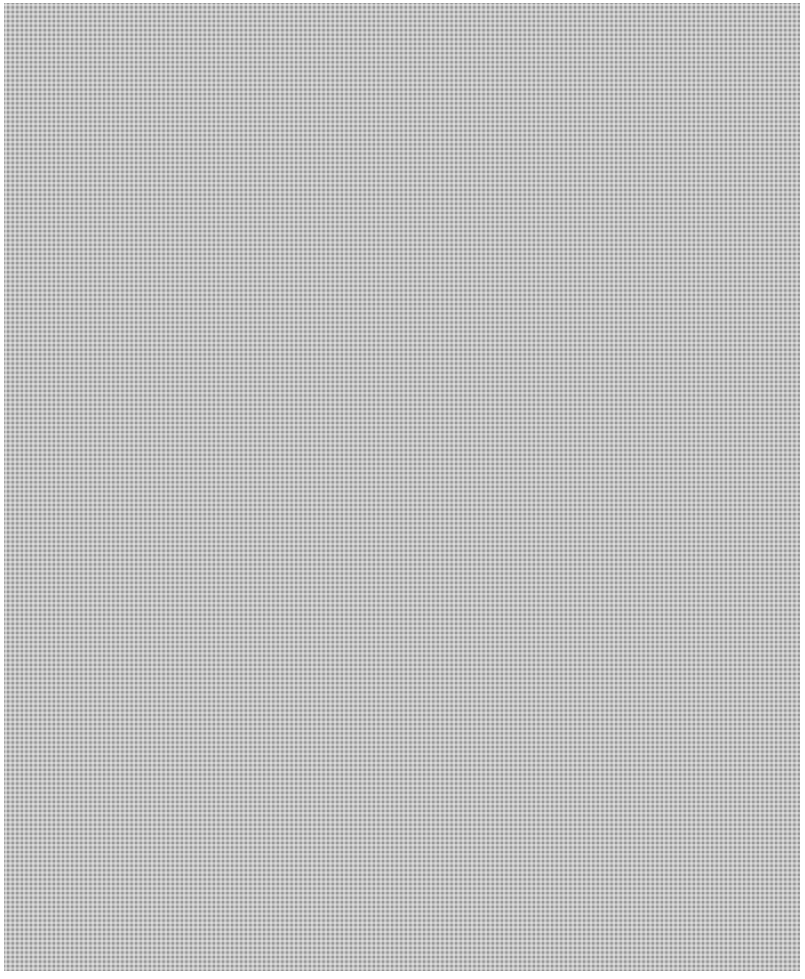
s.20(1)(b)

Bell

s.20(1)(b)

s.20(1)(b)

s.20(1)(b)

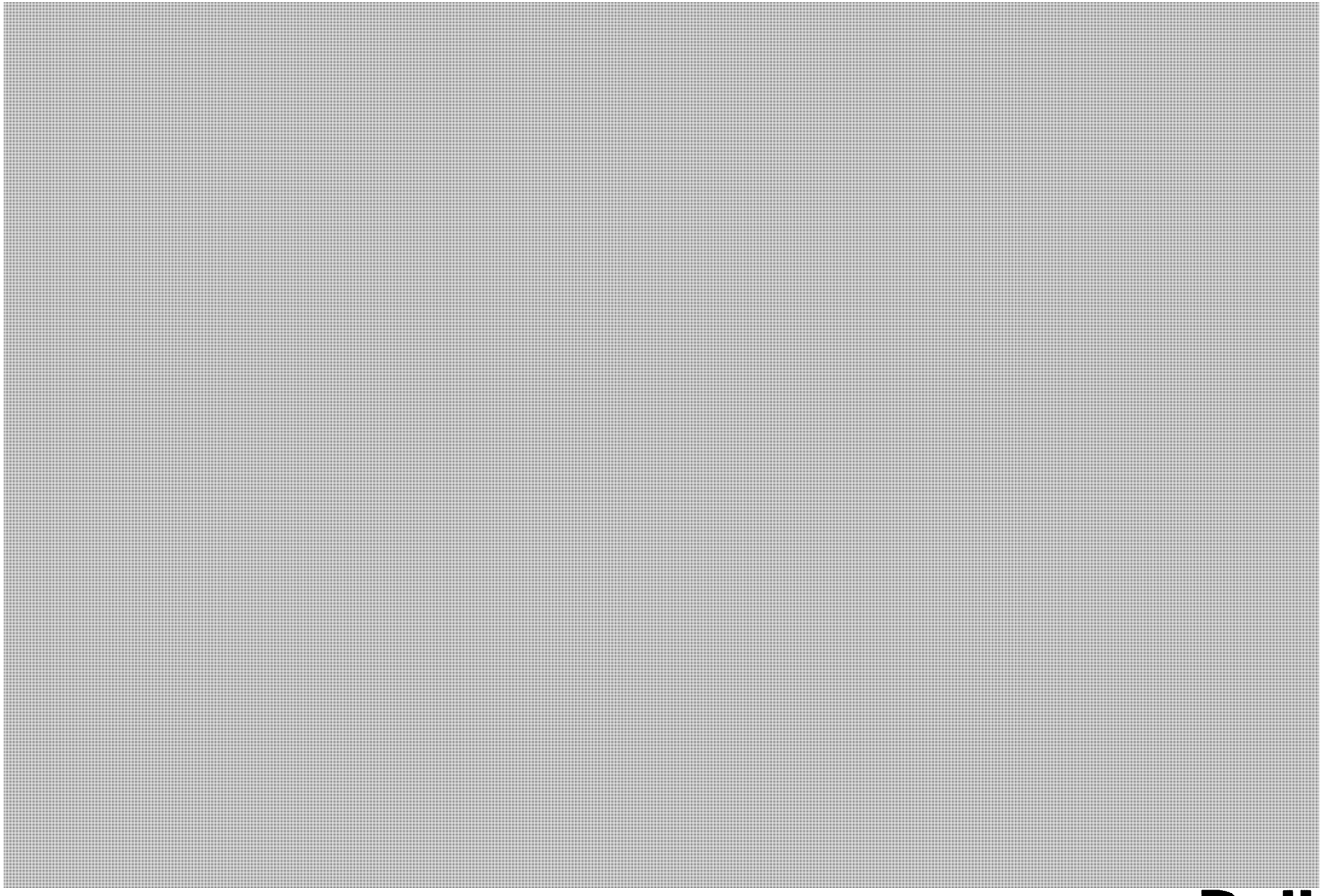


Bell

Background

Bell

s.20(1)(b)



s.20(1)(b)

Plunkett, Shawn

From:
Sent: August-16-12 12:11 PM
To: Plunkett, Shawn
Subject: RE: Costing Matrix for Lawful Interception Equipment - Information on lawful interception in Canada

Excellent thanks

s.19(1)

-----Original Message-----
From: Plunkett, Shawn [Shawn.Plunkett@ps-sp.gc.ca]
Received: Thursday, 16 Aug 2012, 11:16am
To:
Subject: RE: Costing Matrix for Lawful Interception Equipment - Information on lawful interception in Canada

Hi
I spoke with your colleague yesterday. Unfortunately, between our various holidays, we have not yet been able to discuss setting up a call. I will speak with my folks in my office next week and see if we can get a time set-up.

Thanks very much for following up. I hope to be able to speak with you early next week.

Shawn

-----Original Message-----
From:
Sent: August-13-12 9:53 AM
To: Plunkett, Shawn
Subject: RE: Costing Matrix for Lawful Interception Equipment - Information on lawful interception in Canada

Hi Shawn,

Just following up to see if your colleague has returned from holiday and if we can look at schedules to try and set up a call.

Regards,

-----Original Message-----
From: Plunkett, Shawn [mailto:Shawn.Plunkett@ps-sp.gc.ca]
Sent: Friday, July 20, 2012 4:37 PM
To:
Cc:
Subject: RE: Costing Matrix for Lawful Interception Equipment - Information on lawful interception in Canada

Hi

Thank you very much for your response.

We would be interested in setting up a call with you. However, a colleagues of mine who would be ideally placed to join us is on holidays (that time of year!).
Perhaps it would be easiest if I touch base with you once he returns and we can set up some time to discuss developing a costing matrix.

Thanks very much and have a good weekend. s.19(1)

Shawn

Shawn Plunkett
Senior Policy Advisor / Conseiller principal en politiques National Security Operations Directorate / Direction des opérations de sécurité nationale Public Safety Canada / Sécurité Publique Canada
340 Ave Laurier W, Ottawa,
Ontario, Canada, K1A 0P9
Telephone | Téléphone: (613) 990-7066
Facsimile | Télécopieur: (613) 991-4669 Email |
Courriel: shawn.plunkett@ps.gc.ca

-----Original Message-----
From:
Sent: July-16-12 5:13 PM
To: Plunkett, Shawn
Cc:
Subject: FW: Costing Matrix for Lawful Interception Equipment - Information on lawful interception in Canada

Hi Shawn,

I would be happy to discuss your needs in more detail. Is it possible to set up a call.

Kind Regards,

-----Original Message-----
From:
Sent: Monday, July 16, 2012 4:56 PM
To: Plunkett, Shawn
Cc:
Subject: Re: Costing Matrix for Lawful Interception Equipment - Information on lawful interception in Canada

Shawn,

It was great to meet with you at ISS last month. Sorry for not responding sooner, but I've been on vacation until today.

Can I introduce you to ? She looks after Sales for North America. can you address the points which Shawn makes in his email to below?

kind regards,

On 10 Jul 2012, at 15:22, Plunkett, Shawn wrote:

> Hi
>
> It was nice meeting you at ISS World Europe in Prague in early June.
> I had sent the below email to your last month, but
> have
yet to receive a response.

> I understand that as [redacted] time is likely very limited and therefore
> was
wondering if you may have a contact in the North American sales team, that I could possibly discuss this issue with.
>
> Hope all is well.
>
> Thanks very much.
>
> Shawn
>
> From: Plunkett, Shawn
> Sent: June-19-12 12:09 PM
> To: [redacted]
> Subject: Costing Matrix for Lawful Interception Equipment -
> Information on lawful interception in Canada
>
> Hi [redacted]
>
> It was good to meet you at ISS World Europe two weeks ago. I trust you
> had
a safe journey back from Europe.
>
> I was grateful for your time to discuss lawful interception in Canada
> and
how [redacted] might assist the Canadian Government.
>
> As discussed, the Government of Canada has developed lawful access
legislation, which will ensure that telecommunications companies have lawful intercept capabilities. Below is the link to the Canadian legislation on lawful interception tabled in our Parliament earlier this year. The Bill
C-30 is called the Investigative and Preventing Criminal Electronic Communications Act. Due to parliamentary processes in Canada, it may need to be re-tabled in Parliament in the fall, but this is what the legislation looks like right now. Happy to provide some additional details if desired.
>
> http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=5380965
>
> We also spoke of the need for regulators to better understand the
financial costs associated with legislative requirements imposed on telecommunication carriers and service providers. As a result, we had agreed to work together to develop a "cost matrix" to identify some general cost estimates for varying levels of lawful interception equipment. I believe you agreed to have someone from your sales team work with us on this. If you could send along a contact for working on this matter, I would appreciate it.
>
> You would certainly have a better basis for what [redacted] products could be
provided to Telecommunications Service Providers (TSPs) in terms of LI, but the below draft matrix reflects a basic idea of what we are looking for. [redacted]
>
>
> Cost for Wireline solution
> Cost for Wireless solution (Voice and Data) Cost for Internet
> solutions (social media/webmail; not facilities-based) Estimated
> Maintenance costs (per year) Any additional costs (implementation,
> customization)?
> Small TSP (1 mediation box)
>
>
> s.19(1)
>
>
> Medium TSP (2-3 mediation boxes)
>
>
>

>
>
> Large TSP (4-5 mediation boxes)
>
>
>
>
>
>
> Again, we are greatly for your assistance. I look forward to working
> with
you staff to assist us in this matter. Should you wish any further information from us, please do not hesitate to contact me.
>
> All the best.
>
> Shawn Plunkett
> Senior Policy Advisor / Conseiller principal en politiques National
> Security Operations Directorate / Direction des opérations de sécurité
> nationale Public Safety Canada / Sécurité Publique Canada
> 340 Ave Laurier W, Ottawa,
> Ontario, Canada, K1A 0P9
> Telephone | Téléphone: (613) 990-7066
> Facsimile | Télécopieur: (613) 991-4669 Email | Courriel:
> shawn.plunkett@ps.gc.ca
>
> <image001.jpg>
>
>

C-30

First Session, Forty-first Parliament,
60-61 Elizabeth II, 2011-2012

HOUSE OF COMMONS OF CANADA

BILL C-30

An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts

FIRST READING, FEBRUARY 14, 2012

MINISTER OF PUBLIC SAFETY

C-30

Première session, quarante et unième législature,
60-61 Elizabeth II, 2011-2012

CHAMBRE DES COMMUNES DU CANADA

PROJET DE LOI C-30

Loi édictant la Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention et modifiant le Code criminel et d'autres lois

PREMIÈRE LECTURE LE 14 FÉVRIER 2012

MINISTRE DE LA SÉCURITÉ PUBLIQUE

90639

RECOMMENDATION

His Excellency the Governor General recommends to the House of Commons the appropriation of public revenue under the circumstances, in the manner and for the purposes set out in a measure entitled "*An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts*".

RECOMMANDATION

Son Excellence le gouverneur général recommande à la Chambre des communes l'affectation de deniers publics dans les circonstances, de la manière et aux fins prévues dans une mesure intitulée « *Loi édictant la Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention et modifiant le Code criminel et d'autres lois* ».

SUMMARY

Part 1 enacts the *Investigating and Preventing Criminal Electronic Communications Act*, which requires telecommunications service providers to put in place and maintain certain capabilities that facilitate the lawful interception of information transmitted by telecommunications and to provide basic information about their subscribers to the Royal Canadian Mounted Police, the Canadian Security Intelligence Service, the Commissioner of Competition and any police service constituted under the laws of a province.

Part 2 amends the *Criminal Code* in respect of authorizations to intercept private communications, warrants and orders and adds to that Act new investigative powers in relation to computer crime and the use of new technologies in the commission of crimes. Among other things, it

(*a*) provides that if an authorization is given under certain provisions of Part VI, the judge may at the same time issue a warrant or make an order that relates to the investigation in respect of which the authorization is given;

(*b*) provides that the rules respecting confidentiality that apply in respect of a request for an authorization to intercept private communications also apply in respect of a request for a related warrant or order;

(*c*) requires the Minister of Public Safety and Emergency Preparedness to report on the interceptions of private communications made without authorizations;

(*d*) provides that a person who has been the object of an interception made without an authorization must be notified of the interception within a specified period;

(*e*) permits a peace officer or a public officer, in certain circumstances, to install and make use of a number recorder without a warrant;

(*f*) extends to one year the maximum period of validity of a warrant for a tracking device and a number recorder if the warrant is issued in respect of a terrorism offence or an offence relating to a criminal organization;

(*g*) provides the power to make preservation demands and orders to compel the preservation of electronic evidence;

(*h*) provides new production orders to compel the production of data relating to the transmission of communications and the location of transactions, individuals or things;

SOMMAIRE

La partie 1 édicte la *Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention*, laquelle exige des télécommunicateurs qu'ils disposent des moyens nécessaires pour faciliter l'interception licite de l'information transmise par télécommunication et qu'ils fournissent des renseignements de base sur leurs abonnés à la Gendarmerie royale du Canada, au Service canadien du renseignement de sécurité, au commissaire de la concurrence ou à tout service de police constitué sous le régime d'une loi provinciale.

La partie 2 modifie certaines dispositions du *Code criminel* relatives aux autorisations d'intercepter des communications privées, aux mandats et aux ordonnances et ajoute de nouveaux pouvoirs d'enquête liés aux délits informatiques et à l'utilisation de nouvelles technologies pour perpétrer des infractions. Elle prévoit notamment ce qui suit :

a) le fait que, lorsque le juge accorde une autorisation en vertu de certaines dispositions de la partie VI, il peut en même temps rendre certaines ordonnances et délivrer un mandat ayant trait à l'enquête à l'égard de laquelle l'autorisation est accordée;

b) l'application des règles visant à assurer le secret de la demande d'autorisation d'interception de communication privée aux demandes d'ordonnance ou de mandat connexes;

c) l'obligation, pour le ministre de la Sécurité publique et de la Protection civile, de faire rapport sur les interceptions de communications privées faites sans autorisation;

d) le fait que toute personne qui a fait l'objet d'une interception de communication privée sans autorisation doit en être avisée à l'intérieur de certains délais;

e) le fait que, dans certaines circonstances, un agent de la paix ou un fonctionnaire public peut, sans mandat, installer et utiliser un enregistreur de numéro;

f) la prolongation jusqu'à un an de la période de validité maximale d'un mandat pour l'utilisation d'un dispositif de localisation ou d'un enregistreur de numéro lorsque la mandat vise une infraction de terrorisme ou une infraction liée à une organisation criminelle;

Also available on the Parliament of Canada Web Site at the following address: **http://www.parl.gc.ca**

Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante : **http://www.parl.gc.ca**

(*i*) provides a warrant to obtain transmission data that will extend to all means of telecommunication the investigative powers that are currently restricted to data associated with telephones; and

(*j*) provides warrants that will enable the tracking of transactions, individuals and things and that are subject to legal thresholds appropriate to the interests at stake.

It also amends offences in the *Criminal Code* relating to hate propaganda and its communication over the Internet, false information, indecent communications, harassing communications, devices used to obtain telecommunication services without payment and devices used to obtain the unauthorized use of computer systems or to commit mischief.

Part 2 also amends the *Competition Act* to make applicable, for the purpose of enforcing certain provisions of that Act, the new provisions being added to the *Criminal Code* respecting demands and orders for the preservation of computer data and orders for the production of documents relating to the transmission of communications or financial data. It also modernizes the provisions of the Act relating to electronic evidence and provides for more effective enforcement in a technologically advanced environment.

Lastly, it amends the *Mutual Legal Assistance in Criminal Matters Act* to make some of the new investigative powers being added to the *Criminal Code* available to Canadian authorities executing incoming requests for assistance and to allow the Commissioner of Competition to execute search warrants under the *Mutual Legal Assistance in Criminal Matters Act*.

Part 3 contains coordinating amendments and coming-into-force provisions.

g) le pouvoir de donner un ordre de préservation et de rendre une ordonnance au même effet qui rendront obligatoire la préservation de la preuve électronique;

h) de nouvelles ordonnances de communication qui rendront obligatoire la communication de données concernant la transmission de communications et le lieu où se déroulent des opérations ou le lieu où se trouvent des personnes physiques ou des choses;

i) un mandat visant à obtenir des données de transmission afin d'étendre à tout autre moyen de télécommunication les pouvoirs d'enquête actuellement restreints aux données relatives aux téléphones;

j) des mandats, assujettis aux seuils juridiques appropriés aux intérêts en cause, qui permettront de localiser des opérations, des personnes physiques ou des choses.

Elle modifie également le *Code criminel* relativement aux infractions liées à la propagande haineuse et à sa communication par Internet, aux faux renseignements, aux communications indécentes ou faites avec l'intention de harceler, aux dispositifs permettant l'obtention de services de télécommunication sans paiement et aux dispositifs permettant l'utilisation non autorisée d'un ordinateur ou la commission d'un méfait.

Elle modifie aussi la *Loi sur la concurrence* afin de rendre applicables, pour assurer le contrôle d'application de certaines dispositions de cette loi, les nouvelles dispositions du *Code criminel* concernant les ordres et ordonnances de préservation de données informatiques et les ordonnances de communication de documents ayant trait à la transmission de communications ou à des données financières. Elle modernise les dispositions relatives à la preuve électronique et permet un contrôle d'application plus efficace de la loi dans un environnement technologique de pointe.

Elle modifie enfin la *Loi sur l'entraide juridique en matière criminelle* afin de permettre aux autorités canadiennes qui reçoivent des demandes d'assistance d'utiliser certains des nouveaux pouvoirs d'enquête prévus au *Code criminel* et de permettre au commissaire de la concurrence d'exécuter des mandats de perquisition en vertu de la *Loi sur l'entraide juridique en matière criminelle*.

La partie 3 comprend des dispositions de coordination et les dispositions d'entrée en vigueur.

TABLE OF PROVISIONS

AN ACT TO ENACT THE INVESTIGATING AND PREVENTING CRIMINAL ELECTRONIC COMMUNICATIONS ACT AND TO AMEND THE CRIMINAL CODE AND OTHER ACTS

TABLE ANALYTIQUE

LOI ÉDICTANT LA LOI SUR LES ENQUÊTES VISANT LES COMMUNICATIONS ÉLECTRONIQUES CRIMINELLES ET LEUR PRÉVENTION ET MODIFIANT LE CODE CRIMINEL ET D'AUTRES LOIS

1st Session, 41st Parliament,
60-61 Elizabeth II, 2011-2012

HOUSE OF COMMONS OF CANADA

BILL C-30

An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts

Her Majesty, by and with the advice and consent of the Senate and House of Commons of Canada, enacts as follows:

SHORT TITLE

Short title

1. This Act may be cited as the *Protecting Children from Internet Predators Act.*

PART 1

INVESTIGATING AND PREVENTING CRIMINAL ELECTRONIC COMMUNICATIONS ACT

ENACTMENT OF ACT

Enactment

2. The *Investigating and Preventing Criminal Electronic Communications Act*, whose text is as follows and whose Schedules 1 and 2 are set out in the schedule to this Act, is hereby enacted:

An Act regulating telecommunications facilities to support investigations

SHORT TITLE

Short title

1. This Act may be cited as the *Investigating and Preventing Criminal Electronic Communications Act.*

INTERPRETATION

Definitions

2. (1) The following definitions apply in this Act.

1re session, 41e législature,
60-61 Elizabeth II, 2011-2012

CHAMBRE DES COMMUNES DU CANADA

PROJET DE LOI C-30

Loi édictant la Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention et modifiant le Code criminel et d'autres lois

Sa Majesté, sur l'avis et avec le consentement du Sénat et de la Chambre des communes du Canada, édicte :

TITRE ABRÉGÉ

Titre abrégé

1. *Loi sur la protection des enfants contre les cyberprédateurs.*

PARTIE 1

LOI SUR LES ENQUÊTES VISANT LES COMMUNICATIONS ÉLECTRONIQUES CRIMINELLES ET LEUR PRÉVENTION

ÉDICTION DE LA LOI

Édiction

2. Est édictée la *Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention*, dont le texte suit et dont les annexes 1 et 2 figurent à l'annexe de la présente loi :

Loi régissant les installations de télécommunication aux fins de soutien aux enquêtes

TITRE ABRÉGÉ

Titre abrégé

1. *Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention.*

DÉFINITIONS ET INTERPRÉTATION

Définitions

2. (1) Les définitions qui suivent s'appliquent à la présente loi.

"authorized" « *autorisée* »
"authorized", in relation to a person, means having authority, under the *Criminal Code* or the *Canadian Security Intelligence Service Act*, to intercept communications.

"communication" « *communication* »
"communication" means a communication effected by a means of telecommunication and includes any related telecommunications data or other ancillary information.

"intercept" « *intercepter* »
"intercept" includes listen to, record or acquire a communication or acquire the substance, meaning or purport of the communication.

"Minister" « *ministre* »
"Minister" means the Minister of Public Safety and Emergency Preparedness.

"person" « *personne* »
"person" includes a partnership, an unincorporated organization, a government, a government agency and any other person or entity that acts in the name of or for the benefit of another.

"prescribed" *Version anglaise seulement*
"prescribed" means prescribed by the regulations.

"telecommunications data" « *données de télécommunication* »
"telecommunications data" means data relating to the telecommunications functions of dialling, routing, addressing or signalling that identifies or purports to identify the origin, type, direction, date, time, duration, size, destination or termination of a telecommunication generated or received by means of a telecommunications facility or the type of telecommunications service used. It also means any transmission data that may be obtained under subsection 492.2(1) of the *Criminal Code*.

"telecommunications facility" « *installation de télécommunication* »
"telecommunications facility" means any facility, apparatus or other thing that is used for telecommunications or for any operation directly connected with telecommunications.

"telecommunications service" « *service de télécommunication* »
"telecommunications service" means a service, or a feature of a service, that is provided by means of telecommunications facilities, whether the provider owns, leases or has any other interest in or right respecting the telecommunications facilities and any related equipment used to provide the service.

"telecommunications service provider" « *télécommunicateur* »
"telecommunications service provider" means a person that, independently or as part of a group or association, provides telecommunications services.

« appareil de transmission » *"transmission apparatus"*
« appareil de transmission » Appareil qui appartient à une catégorie réglementaire et dont les fonctions principales sont comprises parmi les suivantes :

a) commutation ou routage de communications;

b) saisie, réception, mise en mémoire, classement, modification, récupération ou sortie de communications, ou tout autre traitement de celles-ci;

c) commande de la vitesse, du code, du protocole, du contenu, de la forme, de la commutation, du routage ou des aspects analogues de communications;

d) toute fonction semblable à celles énumérées aux alinéas *a*) à *c*).

« autorisée » *"authorized"*
« autorisée » Se dit de toute personne qui est autorisée, au titre du *Code criminel* ou de la *Loi sur le Service canadien du renseignement de sécurité*, à intercepter des communications.

« communication » *"communication"*
« communication » Communication effectuée par voie de télécommunication, y compris les données de télécommunication connexes et toute autre information accessoire.

« données de télécommunication » *"telecommunications data"*
« données de télécommunication » Données concernant les fonctions de composition, de routage, d'adressage ou de signalisation en matière de télécommunication et indiquant, ou visant à indiquer, l'origine, le type, la direction, la date, l'heure, la durée, le volume, la destination ou la terminaison de la télécommunication produite ou reçue au moyen d'une installation de télécommunication ou le type de service utilisé. Sont également visées les données de transmission obtenues au titre du paragraphe 492.2(1) du *Code criminel*.

« installation de télécommunication » *"telecommunications facility"*
« installation de télécommunication » Installation, appareil ou dispositif quelconque servant à la télécommunication ou à toute opération qui y est directement liée.

« intercepter » *"intercept"*
« intercepter » S'entend notamment du fait d'écouter, d'enregistrer ou de prendre volontairement connaissance d'une communication ou de sa substance, son sens ou son objet.

"transmission apparatus" « *appareil de transmission* »

"transmission apparatus" means any apparatus of a prescribed class whose principal functions are one or more of the following:

(*a*) the switching or routing of communications;

(*b*) the input, capture, storage, organization, modification, retrieval, output or other processing of communications;

(*c*) the control of the speed, code, protocol, content, format, switching or routing or similar aspects of communications; or

(*d*) any other function that is similar to one described in paragraphs (*a*) to (*c*).

« ministre » "*Minister*"

« ministre » Le ministre de la Sécurité publique et de la Protection civile.

« personne » "*person*"

« personne » Sont assimilés à des personnes les sociétés de personnes, les organisations non personnalisées et les administrations et organismes publics. Est assimilée à la personne intéressée toute autre personne ou toute entité qui agit en son nom ou pour elle.

« service de télécommunication » "*telecommunications service*"

« service de télécommunication » Service — ou complément de service — fourni au moyen d'installations de télécommunication, que celles-ci et le matériel connexe appartiennent au télécommunicateur ou soient loués ou fassent l'objet d'un intérêt ou d'un droit en faveur de celui-ci.

« télécommunicateur » "*telecommunications service provider*"

« télécommunicateur » Personne qui fournit des services de télécommunication, seule ou au titre de son appartenance à un groupe ou à une association.

Preservation of existing powers

(2) Nothing in this Act derogates from any power in the *Criminal Code*, the *Canadian Security Intelligence Service Act* or Part V.1 of the *National Defence Act* to intercept communications or to request that telecommunications service providers assist in such interceptions.

Précision

(2) La présente loi ne porte pas atteinte aux pouvoirs prévus par le *Code criminel*, la *Loi sur le Service canadien du renseignement de sécurité* et la partie V.1 de la *Loi sur la défense nationale* concernant l'interception de toute communication ou toute demande d'assistance adressée aux télécommunicateurs en vue de procéder à une telle interception.

PURPOSE

Purpose

3. The purpose of this Act is to ensure that telecommunications service providers have the capability to enable national security and law enforcement agencies to exercise their authority to intercept communications and to require telecommunications service providers to provide subscriber and other information, without unreasonably impairing the privacy of individuals, the provision of telecommunications services to Canadians or the competitiveness of the Canadian telecommunications industry.

OBJET DE LA LOI

Objet

3. La présente loi a pour objet d'exiger des télécommunicateurs qu'ils disposent des moyens nécessaires pour permettre aux organismes chargés de la sécurité nationale ou du contrôle d'application des lois d'exercer leur pouvoir d'intercepter les communications et qu'ils fournissent des renseignements, notamment sur les abonnés, sans toutefois porter atteinte indûment à la vie privée des particuliers ou entraver sérieusement la prestation de services de télécommunication aux Canadiens et la compétitivité de l'industrie canadienne des télécommunications.

HER MAJESTY

Act binding on Her Majesty

4. This Act is binding on Her Majesty in right of Canada or of a province.

SA MAJESTÉ

Obligation de Sa Majesté

4. La présente loi lie Sa Majesté du chef du Canada et des provinces.

APPLICATION

Exclusions — Schedule 1

5. (1) This Act does not apply to telecommunications service providers in respect of the telecommunications services specified in Part 1 of Schedule 1 or to the telecommunications service providers in the classes listed in Part 2 of that Schedule in respect of the activities specified in that Part for that class.

Partial application — Schedule 2, Part 1

(2) This Act — other than sections 8, 9, 14, 15, 24 to 26, 28 and 32 to 64 — does not apply to the telecommunications service providers in the classes listed in Part 1 of Schedule 2 in respect of the activities specified in that Part for that class.

Partial application — Schedule 2, Part 2

(3) This Act, other than section 24, does not apply to the telecommunications service providers in the classes listed in Part 2 of Schedule 2 in respect of the activities specified in that Part for that class.

Amendment of Schedules

(4) The Governor in Council may, by regulation, amend Schedule 1 or 2 by adding, deleting or changing a telecommunications service, an activity or a class of telecommunications service providers.

OBLIGATIONS

OBLIGATIONS CONCERNING INTERCEPTIONS

Obligation to have capabilities

6. (1) For the purpose of enabling authorized persons to exercise their authority to intercept communications, every telecommunications service provider must have the capability to do the following:

(*a*) provide intercepted communications to authorized persons; and

(*b*) provide authorized persons with the prescribed information that is in the possession or control of the service provider respecting the location of equipment used in the transmission of communications.

Confidentiality and security measures

(2) A telecommunications service provider, in connection with the interception of communications, must comply with any prescribed confidentiality or security measures.

CHAMP D'APPLICATION

Non-application — annexe 1

5. (1) La présente loi ne s'applique pas aux télécommunicateurs à l'égard des services de télécommunication prévus à la partie 1 de l'annexe 1 ni aux télécommunicateurs appartenant aux catégories figurant à la partie 2 de cette annexe à l'égard des activités qui y sont précisées.

Application partielle — annexe 2, partie 1

(2) La présente loi, à l'exception des articles 8, 9, 14, 15, 24 à 26, 28 et 32 à 64, ne s'applique pas aux télécommunicateurs appartenant aux catégories figurant à la partie 1 de l'annexe 2 à l'égard des activités qui y sont précisées.

Application partielle — annexe 2, partie 2

(3) La présente loi, à l'exception de l'article 24, ne s'applique pas aux télécommunicateurs appartenant aux catégories figurant à la partie 2 de l'annexe 2 à l'égard des activités qui y sont précisées.

Modification des annexes

(4) Le gouverneur en conseil peut, par règlement, modifier les annexes 1 et 2 pour y ajouter, en retrancher ou y modifier des services de télécommunication, des activités ou des catégories de télécommunicateurs.

OBLIGATIONS

OBLIGATIONS CONCERNANT LES INTERCEPTIONS

Obligations relatives aux mesures de facilitation

6. (1) Afin de permettre à toute personne autorisée d'exercer son pouvoir d'intercepter les communications, il incombe à tout télécommunicateur de disposer des moyens nécessaires pour fournir à celle-ci :

a) toute communication interceptée;

b) toute information réglementaire qu'il a en sa possession ou à sa disposition relativement à l'emplacement de l'équipement utilisé pour la transmission d'une communication.

Confidentialité et sécurité

(2) Le télécommunicateur est tenu d'appliquer, relativement à l'interception de communications, les mesures réglementaires concernant la confidentialité et la sécurité.

Obligations for treated communications

(3) If an intercepted communication is encoded, compressed, encrypted or otherwise treated by a telecommunications service provider, the service provider must use the means in its control to provide the intercepted communication in the same form as it was before the communication was treated by the service provider.

Traitement de la communication

(3) Si la communication interceptée a fait l'objet d'un traitement — notamment codage, compression et chiffrement — par le télécommunicateur, celui-ci est tenu d'utiliser les moyens dont il dispose pour fournir la communication dans la forme où elle était avant ce traitement.

Exceptions

(4) Despite subsection (3), a telecommunications service provider is not required to make the form of an intercepted communication the same as it was before the communication was treated if

(*a*) the service provider would be required to develop or acquire decryption techniques or decryption tools; or

(*b*) the treatment is intended only for the purposes of generating a digital signature or for certifying a communication by a prescribed certification authority, and has not been used for any other purpose.

Exceptions

(4) Il n'est toutefois pas tenu de remettre la communication interceptée dans la forme où elle était avant le traitement dans les cas suivants :

a) il aurait à développer ou à acquérir des méthodes ou des outils de déchiffrement;

b) le traitement visait uniquement à générer une signature numérique ou à faire certifier la communication par une autorité de certification réglementaire et n'a pas été utilisé à d'autres fins.

Providing information as requested

(5) A telecommunications service provider that is capable of providing intercepted communications to an authorized person in more than one form or manner that conforms with the regulations must provide them in whichever of those forms or manners the authorized person requires.

Fourniture de la communication interceptée

(5) Il incombe au télécommunicateur, dans le cas où il est en mesure de fournir à la personne autorisée la communication interceptée sous différentes formes et par différents moyens qui sont conformes aux règlements, de la lui fournir dans la forme et par le moyen qu'elle précise.

Operational requirements for transmission apparatus

7. The operational requirements in respect of any transmission apparatus are that the telecommunications service provider operating the apparatus have the capability to do the following:

(*a*) enable the interception of communications generated by or transmitted through the apparatus to or from any temporary or permanent user of the service provider's telecommunications services;

(*b*) isolate the communication that is authorized to be intercepted from other information, including

(i) isolating the communications of the person whose communications are authorized to be intercepted from those of other persons, and

Exigences opérationnelles liées aux appareils de transmission

7. Constituent des exigences opérationnelles liées à tout appareil de transmission le fait pour le télécommunicateur qui exploite l'appareil d'être en mesure de prendre les dispositions suivantes :

a) permettre l'interception de la communication produite par l'appareil ou transmise ou reçue au moyen de celui-ci par l'utilisateur temporaire ou permanent de ses services de télécommunication;

b) isoler la communication dont l'interception est autorisée de toute autre information, notamment isoler :

(i) les communications de la personne visée de celles de toute autre personne,

(ii) les données de télécommunication du reste de ses communications;

(ii) isolating the telecommunications data of the person whose communications are authorized to be intercepted from the rest of the person's communications;

(*c*) provide prescribed information that permits the accurate correlation of all elements of intercepted communications; and

(*d*) enable simultaneous interceptions by authorized persons from multiple national security and law enforcement agencies of communications of multiple users, including enabling

(i) at least the minimum number of those interceptions, and

(ii) any greater number of those interceptions — up to the maximum number — for the period that an agency requests.

c) fournir l'information réglementaire qui permet de mettre en corrélation avec exactitude tous les éléments des communications interceptées;

d) permettre à des personnes autorisées provenant de plusieurs organismes chargés de la sécurité nationale ou du contrôle d'application des lois d'intercepter simultanément des communications de plusieurs utilisateurs, notamment permettre :

(i) au moins le nombre minimal d'interceptions simultanées,

(ii) un nombre accru d'interceptions — jusqu'à concurrence du nombre maximal — pour la période demandée par un tel organisme.

No degradation of capabilities

8. A telecommunications service provider that meets, in whole or in part, an operational requirement in respect of transmission apparatus that the service provider operates must continue to so meet that operational requirement.

Maintien de la conformité aux exigences opérationnelles

8. Il incombe au télécommunicateur qui satisfait à tout ou partie d'une exigence opérationnelle liée à un appareil de transmission qu'il exploite de continuer d'y satisfaire.

Maintaining capabilities in respect of new services

9. A telecommunications service provider that meets, in whole or in part, an operational requirement in respect of transmission apparatus that the service provider operates in connection with any of the service provider's telecommunications services must meet that operational requirement to the same extent in respect of any new service that the service provider begins to provide using that apparatus.

Maintien de la capacité à l'égard des nouveaux services

9. Il incombe au télécommunicateur qui satisfait à tout ou partie d'une exigence opérationnelle liée à un appareil de transmission qu'il exploite afin de fournir des services de télécommunication d'y satisfaire tout autant à l'égard des nouveaux services qu'il fournit au moyen de l'appareil.

Beginning to operate transmission apparatus

10. (1) A telecommunications service provider that begins to operate any transmission apparatus for the purpose of providing telecommunications services must meet the operational requirements in respect of the apparatus, whether by means of the apparatus itself or by any other means.

Exploitation d'appareils de transmission

10. (1) Le télécommunicateur qui commence à exploiter un appareil de transmission afin de fournir des services de télécommunication est tenu de satisfaire aux exigences opérationnelles liées à l'appareil, au moyen de celui-ci ou autrement.

Acquisition from another provider

(2) Subsection (1) does not apply in respect of transmission apparatus that a telecommunications service provider acquires from another telecommunications service provider and operates in order to continue to provide the same telecommunications service to approximately the same users. However, the acquiring service provider must continue to meet any operational

Transfert de propriété

(2) Le paragraphe (1) ne s'applique pas si le télécommunicateur commence à exploiter un appareil de transmission qu'il acquiert d'un autre télécommunicateur afin de continuer à fournir les mêmes services de télécommunication à approximativement les mêmes utilisateurs. Toutefois, il est tenu de satisfaire aux

requirements in respect of the transmission apparatus that the service provider from whom it was acquired was obligated to meet.

New software

11. (1) When a telecommunications service provider installs new software for any transmission apparatus that the service provider operates, the service provider must meet the operational requirements in respect of that apparatus to the extent that would be enabled by the installation of the software in the form available from the software's manufacturer that would most increase the service provider's ability to meet those operational requirements.

Other software licences or telecommunications facilities

(2) Subsection (1) applies even if the form of the software in question would require the telecommunications service provider to acquire additional software licences or telecommunications facilities to achieve that increased ability.

Global limit

12. Subject to section 14, a telecommunications service provider is not required, under sections 8 to 11, to increase the service provider's capability to enable simultaneous interceptions beyond the applicable global limit.

Order suspending obligations

13. (1) The Minister may, by order made on the application of a telecommunications service provider, suspend in whole or in part any obligation of the service provider to meet an operational requirement that would arise from the operation of section 10 or 11.

Applications

(2) The application must

(*a*) specify the operational requirement with respect to which an order is sought;

(*b*) set out the reasons for making the application;

(*c*) include a plan that

(i) sets out the measures by which and the time within which the telecommunications service provider proposes to meet the operational requirement specified in accordance with paragraph (*a*),

(ii) describes any measures that the service provider proposes to take to improve the service provider's capability to meet the operational requirements, even if they are not yet applicable, and

mêmes exigences opérationnelles liées à l'appareil que celles auxquelles l'autre télécommunicateur devait satisfaire.

Installation d'un nouveau logiciel

11. (1) Lorsqu'il installe un nouveau logiciel pour un appareil de transmission qu'il exploite, le télécommunicateur est tenu de satisfaire aux exigences opérationnelles liées à l'appareil dans la même mesure que s'il installait le logiciel dans la forme offerte par le fabricant la plus susceptible d'accroître sa capacité de satisfaire à ces exigences.

Licence et installation de télécommunication supplémentaires

(2) Le paragraphe (1) s'applique même si la forme du logiciel, pour qu'elle puisse permettre au télécommunicateur d'accroître ainsi sa capacité, nécessitait l'acquisition de licences d'exploitation ou d'installations de télécommunication supplémentaires.

Limite globale

12. Sous réserve de l'article 14, le télécommunicateur n'est pas tenu, au titre des articles 8 à 11, d'augmenter sa capacité de permettre des interceptions simultanées au-delà de la limite globale applicable.

Demande de suspension d'obligation

13. (1) Sur demande de tout télécommunicateur, le ministre peut, par arrêté, suspendre en tout ou en partie l'obligation de satisfaire aux exigences opérationnelles découlant de l'application des articles 10 et 11.

Contenu de la demande

(2) La demande :

a) précise les exigences opérationnelles qui sont visées;

b) énonce les moyens sur lesquels elle est fondée;

c) comporte un plan précisant :

(i) les mesures que se propose de prendre le télécommunicateur pour satisfaire à ces exigences opérationnelles et le délai dans lequel il compte le faire,

(ii) les mesures que le télécommunicateur se propose de prendre pour accroître sa capacité de satisfaire aux exigences opérationnelles même si celles-ci ne lui sont pas encore applicables,

(iii) identifies the stages at which and methods by which the Minister can measure progress in the implementation of the plan and the time, manner and form for reports the service provider proposes to make to the Minister; and

(*d*) conform with the prescribed requirements relating to the content or form of the application or the manner in which it is to be made.

(iii) les étapes de sa mise en oeuvre auxquelles le ministre pourra mesurer les progrès réalisés à cet égard, les méthodes pour ce faire, ainsi que les modalités — de temps et autres — concernant les rapports que le télécommunicateur se propose de soumettre au ministre;

d) satisfait aux exigences réglementaires visant son contenu et les modalités de présentation.

Considerations

(3) In deciding whether to make an order, the Minister must take into account the public interest in national security and law enforcement and the commercial interests of the telecommunications service provider as well as any other matter that the Minister considers relevant.

(3) Avant de statuer sur la demande, le ministre prend en considération tous les facteurs qu'il estime pertinents, notamment l'intérêt public — sécurité nationale et contrôle d'application des lois — et les intérêts commerciaux de l'auteur de la demande.

Facteurs à prendre en considération

Notification of decision

(4) The Minister must, within 120 days after the day on which the Minister receives the application, notify the applicant of the Minister's decision to accept or refuse it and, if no notification has been received by the applicant at the end of that period, the Minister is deemed to have refused the application.

(4) Le ministre a cent vingt jours, après la réception de la demande, pour l'accepter ou la refuser; si le télécommunicateur n'est pas avisé de la décision du ministre dans ce délai, celui-ci est réputé avoir refusé.

Notification de la décision

Conditions and term of order

(5) In the order, the Minister may include any conditions that the Minister considers appropriate and must fix its term for a period of not more than three years.

(5) Le ministre peut, dans l'arrêté, assortir la suspension des conditions qu'il estime indiquées et l'accorde pour une période maximale de trois ans.

Conditions et durée de la suspension

Obligation to comply with conditions of order

(6) The telecommunications service provider must comply with the conditions of the order as soon as the service provider begins to operate the telecommunications apparatus or installs the new software, as the case may be.

(6) Le télécommunicateur est tenu de satisfaire à de telles conditions dès qu'il commence à exploiter l'appareil de transmission en cause ou qu'il installe le nouveau logiciel.

Obligation de satisfaire aux conditions imposées par le ministre

Notice of revocation

(7) The Minister may revoke an order on written notice to the telecommunications service provider if

(*a*) the service provider has contravened this Act, the regulations or the conditions of the order; or

(*b*) the order was obtained through misrepresentation.

(7) Le ministre peut, sur avis écrit donné au télécommunicateur, révoquer l'arrêté :

a) soit au motif que celui-ci a enfreint la présente loi, ses règlements ou les conditions de la suspension;

b) soit au motif que la suspension a été obtenue par des moyens faux ou trompeurs.

Avis de révocation

Amendment

(8) The Minister may amend an order with the consent of the telecommunications service provider.

(8) Il peut modifier l'arrêté avec le consentement du télécommunicateur.

Modification

Ministerial orders

14. (1) The Minister may, at the request of the Commissioner of the Royal Canadian Mounted Police or the Director of the Canadian Security Intelligence Service and if in the Minister's opinion it is necessary to do so, order a telecommunications service provider

(*a*) to comply with any obligation under subsections 6(1) and (2) in a manner or within a time that the Minister specifies;

(*b*) to enable, in a manner or within a time that the Minister specifies, a number of simultaneous interceptions greater than any maximum or limit that would otherwise apply;

(*c*) to comply, in a manner or within a time that the Minister specifies, with any confidentiality or security measures respecting interceptions that the Minister specifies in addition to those referred to in subsection 6(2);

(*d*) to meet an operational requirement in respect of transmission apparatus operated by the service provider that the service provider would not otherwise be required to meet; or

(*e*) to meet an operational requirement in respect of transmission apparatus operated by the service provider in a manner or within a time that the Minister specifies.

Limitation

(2) The Minister is not authorized to make an order under subsection (1) in respect of a telecommunications service provider in relation to a telecommunications service specified in Part 1 of Schedule 1 or in respect of a telecommunications service provider in a class listed in Part 2 of Schedule 1 or Part 2 of Schedule 2 in relation to the activities specified for that class in Part 2 of Schedule 1 or Part 2 of Schedule 2, as the case may be.

Compensation

(3) The Commissioner of the Royal Canadian Mounted Police or the Director of the Canadian Security Intelligence Service, as the case may be, must pay the telecommunications service provider an amount that the Minister considers reasonable towards the expenses that the Minister considers are necessary for the service provider to incur initially to comply with an order made under this section.

Arrêté

14. (1) S'il le juge nécessaire, le ministre peut par arrêté, à la demande du commissaire de la Gendarmerie royale du Canada ou du directeur du Service canadien du renseignement de sécurité, ordonner au télécommunicateur :

a) d'exécuter, selon les modalités — de temps et autres — indiquées, toute obligation prévue aux paragraphes 6(1) et (2);

b) de permettre, selon les modalités — de temps et autres — indiquées, de faire des interceptions simultanées en un nombre supérieur à la limite qui s'appliquerait par ailleurs;

c) d'appliquer, selon les modalités — de temps et autres — indiquées, des mesures concernant la confidentialité ou la sécurité liées aux interceptions qui s'ajoutent à celles visées au paragraphe 6(2);

d) de satisfaire à toute exigence opérationnelle qui ne lui est pas par ailleurs applicable et qui est liée à un appareil de transmission qu'il exploite;

e) de satisfaire, selon les modalités — de temps et autres — indiquées, à toute exigence opérationnelle liée à un appareil de transmission qu'il exploite.

Limite

(2) Il ne peut toutefois prendre d'arrêté en vertu du paragraphe (1) à l'égard des télécommunicateurs relativement aux services de télécommunication prévus à la partie 1 de l'annexe 1 ni à l'égard des télécommunicateurs appartenant aux catégories figurant à la partie 2 de cette annexe ou à la partie 2 de l'annexe 2 relativement aux activités qui y sont précisées.

Indemnisation

(3) Le commissaire de la Gendarmerie royale du Canada ou le directeur du Service canadien du renseignement de sécurité, selon le cas, verse au télécommunicateur l'indemnité que le ministre estime suffisante au regard des dépenses qui, à son avis, sont nécessaires et que le télécommunicateur engage initialement pour se conformer à l'arrêté.

Equipment

(4) The Minister may provide the telecommunications service provider with any equipment or other thing that the Minister considers the service provider needs to comply with an order made under this section.

Équipement

(4) Le ministre peut fournir au télécommunicateur l'équipement et les autres biens qu'il estime nécessaires pour lui permettre de se conformer à l'arrêté.

Non-application of sections 8 and 9

(5) Sections 8 and 9 do not apply in respect of any equipment or other thing provided by the Minister under subsection (4). However, the telecommunications service provider must provide notice to the Minister of any problems with the equipment or other thing provided and provide assistance in resolving the problem.

Non-application des articles 8 et 9

(5) Les articles 8 et 9 ne s'appliquent pas à l'équipement et aux autres biens fournis par le ministre. Toutefois, le télécommunicateur est tenu d'aviser le ministre de tout problème que ceux-ci présentent et de prêter son assistance pour le corriger.

Order prevails

(6) An order made by the Minister under subsection (1) prevails over any regulations, to the extent of any inconsistency.

Incompatibilité

(6) L'arrêté pris en vertu du paragraphe (1) l'emporte sur tout règlement incompatible.

Delegation

(7) The Commissioner of the Royal Canadian Mounted Police and the Director of the Canadian Security Intelligence Service may delegate his or her power to pay amounts under subsection (3) to, respectively, a member of a prescribed class of senior officers of the Royal Canadian Mounted Police or a member of a prescribed class of senior officials of the Canadian Security Intelligence Service.

Délégation

(7) Le commissaire de la Gendarmerie royale du Canada peut déléguer son pouvoir de verser l'indemnité visée au paragraphe (3) à tout membre d'une catégorie réglementaire d'officiers supérieurs de son organisme. Le directeur du Service canadien du renseignement de sécurité peut déléguer son propre pouvoir de verser l'indemnité visée au paragraphe (3) à tout membre d'une catégorie réglementaire de cadres supérieurs de son organisme.

Statutory Instruments Act does not apply

15. The *Statutory Instruments Act* does not apply in respect of an order made under section 13 or 14.

Non-application de la *Loi sur les textes réglementaires*

15. La *Loi sur les textes réglementaires* ne s'applique pas aux arrêtés pris en vertu des articles 13 ou 14.

OBLIGATIONS CONCERNING SUBSCRIBER INFORMATION

OBLIGATIONS CONCERNANT LES RENSEIGNEMENTS SUR LES ABONNÉS

Provision of subscriber information

16. (1) On written request by a person designated under subsection (3) that includes prescribed identifying information, every telecommunications service provider must provide the person with identifying information in the service provider's possession or control respecting the name, address, telephone number and electronic mail address of any subscriber to any of the service provider's telecommunications services and the Internet protocol address and local service provider identifier that are associated with the subscriber's service and equipment.

Accès aux renseignements sur les abonnés

16. (1) Sur demande écrite de toute personne désignée en vertu du paragraphe (3) qui contient les renseignements identificateurs prévus par règlement, le télécommunicateur lui fournit les renseignements identificateurs qu'il a en sa possession ou à sa disposition concernant les nom, adresse, numéro de téléphone et adresse de courriel de tout abonné de ses services de télécommunication et l'adresse de protocole Internet et l'identificateur du fournisseur de services locaux associés aux services et à l'équipement de l'abonné.

Purpose of the request

(2) A designated person must ensure that he or she makes a request under subsection (1) only in performing, as the case may be, a duty or function

Objet de la demande

(2) La personne désignée veille à ce que la demande ne soit faite que dans l'exercice d'une fonction, selon le cas :

(*a*) of the Canadian Security Intelligence Service under the *Canadian Security Intelligence Service Act*;

(*b*) of a police service, including any related to the enforcement of any laws of Canada, of a province or of a foreign jurisdiction; or

(*c*) of the Commissioner of Competition under the *Competition Act*.

a) du Service canadien du renseignement de sécurité au titre de la *Loi sur le Service canadien du renseignement de sécurité*;

b) d'un service de police, notamment en ce qui a trait au contrôle d'application du droit canadien, provincial ou étranger;

c) du commissaire de la concurrence au titre de la *Loi sur la concurrence*.

Designated persons

(3) The Commissioner of the Royal Canadian Mounted Police, the Director of the Canadian Security Intelligence Service, the Commissioner of Competition and the chief or head of a police service constituted under the laws of a province may designate for the purposes of this section any employee of his or her agency, or a class of such employees, whose duties are related to protecting national security or to law enforcement.

Personnes désignées

(3) Pour l'application du présent article, le commissaire de la Gendarmerie royale du Canada, le directeur du Service canadien du renseignement de sécurité, le commissaire de la concurrence ou le chef ou directeur d'un service de police constitué sous le régime d'une loi provinciale peut désigner, nommément ou par catégorie, les employés de son organisme dont les fonctions sont liées à la protection de la sécurité nationale ou au contrôle d'application des lois.

Limit on number of designated persons

(4) The number of persons designated under subsection (3) in respect of a particular agency may not exceed the greater of five and the number that is equal to five per cent of the total number of employees of that agency.

Limite du nombre de personnes désignées

(4) Le nombre de personnes désignées par organisme ne peut dépasser cinq ou, s'il est supérieur, le nombre correspondant à cinq pour cent des effectifs.

Delegation

(5) The Commissioner of the Royal Canadian Mounted Police and the Director of the Canadian Security Intelligence Service may delegate his or her power to designate persons under subsection (3) to, respectively, a member of a prescribed class of senior officers of the Royal Canadian Mounted Police or a member of a prescribed class of senior officials of the Canadian Security Intelligence Service.

Délégation

(5) Le commissaire de la Gendarmerie royale du Canada peut déléguer son pouvoir de désignation à tout membre d'une catégorie réglementaire d'officiers supérieurs de son organisme. Le directeur du Service canadien du renseignement de sécurité peut déléguer son propre pouvoir de désignation à tout membre d'une catégorie réglementaire de cadres supérieurs de son organisme.

Exceptional circumstances

17. (1) Any police officer may, orally or in writing, request a telecommunications service provider to provide the officer with the information referred to in subsection 16(1) in the following circumstances:

(*a*) the officer believes on reasonable grounds that the urgency of the situation is such that the request cannot, with reasonable diligence, be made under that subsection;

(*b*) the officer believes on reasonable grounds that the information requested is immediately necessary to prevent an unlawful act that would cause serious harm to any person or to property; and

Circonstances exceptionnelles

17. (1) Tout officier de police peut demander, oralement ou par écrit, au télécommunicateur de lui fournir les renseignements visés au paragraphe 16(1) si, à la fois :

a) il a des motifs raisonnables de croire que l'urgence de la situation est telle qu'une demande ne peut, avec toute la diligence voulue, être faite en vertu de ce paragraphe;

b) il a des motifs raisonnables de croire que les renseignements demandés sont immédiatement nécessaires pour empêcher la perpétration d'un acte illicite qui causerait des blessures corporelles graves ou des dommages importants à un bien;

(*c*) the information directly concerns either the person who would perform the act that is likely to cause the harm or is the victim, or intended victim, of the harm.

The police officer must inform the telecommunications service provider of his or her name, rank, badge number and the agency in which he or she is employed and state that the request is being made in exceptional circumstances and under the authority of this subsection.

Obligation of telecommunications service provider

(2) The telecommunications service provider must provide the information to the police officer as if the request were made by a designated person under subsection 16(1).

Communication

(3) The police officer must, within 24 hours after making a request under subsection (1), communicate to a designated person employed in the same agency as the officer all of the information relating to the request that would be necessary if it had been made under subsection 16(1) and inform that person of the circumstances referred to in paragraphs (1)(*a*) to (*c*).

Notice

(4) On receiving the information, the designated person must in writing inform the telecommunications service provider that the request was made in exceptional circumstances under the authority of subsection (1).

Creation of record by designated person

18. (1) A designated person who makes a request under subsection 16(1), or who receives information under subsection 17(3), must create a record that

(*a*) in the case of a request made under subsection 16(1), identifies the duty or function referred to in subsection 16(2) in the performance of which the request is made, describes the relevance of the information requested to that duty or function and includes any other information that justifies the request and any other prescribed information; and

(*b*) in the case where the designated person receives information under subsection 17(3), includes the information referred to in paragraph (*a*) as well as the circumstances referred to in paragraphs 17(1)(*a*) to (*c*).

c) les renseignements portent directement sur soit la personne dont les actes sont susceptibles de causer les blessures ou les dommages, soit la victime ou la personne menacée.

Il communique au télécommunicateur ses nom, rang et numéro d'insigne ainsi que le nom de son organisme et l'informe que la demande est faite en vertu du présent paragraphe en raison de circonstances exceptionnelles.

Obligation du télécommunicateur

(2) Le télécommunicateur lui fournit les renseignements demandés comme si la demande avait été faite en vertu du paragraphe 16(1) par une personne désignée.

Transmission d'information

(3) Dans les vingt-quatre heures suivant la présentation de sa demande, l'officier de police transmet à toute personne désignée relevant de son organisme l'information concernant la demande qui aurait été nécessaire si celle-ci avait été faite en vertu du paragraphe 16(1) et l'informe des circonstances visées aux alinéas (1)*a*) à *c*).

Avis

(4) Sur réception de l'information, la personne désignée informe par écrit le télécommunicateur du fait que la demande a été faite en vertu du paragraphe (1) en raison de circonstances exceptionnelles.

Création d'un registre — personne désignée

18. (1) La personne désignée qui fait une demande en vertu du paragraphe 16(1) ou qui reçoit de l'information au titre du paragraphe 17(3) est tenue de créer un registre faisant état de ce qui suit :

a) dans le cas où elle a fait la demande, la fonction visée au paragraphe 16(2) dans l'exercice de laquelle elle l'a faite et la pertinence des renseignements demandés au regard de l'exercice de cette fonction, y compris tout autre justificatif et tout autre renseignement prévus par règlement;

b) dans le cas où elle a reçu l'information, les renseignements visés à l'alinéa *a*) et les circonstances visées aux alinéas 17(1)*a*) à *c*).

Retention of records and dealing with information

(2) The agency that employs the designated person must retain records created under subsection (1) and deal with the information provided in response to requests made under subsection 16(1) or 17(1).

(2) L'organisme dont relève la personne désignée est tenu de conserver le registre et de traiter les renseignements obtenus dans le cadre des demandes faites en vertu des paragraphes 16(1) ou 17(1).

Tenue du registre et traitement des renseignements

Use of information

19. Information that is provided in response to a request made under subsection 16(1) or 17(1) must not, without the consent of the individual to whom it relates, be used by the agency in which the designated person or police officer is employed except for the purpose for which the information was obtained or for a use consistent with that purpose.

19. Sauf consentement de l'intéressé, les renseignements obtenus par la personne désignée ou l'officier de police ne peuvent servir à son organisme qu'aux fins auxquelles ils ont été obtenus ou que pour des usages compatibles avec ces fins.

Usage des renseignements recueillis

Internal audit

20. (1) The Commissioner of the Royal Canadian Mounted Police, the Director of the Canadian Security Intelligence Service, the Commissioner of Competition and any chief or head of a police service constituted under the laws of a province who makes a designation under subsection 16(3) must cause internal audits to be regularly conducted of the practices of his or her agency to ensure compliance with sections 16 to 19 and the regulations made for the purposes of those sections and of the internal management and information systems and controls concerning requests made under sections 16 and 17.

20. (1) Le commissaire de la Gendarmerie royale du Canada, le directeur du Service canadien du renseignement de sécurité, le commissaire de la concurrence ou le chef ou directeur d'un service de police constitué sous le régime d'une loi provinciale qui a fait la désignation prévue au paragraphe 16(3) fait procéder régulièrement, d'une part, à des vérifications internes des méthodes et usages de son organisme afin de contrôler l'observation des articles 16 à 19 et de leurs règlements d'application et, d'autre part, à des vérifications internes des moyens de contrôle et des systèmes en matière de gestion et d'information concernant les demandes prévues aux articles 16 et 17.

Vérification interne

Report to responsible minister

(2) The person who causes an internal audit to be conducted must, without delay, report on the findings of the audit to the responsible minister.

(2) La personne qui fait procéder à une vérification interne en transmet les conclusions au ministre compétent sans délai.

Transmission au ministre compétent

Copy of report

(3) A copy of the report on the findings of the audit must be provided by that person

(*a*) if it concerns the Royal Canadian Mounted Police or the Commissioner of Competition, to the Privacy Commissioner appointed under section 53 of the *Privacy Act*;

(*b*) if it concerns the Canadian Security Intelligence Service, to the Security Intelligence Review Committee established by subsection 34(1) of the *Canadian Security Intelligence Service Act*; and

(3) Elle transmet aussi une copie des conclusions de la vérification :

a) si celle-ci vise la Gendarmerie royale du Canada ou le commissaire de la concurrence, au Commissaire à la protection de la vie privée nommé en vertu de l'article 53 de la *Loi sur la protection des renseignements personnels*;

b) si celle-ci vise le Service canadien du renseignement de sécurité, au comité de surveillance des activités de renseignement de sécurité constitué par le paragraphe 34(1) de la *Loi sur le Service canadien du renseignement de sécurité*;

Copie des conclusions

(*c*) if it concerns a police service constituted under the laws of a province, to the public officer for that province whose duties include investigations relating to the protection of privacy.

c) si celle-ci vise un service de police constitué sous le régime d'une loi provinciale, au fonctionnaire de la province dont les fonctions comportent les enquêtes relatives à la protection de la vie privée.

Audit — Privacy Commissioner

(4) The Privacy Commissioner may, on reasonable notice, conduct an audit of the practices of the Royal Canadian Mounted Police or the Commissioner of Competition to ensure compliance with sections 16 to 19 and the regulations made for the purposes of those sections and of the internal management and information systems and controls concerning requests made under sections 16 and 17. The provisions of the *Privacy Act* apply, with any necessary modifications, in respect of the audit as if it were an investigation under that Act.

Vérification : Commissaire à la protection de la vie privée

(4) Le Commissaire à la protection de la vie privée peut, sur préavis suffisant, procéder, d'une part, à des vérifications des méthodes et usages de la Gendarmerie royale du Canada ou du commissaire de la concurrence afin de contrôler l'observation des articles 16 à 19 et de leurs règlements d'application et, d'autre part, à des vérifications des moyens de contrôle et des systèmes en matière de gestion et d'information de l'un ou l'autre concernant les demandes prévues aux articles 16 et 17. La *Loi sur la protection des renseignements personnels* s'applique, avec les adaptations nécessaires, à la vérification comme si elle constituait une enquête en vertu de cette loi.

Audit — Security Intelligence Review Committee

(5) For greater certainty, the functions of the Security Intelligence Review Committee under section 38 of the *Canadian Security Intelligence Service Act* include the power to conduct an audit of the practices of the Canadian Security Intelligence Service to ensure compliance with sections 16, 18 and 19 and the regulations made for the purposes of those sections and of the internal management and information systems and controls concerning requests made under section 16.

Vérification : comité de surveillance des activités de renseignement de sécurité

(5) Il est entendu que les fonctions du comité de surveillance des activités de renseignement de sécurité prévues à l'article 38 de la *Loi sur le Service canadien du renseignement de sécurité* comportent le pouvoir de procéder aux vérifications des méthodes et usages du Service canadien du renseignement de sécurité afin de contrôler l'observation des articles 16, 18 et 19 et de leurs règlements d'application et aux vérifications des moyens de contrôle et des systèmes en matière de gestion et d'information de celui-ci concernant les demandes prévues à l'article 16.

Report concerning provincial audit capability

(6) The Privacy Commissioner must, in the report made to Parliament for each financial year, identify the public officers to whom copies of reports are to be provided under paragraph (3)(*c*) and report on the powers that they have to conduct audits similar to those referred to in subsection (4) with respect to the police services constituted under the laws of their province.

Rapport concernant la vérification faite au niveau provincial

(6) Le Commissaire à la protection de la vie privée fait état, dans le rapport qu'il présente pour chaque exercice au Parlement, des fonctionnaires à qui des conclusions doivent être transmises en application de l'alinéa (3)*c*) et du pouvoir qu'ils possèdent de procéder à des vérifications semblables à celles visées au paragraphe (4) à l'égard des services de police constitués sous le régime des lois de leur province.

Records of service provider

(7) A person conducting an internal audit under this section may require a telecommunications service provider to give the person

Registres des télécommunicateurs

(7) Toute personne procédant à une vérification interne au titre du présent article peut exiger de tout télécommunicateur qu'il lui donne accès à tout registre qu'il possède ou dont il dispose et qui est pertinent.

access to any records in the possession or control of the service provider that are relevant to the audit.

Definition of "responsible minister"

(8) For the purposes of this section, "responsible minister" means

(*a*) in relation to the Commissioner of the Royal Canadian Mounted Police and the Director of the Canadian Security Intelligence Service, the Minister of Public Safety and Emergency Preparedness;

(*b*) in relation to the Commissioner of Competition, the Minister of Industry; and

(*c*) in relation to the chief or head of a police service constituted under the laws of a province, the Attorney General of that province.

Définition de « ministre compétent »

(8) Pour l'application du présent article, « ministre compétent » s'entend :

a) s'agissant du commissaire de la Gendarmerie royale du Canada et du directeur du Service canadien du renseignement de sécurité, du ministre de la Sécurité publique et de la Protection civile;

b) s'agissant du commissaire de la concurrence, du ministre de l'Industrie;

c) s'agissant du chef ou directeur d'un service de police constitué sous le régime d'une loi provinciale, du procureur général de la province.

Entitlement to fee

21. (1) A telecommunications service provider that provides information to a person under section 16 or 17 is entitled to be paid the prescribed fee for providing the information.

Droits

21. (1) Le télécommunicateur qui fournit des renseignements en application des articles 16 ou 17 a le droit de recevoir les droits réglementaires.

Payment of fee by designating authority

(2) If the information is requested by a designated person under section 16, the fee is to be paid by the designating authority.

Paiement des droits — personne désignée

(2) Si la demande est faite par une personne désignée au titre de l'article 16, les droits sont payés par la personne qui l'a désignée.

Payment of fee by police service

(3) If the information is requested by a police officer under section 17, the fee is to be paid by the chief or head of the police service that employs the police officer.

Paiement des droits — officier de police

(3) Si elle est faite par un officier de police au titre de l'article 17, ils sont payés par le chef ou directeur du service de police de qui relève l'officier.

Preservation of existing authority

22. Nothing in this Act derogates from any other authority under law to obtain the information referred to in subsection 16(1) from a telecommunications service provider.

Précision

22. La présente loi n'a pas pour effet de porter atteinte aux pouvoirs de quiconque d'obtenir, en application d'une règle de droit, les renseignements visés au paragraphe 16(1) auprès d'un télécommunicateur.

Deemed nature of information

23. Personal information, as defined in subsection 2(1) of the *Personal Information Protection and Electronic Documents Act*, that is provided under subsection 16(1) or 17(1) is deemed, for the purposes of subsections 9(2.1) to (2.4) of that Act, to be disclosed under subparagraph 7(3)(*c.1*)(i) or (ii), and not under paragraph 7(3)(*i*), of that Act. This section operates despite the other provisions of Part 1 of that Act.

Dérogation

23. Pour l'application des paragraphes 9(2.1) à (2.4) de la *Loi sur la protection des renseignements personnels et les documents électroniques*, les renseignements personnels au sens du paragraphe 2(1) de cette loi qui sont fournis au titre des paragraphes 16(1) ou 17(1) sont réputés être communiqués au titre des sous-alinéas 7(3)*c.1*)(i) ou (ii) de cette loi et non de son alinéa 7(3)*i*). Le présent article s'applique malgré les autres dispositions de la partie 1 de la même loi.

MISCELLANEOUS PROVISIONS

Facility and service information

24. (1) A telecommunications service provider must, on the request of a police officer or of an employee of the Royal Canadian Mounted Police or the Canadian Security Intelligence Service,

(*a*) provide the prescribed information relating to the service provider's telecommunications facilities;

(*b*) indicate what telecommunications services the service provider offers to subscribers; and

(*c*) provide the name, address and telephone number of any telecommunications service providers from whom the service provider obtains or to whom the service provider provides telecommunications services, if the service provider has that information.

Obligation to provide information to authorized persons

(2) A telecommunications service provider must, on the request of an authorized person, provide the prescribed information concerning

(*a*) telecommunications services that are provided by the service provider to a person whose communications are the subject of a court order authorizing their interception; and

(*b*) telecommunications facilities that are used by the service provider in providing those telecommunications services.

Obligation to assist — assessment and testing

25. A telecommunications service provider must, on the request of a police officer or of an employee of the Royal Canadian Mounted Police or the Canadian Security Intelligence Service, provide all reasonable assistance to permit the police officer or employee to assess or to test the service provider's telecommunications facilities that may be used to intercept communications.

Notification of change

26. If the Canadian Security Intelligence Service or a law enforcement agency has provided a telecommunications service provider with any equipment or other thing for intercepting communications, the service provider must, before making any change to the service provider's telecommunications facilities that is likely to impair or reduce the interception capability of the equipment or other thing,

DISPOSITIONS DIVERSES

Renseignements sur les installations et les services

24. (1) Sur demande de tout officier de police ou employé de la Gendarmerie royale du Canada ou du Service canadien du renseignement de sécurité, le télécommunicateur :

a) lui fournit l'information réglementaire se rapportant à ses installations de télécommunication;

b) lui indique la nature des services de télécommunication qu'il offre à ses abonnés;

c) lui fournit les nom, adresse et numéro de téléphone, s'il les connaît, de tout autre télécommunicateur dont il obtient des services de télécommunication ou à qui il en fournit.

Obligation de fournir des renseignements à une personne autorisée

(2) Sur demande de toute personne autorisée, le télécommunicateur lui fournit l'information réglementaire concernant :

a) les services de télécommunication qu'il fournit à la personne dont les communications font l'objet d'une ordonnance judiciaire autorisant leur interception;

b) les installations de télécommunication qu'il utilise pour lui fournir ces services de télécommunication.

Obligation de prêter assistance : évaluation et mise à l'essai

25. Sur demande de tout officier de police ou employé de la Gendarmerie royale du Canada ou du Service canadien du renseignement de sécurité, le télécommunicateur lui prête toute l'assistance possible pour évaluer ou mettre à l'essai celles de ses installations de télécommunication pouvant servir aux interceptions.

Notification

26. Si le Service canadien du renseignement de sécurité ou tout organisme chargé du contrôle d'application des lois lui a fourni tout équipement ou autre bien pouvant servir aux interceptions, le télécommunicateur notifie préalablement au Service ou à l'organisme, selon le cas, toute modification à ses installations qui portera vraisemblablement atteinte à la capacité d'interception de l'équipement ou du bien.

notify the Canadian Security Intelligence Service or law enforcement agency, as the case may be, of the change.

Notification — simultaneous interception capability

27. A telecommunications service provider must notify the Minister when

(*a*) in respect of any particular transmission apparatus, the increased number of simultaneous interceptions that the service provider is required, as a result of a request referred to in subparagraph 7(*d*)(ii), to be capable of enabling is 75% or more of the maximum number that is applicable under that subparagraph; or

(*b*) the number of simultaneous interceptions that the service provider is required, under sections 8 to 11, to be capable of enabling is 75% or more of the global limit that is applicable under section 12.

Notification : interceptions simultanées

27. Le télécommunicateur informe le ministre lorsque :

a) à l'égard d'un appareil de transmission donné, le nombre accru d'interceptions simultanées qu'il doit être en mesure de permettre par suite de la demande visée au sous-alinéa 7*d*)(ii) atteint 75 % du nombre maximal applicable au titre de ce sous-alinéa;

b) le nombre d'interceptions simultanées qu'il doit être en mesure de permettre en application des articles 8 à 11 atteint 75 % de la limite globale applicable au titre de l'article 12.

Persons engaged in interceptions

28. (1) A telecommunications service provider must, on the request of the Royal Canadian Mounted Police or the Canadian Security Intelligence Service, provide a list of the names of the persons who are employed by or carrying out work for the service provider who may assist in the interception of communications.

Liste d'employés pouvant prêter assistance

28. (1) Sur demande de la Gendarmerie royale du Canada ou du Service canadien du renseignement de sécurité, le télécommunicateur lui fournit la liste des noms de ses employés ou contractuels qui peuvent prêter assistance dans le cadre de l'interception d'une communication.

Changes to the list

(2) A telecommunications service provider must provide any changes to the list to the agency who made the request.

Modification à la liste

(2) Il informe l'organisme qui a fait la demande de toute modification à la liste.

Security assessments

(3) The Royal Canadian Mounted Police or the Canadian Security Intelligence Service may conduct an investigation for the purposes of a security assessment of any of those persons who consent to the investigation.

Évaluation de sécurité

(3) La Gendarmerie royale du Canada ou le Service canadien du renseignement de sécurité peut tenir une enquête en vue d'une évaluation de sécurité de ces employés et contractuels s'ils y consentent.

Specialized telecommunications support

29. (1) If the prescribed conditions are met, a telecommunications service provider that provides under this Act prescribed specialized telecommunications support to the Canadian Security Intelligence Service or a law enforcement agency is entitled, on request, to be paid an amount determined in accordance with the regulations for providing that support.

Appui spécialisé en télécommunication

29. (1) Le télécommunicateur qui, au titre de la présente loi, fournit de l'appui spécialisé en télécommunication, prévu par règlement, au Service canadien du renseignement de sécurité ou à tout organisme chargé du contrôle d'application des lois a le droit de recevoir, sur demande, si les conditions réglementaires sont satisfaites, la somme établie conformément aux règlements.

Payment

(2) The amount must be paid by the agency that received the specialized telecommunications support.

Paiement

(2) La somme est payée par l'organisme qui a reçu l'appui spécialisé en télécommunication.

Mandatory reporting — acquisition of transmission apparatus

30. (1) A telecommunications service provider that acquires transmission apparatus referred to in subsection 10(2) must, before using it in providing telecommunications services, submit to the Minister a report in the prescribed form and manner containing the following information:

(*a*) the prescribed information concerning the extent to which the service provider meets operational requirements in respect of the transmission apparatus; and

(*b*) any prescribed information relevant to the administration of this Act.

Other reporting

(2) A telecommunications service provider must, at the request of the Minister, submit a report in the form and manner, and within the period, that the Minister specifies containing the information referred to in paragraphs (1)(*a*) and (*b*) and any additional related information that the Minister specifies.

Statement

(3) Every report submitted under this section must include a written statement certifying that it does not contain any untrue statements or omissions of material facts, that it fairly presents the telecommunications service provider's operations at the time of submission and that the signator has taken steps to ensure the report's accuracy and promises to correct any material error that is detected in the report after its submission and to submit a revised report to the Minister as soon as possible, with another similar written statement accompanying it.

Signator of statement

(4) The statement must be signed

(*a*) if the telecommunications service provider is a corporation, by one of its officers or directors; and

(*b*) in any other case, by an individual who is an owner of the telecommunications service provider or by an officer or a director of a corporation that is an owner of the telecommunications service provider.

No redundant performance required

31. If two or more telecommunications service providers have, in effect, the same obligation under this Act in connection with

Rapport : acquisition d'appareil

30. (1) Le télécommunicateur qui acquiert tout appareil de transmission visé au paragraphe 10(2) présente au ministre, avant de fournir des services de télécommunication au moyen de l'appareil, un rapport établi selon les modalités réglementaires et contenant les renseignements suivants :

a) les renseignements réglementaires indiquant la mesure dans laquelle il satisfait aux exigences opérationnelles liées à l'appareil;

b) tout renseignement réglementaire qui touche à l'application de la présente loi.

Autre rapport

(2) Sur demande du ministre, le télécommunicateur présente, selon les modalités de temps et autres précisées, un rapport contenant les renseignements visés aux alinéas (1)*a*) et *b*) et les renseignements complémentaires précisés.

Attestation

(3) Le rapport présenté en conformité avec le présent article comprend une attestation portant qu'il ne comporte aucun faux renseignement, qu'il comporte tous les renseignements importants et qu'il présente fidèlement la situation du télécommunicateur à la date de sa présentation. Le signataire atteste également qu'il a pris toutes les mesures nécessaires pour s'assurer de l'exactitude du rapport. Si des erreurs importantes sont découvertes dans le rapport après sa présentation, il s'engage à faire parvenir au ministre, dans les meilleurs délais, un rapport corrigé qui comprend une autre attestation.

Signataire

(4) Le signataire de l'attestation est :

a) dans le cas où le télécommunicateur est une personne morale, un de ses dirigeants ou administrateurs;

b) dans les autres cas, soit le particulier qui est propriétaire du télécommunicateur, seul ou avec d'autres, soit un des dirigeants ou administrateurs de la personne morale qui en est propriétaire, seule ou avec d'autres.

Exécution d'une obligation

31. Si plusieurs télécommunicateurs sont tenus d'exécuter la même obligation prévue par la présente loi dans le cadre de l'exploitation

any given transmission apparatus or a given interception and any one of them performs that obligation, it is deemed to be performed by all.

d'un appareil de transmission ou d'une interception, ils sont solidaires de l'exécution de cette obligation par l'un d'eux.

EXEMPTIONS

EXEMPTIONS

Exemption regulation

32. (1) The Governor in Council may, on the recommendation of the Minister and the Minister of Industry, by regulation, exempt any class of telecommunications service providers from all or part of the obligations under any of sections 6, 9 to 11, 16, 17 and 30 or under any regulations made for the purposes of those sections.

32. (1) Sur recommandation du ministre et du ministre de l'Industrie, le gouverneur en conseil peut par règlement exempter, par catégorie, des télécommunicateurs de tout ou partie des obligations prévues aux articles 6, 9 à 11, 16, 17 et 30 et par leurs règlements d'application.

Règlement d'exemption

Considerations

(2) Before making or amending such a regulation, the Governor in Council must consider

(*a*) the extent to which the exemption would adversely affect national security or law enforcement;

(*b*) whether the telecommunications service providers can comply with the obligations from which they would be exempted;

(*c*) whether the costs of compliance with those obligations would have an unreasonable adverse effect on the business of the telecommunications service providers; and

(*d*) whether compliance with those obligations would unreasonably impair the provision of telecommunications services to Canadians or the competitiveness of the Canadian telecommunications industry.

(2) Avant de prendre ou de modifier un tel règlement, le gouverneur en conseil prend en considération :

a) la mesure dans laquelle l'exemption est susceptible de nuire à la sécurité nationale ou au contrôle d'application des lois;

b) le fait que les télécommunicateurs visés ont la capacité ou non d'exécuter les obligations en cause;

c) le fait que les dépenses liées au respect des obligations en cause auraient ou non des effets négatifs injustifiés sur les activités commerciales des télécommunicateurs;

d) le fait que l'exécution des obligations en cause entraverait ou non sérieusement la prestation de services de télécommunication aux Canadiens ou la compétitivité de l'industrie canadienne des télécommunications.

Éléments à prendre en considération

Conditions and term of regulation

(3) In the regulation, the Governor in Council may include any conditions that the Governor in Council considers appropriate and must fix its term for a period of not more than two years.

(3) Il peut assortir l'exemption des conditions qu'il estime indiquées et l'accorde pour une période maximale de deux ans.

Conditions et durée de l'exemption

Exemptions related to section 10 or 11

(4) When a regulation under which a telecommunications service provider is exempted from an obligation under section 10 or 11 expires or is repealed, section 10 or 11, as the case may be, applies to the telecommunications service provider that was exempted as of the date of expiry or repeal as if the exemption had never been made.

(4) À la date d'expiration de l'exemption d'une obligation prévue aux articles 10 ou 11 ou de l'abrogation du règlement, l'article en cause s'applique au télécommunicateur pour l'avenir comme si l'exemption n'avait jamais été accordée.

Exemption de l'application des articles 10 et 11

ADMINISTRATION AND ENFORCEMENT

EXÉCUTION ET CONTRÔLE D'APPLICATION

Designation

33. (1) The Minister may designate persons or classes of persons as inspectors for the purposes of the administration and enforcement of this Act.

33. (1) Le ministre peut désigner toute personne — à titre individuel ou au titre de son appartenance à une catégorie déterminée — comme inspecteur pour l'exécution et le contrôle d'application de la présente loi.

Désignation

Certificate of designation

(2) An inspector is to receive a certificate attesting to their designation and must, on request, present the certificate to any person appearing to be in charge of any place that the inspector enters under subsection 34(1).

(2) L'inspecteur reçoit un certificat attestant sa qualité, qu'il présente, sur demande, à toute personne apparemment responsable du lieu visé au paragraphe 34(1).

Certificat

Authority to enter

34. (1) An inspector may, for a purpose related to verifying compliance with this Act, enter any place owned by, or under the control of, any telecommunications service provider in which the inspector has reasonable grounds to believe there is any document, information, transmission apparatus, telecommunications facility or any other thing to which this Act applies.

34. (1) L'inspecteur peut, à toute fin liée à la vérification du respect de la présente loi, entrer dans tout lieu appartenant à un télécommunicateur — ou placé sous sa responsabilité — s'il a des motifs raisonnables de croire que s'y trouvent des installations de télécommunication, des appareils de transmission, des documents, des renseignements ou des objets visés par la présente loi.

Accès au lieu

Powers on entry

(2) The inspector may, for that purpose,

(*a*) examine any document, information or thing found in the place and open or cause to be opened any container or other thing;

(*b*) examine or test or cause to be tested any telecommunications facility or transmission apparatus or related equipment found in the place;

(*c*) use, or cause to be used, any computer system in the place to search and examine any information contained in or available to the system;

(*d*) reproduce, or cause to be reproduced, any information in the form of a printout, or other intelligible output, and remove the printout, or other output, for examination or copying; or

(*e*) use, or cause to be used, any copying equipment or means of telecommunication at the place.

(2) Il peut, à cette même fin :

a) examiner les documents, les renseignements ou les objets se trouvant dans le lieu et ouvrir, directement ou indirectement, tout contenant ou autre objet;

b) examiner toute installation de télécommunication ou tout appareil de transmission ou matériel connexe s'y trouvant et lui faire subir, directement ou indirectement, des essais;

c) faire usage, directement ou indirectement, de tout système informatique s'y trouvant pour vérifier les données qu'il contient ou auxquelles il donne accès;

d) reproduire ou faire reproduire toute information sous forme d'imprimé ou toute autre forme intelligible qu'il peut emporter pour examen ou reproduction;

e) faire usage, directement ou indirectement, du matériel de reproduction et des moyens de télécommunication se trouvant dans le lieu.

Autres pouvoirs

Duty to assist

(3) The owner or person in charge of the place and every person in the place must give all assistance that is reasonably required to enable the inspector to perform their functions under

(3) Le propriétaire ou le responsable du lieu, ainsi que quiconque s'y trouve, sont tenus de prêter à l'inspecteur toute l'assistance qu'il peut valablement exiger pour lui permettre d'exercer

Assistance

this section and must provide any documents or information, and access to any data, that are reasonably required for that purpose.

ses attributions au titre du présent article, et de lui fournir les documents, les renseignements et l'accès aux données qu'il peut valablement exiger à cette fin.

Inspector may be accompanied

(4) The inspector may be accompanied by any other person that they believe is necessary to help them perform their functions under this section.

(4) L'inspecteur peut être accompagné des personnes qu'il estime nécessaires pour l'aider dans l'exercice de ses attributions au titre du présent article.

Inspecteur accompagné d'un tiers

Warrant for dwelling-house

35. (1) If the place referred to in subsection 34(1) is a dwelling-house, the inspector may enter it without the occupant's consent only under the authority of a warrant issued under subsection (2).

35. (1) Dans le cas d'une maison d'habitation, l'inspecteur ne peut toutefois y entrer sans le consentement de l'occupant que s'il est muni du mandat décerné en vertu du paragraphe (2).

Mandat pour maison d'habitation

Authority to issue warrant

(2) On *ex parte* application, a justice of the peace may issue a warrant authorizing the inspector to enter a dwelling-house, subject to any conditions specified in the warrant, if the justice is satisfied by information on oath that

(*a*) the dwelling-house is a place referred to in subsection 34(1);

(*b*) entry to the dwelling-house is necessary for a purpose related to verifying compliance with this Act; and

(*c*) entry was refused by the occupant or there are reasonable grounds to believe that entry will be refused by, or that consent to entry cannot be obtained from, the occupant.

(2) Sur demande *ex parte*, le juge de paix peut décerner un mandat autorisant, sous réserve des conditions éventuellement fixées, l'inspecteur à entrer dans une maison d'habitation s'il est convaincu, sur la foi d'une dénonciation sous serment, que sont réunies les conditions suivantes :

a) la maison d'habitation est un lieu visé au paragraphe 34(1);

b) l'entrée est nécessaire à toute fin liée à la vérification du respect de la présente loi;

c) soit l'occupant a refusé l'entrée à l'inspecteur, soit il y a des motifs raisonnables de croire que tel sera le cas ou qu'il est impossible d'obtenir le consentement de l'occupant.

Délivrance du mandat

Entry onto private property

36. An inspector and any person accompanying them may enter private property — other than a dwelling-house — and pass through it in order to gain entry to a place referred to in subsection 34(1). For greater certainty, they are not liable for doing so.

36. L'inspecteur et toute personne l'accompagnant peuvent, afin d'accéder au lieu visé au paragraphe 34(1), pénétrer dans une propriété privée — à l'exclusion de toute maison d'habitation — et y circuler. Il est entendu qu'ils ne peuvent encourir de poursuites à cet égard.

Droit de passer sur une propriété privée

Use of force

37. In executing a warrant to enter a dwelling-house, an inspector may use force only if the use of force has been specifically authorized in the warrant and they are accompanied by a peace officer.

37. L'inspecteur ne peut recourir à la force dans l'exécution d'un mandat autorisant l'entrée dans une maison d'habitation que si celui-ci en autorise expressément l'usage et que l'inspecteur est accompagné d'un agent de la paix.

Usage de la force

False statements or information

38. (1) A person must not knowingly make a false or misleading statement or provide false or misleading information, in connection with any matter under this Act, to an inspector who is performing their functions under section 34.

38. (1) Il est interdit à toute personne de faire sciemment une déclaration fausse ou trompeuse ou de communiquer sciemment des renseignements faux ou trompeurs, relativement à toute question visée par la présente loi, à

Renseignements faux ou trompeurs

l'inspecteur qui agit dans l'exercice des attributions qui lui sont conférées au titre de l'article 34.

Obstruction

(2) A person must not obstruct or hinder an inspector who is performing their functions under section 34.

Entrave

(2) Il est interdit à toute personne d'entraver l'action de l'inspecteur qui agit dans l'exercice des attributions qui lui sont conférées au titre de l'article 34.

ADMINISTRATIVE MONETARY PENALTIES

PÉNALITÉS

VIOLATIONS

VIOLATIONS

Violations

39. Every person who contravenes a provision, order, requirement or condition designated under subparagraph 64(1)(*p*)(i) commits a violation and is liable to an administrative monetary penalty not exceeding the prescribed maximum or, if no maximum has been prescribed, to a penalty not exceeding $50,000, in the case of an individual, and $250,000, in any other case.

Violations

39. Toute contravention à un texte désigné en vertu du sous-alinéa 64(1)*p*)(i) constitue une violation passible d'une pénalité ne dépassant pas le maximum réglementaire; à défaut de ce maximum, la pénalité maximale est de 50 000 $, dans le cas des personnes physiques, et de 250 000 $, dans les autres cas.

Designation

40. For the purposes of any of sections 39 and 41 to 53, the Minister may designate persons or classes of persons to exercise powers in relation to any matter referred to in the designation.

Désignation

40. Pour l'application de l'un ou l'autre des articles 39 et 41 à 53, le ministre peut désigner toute personne — individuellement ou au titre de son appartenance à une catégorie — pour exercer des pouvoirs relativement à toute question mentionnée dans la désignation.

NOTICES OF VIOLATION

PROCÈS-VERBAUX

Issuance and service

41. (1) A designated person may issue a notice of violation and cause it to be served on a person if they believe on reasonable grounds that the person has committed a violation.

Procès-verbal

41. (1) La personne désignée qui a des motifs raisonnables de croire qu'une violation a été commise peut dresser un procès-verbal qu'elle fait signifier à l'auteur présumé.

Contents of notice

(2) The Minister may establish the form and content of notices of violation, but each notice of violation must

Contenu

(2) Le ministre peut déterminer la forme et la teneur des procès-verbaux de violation. Tout procès-verbal mentionne :

(*a*) set out the name of the person believed to have committed the violation;

a) le nom de l'auteur présumé de la violation;

(*b*) identify the violation;

b) les faits reprochés;

(*c*) set out the penalty that the person is liable to pay;

c) le montant de la pénalité à payer;

(*d*) inform the person that they may, within 30 days after the day on which the notice is served or within any longer period specified in it, either pay the penalty set out in the notice or make representations with respect to the alleged violation or penalty — including

d) la faculté qu'a l'intéressé soit de payer la pénalité, soit de présenter des observations relativement à la violation ou à la pénalité — y compris en ce qui touche la conclusion d'une transaction —, et ce, dans les trente jours suivant la signification du procès-verbal

any representations about entering into a compliance agreement — and set out the manner for doing so; and

(*e*) inform the person that, if they fail to pay the penalty or make representations in accordance with the notice, they will be considered to have committed the violation and the penalty will be imposed.

ou dans le délai plus long précisé dans celui-ci, ainsi que les modalités d'exercice de cette faculté;

e) le fait que le non-exercice de cette faculté vaut aveu de responsabilité et entraîne l'imposition de la pénalité.

Criteria for penalty

(3) The amount of a penalty is, in each case, to be determined taking into account the following matters:

(*a*) that administrative monetary penalties have as their purpose to encourage compliance rather than to punish;

(*b*) the nature and scope of the violation;

(*c*) the person's history of prior violations or convictions — or compliance agreements entered into — under this Act during the five-year period immediately before the violation;

(*d*) the cumulative amount of the penalties that may be imposed for any violation in respect of which section 48 applies;

(*e*) any prescribed criteria; and

(*f*) any other relevant matter.

Détermination du montant de la pénalité

(3) Pour la détermination du montant de la pénalité, il est tenu compte des éléments suivants :

a) le caractère non punitif de la pénalité, laquelle est destinée à encourager l'observation de la présente loi;

b) la nature et la portée de la violation;

c) les antécédents de l'auteur présumé — violation ou condamnation pour infraction à la présente loi ou conclusion de transactions en application de celle-ci — au cours des cinq ans précédant la violation;

d) la totalité des montants des pénalités qui peuvent être imposées en application de l'article 48;

e) tout critère réglementaire;

f) tout autre élément pertinent.

DETERMINATION OF RESPONSIBILITY AND PENALTY

RESPONSABILITÉ ET PÉNALITÉ

Options

42. (1) A person who is served with a notice of violation must, in accordance with the notice, pay the penalty set out in the notice or make representations with respect to the amount of the penalty or the acts or omissions that constitute the alleged violation.

Option

42. (1) La personne à qui est signifié le procès-verbal est tenue, selon les modalités qui sont prévues dans celui-ci, soit de payer le montant de la pénalité, soit de présenter des observations relativement à celui-ci ou aux actes ou omissions en cause.

Deemed violation

(2) A person is deemed to have committed the violation if they either pay the penalty in accordance with the notice of violation or do not pay the penalty and do not make representations in accordance with the notice of violation.

Responsabilité réputée

(2) Vaut déclaration de responsabilité à l'égard de la violation soit le paiement du montant de la pénalité selon les modalités prévues dans le procès-verbal, soit le défaut de paiement si l'intéressé a omis de présenter des observations selon ces modalités.

Making representations

43. (1) The person alleged to have committed a violation may make representations to a designated person other than the one who issued the notice of violation.

Observations

43. (1) L'auteur présumé de la violation peut présenter des observations à toute personne désignée autre que celle qui a dressé le procès-verbal.

Compliance agreement or decision

(2) The designated person to whom the representations are made must either

(*a*) enter into a compliance agreement with the person on behalf of the Minister; or

(*b*) decide on a balance of probabilities whether the person committed the violation and, if so, impose the penalty set out in the notice of violation, a lesser penalty or no penalty, taking into account the matters mentioned in subsection 41(3).

The designated person must cause notice of any decision made under paragraph (*b*) to be issued and served on the person together with written reasons for the decision and notice of the person's right of appeal under subsection 44(1).

Transaction ou décision

(2) La personne désignée à qui l'auteur présumé de la violation présente des observations :

a) soit conclut avec lui une transaction au nom du ministre;

b) soit détermine, selon la prépondérance des probabilités, sa responsabilité et, le cas échéant, lui impose la pénalité mentionnée au procès-verbal ou une pénalité réduite, ou encore n'impose aucune pénalité, compte tenu des éléments énumérés au paragraphe 41(3).

Elle lui fait signifier avis de la décision motivée prise au titre de l'alinéa *b*) et l'informe par la même occasion de son droit d'interjeter appel au titre du paragraphe 44(1).

Terms of compliance agreements

(3) A compliance agreement

(*a*) may include any terms that the designated person considers appropriate including a requirement that the person alleged to have committed a violation give reasonable security — in a form and an amount that the designated person considers satisfactory — for the person's performance of the agreement; and

(*b*) must provide for payment by the person alleged to have committed a violation to the Receiver General of a specified amount not greater than the penalty set out in the notice of violation if the person does not comply with the agreement.

Conditions de la transaction

(3) La transaction :

a) peut être assortie des conditions que la personne désignée estime indiquées, notamment la fourniture d'une sûreté suffisante — dont le montant et la nature doivent lui agréer — en garantie de l'exécution de la transaction;

b) doit exiger de l'auteur présumé qu'il verse au receveur général une somme ne pouvant dépasser le montant de la pénalité mentionné au procès-verbal s'il ne se conforme pas aux conditions prévues.

Agreement ends proceedings

(4) Entry into a compliance agreement ends the violation proceedings and precludes any further violation or offence proceedings in relation to the act or omission in question.

La transaction met fin à la procédure

(4) La conclusion de la transaction met fin à la procédure et fait obstacle à toute autre procédure en violation ou procédure pénale à l'égard de l'acte ou de l'omission en cause.

If agreement not complied with

(5) The Minister may issue and serve a notice of default on a person who has entered into a compliance agreement but has not complied with it. On service of the notice, the person is liable to pay without delay the amount provided for in the agreement, failing which, the Minister may realize any security for the person's performance of the agreement.

Avis de défaut d'exécution

(5) Le cas échéant, le ministre peut dresser et signifier à l'intéressé un avis du défaut d'exécution de la transaction, la somme prévue par la transaction devenant exigible, à défaut de quoi le ministre peut réaliser la sûreté.

APPEAL TO MINISTER

Right of appeal

44. (1) A person served with notice of a decision made under paragraph 43(2)(*b*) may, within 30 days after the day on which the notice is served or within any longer period that the Minister allows in accordance with the regulations, appeal the decision to the Minister.

Powers of Minister

(2) On an appeal, the Minister may confirm, set aside or vary the decision of the designated person.

APPEL AUPRÈS DU MINISTRE

Droit d'appel

44. (1) Il peut être interjeté appel auprès du ministre de la décision prise au titre de l'alinéa 43(2)*b*), dans les trente jours suivant la signification de l'avis de la décision ou dans le délai supérieur que le ministre peut accorder en conformité avec les règlements.

Pouvoirs du ministre

(2) Le cas échéant, le ministre confirme, annule ou modifie la décision.

RULES ABOUT VIOLATIONS

Vicarious liability — acts of employees, agents and mandataries

45. A person is liable for a violation that is committed by the person's employee acting in the course of his or her employment or the person's agent or mandatary acting within the scope of his or her authority, whether or not the employee, agent or mandatary who actually committed the violation is identified or proceeded against.

Officers of corporations, etc.

46. An officer, director, agent or mandatary of a person other than an individual that commits a violation is a party to the violation if he or she directed, authorized, assented to, acquiesced in or participated in the commission of the violation and is liable to the administrative monetary penalty provided for that violation whether or not the person that committed the violation has been proceeded against under sections 41 to 43. For greater certainty, an officer or director, or any agent or mandatary who is an individual, is liable only to the penalty provided in respect of an individual.

Defence of due diligence

47. A person is not liable for a violation if they establish that they exercised due diligence to prevent the commission of the violation.

Continuing violation

48. A violation that is committed or continued on more than one day constitutes a separate violation for each day on which it is committed or continued.

Limitation period or prescription

49. Any proceedings in respect of a violation may be instituted at any time within, but not later than, two years after the day on which the subject matter of the proceedings arose.

RÈGLES PROPRES AUX VIOLATIONS

Responsabilité indirecte — employés et mandataires

45. L'employeur ou le mandant est responsable de la violation commise par son employé ou son mandataire dans le cadre de son emploi ou du mandat, que celui-ci soit ou non connu ou poursuivi.

Cadres des personnes morales

46. En cas de commission par une personne autre qu'une personne physique d'une violation, ceux de ses dirigeants, administrateurs ou mandataires qui l'ont ordonnée ou autorisée, ou qui y ont consenti ou participé, sont considérés comme des coauteurs de la violation et encourent la pénalité prévue, que la personne ayant commis la violation ait été ou non poursuivie au titre des articles 41 à 43. Il est entendu que les dirigeants et administrateurs, ainsi que les mandataires qui sont des personnes physiques, n'encourent que la pénalité prévue pour une personne physique.

Précautions voulues

47. Nul ne peut être tenu responsable d'une violation s'il prouve qu'il a pris toutes les précautions voulues pour prévenir sa commission.

Violation continue

48. Il est compté une violation distincte pour chacun des jours au cours desquels se commet ou se continue la violation.

Prescription

49. Toute procédure en violation se prescrit par deux ans après le fait reproché.

Violation or offence

50. (1) If it is possible to proceed with any act or omission as a violation and it is also possible to proceed with it as an offence, proceeding in one manner precludes proceeding in the other.

Précision

50. (1) L'acte ou l'omission qualifiable à la fois de violation et d'infraction peut être réprimé soit comme violation, soit comme infraction, la procédure en violation et la poursuite pour infraction s'excluant toutefois mutuellement.

Violation not an offence

(2) For greater certainty, a violation is not an offence.

Précision

(2) Il est entendu que les violations ne sont pas des infractions.

Non-application of section 126 of *Criminal Code*

(3) Section 126 of the *Criminal Code* does not apply in respect of any obligation or prohibition under this Act whose contravention is a violation under this Act.

Non-application — article 126 du *Code criminel*

(3) L'article 126 du *Code criminel* ne s'applique pas aux obligations ou interdictions prévues par la présente loi dont la contravention constitue une violation aux termes de celle-ci.

Admissibility of documents

51. In any proceeding, in the absence of evidence to the contrary, a document that appears to be a notice issued under subsection 41(1) or 43(2) or (5) or a certificate issued under subsection 53(1) is presumed to be authentic and is proof of its contents.

Admissibilité des documents

51. Dans toute instance, le document qui paraît être un procès-verbal dressé en vertu du paragraphe 41(1), un avis signifié en vertu des paragraphes 43(2) ou (5) ou un certificat de non-paiement établi en vertu du paragraphe 53(1) fait foi, sauf preuve contraire, de son authenticité et de son contenu.

RECOVERY OF PENALTIES AND OTHER AMOUNTS

RECOUVREMENT DES PÉNALITÉS ET AUTRES SOMMES

Debts to Her Majesty

52. (1) A penalty imposed under this Act and an amount referred to in subsection 43(5) each constitute a debt due to Her Majesty in right of Canada and may be recovered in the Federal Court or any other court of competent jurisdiction.

Créance de Sa Majesté

52. (1) Les pénalités et toute somme visée au paragraphe 43(5) constituent des créances de Sa Majesté du chef du Canada, dont le recouvrement peut être poursuivi à ce titre devant la Cour fédérale ou tout autre tribunal compétent.

Limitation period or prescription

(2) No proceedings to recover such a debt may be commenced later than five years after the day on which the debt became payable.

Prescription

(2) Le recouvrement de la créance se prescrit par cinq ans après la date à laquelle elle est devenue exigible.

Proceeds payable to Receiver General

(3) Each such debt is payable to the Receiver General.

Receveur général

(3) Les sommes en cause sont versées au receveur général.

Certificate

53. (1) The Minister may issue a certificate certifying the unpaid amount of any debt referred to in subsection 52(1).

Certificat de non-paiement

53. (1) Le ministre peut établir un certificat de non-paiement pour la partie impayée de toute créance visée au paragraphe 52(1).

Registration in Federal Court

(2) Registration in the Federal Court or in any other court of competent jurisdiction of the certificate has the same effect as a judgment of that court for a debt of the amount specified in the certificate and all related registration costs.

Enregistrement en Cour fédérale

(2) L'enregistrement à la Cour fédérale ou à tout autre tribunal compétent confère au certificat valeur de jugement pour la somme visée et les frais afférents.

OFFENCES AND PUNISHMENT

Misleading statements and information

54. A person must not do any of the following things in performing any obligation under this Act or in any application, declaration or report made under it:

(*a*) knowingly make a false or misleading statement or knowingly provide false or misleading information; or

(*b*) knowingly omit to state a material fact or to provide material information.

Offence

55. Every person who wilfully contravenes subsection 6(1) or (2), any of sections 8 to 11, an order made under subsection 14(1) or any regulations made under paragraph 64(1)(*a*) commits an offence and is liable on prosecution by summary conviction

(*a*) in the case of an individual, to a fine not exceeding $100,000; or

(*b*) in any other case, to a fine not exceeding $500,000.

Offence

56. (1) Every person who contravenes subsection 13(6), section 26, 30 or 54 or a condition referred to in subsection 32(3) is guilty of an offence punishable on summary conviction and liable

(*a*) in the case of an individual, to a fine not exceeding $25,000 for a first offence, or $50,000 for a subsequent offence; or

(*b*) in any other case, to a fine not exceeding $100,000 for a first offence, or $250,000 for a subsequent offence.

Obstruction of designated person

(2) Every person who contravenes subsection 34(3) or 38(1) or (2) is guilty of an offence punishable on summary conviction and liable to a fine not exceeding $15,000.

Offence

57. Every person who contravenes any provision of this Act or a regulation made under this Act, except in the case of an offence referred to in sections 55 and 56, is guilty of an offence punishable on summary conviction and liable to a fine not exceeding $250,000.

INFRACTIONS ET PEINES

Fausses déclarations

54. Il est interdit, dans le cadre de l'exécution d'une obligation prévue par la présente loi ou dans une demande, un rapport ou une déclaration faits sous son régime :

a) de faire sciemment une déclaration fausse ou trompeuse ou de fournir sciemment des renseignements faux ou trompeurs;

b) d'omettre sciemment de mentionner un fait important ou de fournir des renseignements importants.

Infraction

55. Quiconque contrevient volontairement aux paragraphes 6(1) ou (2), à l'un ou l'autre des articles 8 à 11, à un arrêté pris en vertu du paragraphe 14(1) ou à tout règlement pris en vertu de l'alinéa 64(1)*a*) commet une infraction passible, sur déclaration de culpabilité par procédure sommaire :

a) dans le cas d'une personne physique, d'une amende maximale de 100 000 $;

b) dans les autres cas, d'une amende maximale de 500 000 $.

Infraction

56. (1) Quiconque contrevient au paragraphe 13(6), aux articles 26, 30 ou 54 ou à toute condition visée au paragraphe 32(3) commet une infraction passible, sur déclaration de culpabilité par procédure sommaire :

a) dans le cas d'une personne physique, d'une amende maximale de 25 000 $ et, en cas de récidive, d'une amende maximale de 50 000 $;

b) dans les autres cas, d'une amende maximale de 100 000 $ et, en cas de récidive, d'une amende maximale de 250 000 $.

Infraction

(2) Quiconque contrevient aux paragraphes 34(3) ou 38(1) ou (2) commet une infraction passible, sur déclaration de culpabilité par procédure sommaire, d'une amende maximale de 15 000 $.

Infraction

57. Quiconque contrevient à toute disposition de la présente loi ou de ses règlements — sauf s'il s'agit d'une infraction prévue aux articles 55 ou 56 — commet une infraction

passible, sur déclaration de culpabilité par procédure sommaire, d'une amende maximale de 250 000 $.

Consent of Attorney General of Canada required

58. A prosecution is not to be commenced in respect of an offence referred to in section 55 or subsection 56(1) without the consent of the Attorney General of Canada.

58. La poursuite des infractions prévues à l'article 55 et au paragraphe 56(1) est subordonnée au consentement du procureur général du Canada.

Consentement du procureur général du Canada

Defence of due diligence

59. A person is not to be convicted of an offence under this Act, other than for a contravention of subsection 38(1) or section 54 or an offence referred to in section 55, if they establish that they exercised due diligence to prevent the commission of the offence.

59. Nul ne peut être déclaré coupable d'une infraction à la présente loi, sauf pour une contravention au paragraphe 38(1) ou à l'article 54 ou dans le cas d'une infraction prévue à l'article 55, s'il prouve qu'il a pris toutes les précautions voulues pour prévenir sa perpétration.

Précautions voulues

Officers of corporations, etc.

60. If a person other than an individual commits an offence under this Act, every officer, director, agent or mandatary of the person who directed, authorized, assented to, acquiesced in or participated in the commission of the offence is a party to and guilty of the offence and liable on conviction to the punishment provided for the offence whether or not the person that committed the offence has been prosecuted or convicted. For greater certainty, an officer or director, or any agent or mandatary who is an individual, is liable only to the punishment provided in respect of an individual.

60. En cas de perpétration par une personne autre qu'une personne physique d'une infraction à la présente loi, ceux de ses dirigeants, administrateurs ou mandataires qui l'ont ordonnée ou autorisée, ou qui y ont consenti ou participé, sont considérés comme des coauteurs de l'infraction et encourent, sur déclaration de culpabilité, la peine prévue, que la personne ayant perpétré l'infraction ait été ou non poursuivie ou déclarée coupable. Il est entendu que les dirigeants et les administrateurs, ainsi que les mandataires qui sont des personnes physiques, n'encourent que la peine prévue pour une personne physique.

Cadres des personnes morales

Continuing offence

61. If an offence under this Act is committed or continued on more than one day, the person who committed the offence is liable to be convicted for a separate offence for each day on which the offence is committed or continued.

61. Il est compté une infraction distincte pour chacun des jours au cours desquels se commet ou se continue l'infraction à la présente loi.

Infraction continue

Limitation period or prescription

62. Proceedings in respect of an offence under this Act may be instituted at any time within, but not later than, two years after the day on which the subject matter of the proceedings arose.

62. La poursuite de toute infraction à la présente loi se prescrit par deux ans après le fait reproché.

Prescription

Injunctions

63. (1) If a court of competent jurisdiction is satisfied that a contravention of subsection 10(1) or section 11 is being or is likely to be committed, the court may, on application by the Minister, grant an injunction, subject to any conditions that it considers appropriate, ordering any person to cease or refrain from operating the transmission apparatus referred to in subsection

63. (1) S'il est convaincu qu'une contravention au paragraphe 10(1) ou à l'article 11 se commet ou est sur le point d'être commise, le tribunal compétent peut, sur demande du ministre, accorder une injonction, assortie des conditions qu'il juge indiquées, interdisant à quiconque, selon le cas, d'exploiter l'appareil de

Injonctions

10(1) or to refrain from acquiring, installing or operating the new software referred to in section 11.

Federal Court

(2) For the purposes of subsection (1), the Federal Court is a court of competent jurisdiction.

transmission visé au paragraphe 10(1) ou d'acquérir, d'installer ou d'exploiter le nouveau logiciel visé à l'article 11.

Cour fédérale

(2) La Cour fédérale est, pour l'application du paragraphe (1), un tribunal compétent.

REGULATIONS

Regulations

64. (1) The Governor in Council may make regulations

(*a*) respecting the obligations to be performed under subsections 6(1) and (2), including specifying the circumstances in which those obligations do not apply or need not be performed;

(*b*) respecting the time, manner and form in which the information referred to in paragraph 6(1)(*b*) is to be provided to an authorized person;

(*c*) respecting the time, manner and form in which an intercepted communication is to be provided to an authorized person;

(*d*) requiring telecommunications service providers to specify the locations where intercepted communications will be provided, respecting the time, manner and form in which the locations are specified and respecting which locations may be so specified;

(*e*) requiring telecommunications service providers to create and keep records with respect to interceptions;

(*f*) respecting the operational requirements referred to in section 7, including matters of time, manner and form in relation to them and the circumstances in which they do not apply or need not be met;

(*g*) for the purposes of paragraph 7(*a*), specifying what is a communication;

(*h*) for the purposes of paragraph 7(*d*)

(i) providing for the minimum number and maximum number of simultaneous interceptions or the manner of determining them,

(ii) prescribing what is to be counted as a single interception,

RÈGLEMENTS

Règlements

64. (1) Le gouverneur en conseil peut prendre des règlements :

a) concernant les obligations prévues aux paragraphes 6(1) et (2), notamment les circonstances où elles ne s'appliquent pas ou celles où il n'est pas nécessaire de les exécuter;

b) concernant les modalités de temps et autres afférentes à la fourniture, à la personne autorisée, de l'information visée à l'alinéa 6(1)*b*);

c) concernant les modalités de temps et autres afférentes à la fourniture, à la personne autorisée, de la communication interceptée;

d) exigeant des télécommunicateurs qu'ils précisent les lieux où les communications interceptées seront fournies et concernant les modalités de temps et autres à cet égard et les lieux qui peuvent être ainsi précisés;

e) exigeant des télécommunicateurs la création et la conservation de registres relativement aux interceptions;

f) concernant les exigences opérationnelles prévues à l'article 7, notamment les modalités de temps et autres afférentes et les circonstances où elles ne s'appliquent pas ou celles où il n'est pas nécessaire d'y satisfaire;

g) en ce qui a trait à l'alinéa 7*a*), précisant ce qui constitue une communication;

h) pour l'application de l'alinéa 7*d*) :

(i) prévoyant le nombre minimal et le nombre maximal d'interceptions simultanées ou la façon de les calculer,

(ii) déterminant ce qui constitue une seule interception,

(iii) respecting the time, manner and form in which a request to increase the number of those interceptions is to be made, the circumstances in which such a request may be made, the time within which the increase is to be made and the duration of the increase, and

(iv) respecting the maximum number of agencies for which a telecommunications service provider is to simultaneously enable interceptions;

(*i*) providing for the global limit referred to in section 12, or the manner of determining it, respecting the circumstances in which it does not apply or need not be met and prescribing what is to be counted as a single interception;

(*j*) for the purposes of subsection 14(3), prescribing expenses and prescribing matters that the Minister is to consider in deciding what amount is reasonable or what prescribed expenses are necessary;

(*k*) for the purposes of subsection 14(5), respecting the provision of notice and assistance;

(*l*) for the purposes of sections 16 and 17, respecting requests made under those sections and the provision of information under those sections, including

(i) respecting the form of that information, the manner of — and time for — providing it and the circumstances under which particular information is to be provided, and

(ii) prescribing any confidentiality or security measures with which the telecommunications service provider must comply;

(*m*) for the purposes of section 18, respecting the creation and retention of records and the dealing with information;

(*n*) for the purposes of section 25, respecting the assistance to be provided in the assessment and testing of telecommunications facilities;

(*o*) for the purposes of section 29, respecting requests for payment and the making of payments;

(iii) concernant les modalités de temps et autres visant toute demande d'augmentation du nombre de telles interceptions, les circonstances dans lesquelles elle est faite, le délai pour procéder à l'augmentation et la période visée,

(iv) concernant le nombre maximal d'organismes pour lesquels le télécommunicateur est tenu de permettre des interceptions simultanées;

i) prévoyant la limite globale visée à l'article 12 ou la façon de la calculer et les circonstances où elle ne s'applique pas ou celles où il n'est pas nécessaire de la respecter et déterminant ce qui constitue une seule interception;

j) pour l'application du paragraphe 14(3), établissant les dépenses et les éléments que le ministre doit prendre en considération pour décider d'une indemnité suffisante ou des dépenses nécessaires;

k) pour l'application du paragraphe 14(5), concernant l'avis à donner et l'assistance à prêter;

l) pour l'application des articles 16 et 17, concernant les demandes et la fourniture des renseignements visés à ces articles, notamment :

(i) concernant les modalités de présentation et de temps visant ces renseignements et les circonstances dans lesquelles certains de ceux-ci sont fournis,

(ii) prévoyant les mesures concernant la confidentialité ou la sécurité que le télécommunicateur doit prendre;

m) pour l'application de l'article 18, concernant la création et la conservation des registres et le traitement des renseignements;

n) pour l'application de l'article 25, concernant l'assistance à prêter pour l'évaluation et la mise à l'essai des installations de télécommunication;

o) pour l'application de l'article 29, concernant les demandes de paiement et le versement de ceux-ci;

(*p*) for carrying out sections 39 to 53, including

(i) designating any provision of this Act or of any regulation, or any order or class of orders made under this Act or any requirement or condition of such a provision or order or class of orders — or class of such requirements or conditions — as a provision, order, requirement or condition whose contravention may be proceeded with as a violation,

(ii) prescribing the maximum administrative monetary penalty for a particular violation, which maximum may not exceed $50,000, in the case of an individual, and $250,000, in any other case,

(iii) respecting compliance agreements referred to in subsection 43(3),

(iv) respecting the service of notices referred to in those sections, including the manner of serving them, the proof of their service and the circumstances under which they are deemed to have been served, and

(v) respecting procedure on appeals, which procedure must provide for a reasonable opportunity for the appellant to present written evidence and make representations in writing;

(*q*) prescribing anything that is to be prescribed under this Act; and

(*r*) generally, for carrying out the purposes and provisions of this Act.

p) prévoyant les mesures d'application des articles 39 à 53, notamment :

(i) désignant comme texte dont la contravention constitue une violation toute disposition de la présente loi ou de ses règlements, tout arrêté pris en vertu de celle-ci, ou toute catégorie de tels arrêtés, ou toute condition ou exigence prévue — ou catégorie de conditions ou d'exigences prévue — par une telle disposition ou un tel arrêté, ou une telle catégorie d'arrêtés,

(ii) prévoyant le montant maximal — plafonné, dans le cas des personnes physiques, à 50 000 $ et, dans les autres cas, à 250 000 $ — de la pénalité applicable à chaque violation,

(iii) concernant les transactions visées au paragraphe 43(3),

(iv) concernant, notamment par l'établissement de présomptions et de règles de preuve, la signification des avis ou des procès-verbaux prévus par ces articles,

(v) concernant la procédure d'appel, qui doit comporter notamment la possibilité pour l'appelant de présenter, par écrit, ses éléments de preuve et ses observations;

q) concernant toute mesure d'ordre réglementaire prévue par la présente loi;

r) d'une façon générale, concernant toute mesure d'application de la présente loi.

Regulations may be limited or vary

(2) Regulations made under subsection (1) may apply generally or to particular classes of telecommunications service providers and may vary by class of telecommunications service provider, by class of telecommunications service provided, by class of telecommunications facility, according to the population of the region in which a telecommunications facility of a given class is located or by the manner in which information is provided.

Catégories

(2) Les règlements peuvent être d'application générale, ou ne viser que telle ou telle catégorie de télécommunicateurs et s'appliquer de manière différente selon la catégorie de télécommunicateurs, la catégorie de services de télécommunication fournis, la catégorie d'installations de télécommunication, la population de la région où est située une installation de télécommunication d'une catégorie donnée ou la façon dont les renseignements sont fournis.

Incorporation by reference

(3) Regulations made under subsection (1) that incorporate documents by reference may incorporate them as amended from time to time.

Incorporation par renvoi

(3) Les règlements qui incorporent des documents par renvoi peuvent les incorporer dans leur version éventuellement modifiée.

COMPENSATION

Consolidated Revenue Fund

65. There is to be paid out of the Consolidated Revenue Fund the sums required to meet the monetary obligations of Her Majesty in right of Canada under subsections 14(3), 21(1) and 29(1).

Compensation

66. If compensation for the provision of information or specialized telecommunications support is to be paid under section 21 or 29, no such compensation is to be paid under any other Act of Parliament.

INDEMNISATION

Paiement sur le Trésor

65. Sont prélevées sur le Trésor les sommes nécessaires pour satisfaire aux obligations pécuniaires de Sa Majesté du chef du Canada aux termes des paragraphes 14(3), 21(1) et 29(1).

Indemnisation

66. Lorsqu'une indemnité peut être payée en vertu des articles 21 ou 29 pour la fourniture de renseignements ou de l'appui spécialisé en télécommunication, aucune indemnité ne peut être payée en vertu d'une autre loi fédérale à ce titre.

REVIEW OF ACT

Review

67. Five years after the day on which this section comes into force, a committee of the House of Commons, of the Senate or of both Houses of Parliament is to be designated or established for the purpose of reviewing this Act.

EXAMEN DE LA LOI

Examen

67. Cinq ans après la date d'entrée en vigueur du présent article, le comité de la Chambre des communes, du Sénat ou des deux chambres désigné ou constitué à cette fin entreprend l'examen de l'application de la présente loi.

TRANSITIONAL PROVISIONS

Delayed application — section 10 of Act

3. (1) The application of section 10 of the *Investigating and Preventing Criminal Electronic Communications Act*, as enacted by section 2, with respect to transmission apparatus that a telecommunications service provider begins to operate in the 18-month period beginning on the day on which that section 10 comes into force is suspended for the duration of that period.

Delayed application — section 11 of Act

(2) The application of section 11 of the *Investigating and Preventing Criminal Electronic Communications Act* with respect to transmission apparatus for which a telecommunications service provider installs new software in the 18-month period beginning on the day on which that section comes into force is suspended for the duration of that period.

Presumption — operational requirements

4. (1) A telecommunications service provider that, together with any affiliated or associated telecommunications service provid-er, has fewer than 100,000 subscribers, without regard to the telecommunications service to which they subscribe, is considered — during the three years after the day on which section 10 or 11 of the *Investigating*

DISPOSITIONS TRANSITOIRES

Suspension de l'application de l'article 10 de la loi

3. (1) L'application de l'article 10 de la *Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention*, édictée par l'article 2, à un appareil de transmission que le télécommunicateur commence à exploiter au cours de la période de dix-huit mois commençant à la date d'entrée en vigueur de cet article 10 est suspendue jusqu'à l'expiration de cette période.

Suspension de l'application de l'article 11 de la loi

(2) L'application de l'article 11 de la *Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention* à un appareil de transmission pour lequel le télécommunicateur installe un nouveau logiciel au cours de la période de dix-huit mois commençant à la date d'entrée en vigueur de cet article est suspendue jusqu'à l'expiration de cette période.

Présomption : exigences opérationnelles

4. (1) Au cours des trois années suivant la date d'entrée en vigueur des articles 10 ou 11 de la *Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention*, édictée par l'article 2, selon le cas, le télécommunicateur qui, avec les télécommunicateurs qui font partie de son groupe ou avec lesquels il a des liens, compte

***and Preventing Criminal Electronic Communications Act*, as enacted by section 2, comes into force, as the case may be — to meet any operational requirement in respect of transmission apparatus that the service provider is obligated to meet by virtue of that section 10 or 11, as the case may be, if the service provider provides a physical connection point for the transmission apparatus permitting an authorized person to effect an interception.**

moins de 100 000 abonnés, tous services de télécommunication confondus, est réputé satisfaire à toute exigence opérationnelle à laquelle il est tenu de satisfaire au titre de l'un ou l'autre de ces articles 10 ou 11, s'il fournit un point de raccordement physique à l'appareil de transmission en cause qui permet à toute personne autorisée de procéder à une interception.

Regulations

(2) For the purposes of subsection (1), the Governor in Council may make regulations defining the expression "affiliated or associated telecommunications service provider" and respecting the provision of a physical connection point.

(2) Pour l'application du paragraphe (1), le gouverneur en conseil peut prendre des règlements définissant l'expression « les télécommunicateurs qui font partie de son groupe ou avec lesquels il a des liens » et concernant la fourniture d'un point de raccordement physique. Règlements

Mandatory reporting — existing service providers

5. Every telecommunications service provider that is providing telecommunications services on the day on which section 30 of the *Investigating and Preventing Criminal Electronic Communications Act*, as enacted by section 2, comes into force must, within six months after that day and in accordance with that section 30, submit a report to the Minister of Public Safety and Emergency Preparedness respecting the telecommunications facilities that it operates on that day.

5. Le télécommunicateur qui fournit des services de télécommunication à la date d'entrée en vigueur de l'article 30 de la *Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention*, édictée par l'article 2, présente au ministre de la Sécurité publique et de la Protection civile, dans les six mois suivant cette date et en conformité avec cet article 30, un rapport concernant les installations de télécommunication qu'il exploite à cette date. Rapport : télécommunicateurs existants

PART 2

AMENDMENTS TO THE CRIMINAL CODE AND OTHER ACTS

PARTIE 2

MODIFICATION DU CODE CRIMINEL ET D'AUTRES LOIS

R.S., c. C-46

CRIMINAL CODE

CODE CRIMINEL

L.R., ch. C-46

2005, c. 32, s. 9(1)

6. (1) The portion of subsection 164.1(1) of the *Criminal Code* before paragraph (*a*) is replaced by the following:

6. (1) Le passage du paragraphe 164.1(1) du *Code criminel* précédant l'alinéa *a*) est remplacé par ce qui suit : 2005, ch. 32, par. 9(1)

Warrant of seizure

164.1 (1) If a judge is satisfied by information on oath that there are reasonable grounds to believe that there is material — namely child pornography within the meaning of section 163.1, a voyeuristic recording within the meaning of subsection 164(8) or computer data within the meaning of subsection 342.1(2) that makes child pornography or a voyeuristic recording available — that is stored on and made available through a computer system

164.1 (1) Le juge peut, s'il est convaincu par une dénonciation sous serment qu'il y a des motifs raisonnables de croire qu'il existe une matière — constituant de la pornographie juvénile au sens de l'article 163.1, un enregistrement voyeuriste au sens du paragraphe 164(8) ou des données informatiques au sens du paragraphe 342.1(2) rendant la pornographie juvénile ou l'enregistrement voyeuriste accessible — qui est emmagasinée et rendue Mandat de saisie

within the meaning of subsection 342.1(2) that is within the jurisdiction of the court, the judge may order the custodian of the computer system to

accessible au moyen d'un ordinateur au sens de ce paragraphe, situé dans le ressort du tribunal, ordonner au gardien de l'ordinateur :

2005, c. 32, s. 9(2)

(2) Subsection 164.1(5) of the Act is replaced by the following:

(2) Le paragraphe 164.1(5) de la même loi est remplacé par ce qui suit :

2005, ch. 32, par. 9(2)

Order

(5) If the court is satisfied, on a balance of probabilities, that the material is child pornography within the meaning of section 163.1, a voyeuristic recording within the meaning of subsection 164(8) or computer data within the meaning of subsection 342.1(2) that makes child pornography or the voyeuristic recording available, it may order the custodian of the computer system to delete the material.

(5) Si le tribunal est convaincu, selon la prépondérance des probabilités, que la matière constitue de la pornographie juvénile au sens de l'article 163.1, un enregistrement voyeuriste au sens du paragraphe 164(8) ou des données informatiques au sens du paragraphe 342.1(2) qui rendent la pornographie juvénile ou l'enregistrement voyeuriste accessible, il peut ordonner au gardien de l'ordinateur de l'effacer.

Ordonnance

2005, c. 32, s. 9(3)

(3) Subsection 164.1(7) of the Act is replaced by the following:

(3) Le paragraphe 164.1(7) de la même loi est remplacé par ce qui suit :

2005, ch. 32, par. 9(3)

Return of material

(7) If the court is not satisfied that the material is child pornography within the meaning of section 163.1, a voyeuristic recording within the meaning of subsection 164(8) or computer data within the meaning of subsection 342.1(2) that makes child pornography or the voyeuristic recording available, the court shall order that the electronic copy be returned to the custodian and terminate the order under paragraph (1)(*b*).

(7) Si le tribunal n'est pas convaincu que la matière constitue de la pornographie juvénile au sens de l'article 163.1, un enregistrement voyeuriste au sens du paragraphe 164(8) ou des données informatiques au sens du paragraphe 342.1(2) qui rendent la pornographie juvénile ou l'enregistrement voyeuriste accessible, il ordonne que la copie électronique soit remise au gardien de l'ordinateur et met fin à l'ordonnance visée à l'alinéa (1)*b*).

Sort de la matière

2004, c. 15, s. 108

7. (1) Subparagraph (*a*)(lviii) of the definition "offence" in section 183 of the Act is replaced by the following:

7. (1) Le sous-alinéa *a*)(lviii) de la définition de « infraction », à l'article 183 de la même loi, est remplacé par ce qui suit :

2004, ch. 15, art. 108

(lviii) section 342.2 (possession of device to obtain unauthorized use of computer system or to commit mischief),

(lviii) l'article 342.2 (possession d'un dispositif permettant l'utilisation non autorisée d'un ordinateur ou la commission d'un méfait),

2004, c. 15, s. 108

(2) Subparagraph (*a*)(lxvii) of the definition "offence" in section 183 of the Act is replaced by the following:

(2) Le sous-alinéa *a*)(lxvii) de la définition de « infraction », à l'article 183 de la même loi, est remplacé par ce qui suit :

2004, ch. 15, art. 108

(lxvii) section 372 (false information),

(lxvii) l'article 372 (faux renseignements),

8. Section 184.2 of the Act is amended by adding the following after subsection (4):

8. L'article 184.2 de la même loi est modifié par adjonction, après le paragraphe (4), de ce qui suit :

Related warrant or order

(5) A judge who gives an authorization under this section may, at the same time, issue a warrant or make an order under any of sections 487, 487.01, 487.014 to 487.018,

(5) Lorsqu'il accorde une autorisation en vertu du présent article, le juge peut simultanément rendre une ordonnance ou délivrer un mandat en vertu de l'un des articles 487,

Ordonnance ou mandat connexe

487.02, 492.1 and 492.2 if the judge is of the opinion that the requested warrant or order relates to the investigation in respect of which the application for the authorization is made.

487.01, 487.014 à 487.018, 487.02, 492.1 et 492.2 s'il est d'avis que l'ordonnance ou le mandat demandé a trait à l'enquête à l'égard de laquelle l'autorisation est demandée.

1993, c. 40, s. 4

9. Section 184.4 of the Act is replaced by the following:

9. L'article 184.4 de la même loi est remplacé par ce qui suit :

1993, ch. 40, art. 4

Interception in exceptional circumstances

184.4 A peace officer may intercept, by means of any electro-magnetic, acoustic, mechanical or other device, a private communication if the peace officer has reasonable grounds to believe that

(*a*) the urgency of the situation is such that an authorization could not, with reasonable diligence, be obtained under any other provision of this Part;

(*b*) the interception is immediately necessary to prevent an offence that would cause serious harm to any person or to property; and

(*c*) either the originator of the private communication or the person intended by the originator to receive it is the person who would commit the offence that is likely to cause the harm or is the victim, or intended victim, of the harm.

Interception dans des circonstances exceptionnelles

184.4 L'agent de la paix peut intercepter, au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, une communication privée s'il a des motifs raisonnables de croire que, à la fois :

a) l'urgence de la situation est telle qu'une autorisation ne peut, avec toute la diligence raisonnable, être obtenue sous le régime de la présente partie;

b) une interception immédiate est nécessaire pour empêcher une infraction qui causerait des dommages sérieux à une personne ou un bien;

c) l'auteur de la communication ou la personne à qui celui-ci la destine est soit la personne dont l'infraction causerait des dommages, soit la victime de ces dommages ou la cible de ceux-ci.

10. Section 186 of the Act is amended by adding the following after subsection (7):

10. L'article 186 de la même loi est modifié par adjonction, après le paragraphe (7), de ce qui suit :

Related warrant or order

(8) A judge who gives an authorization under this section may, at the same time, issue a warrant or make an order under any of sections 487, 487.01, 487.014 to 487.018, 487.02, 492.1 and 492.2 if the judge is of the opinion that the requested warrant or order relates to the investigation in respect of which the application for the authorization is made.

Ordonnance ou mandat connexe

(8) Lorsqu'il accorde une autorisation en vertu du présent article, le juge peut simultanément rendre une ordonnance ou délivrer un mandat en vertu de l'un des articles 487, 487.01, 487.014 à 487.018, 487.02, 492.1 et 492.2 s'il est d'avis que l'ordonnance ou le mandat demandé a trait à l'enquête à l'égard de laquelle l'autorisation est demandée.

11. Section 187 of the Act is amended by adding the following after subsection (7):

11. L'article 187 de la même loi est modifié par adjonction, après le paragraphe (7), de ce qui suit :

Documents to be kept secret — related warrant or order

(8) The rules provided for in this section apply to all documents relating to a request for a related warrant or order referred to in subsection 184.2(5), 186(8) or 188(6) with any necessary modifications.

Façon d'assurer le secret de la demande — ordonnance ou mandat connexe

(8) Les règles prévues au présent article s'appliquent, avec les adaptations nécessaires, à tous les documents relatifs aux demandes d'ordonnances ou de mandats connexes visés aux paragraphes 184.2(5), 186(8) ou 188(6).

12. Section 188 of the Act is amended by adding the following after subsection (5):

Related warrant or order

(6) A judge who gives an authorization under this section may, at the same time, issue a warrant or make an order under section 487, 487.02, 492.1 or 492.2 if the judge is of the opinion that the requested warrant or order relates to the investigation in respect of which the authorization is given.

12. L'article 188 de la même loi est modifié par adjonction, après le paragraphe (5), de ce qui suit :

Ordonnance ou mandat connexe

(6) Lorsqu'il accorde une autorisation en vertu du présent article, le juge peut simultanément rendre une ordonnance ou délivrer un mandat en vertu des articles 487, 487.02, 492.1 ou 492.2 s'il est d'avis que l'ordonnance ou le mandat demandé a trait à l'enquête à l'égard de laquelle l'autorisation est accordée.

2005, c. 10, subpar. 34(1)(*f*)(ix)

13. (1) Subsection 195(1) of the Act is replaced by the following:

2005, ch. 10, sous-al. 34(1)*f*)(ix)

13. (1) Le paragraphe 195(1) de la même loi est remplacé par ce qui suit :

Annual report

195. (1) The Minister of Public Safety and Emergency Preparedness shall, as soon as possible after the end of each year, prepare a report relating to

(*a*) authorizations for which that Minister and agents to be named in the report who were specially designated in writing by that Minister for the purposes of section 185 applied and to the interceptions made under those authorizations in the immediately preceding year;

(*b*) authorizations given under section 188 for which peace officers to be named in the report who were specially designated by that Minister for the purposes of that section applied and to the interceptions made under those authorizations in the immediately preceding year; and

(*c*) interceptions made under section 184.4 in the immediately preceding year if the interceptions relate to an offence for which proceedings may be commenced by the Attorney General of Canada.

Rapport annuel

195. (1) Le ministre de la Sécurité publique et de la Protection civile établit, après la fin de chaque année, aussitôt que possible, un rapport comportant l'information relative :

a) aux autorisations demandées par lui-même et les mandataires, nommés dans le rapport, qu'il a spécialement désignés par écrit pour l'application de l'article 185 et aux interceptions faites en vertu de ces autorisations au cours de l'année précédente;

b) aux autorisations données en vertu de l'article 188 demandées par les agents de la paix, nommés dans le rapport, qu'il a spécialement désignés pour l'application de cet article et aux interceptions faites en vertu de ces autorisations au cours de l'année précédente;

c) aux interceptions faites en vertu de l'article 184.4 au cours de l'année précédente, si elles ont trait à une infraction pour laquelle des poursuites peuvent être intentées par le procureur général du Canada.

(2) The portion of subsection 195(2) of the Act before paragraph (*a*) is replaced by the following:

Information respecting authorizations — sections 185 and 188

(2) The report shall, in relation to the authorizations and interceptions referred to in paragraphs (1)(*a*) and (*b*), set out

(2) Le passage du paragraphe 195(2) de la même loi précédant l'alinéa *a*) est remplacé par ce qui suit :

Renseignements concernant les autorisations — articles 185 et 188

(2) Le rapport indique, en ce qui concerne les autorisations et les interceptions visées aux alinéas (1)*a*) et *b*) :

(3) Section 195 of the Act is amended by adding the following after subsection (2):

(3) L'article 195 de la même loi est modifié par adjonction, après le paragraphe (2), de ce qui suit :

Information respecting interceptions — section 184.4

(2.1) The report shall, in relation to the interceptions referred to in paragraph (1)(*c*), set out

(*a*) the number of interceptions made;

(*b*) the number of parties to each intercepted private communication against whom proceedings were commenced in respect of the offence that the peace officer sought to prevent in intercepting the private communication or in respect of any other offence that was detected as a result of the interception;

(*c*) the number of persons who were not parties to an intercepted private communication but whose commission or alleged commission of an offence became known to a peace officer as a result of the interception of a private communication, and against whom proceedings were commenced in respect of the offence that the peace officer sought to prevent in intercepting the private communication or in respect of any other offence that was detected as a result of the interception;

(*d*) the number of notifications given under section 196.1;

(*e*) the offences in respect of which interceptions were made and any other offences for which proceedings were commenced as a result of an interception, as well as the number of interceptions made with respect to each offence;

(*f*) a general description of the methods of interception used for each interception;

(*g*) the number of persons arrested whose identity became known to a peace officer as a result of an interception;

(*h*) the number of criminal proceedings commenced in which private communications obtained by interception were adduced in evidence and the number of those proceedings that resulted in a conviction;

(*i*) the number of criminal investigations in which information obtained as a result of the interception of a private communication was used even though the private communication

Renseignements concernant les interceptions — article 184.4

(2.1) Le rapport indique aussi, en ce qui concerne les interceptions qui sont visées à l'alinéa (1)*c*) :

a) le nombre d'interceptions qui ont été effectuées;

b) le nombre de personnes qui sont partie à chaque communication privée interceptée et contre lesquelles des poursuites ont été intentées relativement à l'infraction que l'agent de la paix a tenté de prévenir par l'interception de la communication privée ou à toute autre infraction découverte à cette occasion;

c) le nombre de personnes qui ne sont partie à aucune communication privée interceptée — lorsque la perpétration ou prétendue perpétration de l'infraction a été découverte par un agent de la paix par suite de l'interception d'une communication privée — et contre lesquelles des poursuites ont été intentées relativement à l'infraction que l'agent de la paix a tenté de prévenir en interceptant la communication privée et toute autre infraction;

d) le nombre d'avis donnés conformément à l'article 196.1;

e) les infractions visées par des interceptions, celles qui ont donné lieu à des poursuites par suite d'une interception, ainsi que le nombre d'interceptions effectuées pour chacune des infractions;

f) une description sommaire des méthodes d'interception utilisées pour chaque interception;

g) le nombre de personnes arrêtées dont l'identité a été découverte par un agent de la paix par suite d'une interception;

h) le nombre de poursuites pénales intentées dans lesquelles des communications privées interceptées ont été produites en preuve et le nombre de ces poursuites qui ont donné lieu à une condamnation;

i) le nombre d'enquêtes en matière pénale au cours desquelles des renseignements obtenus par suite de l'interception d'une communication privée ont été utilisés, même si la

was not adduced in evidence in criminal proceedings commenced as a result of the investigations; and

(*j*) the duration of each interception and the aggregate duration of all the interceptions related to the investigation of the offence that the peace officer sought to prevent in intercepting the private communication.

(4) The portion of subsection 195(3) of the Act before paragraph (*a*) is replaced by the following:

Other information

(3) The report shall, in addition to the information referred to in subsections (2) and (2.1), set out

(5) Subsection 195(5) of the Act is replaced by the following:

Report by Attorneys General

(5) The Attorney General of each province shall, as soon as possible after the end of each year, prepare and publish or otherwise make available to the public a report relating to

(*a*) authorizations for which the Attorney General and agents specially designated in writing by the Attorney General for the purposes of section 185 applied and to the interceptions made under those authorizations in the immediately preceding year;

(*b*) authorizations given under section 188 for which peace officers specially designated by the Attorney General for the purposes of that section applied and to the interceptions made under those authorizations in the immediately preceding year; and

(*c*) interceptions made under section 184.4 in the immediately preceding year, if the interceptions relate to an offence not referred to in paragraph (1)(*c*).

The report must set out, with any modifications that the circumstances require, the information described in subsections (2) to (3).

14. The Act is amended by adding the following after section 196:

Written notice — interception in exceptional circumstances

196.1 (1) Subject to subsections (3) and (5), the Attorney General of the province in which a peace officer intercepts a private communication under section 184.4 or, if the interception

communication n'a pas été produite en preuve dans des poursuites pénales intentées par suite des enquêtes;

j) la durée de chaque interception et la durée totale des interceptions liées à l'enquête relative à l'infraction que l'agent de la paix a tenté de prévenir en interceptant la communication privée.

(4) Le passage du paragraphe 195(3) de la même loi précédant l'alinéa *a*) est remplacé par ce qui suit :

Autres renseignements

(3) Le rapport contient, outre les renseignements visés aux paragraphes (2) et (2.1) :

(5) Le paragraphe 195(5) de la même loi est remplacé par ce qui suit :

Rapport par les procureurs généraux

(5) Aussitôt que possible après la fin de chaque année, le procureur général de chaque province établit et publie — ou met à la disposition du public de toute autre façon — un rapport comportant l'information relative :

a) aux autorisations demandées par lui-même et les mandataires qu'il a spécialement désignés par écrit pour l'application de l'article 185 et aux interceptions faites en vertu de ces autorisations au cours de l'année précédente;

b) aux autorisations données en vertu de l'article 188 demandées par les agents de la paix qu'il a spécialement désignés pour l'application de cet article et aux interceptions faites en vertu de ces autorisations au cours de l'année précédente;

c) aux interceptions faites en vertu de l'article 184.4 au cours de l'année précédente, dans les cas non visés à l'alinéa (1)*c*).

Le rapport contient les renseignements visés aux paragraphes (2) à (3), compte tenu des adaptations nécessaires.

14. La même loi est modifiée par adjonction, après l'article 196, de ce qui suit :

Avis écrit — interception dans des circonstances exceptionnelles

196.1 (1) Sous réserve des paragraphes (3) et (5), soit le procureur général de la province dans laquelle l'agent de la paix a intercepté une communication privée en vertu de l'article

relates to an offence for which proceedings may be commenced by the Attorney General of Canada, the Minister of Public Safety and Emergency Preparedness shall give notice in writing of the interception to any person who was the object of the interception within 90 days after the day on which it occurred.

Extension of period for notification

(2) The running of the 90-day period or of any extension granted under subsection (3) or (5) is suspended until any application made by the Attorney General of the province or the Minister to a judge of a superior court of criminal jurisdiction or a judge as defined in section 552 for an extension or a subsequent extension of the period has been heard and disposed of.

Where extension to be granted

(3) The judge to whom an application under subsection (2) is made shall grant an extension or a subsequent extension of the 90-day period — each extension not to exceed three years — if the judge is of the opinion that the interests of justice warrant granting the application and is satisfied, on the basis of an affidavit submitted in support of the application, that one of the following investigations is continuing:

(*a*) the investigation of the offence to which the interception relates; or

(*b*) a subsequent investigation of an offence commenced as a result of information obtained from the investigation referred to in paragraph (*a*).

Application to be accompanied by affidavit

(4) An application shall be accompanied by an affidavit deposing to

(*a*) the facts known or believed by the deponent and relied on to justify the belief that an extension should be granted; and

(*b*) the number of instances, if any, on which an application has, to the knowledge or belief of the deponent, been made under subsection (2) in relation to the particular interception and on which the application was withdrawn or the application was not granted, the date on which each application was made and the judge to whom each application was made.

184.4, soit le ministre de la Sécurité publique et de la Protection civile, si l'interception vise une infraction pour laquelle des poursuites peuvent être intentées par le procureur général du Canada, avise par écrit, dans les quatre-vingt-dix jours suivant l'interception, toute personne qui en a fait l'objet.

Prolongation du délai

(2) Le délai initial de quatre-vingt-dix jours ou la période de la prolongation obtenue en vertu des paragraphes (3) ou (5) est interrompu par toute demande de prolongation présentée par le procureur général de la province ou par le ministre à un juge d'une cour supérieure de juridiction criminelle ou à un juge au sens de l'article 552 jusqu'à ce qu'il soit statué sur la demande.

Cas où la prolongation est accordée

(3) Le juge saisi de la demande visée au paragraphe (2), s'il l'estime dans l'intérêt de la justice et s'il est convaincu par l'affidavit appuyant la demande que l'une des enquêtes ci-après continue, accorde une prolongation — initiale ou ultérieure — du délai de quatre-vingt-dix jours, d'une durée maximale de trois ans :

a) l'enquête au sujet de l'infraction visée par l'interception;

b) toute enquête subséquente à l'égard d'une infraction entreprise en raison de renseignements obtenus lors de l'enquête visée à l'alinéa *a*).

Demande accompagnée d'un affidavit

(4) La demande est accompagnée d'un affidavit indiquant ce qui suit :

a) les faits connus du déclarant ou auxquels il croit et sur lesquels il se fonde pour justifier que, à son avis, il y a lieu d'accorder une prolongation;

b) le nombre de cas, s'il y a lieu, où, à la connaissance ou selon la croyance du déclarant, une demande a été faite en vertu du paragraphe (2) au sujet de cette interception et où la demande a été retirée ou refusée, la date de chacune de ces demandes et le juge auquel chacune a été présentée.

Exception — criminal organization or terrorism offence

(5) Despite subsection (3), the judge to whom an application under subsection (2) is made shall grant an extension or a subsequent extension of the 90-day period — each extension not to exceed three years — if the judge is of the opinion that the interests of justice warrant granting the application and is satisfied, on the basis of an affidavit submitted in support of the application, that the interception of the communication relates to an investigation of

(*a*) an offence under section 467.11, 467.12 or 467.13;

(*b*) an offence committed for the benefit of, at the direction of or in association with a criminal organization; or

(*c*) a terrorism offence.

Exception dans le cas d'une organisation criminelle ou d'une infraction de terrorisme

(5) Malgré le paragraphe (3), le juge saisi de la demande visée au paragraphe (2) accorde une prolongation — initiale ou ultérieure — du délai de quatre-vingt-dix jours, d'une durée maximale de trois ans, s'il l'estime dans l'intérêt de la justice et s'il est convaincu par l'affidavit appuyant la demande que l'interception est liée à une enquête visant l'une des infractions suivantes :

a) une infraction prévue aux articles 467.11, 467.12 ou 467.13;

b) une infraction commise au profit ou sous la direction d'une organisation criminelle, ou en association avec elle;

c) une infraction de terrorisme.

2004, c. 14, s. 1

15. Subsection 318(4) of the Act is replaced by the following:

15. Le paragraphe 318(4) de la même loi est remplacé par ce qui suit :

2004, ch. 14, art. 1

Definition of "identifiable group"

(4) In this section, "identifiable group" means any section of the public distinguished by colour, race, religion, national or ethnic origin or sexual orientation.

Définition de « groupe identifiable »

(4) Au présent article, « groupe identifiable » s'entend de toute section du public qui se différencie des autres par la couleur, la race, la religion, l'origine nationale ou ethnique ou l'orientation sexuelle.

16. The definition "identifiable group" in subsection 319(7) of the Act is replaced by the following:

16. La définition de « groupe identifiable », au paragraphe 319(7) de la même loi, est remplacée par ce qui suit :

"identifiable group" « *groupe identifiable* »

"identifiable group" means any section of the public distinguished by colour, race, religion, national or ethnic origin, age, sex, sexual orientation or mental or physical disability;

« groupe identifiable » "*identifiable group*"

« groupe identifiable » Toute section du public qui se différencie des autres par la couleur, la race, la religion, l'origine nationale ou ethnique, l'âge, le sexe, l'orientation sexuelle ou la déficience mentale ou physique.

2001, c. 41, s. 10

17. (1) The portion of subsection 320.1(1) of the Act before paragraph (*a*) is replaced by the following:

17. (1) Le passage du paragraphe 320.1(1) de la même loi précédant l'alinéa *a*) est remplacé par ce qui suit :

2001, ch. 41, art. 10

Warrant of seizure

320.1 (1) If a judge is satisfied by information on oath that there are reasonable grounds to believe that there is material that is hate propaganda within the meaning of subsection 320(8) or computer data within the meaning of subsection 342.1(2) that makes hate propaganda available, that is stored on and made available to the public through a computer system within the meaning of subsection 342.1(2) that is within the jurisdiction of the court, the judge may order the custodian of the computer system to

Mandat de saisie

320.1 (1) Le juge peut, s'il est convaincu par une dénonciation sous serment qu'il y a des motifs raisonnables de croire qu'il existe une matière — qui constitue de la propagande haineuse au sens du paragraphe 320(8) ou contient des données informatiques, au sens du paragraphe 342.1(2), qui rendent la propagande haineuse accessible — qui est emmagasinée et rendue accessible au public au moyen d'un ordinateur au sens du paragraphe 342.1(2) situé dans le ressort du tribunal, ordonner au gardien de l'ordinateur :

2001, c. 41, s. 10

(2) Subsection 320.1(5) of the Act is replaced by the following:

Order

(5) If the court is satisfied, on a balance of probabilities, that the material is available to the public and is hate propaganda within the meaning of subsection 320(8) or computer data within the meaning of subsection 342.1(2) that makes hate propaganda available, it may order the custodian of the computer system to delete the material.

2001, c. 41, s. 10

(3) Subsection 320.1(7) of the Act is replaced by the following:

Return of material

(7) If the court is not satisfied that the material is available to the public and is hate propaganda within the meaning of subsection 320(8) or computer data within the meaning of subsection 342.1(2) that makes hate propaganda available, the court shall order that the electronic copy be returned to the custodian and terminate the order under paragraph (1)(*b*).

18. (1) Paragraph 326(1)(*b*) of the French version of the Act is replaced by the following:

b) soit utilise une installation de télécommunication ou obtient un service de télécommunication.

(2) Subsection 326(2) of the Act is repealed.

19. Section 327 of the Act is replaced by the following:

Possession, etc., of device to obtain use of telecommunication facility or telecommunication service

327. (1) Everyone who, without lawful excuse, makes, possesses, sells, offers for sale, imports, obtains for use, distributes or makes available a device that is designed or adapted primarily to use a telecommunication facility or obtain a telecommunication service without payment of a lawful charge, under circumstances that give rise to a reasonable inference that the device has been used or is or was intended to be used for that purpose, is

(*a*) guilty of an indictable offence and liable to imprisonment for a term of not more than two years; or

(2) Le paragraphe 320.1(5) de la même loi est remplacé par ce qui suit :

2001, ch. 41, art. 10

Ordonnance

(5) Si le tribunal est convaincu, selon la prépondérance des probabilités, que la matière est accessible au public et constitue de la propagande haineuse au sens du paragraphe 320(8) ou contient des données informatiques, au sens du paragraphe 342.1(2), qui rendent la propagande haineuse accessible, il peut ordonner au gardien de l'ordinateur de l'effacer.

(3) Le paragraphe 320.1(7) de la même loi est remplacé par ce qui suit :

2001, ch. 41, art. 10

Sort de la matière

(7) Si le tribunal n'est pas convaincu que la matière est accessible au public et constitue de la propagande haineuse au sens du paragraphe 320(8) ou contient des données informatiques, au sens du paragraphe 342.1(2), qui rendent la propagande haineuse accessible, il ordonne que la copie électronique soit remise au gardien de l'ordinateur et met fin à l'ordonnance visée à l'alinéa (1)*b*).

18. (1) L'alinéa 326(1)*b*) de la version française de la même loi est remplacé par ce qui suit :

b) soit utilise une installation de télécommunication ou obtient un service de télécommunication.

(2) Le paragraphe 326(2) de la même loi est abrogé.

19. L'article 327 de la même loi est remplacé par ce qui suit :

Possession, etc. d'un dispositif pour l'utilisation d'installations de télécommunication ou l'obtention de services de télécommunication

327. (1) Quiconque, sans excuse légitime, produit, a en sa possession, vend ou offre en vente, importe, obtient en vue de l'utiliser, écoule ou rend accessible un dispositif conçu ou adapté principalement pour, sans acquittement des droits exigibles, utiliser une installation de télécommunication ou obtenir un service de télécommunication dans des circonstances qui permettent raisonnablement de conclure que le dispositif a été utilisé à cette fin ou est ou était destiné à l'être, est coupable :

a) soit d'un acte criminel passible d'un emprisonnement maximal de deux ans;

(*b*) guilty of an offence punishable on summary conviction.

b) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire.

Forfeiture

(2) If a person is convicted of an offence under subsection (1) or paragraph 326(1)(*b*), in addition to any punishment that is imposed, any device in relation to which the offence was committed or the possession of which constituted the offence may be ordered forfeited to Her Majesty and may be disposed of as the Attorney General directs.

Confiscation

(2) Lorsqu'une personne est déclarée coupable d'une infraction prévue au paragraphe (1) ou à l'alinéa 326(1)*b*), tout dispositif au moyen duquel l'infraction a été commise ou dont la possession a constitué l'infraction peut, en plus de toute peine qui est imposée, être, par ordonnance, confisqué au profit de Sa Majesté, après quoi il peut en être disposé conformément aux instructions du procureur général.

Limitation

(3) No order for forfeiture is to be made in respect of telecommunication facilities or equipment by means of which an offence under subsection (1) is committed if they are owned by a person engaged in providing a telecommunication service to the public or form part of such a person's telecommunication service or system and that person is not a party to the offence.

Restriction

(3) Aucune ordonnance de confiscation ne peut être rendue relativement à des installations ou du matériel de télécommunication qui sont la propriété d'une personne fournissant au public un service de télécommunication, ou qui font partie du service ou réseau de télécommunication d'une telle personne, et au moyen desquels une infraction prévue au paragraphe (1) a été commise, si cette personne n'était pas partie à l'infraction.

Definition of "device"

(4) In this section, "device" includes

(*a*) a component of a device; and

(*b*) a computer program within the meaning of subsection 342.1(2).

Définition de « dispositif »

(4) Au présent article, « dispositif » s'entend notamment :

a) de ses pièces;

b) d'un programme d'ordinateur au sens du paragraphe 342.1(2).

R.S., c. 27 (1st Supp.), s. 45; 1997, c. 18, s. 18(1)

20. (1) Subsection 342.1(1) of the Act is replaced by the following:

L.R., ch. 27 (1er suppl.), art. 45; 1997, ch. 18, par. 18(1)

20. (1) Le paragraphe 342.1(1) de la même loi est remplacé par ce qui suit :

Unauthorized use of computer

342.1 (1) Everyone is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years, or is guilty of an offence punishable on summary conviction who, fraudulently and without colour of right,

(*a*) obtains, directly or indirectly, any computer service;

(*b*) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system;

(*c*) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (*a*) or (*b*) or under section 430 in relation to computer data or a computer system; or

Utilisation non autorisée d'ordinateur

342.1 (1) Est coupable d'un acte criminel et passible d'un emprisonnement maximal de dix ans ou d'une infraction punissable sur déclaration de culpabilité par procédure sommaire, quiconque, frauduleusement et sans apparence de droit :

a) directement ou indirectement, obtient des services d'ordinateur;

b) au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, directement ou indirectement, intercepte ou fait intercepter toute fonction d'un ordinateur;

(*d*) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (*a*), (*b*) or (*c*).

c) directement ou indirectement, utilise ou fait utiliser un ordinateur dans l'intention de commettre une infraction prévue aux alinéas *a*) ou *b*) ou à l'article 430 concernant des données informatiques ou un ordinateur;

d) a en sa possession ou utilise un mot de passe d'ordinateur qui permettrait la perpétration des infractions prévues aux alinéas *a*), *b*) ou *c*), ou en fait le trafic ou permet à une autre personne de l'utiliser.

R.S., c. 27 (1st Supp.), s. 45

(2) The definition "data" in subsection 342.1(2) of the Act is repealed.

(2) La définition de « données », au paragraphe 342.1(2) de la même loi, est abrogée.

L.R., ch. 27 (1er suppl.), art. 45

R.S., c. 27 (1st Supp.), s. 45; 1997, c. 18, s. 18(2)

(3) The definitions "computer password", "computer program", "computer service" and "computer system" in subsection 342.1(2) of the Act are replaced by the following:

(3) Les définitions de « mot de passe », « ordinateur », « programme d'ordinateur » et « service d'ordinateur », au paragraphe 342.1(2) de la même loi, sont respectivement remplacées par ce qui suit :

L.R., ch. 27 (1er suppl.), art. 45; 1997, ch. 18, par. 18(2)

"computer password" « *mot de passe* »

"computer password" means any computer data by which a computer service or computer system is capable of being obtained or used;

« mot de passe » Données informatiques permettant d'utiliser un ordinateur ou d'obtenir des services d'ordinateur.

« mot de passe » "*computer password*"

"computer program" « *programme d'ordinateur* »

"computer program" means computer data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

« ordinateur » Dispositif ou ensemble de dispositifs connectés ou reliés les uns aux autres, dont l'un ou plusieurs d'entre eux :

« ordinateur » "*computer system*"

"computer service" « *service d'ordinateur* »

"computer service" includes data processing and the storage or retrieval of computer data;

a) contiennent des programmes d'ordinateur ou d'autres données informatiques;

b) conformément à des programmes d'ordinateur :

(i) exécutent des fonctions logiques et de commande,

(ii) peuvent exécuter toute autre fonction.

"computer system" « *ordinateur* »

"computer system" means a device that, or a group of interconnected or related devices one or more of which,

(*a*) contains computer programs or other computer data, and

(*b*) by means of computer programs,

(i) performs logic and control, and

(ii) may perform any other function;

« programme d'ordinateur » Ensemble de données informatiques qui représentent des instructions ou des relevés et qui, lorsque traités par l'ordinateur, lui font exécuter une fonction.

« programme d'ordinateur » "*computer program*"

« service d'ordinateur » S'entend notamment du traitement des données de même que de la mémorisation et du recouvrement ou du relevé des données informatiques.

« service d'ordinateur » "*computer service*"

(4) Subsection 342.1(2) of the Act is amended by adding the following in alphabetical order:

(4) Le paragraphe 342.1(2) de la même loi est modifié par adjonction, selon l'ordre alphabétique, de ce qui suit :

"computer data" «*données informatiques*»

"computer data" means representations, including signs, signals or symbols, that are in a form suitable for processing in a computer system;

« données informatiques » Représentations, notamment signes, signaux ou symboles, qui sont sous une forme qui en permet le traitement par un ordinateur.

« données informatiques » "*computer data*"

1997, c. 18, s. 19

21. (1) Subsections 342.2(1) and (2) of the Act are replaced by the following:

21. (1) Les paragraphes 342.2(1) et (2) de la même loi sont remplacés par ce qui suit :

1997, ch. 18, art. 19

Possession of device to obtain unauthorized use of computer system or to commit mischief

342.2 (1) Everyone who, without lawful excuse, makes, possesses, sells, offers for sale, imports, obtains for use, distributes or makes available a device that is designed or adapted primarily to commit an offence under section 342.1 or 430, under circumstances that give rise to a reasonable inference that the device has been used or is or was intended to be used to commit such an offence, is

(*a*) guilty of an indictable offence and liable to imprisonment for a term of not more than two years; or

(*b*) guilty of an offence punishable on summary conviction.

342.2 (1) Quiconque, sans excuse légitime, produit, a en sa possession, vend ou offre en vente, importe, obtient en vue de l'utiliser, écoule ou rend accessible un dispositif conçu ou adapté principalement pour commettre une infraction prévue aux articles 342.1 ou 430, dans des circonstances qui permettent raisonnablement de conclure que le dispositif a été utilisé pour commettre une telle infraction ou est ou était destiné à cette fin, est coupable :

a) soit d'un acte criminel et passible d'un emprisonnement maximal de deux ans;

b) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire.

Possession d'un dispositif permettant l'utilisation non autorisée d'un ordinateur ou la commission d'un méfait

Forfeiture

(2) If a person is convicted of an offence under subsection (1), in addition to any punishment that is imposed, any device in relation to which the offence was committed or the possession of which constituted the offence may be ordered forfeited to Her Majesty and may be disposed of as the Attorney General directs.

(2) Lorsqu'une personne est déclarée coupable d'une infraction prévue au paragraphe (1), tout dispositif au moyen duquel l'infraction a été commise ou dont la possession a constitué l'infraction peut, en plus de toute peine applicable en l'espèce, être, par ordonnance, confisqué au profit de Sa Majesté, après quoi il peut en être disposé conformément aux instructions du procureur général.

Confiscation

(2) Section 342.2 of the Act is amended by adding the following after subsection (3):

(2) L'article 342.2 de la même loi est modifié par adjonction, après le paragraphe (3), de ce qui suit :

Definition of "device"

(4) In this section, "device" includes

(*a*) a component of a device; and

(*b*) a computer program within the meaning of subsection 342.1(2).

(4) Au présent article, « dispositif » s'entend notamment :

a) de ses pièces;

b) d'un programme d'ordinateur au sens du paragraphe 342.1(2).

Définition de « dispositif »

22. Sections 371 and 372 of the Act are replaced by the following:

22. Les articles 371 et 372 de la même loi sont remplacés par ce qui suit :

Message in false name

371. Everyone who, with intent to defraud, causes a message to be sent as if it were sent under the authority of another person, knowing that it is not sent under that authority and with intent that it should be acted on as if it were, is

371. Est coupable d'un acte criminel et passible d'un emprisonnement maximal de cinq ans quiconque, avec l'intention de frauder, fait en sorte qu'un message soit expédié comme si l'envoi en était autorisé par une autre personne,

Messages sous un faux nom

guilty of an indictable offence and liable to imprisonment for a term of not more than five years.

False information

372. (1) Everyone commits an offence who, with intent to injure or alarm a person, conveys information that they know is false, or causes such information to be conveyed by letter or any means of telecommunication.

Indecent communications

(2) Everyone commits an offence who, with intent to alarm or annoy a person, makes an indecent communication to that person or to any other person by a means of telecommunication.

Harassing communications

(3) Everyone commits an offence who, without lawful excuse and with intent to harass a person, repeatedly communicates, or causes repeated communications to be made, with them by a means of telecommunication.

Punishment

(4) Everyone who commits an offence under this section is

(*a*) guilty of an indictable offence and liable to imprisonment for a term of not more than two years; or

(*b*) guilty of an offence punishable on summary conviction.

R.S., c. 27 (1st Supp.), s. 57(1)

23. (1) Subsection 430(1.1) of the Act is replaced by the following:

Mischief in relation to computer data

(1.1) Everyone commits mischief who wilfully

(*a*) destroys or alters computer data;

(*b*) renders computer data meaningless, useless or ineffective;

(*c*) obstructs, interrupts or interferes with the lawful use of computer data; or

(*d*) obstructs, interrupts or interferes with a person in the lawful use of computer data or denies access to computer data to a person who is entitled to access to it.

R.S., c. 27 (1st Supp.), s. 57(2)

(2) The portion of subsection 430(5) of the Act before paragraph (*a*) is replaced by the following:

en sachant que ce n'est pas le cas, et dans le dessein qu'il soit donné suite au message comme s'il était ainsi expédié.

Faux renseignements

372. (1) Commet une infraction quiconque, avec l'intention de nuire à quelqu'un ou de l'alarmer, transmet ou fait en sorte que soient transmis par lettre ou tout moyen de télécommunication des renseignements qu'il sait être faux.

Communications indécentes

(2) Commet une infraction quiconque, avec l'intention d'alarmer ou d'ennuyer quelqu'un lui fait ou fait à toute autre personne une communication indécente par un moyen de télécommunication.

Communications harcelantes

(3) Commet une infraction quiconque, sans excuse légitime et avec l'intention de harceler quelqu'un, communique avec lui de façon répétée ou fait en sorte que des communications répétées lui soient faites, par un moyen de télécommunication.

Peine

(4) Quiconque commet une infraction prévue au présent article est coupable :

a) soit d'un acte criminel passible d'un emprisonnement maximal de deux ans;

b) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire.

L.R., ch. 27 (1er suppl.), par. 57(1)

23. (1) Le paragraphe 430(1.1) de la même loi est remplacé par ce qui suit :

Méfait à l'égard de données informatiques

(1.1) Commet un méfait quiconque volontairement, selon le cas :

a) détruit ou modifie des données informatiques;

b) dépouille des données informatiques de leur sens, les rend inutiles ou inopérantes;

c) empêche, interrompt ou gêne l'emploi légitime des données informatiques;

d) empêche, interrompt ou gêne une personne dans l'emploi légitime des données informatiques ou refuse l'accès aux données informatiques à une personne qui y a droit.

L.R., ch. 27 (1er suppl.), par. 57(2)

(2) Le passage du paragraphe 430(5) de la même loi précédant l'alinéa *a*) est remplacé par ce qui suit :

Mischief in relation to computer data

(5) Everyone who commits mischief in relation to computer data

(5) Quiconque commet un méfait à l'égard de données informatiques est coupable :

Méfait à l'égard de données informatiques

R.S., c. 27 (1st Supp.), s. 57(2)

(3) The portion of subsection 430(5.1) of the Act before paragraph (*a*) is replaced by the following:

(3) Le passage du paragraphe 430(5.1) de la même loi précédant l'alinéa *a*) est remplacé par ce qui suit :

L.R., ch. 27 (1er suppl.), par. 57(2)

Offence

(5.1) Everyone who wilfully does an act or wilfully omits to do an act that it is their duty to do, if that act or omission is likely to constitute mischief causing actual danger to life, or to constitute mischief in relation to property or computer data,

(5.1) Quiconque volontairement accomplit un acte ou volontairement omet d'accomplir un acte qu'il a le devoir d'accomplir, si cet acte ou cette omission est susceptible de constituer un méfait qui cause un danger réel pour la vie des gens ou de constituer un méfait à l'égard de biens ou de données informatiques est coupable :

Infraction

R.S., c. 27 (1st Supp.), s. 57(3)

(4) Subsection 430(8) of the Act is replaced by the following:

(4) Le paragraphe 430(8) de la même loi est remplacé par ce qui suit :

L.R., ch. 27 (1er suppl.), par. 57(3)

Definition of "computer data"

(8) In this section, "computer data" has the same meaning as in subsection 342.1(2).

(8) Au présent article, « données informatiques » s'entend au sens du paragraphe 342.1(2).

Définition de « données informatiques »

1997, c. 18, s. 43; 2004, c. 3, s. 7

24. Sections 487.011 to 487.02 of the Act are replaced by the following:

24. Les articles 487.011 à 487.02 de la même loi sont remplacés par ce qui suit :

1997, ch. 18, art. 43; 2004, ch. 3, art. 7

Definitions

487.011 The following definitions apply in this section and in sections 487.012 to 487.0199.

487.011 *Les définitions qui suivent* s'appliquent au présent article et aux articles 487.012 à 487.0199.

Définitions

"computer data" « *données informatiques* »

"computer data" has the same meaning as in subsection 342.1(2).

« document » Tout support sur lequel sont enregistrées ou inscrites des données.

« document » "*document*"

"data" « *données* »

"data" means representations, including signs, signals or symbols, that are capable of being understood by an individual or processed by a computer system or other device.

« données » Représentations, notamment signes, signaux ou symboles, qui peuvent être compris par une personne physique ou traités par un ordinateur ou un autre dispositif.

« données » "*data*"

"document" « *document* »

"document" means a medium on which data is registered or marked.

« données de localisation » Données qui concernent le lieu d'une opération ou d'une chose ou le lieu où est située une personne physique.

« données de localisation » "*tracking data*"

"judge" « *juge* »

"judge" means a judge of a superior court of criminal jurisdiction or a judge of the Court of Quebec.

« données de transmission » Données qui, à la fois :

« données de transmission » "*transmission data*"

"public officer" « *fonctionnaire public* »

"public officer" means a public officer who is appointed or designated to administer or enforce a federal or provincial law and whose duties include the enforcement of this Act or any other Act of Parliament.

a) concernent les fonctions de composition, de routage, d'adressage ou de signalisation en matière de télécommunication;

b) soit sont transmises pour identifier, activer ou configurer un dispositif, notamment un programme d'ordinateur au sens du paragraphe 342.1(2), en vue d'établir ou de maintenir l'accès à un service de

"tracking data" "tracking data" means data that relates to the location of a transaction, individual or thing.

"transmission data" "transmission data" means data that

(*a*) relates to the telecommunication functions of dialling, routing, addressing or signalling;

(*b*) is transmitted to identify, activate or configure a device, including a computer program as defined in subsection 342.1(2), in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and

(*c*) does not reveal the substance, meaning or purpose of the communication.

Preservation demand

487.012 (1) A peace officer or public officer may make a demand to a person in Form 5.001 requiring them to preserve computer data that is in their possession or control when the demand is made.

Conditions for making demand

(2) The peace officer or public officer may make the demand only if they have reasonable grounds to suspect that

(*a*) an offence has been or will be committed under this or any other Act of Parliament or has been committed under a law of a foreign state;

(*b*) in the case of an offence committed under a law of a foreign state, an investigation is being conducted by a person or authority with responsibility in that state for the investigation of such offences; and

(*c*) the computer data is in the person's possession or control and will assist in the investigation of the offence.

Limitation

(3) A demand may not be made to a person who is under investigation for the offence referred to in paragraph (2)(*a*).

télécommunication afin de rendre possible une communication, soit sont produites durant la création, la transmission ou la réception d'une communication et indiquent, ou sont censées indiquer, le type, la direction, la date, l'heure, la durée, le volume, le point d'envoi, la destination ou le point d'arrivée de la communication;

c) ne révèlent pas la substance, le sens ou l'objet de la communication.

« données informatiques » S'entend au sens du paragraphe 342.1(2). « données informatiques » "*computer data*"

« fonctionnaire public » Fonctionnaire public nommé ou désigné pour l'exécution ou le contrôle d'application d'une loi fédérale ou provinciale et chargé notamment de faire observer la présente loi ou toute autre loi fédérale. « fonctionnaire public » "*public officer*"

« juge » Juge de la cour supérieure de juridiction criminelle ou juge de la Cour du Québec. « juge » "*judge*"

Ordre de préservation

487.012 (1) L'agent de la paix ou le fonctionnaire public peut, selon la formule 5.001, ordonner à toute personne de préserver des données informatiques qui sont en sa possession ou à sa disposition au moment où l'ordre lui est donné.

Conditions préalables à l'ordre

(2) Il ne donne l'ordre que s'il a des motifs raisonnables de soupçonner, à la fois :

a) qu'une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise ou qu'une infraction à la loi d'un État étranger a été commise;

b) dans le cas d'une infraction à la loi d'un État étranger, qu'une enquête relative à l'infraction est menée par une personne ou un organisme chargé dans cet État des enquêtes relatives à de telles infractions;

c) que les données informatiques sont en la possession de la personne ou à sa disposition et seront utiles à l'enquête.

Limite

(3) L'ordre ne peut être donné à une personne faisant l'objet d'une enquête relative à l'infraction visée à l'alinéa (2)*a*).

Expiry and revocation of demand

(4) A peace officer or public officer may revoke the demand by notice given to the person at any time. Unless the demand is revoked earlier, the demand expires

(*a*) in the case of an offence that has been or will be committed under this or any other Act of Parliament, 21 days after the day on which it is made; and

(*b*) in the case of an offence committed under a law of a foreign state, 90 days after the day on which it is made.

Conditions in demand

(5) The peace officer or public officer who makes the demand may impose any conditions in the demand that they consider appropriate — including conditions prohibiting the disclosure of its existence or some or all of its contents — and may revoke a condition at any time by notice given to the person.

No further demand

(6) A peace officer or public officer may not make another demand requiring the person to preserve the same computer data in connection with the investigation.

Preservation order — computer data

487.013 (1) On *ex parte* application made by a peace officer or public officer, a justice or judge may order a person to preserve computer data that is in their possession or control when they receive the order.

Conditions for making order

(2) Before making the order, the justice or judge must be satisfied by information on oath in Form 5.002

(*a*) that there are reasonable grounds to suspect that an offence has been or will be committed under this or any other Act of Parliament or has been committed under a law of a foreign state, that the computer data is in the person's possession or control and that it will assist in the investigation of the offence; and

(*b*) that a peace officer or public officer intends to apply or has applied for a warrant or an order in connection with the investigation to obtain a document that contains the computer data.

Expiration et annulation de l'ordre

(4) Un agent de la paix ou un fonctionnaire public peut annuler l'ordre à tout moment, par avis remis à l'intéressé. À moins que l'ordre n'ait été annulé auparavant, il expire :

a) dans le cas où une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise, vingt et un jours après qu'il a été donné;

b) dans le cas d'une infraction à la loi d'un État étranger, quatre-vingt-dix jours après qu'il a été donné.

Conditions

(5) L'agent de la paix ou le fonctionnaire public qui donne l'ordre peut l'assortir des conditions qu'il estime indiquées, notamment pour interdire la divulgation de son existence ou de tout ou partie de son contenu. Il peut, par avis, annuler toute condition à tout moment.

Ordre unique

(6) Un agent de la paix ou un fonctionnaire public ne peut donner l'ordre à la même personne à l'égard des mêmes données informatiques qu'une seule fois dans le cadre de l'enquête.

Ordonnance de préservation : données informatiques

487.013 (1) Le juge de paix ou le juge peut, sur demande *ex parte* présentée par un agent de la paix ou un fonctionnaire public, ordonner à toute personne de préserver des données informatiques qui sont en sa possession ou à sa disposition au moment où elle reçoit l'ordonnance.

Conditions préalables à l'ordonnance

(2) Il ne rend l'ordonnance que s'il est convaincu, par une dénonciation sous serment faite selon la formule 5.002, que les conditions suivantes sont réunies :

a) il existe des motifs raisonnables de soupçonner qu'une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise ou qu'une infraction à la loi d'un État étranger a été commise et que les données informatiques sont en la possession de la personne ou à sa disposition et seront utiles à l'enquête relative à l'infraction;

b) un agent de la paix ou un fonctionnaire public a l'intention de demander ou a demandé la délivrance d'un mandat ou d'une

ordonnance en vue d'obtenir un document comportant les données informatiques relativement à cette enquête.

Offence against law of foreign state

(3) If an offence has been committed under a law of a foreign state, the justice or judge must also be satisfied that a person or authority with responsibility in that state for the investigation of such offences is conducting the investigation.

(3) Dans le cas d'une infraction à la loi d'un État étranger, il doit aussi être convaincu qu'une personne ou un organisme chargé dans cet État des enquêtes relatives à de telles infractions mène l'enquête.

Infraction à la loi d'un État étranger

Form

(4) The order is to be in Form 5.003.

(4) L'ordonnance est rendue selon la formule 5.003.

Formule

Limitation

(5) A person who is under investigation for an offence referred to in paragraph (2)(*a*) may not be made subject to an order.

(5) La personne faisant l'objet d'une enquête relative à l'infraction visée à l'alinéa (2)*a*) ne peut être assujettie à l'ordonnance.

Limite

Expiry of order

(6) Unless the order is revoked earlier, it expires 90 days after the day on which it is made.

(6) L'ordonnance expire quatre-vingt-dix jours après qu'elle ait été rendue, à moins qu'elle n'ait été révoquée auparavant.

Expiration de l'ordonnance

General production order

487.014 (1) Subject to sections 487.015 to 487.018, on *ex parte* application made by a peace officer or public officer, a justice or judge may order a person to produce a document that is a copy of a document that is in their possession or control when they receive the order, or to prepare and produce a document containing data that is in their possession or control at that time.

487.014 (1) Sous réserve des articles 487.015 à 487.018, le juge de paix ou le juge peut, sur demande *ex parte* présentée par un agent de la paix ou un fonctionnaire public, ordonner à toute personne de communiquer un document qui est la copie d'un document qui est en sa possession ou à sa disposition au moment où elle reçoit l'ordonnance ou d'établir et de communiquer un document comportant des données qui sont en sa possession ou à sa disposition à ce moment.

Ordonnance générale de communication

Conditions for making order

(2) Before making the order, the justice or judge must be satisfied by information on oath in Form 5.004 that there are reasonable grounds to believe that

(2) Il ne rend l'ordonnance que s'il est convaincu, par une dénonciation sous serment faite selon la formule 5.004, qu'il existe des motifs raisonnables de croire, à la fois :

Conditions préalables à l'ordonnance

(*a*) an offence has been or will be committed under this or any other Act of Parliament; and

a) qu'une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise;

(*b*) the document or data is in the person's possession or control and will afford evidence respecting the commission of the offence.

b) que le document ou les données sont en la possession de la personne ou à sa disposition et fourniront une preuve concernant la perpétration de l'infraction.

Form

(3) The order is to be in Form 5.005.

(3) L'ordonnance est rendue selon la formule 5.005.

Formule

Limitation

(4) A person who is under investigation for the offence referred to in subsection (2) may not be made subject to an order.

(4) La personne faisant l'objet d'une enquête relative à l'infraction visée au paragraphe (2) ne peut être assujettie à l'ordonnance.

Limite

Production order to trace specified communication

487.015 (1) On *ex parte* application made by a peace officer or public officer for the purpose of identifying a device or person involved in the transmission of a communication, a justice or judge may order a person to prepare and produce a document containing transmission data that is related to that purpose and that is, when they are served with the order, in their possession or control.

Conditions for making order

(2) Before making the order, the justice or judge must be satisfied by information on oath in Form 5.004 that there are reasonable grounds to suspect that

(*a*) an offence has been or will be committed under this or any other Act of Parliament;

(*b*) the identification of a device or person involved in the transmission of a communication will assist in the investigation of the offence; and

(*c*) transmission data that is in the possession or control of one or more persons whose identity is unknown when the application is made will enable that identification.

Form

(3) The order is to be in Form 5.006.

Service

(4) A peace officer or public officer may serve the order on any person who was involved in the transmission of the communication and whose identity was unknown when the application was made

(*a*) within 60 days after the day on which the order is made; or

(*b*) within one year after the day on which the order is made, in the case of an offence under section 467.11, 467.12 or 467.13, an offence committed for the benefit of, at the direction of or in association with a criminal organization, or a terrorism offence.

Limitation

(5) A person who is under investigation for the offence referred to in subsection (2) may not be made subject to an order.

Ordonnance de communication en vue de retracer une communication donnée

487.015 (1) Le juge de paix ou le juge peut, sur demande *ex parte* présentée par un agent de la paix ou un fonctionnaire public afin d'identifier tout dispositif ayant servi à la transmission de la communication ou toute personne y ayant participé, ordonner à toute personne d'établir et de communiquer un document comportant des données de transmission qui ont trait à l'identification et qui, au moment où l'ordonnance lui est signifiée, sont en sa possession ou à sa disposition.

Conditions préalables à l'ordonnance

(2) Il ne rend l'ordonnance que s'il est convaincu, par une dénonciation sous serment faite selon la formule 5.004, qu'il existe des motifs raisonnables de soupçonner, à la fois :

a) qu'une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise;

b) que l'identification de tout dispositif ayant servi à la transmission d'une communication ou de toute personne y ayant participé sera utile à l'enquête relative à l'infraction;

c) que les données de transmission en la possession ou à la disposition d'une ou de plusieurs personnes — dont l'identité n'est pas connue au moment de la présentation de la demande — permettront cette identification.

Formule

(3) L'ordonnance est rendue selon la formule 5.006.

Signification

(4) Un agent de la paix ou un fonctionnaire public peut signifier l'ordonnance à toute personne ayant participé à la transmission de la communication et dont l'identité n'était pas connue au moment de la présentation de la demande :

a) dans les soixante jours suivant la date à laquelle l'ordonnance est rendue;

b) dans l'année suivant la date à laquelle elle est rendue, s'il s'agit d'une infraction prévue à l'un des articles 467.11, 467.12 ou 467.13, d'une infraction commise au profit d'une organisation criminelle, ou en association avec elle, ou d'une infraction de terrorisme.

Limite

(5) La personne faisant l'objet d'une enquête relative à l'infraction visée au paragraphe (2) ne peut être assujettie à l'ordonnance.

Report

(6) A peace officer or public officer named in the order must provide a written report to the justice or judge who made the order as soon as feasible after the person from whom the communication originated is identified or after the expiry of the period referred to in subsection (4), whichever occurs first. The report must state the name and address of each person on whom the order was served, and the date of service.

(6) L'agent de la paix ou le fonctionnaire public nommé dans l'ordonnance transmet au juge de paix ou au juge qui l'a rendue, dans les meilleurs délais après l'identification de l'auteur de la communication ou l'expiration de la période mentionnée au paragraphe (4), selon la première de ces éventualités à se présenter, un rapport écrit indiquant les nom et adresse des personnes à qui l'ordonnance a été signifiée ainsi que la date de signification. Rapport

Production order — transmission data

487.016 (1) On *ex parte* application made by a peace officer or public officer, a justice or judge may order a person to prepare and produce a document containing transmission data that is in their possession or control when they receive the order.

487.016 (1) Le juge de paix ou le juge peut, sur demande *ex parte* présentée par un agent de la paix ou un fonctionnaire public, ordonner à toute personne d'établir et de communiquer un document comportant des données de transmission qui sont en sa possession ou à sa disposition au moment où elle reçoit l'ordonnance. Ordonnance de communication : données de transmission

Conditions for making order

(2) Before making the order, the justice or judge must be satisfied by information on oath in Form 5.004 that there are reasonable grounds to suspect that

(2) Il ne rend l'ordonnance que s'il est convaincu, par une dénonciation sous serment faite selon la formule 5.004, qu'il existe des motifs raisonnables de soupçonner, à la fois : Conditions préalables à l'ordonnance

(*a*) an offence has been or will be committed under this or any other Act of Parliament; and

a) qu'une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise;

(*b*) the transmission data is in the person's possession or control and will assist in the investigation of the offence.

b) que les données de transmission sont en la possession de la personne ou à sa disposition et seront utiles à l'enquête relative à l'infraction.

Form

(3) The order is to be in Form 5.007.

(3) L'ordonnance est rendue selon la formule 5.007. Formule

Limitation

(4) A person who is under investigation for the offence referred to in subsection (2) may not be made subject to an order.

(4) La personne faisant l'objet d'une enquête relative à l'infraction visée au paragraphe (2) ne peut être assujettie à l'ordonnance. Limite

Production order — tracking data

487.017 (1) On *ex parte* application made by a peace officer or public officer, a justice or judge may order a person to prepare and produce a document containing tracking data that is in their possession or control when they receive the order.

487.017 (1) Le juge de paix ou le juge peut, sur demande *ex parte* présentée par un agent de la paix ou un fonctionnaire public, ordonner à toute personne d'établir et de communiquer un document comportant des données de localisation qui sont en sa possession ou à sa disposition au moment où elle reçoit l'ordonnance. Ordonnance de communication : données de localisation

Conditions for making order

(2) Before making the order, the justice or judge must be satisfied by information on oath in Form 5.004 that there are reasonable grounds to suspect that

(2) Il ne rend l'ordonnance que s'il est convaincu, par une dénonciation sous serment faite selon la formule 5.004, qu'il existe des motifs raisonnables de soupçonner, à la fois : Conditions préalables à l'ordonnance

(*a*) an offence has been or will be committed under this or any other Act of Parliament; and

(*b*) the tracking data is in the person's possession or control and will assist in the investigation of the offence.

a) qu'une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise;

b) que les données de localisation sont en la possession de la personne ou à sa disposition et seront utiles à l'enquête relative à l'infraction.

Form

(3) The order is to be in Form 5.007.

Formule

(3) L'ordonnance est rendue selon la formule 5.007.

Limitation

(4) A person who is under investigation for the offence referred to in subsection (2) may not be made subject to an order.

Limite

(4) La personne faisant l'objet d'une enquête relative à l'infraction visée au paragraphe (2) ne peut être assujettie à l'ordonnance.

Production order — financial data

487.018 (1) On *ex parte* application made by a peace officer or public officer, a justice or judge may order a financial institution, as defined in section 2 of the *Bank Act*, or a person or entity referred to in section 5 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, to prepare and produce a document setting out the following data that is in their possession or control when they receive the order:

(*a*) either the account number of a person named in the order or the name of a person whose account number is specified in the order;

(*b*) the type of account;

(*c*) the status of the account; and

(*d*) the date on which it was opened or closed.

Ordonnance de communication : données financières

487.018 (1) Le juge de paix ou le juge peut, sur demande *ex parte* présentée par un agent de la paix ou un fonctionnaire public, ordonner à toute institution financière au sens de l'article 2 de la *Loi sur les banques* ou à toute personne ou entité visée à l'article 5 de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* d'établir et de communiquer un document énonçant les données ci-après qui sont en sa possession ou à sa disposition au moment où elle reçoit l'ordonnance :

a) le numéro de compte de la personne nommée dans l'ordonnance ou le nom de celle dont le numéro de compte y est mentionné;

b) la catégorie du compte;

c) son état;

d) la date à laquelle il a été ouvert ou fermé.

Identification of person

(2) For the purpose of confirming the identity of a person who is named or whose account number is specified in the order, the order may also require the institution, person or entity to prepare and produce a document setting out the following data that is in their possession or control:

(*a*) the date of birth of a person who is named or whose account number is specified in the order;

(*b*) that person's current address; and

(*c*) any previous addresses of that person.

Identification d'une personne

(2) Afin que l'identité de la personne qui y est nommée ou de celle dont le numéro de compte y est mentionné puisse être confirmée, l'ordonnance peut aussi exiger que l'institution financière, la personne ou l'entité établisse et communique un document énonçant les données ci-après qui sont en sa possession ou à sa disposition :

a) la date de naissance de la personne qui y est nommée ou dont le numéro de compte y est mentionné;

b) son adresse actuelle;

c) toutes ses adresses antérieures.

Conditions for making order

(3) Before making the order, the justice or judge must be satisfied by information on oath in Form 5.004 that there are reasonable grounds to suspect that

(*a*) an offence has been or will be committed under this or any other Act of Parliament; and

(*b*) the data is in the possession or control of the institution, person or entity and will assist in the investigation of the offence.

Form

(4) The order is to be in Form 5.008.

Limitation

(5) A financial institution, person or entity that is under investigation for the offence referred to in subsection (3) may not be made subject to an order.

Conditions in preservation and production orders

487.019 (1) An order made under any of sections 487.013 to 487.018 may contain any conditions that the justice or judge considers appropriate including, in the case of an order made under section 487.014, conditions to protect a privileged communication between a person who is qualified to give legal advice and their client.

Effect of order

(2) The order has effect throughout Canada and, for greater certainty, no endorsement is needed for the order to be effective in a territorial division that is not the one in which the order is made.

Power to revoke or vary order

(3) On *ex parte* application made by a peace officer or public officer, the justice or judge who made the order — or a judge in the judicial district where the order was made — may, on the basis of an information on oath in Form 5.0081, revoke or vary the order. The peace officer or public officer must give notice of the revocation or variation to the person who is subject to the order as soon as feasible.

Order prohibiting disclosure

487.0191 (1) On *ex parte* application made by a peace officer or public officer, a justice or judge may make an order prohibiting a person from disclosing the existence or some or all of the contents of a preservation demand made under section 487.012 or a preservation or

Conditions préalables à l'ordonnance

(3) Le juge de paix ou le juge ne rend l'ordonnance que s'il est convaincu, par une dénonciation sous serment faite selon la formule 5.004, qu'il existe des motifs raisonnables de soupçonner, à la fois :

a) qu'une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise;

b) que les données sont en la possession de l'institution financière, de la personne ou de l'entité ou à sa disposition et seront utiles à l'enquête relative à l'infraction.

Formule

(4) L'ordonnance est rendue selon la formule 5.008.

Limite

(5) L'institution financière, la personne ou l'entité faisant l'objet d'une enquête relative à l'infraction visée au paragraphe (3) ne peut être assujettie à l'ordonnance.

Conditions des ordonnances de préservation ou de communication

487.019 (1) L'ordonnance rendue en vertu de l'un des articles 487.013 à 487.018 peut être assortie des conditions que le juge de paix ou le juge estime indiquées, notamment, dans le cas d'une ordonnance rendue en vertu de l'article 487.014, pour protéger les communications privilégiées entre la personne habilitée à donner des avis juridiques et son client.

Effet de l'ordonnance

(2) L'ordonnance a effet partout au Canada. Il est entendu qu'il n'est pas nécessaire que l'ordonnance soit visée dans une autre circonscription territoriale pour y avoir effet.

Pouvoir de révoquer ou de modifier

(3) Sur demande *ex parte* présentée par un agent de la paix ou un fonctionnaire public, le juge de paix ou le juge qui a rendu l'ordonnance — ou tout autre juge du district judiciaire où l'ordonnance a été rendue — peut, sur la foi d'une dénonciation sous serment faite selon la formule 5.0081, la révoquer ou la modifier. L'agent de la paix ou le fonctionnaire public avise, dans les meilleurs délais, la personne assujettie à l'ordonnance de la révocation de celle-ci ou de sa modification.

Ordonnance de non-divulgation

487.0191 (1) Le juge de paix ou le juge peut, sur demande *ex parte* présentée par un agent de la paix ou un fonctionnaire public, rendre une ordonnance interdisant à toute personne de divulguer l'existence ou tout ou partie du contenu d'un ordre de préservation

production order made under any of sections 487.013 to 487.018 during the period set out in the order.

donné en vertu de l'article 487.012, d'une ordonnance de préservation rendue en vertu de l'article 487.013 ou d'une ordonnance de communication rendue en vertu de l'un des articles 487.014 à 487.018, pendant la période indiquée dans l'ordonnance.

Conditions for making order

(2) Before making the order, the justice or judge must be satisfied by information on oath in Form 5.009 that there are reasonable grounds to believe that the disclosure during that period would jeopardize the conduct of the investigation of the offence to which the preservation demand or the preservation or production order relates.

(2) Il ne rend l'ordonnance que s'il est convaincu, par une dénonciation sous serment faite selon la formule 5.009, qu'il existe des motifs raisonnables de croire que la divulgation, pendant la période visée, compromettrait le déroulement de l'enquête relative à l'infraction visée dans l'ordre de préservation ou l'ordonnance de préservation ou de communication.

Conditions préalables à l'ordonnance

Form

(3) The order is to be in Form 5.0091.

(3) L'ordonnance est rendue selon la formule 5.0091.

Formule

Application to revoke or vary order

(4) A peace officer or a public officer or a person, financial institution or entity that is subject to an order made under subsection (1) may apply in writing to the justice or judge who made the order — or to a judge in the judicial district where the order was made — to revoke or vary the order.

(4) L'agent de la paix ou le fonctionnaire public ou la personne, l'institution financière ou l'entité assujettie à l'ordonnance rendue en vertu du paragraphe (1) peut, sur demande écrite présentée au juge de paix ou au juge qui l'a rendue — ou tout autre juge du district judiciaire où elle a été rendue — en demander la révocation ou la modification.

Demande de révocation ou de modification

Particulars — production orders

487.0192 (1) An order made under any of sections 487.014 and 487.016 to 487.018 must require a person, financial institution or entity to produce the document to a peace officer or public officer named in the order within the time, at the place and in the form specified in the order.

487.0192 (1) L'ordonnance rendue en vertu de l'un des articles 487.014 et 487.016 à 487.018 précise à la personne, à l'institution financière ou à l'entité, le lieu et la forme de la communication du document, le délai dans lequel elle doit être faite ainsi que le nom de l'agent de la paix ou du fonctionnaire public à qui elle doit l'être.

Précisions concernant des ordonnances de communication

Particulars — production order to trace specified communication

(2) An order made under section 487.015 must require a person to produce the document to a peace officer or public officer named in the order as soon as feasible after they are served with the order at the place and in the form specified in the order.

(2) L'ordonnance rendue en vertu de l'article 487.015 précise à la personne que la communication du document doit être faite dans les meilleurs délais après que l'ordonnance lui est signifiée, le lieu et la forme de cette communication ainsi que le nom de l'agent de la paix ou du fonctionnaire public à qui elle doit être faite.

Précisions concernant l'ordonnance de communication en vue de retracer une communication donnée

Form of production

(3) For greater certainty, an order under any of sections 487.014 to 487.018 may specify that a document may be produced on or through an electro-magnetic medium.

(3) Il est entendu qu'une ordonnance rendue en vertu de l'un des articles 487.014 à 487.018 peut préciser que le document peut être communiqué sur un support électromagnétique ou par l'entremise d'un tel support.

Forme de la communication

Non-application

(4) For greater certainty, sections 489.1 and 490 do not apply to a document that is produced under an order under any of sections 487.014 to 487.018.

Non-application

(4) Il est entendu que les articles 489.1 et 490 ne s'appliquent pas au document communiqué au titre d'une ordonnance rendue en vertu de l'un des articles 487.014 à 487.018.

Probative force of copies

(5) Every copy of a document produced under section 487.014 is admissible in evidence in proceedings under this or any other Act of Parliament on proof by affidavit that it is a true copy and has the same probative force as the document would have if it were proved in the ordinary way.

Valeur probante des copies

(5) Toute copie communiquée en application de l'article 487.014 est, à la condition d'être certifiée conforme à l'original par affidavit, admissible en preuve dans toute procédure sous le régime de la présente loi ou de toute autre loi fédérale et a la même valeur probante que l'original aurait eue s'il avait été déposé en preuve de la façon normale.

Canada Evidence Act

(6) A document that is prepared for the purpose of production is considered to be original for the purposes of the *Canada Evidence Act*.

Loi sur la preuve au Canada

(6) Le document établi aux fins de communication est considéré comme un original pour l'application de la *Loi sur la preuve au Canada*.

Application for review of production order

487.0193 (1) Before they are required by an order made under any of sections 487.014 to 487.018 to produce a document, a person, financial institution or entity may apply in writing to the justice or judge who made the order — or to a judge in the judicial district where the order was made — to revoke or vary the order.

Demande de révision de l'ordonnance de communication

487.0193 (1) La personne, l'institution financière ou l'entité, avant qu'elle soit tenue de communiquer un document au titre d'une ordonnance rendue en vertu de l'un des articles 487.014 à 487.018, peut demander par écrit au juge de paix ou au juge qui l'a rendue — ou à tout autre juge du district judiciaire où elle a été rendue — de la révoquer ou de la modifier.

Notice required

(2) The person, institution or entity may make the application within 30 days after the day on which the order is made and only if they give notice of their intention to do so to a peace officer or public officer named in the order within 15 days after that day.

Préavis obligatoire

(2) Elle peut présenter la demande dans les trente jours suivant la date à laquelle l'ordonnance a été rendue, à la condition d'avoir donné un préavis de son intention à l'agent de la paix ou au fonctionnaire public nommé dans celle-ci dans les quinze jours suivant cette date.

No obligation to produce

(3) The person, institution or entity is not required to prepare or produce the document until a final decision is made with respect to the application.

Aucune obligation d'établir ou de communiquer un document

(3) Elle n'a pas à établir ou communiquer le document tant qu'il n'a pas été statué en dernier ressort sur sa demande.

Revocation or variation of order

(4) The justice or judge may revoke or vary the order if satisfied that

(*a*) it is unreasonable in the circumstances to require the applicant to prepare or produce the document; or

(*b*) production of the document would disclose information that is privileged or otherwise protected from disclosure by law.

Révocation ou modification de l'ordonnance

(4) Le juge de paix ou le juge peut révoquer l'ordonnance ou la modifier s'il est convaincu, selon le cas :

a) qu'il est déraisonnable, dans les circonstances, d'obliger l'intéressé à établir ou communiquer le document;

b) que la communication révélerait des renseignements protégés par le droit applicable en matière de divulgation ou de privilèges.

Destruction of preserved computer data and documents — preservation demand

487.0194 (1) A person to whom a preservation demand is made under section 487.012 shall destroy the computer data that would not be retained in the ordinary course of business and any document that is prepared for the purpose of preserving computer data under that section as soon as feasible after the demand expires or is revoked, unless they are subject to an order made under any of sections 487.013 to 487.017 with respect to the computer data.

Destruction des données informatiques préservées et de documents : ordre de préservation

487.0194 (1) La personne à qui est donné un ordre de préservation en vertu de l'article 487.012 est tenue de détruire les données informatiques qui ne seraient pas conservées dans le cadre normal de son activité commerciale et tout document établi en vue de les préserver en application de cet article dans les meilleurs délais après l'expiration de l'ordre ou son annulation, à moins qu'elle ne soit assujettie à une ordonnance rendue en vertu de l'un des articles 487.013 à 487.017 à l'égard de ces données informatiques.

Destruction of preserved computer data and documents — preservation order

(2) A person who is subject to a preservation order made under section 487.013 shall destroy the computer data that would not be retained in the ordinary course of business and any document that is prepared for the purpose of preserving computer data under that section as soon as feasible after the order expires or is revoked, unless they are subject to a production order made under any of sections 487.014 to 487.017 with respect to the computer data.

Destruction des données informatiques préservées et de documents : ordonnance de préservation

(2) La personne assujettie à une ordonnance de préservation rendue en vertu de l'article 487.013 est tenue de détruire les données informatiques qui ne seraient pas conservées dans le cadre normal de son activité commerciale et tout document établi en vue de les préserver en application de cet article dans les meilleurs délais après l'expiration de l'ordonnance ou sa révocation, à moins qu'elle ne soit assujettie à une ordonnance de communication rendue en vertu de l'un des articles 487.014 à 487.017 à l'égard de ces données informatiques.

Destruction of preserved computer data and documents — production order

(3) A person who is subject to a production order made under any of sections 487.014 to 487.017 with respect to computer data that they preserved under a preservation demand or order made under section 487.012 or 487.013 shall destroy the computer data that would not be retained in the ordinary course of business and any document that is prepared for the purpose of preserving computer data under that section as soon as feasible after the earlier of

(*a*) the day on which the production order is revoked, and

(*b*) the day on which a document that contains the computer data is produced under the production order.

Destruction des données informatiques préservées et de documents : ordonnance de communication

(3) La personne assujettie à une ordonnance de communication rendue en vertu de l'un des articles 487.014 à 487.017 à l'égard de données informatiques qu'elle a préservées en application d'un ordre ou d'une ordonnance de préservation rendus en vertu de l'un des articles 487.012 et 487.013 est tenue de détruire celles qui ne seraient pas conservées dans le cadre normal de son activité commerciale et tout document établi en vue de les préserver en application de cet article dans les meilleurs délais après la première des éventualités suivantes à survenir :

a) la révocation de l'ordonnance de communication;

b) la communication du document comportant les données informatiques en vertu de l'ordonnance de communication.

Destruction of preserved computer data and documents — warrant

(4) Despite subsections (1) to (3), a person who preserved computer data under a preservation demand or order made under section 487.012 or 487.013 shall destroy the computer data that would not be retained in the ordinary course of business and any document that is

Destruction des données informatiques préservées et de documents : mandat

(4) Malgré les paragraphes (1) à (3), la personne qui a préservé des données informatiques en application d'un ordre ou d'une ordonnance de préservation rendus en vertu de l'un des articles 487.012 et 487.013 est tenue de détruire les données informatiques qui ne

prepared for the purpose of preserving computer data under that section when a document that contains the computer data is obtained under a warrant.

seraient pas conservées dans le cadre normal de son activité commerciale et tout document établi en vue de les préserver en application de cet article dès l'obtention d'un document comportant ces données informatiques en exécution d'un mandat de perquisition.

For greater certainty

487.0195 (1) For greater certainty, no preservation demand, preservation order or production order is necessary for a peace officer or public officer to ask a person to voluntarily preserve data that the person is not prohibited by law from preserving or to voluntarily provide a document to the officer that the person is not prohibited by law from disclosing.

Précision

487.0195 (1) Il est entendu qu'aucun ordre de préservation ni aucune ordonnance de préservation ou de communication n'est nécessaire pour que l'agent de la paix ou le fonctionnaire public demande à une personne de préserver volontairement des données ou de lui communiquer volontairement un document qu'aucune règle de droit n'interdit à celle-ci de préserver ou de communiquer.

No civil or criminal liability

(2) A person who preserves data or provides a document in those circumstances does not incur any criminal or civil liability for doing so.

Immunité

(2) La personne qui préserve des données ou communique un document dans de telles circonstances bénéficie de l'immunité en matière civile ou pénale pour les actes ainsi accomplis.

Self-incrimination

487.0196 No one is excused from complying with an order made under any of sections 487.014 to 487.018 on the ground that the document that they are required to produce may tend to incriminate them or subject them to a proceeding or penalty. However, no document that an individual is required to prepare may be used or received in evidence against them in a criminal proceeding that is subsequently instituted against them, other than a prosecution for an offence under section 132, 136 or 137.

Documents incriminants

487.0196 Nul n'est dispensé de se conformer à une ordonnance rendue en vertu de l'un des articles 487.014 à 487.018 du fait que des documents à communiquer peuvent tendre à l'incriminer ou à l'exposer à quelque procédure ou pénalité; toutefois, les documents qu'une personne physique est tenue d'établir ne peuvent être utilisés ou admis en preuve contre elle dans le cadre de poursuites criminelles intentées contre elle par la suite, sauf en ce qui concerne les poursuites pour toute infraction prévue aux articles 132, 136 ou 137.

Offence — preservation demand

487.0197 A person who contravenes a preservation demand made under section 487.012 without lawful excuse is guilty of an offence punishable on summary conviction and is liable to a fine of not more than $5,000.

Infraction : ordre de préservation

487.0197 Quiconque, sans excuse légitime, contrevient à l'ordre donné en vertu de l'article 487.012 commet une infraction et encourt, sur déclaration de culpabilité par procédure sommaire, une amende maximale de 5 000 $.

Offence — preservation or production order

487.0198 A person, financial institution or entity that contravenes an order made under any of sections 487.013 to 487.018 without lawful excuse is guilty of an offence punishable on summary conviction and is liable to a fine of not more than $250,000 or to imprisonment for a term of not more than six months, or to both.

Infraction : ordonnance de préservation ou de communication

487.0198 La personne, l'institution financière ou l'entité qui, sans excuse légitime, contrevient à une ordonnance rendue en vertu de l'un des articles 487.013 à 487.018 commet une infraction et encourt, sur déclaration de culpabilité par procédure sommaire, une amende maximale de 250 000 $ et un emprisonnement maximal de six mois, ou l'une de ces peines.

Offence — destruction of preserved data

487.0199 A person who contravenes section 487.0194 without lawful excuse is guilty of an offence punishable on summary conviction.

487.0199 Quiconque, sans excuse légitime, contrevient à l'article 487.0194 commet une infraction punissable sur déclaration de culpabilité par procédure sommaire.

Infraction : destruction de données préservées

Assistance order

487.02 If an authorization is given under section 184.2, 184.3, 186 or 188 or a warrant is issued under this Act, the judge or justice who gives the authorization or issues the warrant may order a person to provide assistance, if the person's assistance may reasonably be considered to be required to give effect to the authorization or warrant.

487.02 Le juge ou le juge de paix qui a accordé une autorisation en vertu des articles 184.2, 184.3, 186 ou 188 ou a délivré un mandat en vertu de la présente loi peut ordonner à toute personne de prêter son assistance si celle-ci peut raisonnablement être jugée nécessaire à l'exécution des actes autorisés ou du mandat.

Ordonnance d'assistance

1995, c. 27, s. 1

25. The heading before section 487.1 of the Act is replaced by the following:

25. L'intertitre précédant l'article 487.1 de la même loi est remplacé par ce qui suit :

1995, ch. 27, art. 1

OTHER PROVISIONS RESPECTING SEARCH WARRANTS, PRESERVATION ORDERS AND PRODUCTION ORDERS

AUTRES DISPOSITIONS : MANDATS DE PERQUISITION ET ORDONNANCES DE PRÉSERVATION OU DE COMMUNICATION

1997, c. 18, s. 46

26. Section 487.11 of the Act is replaced by the following:

26. L'article 487.11 de la même loi est remplacé par ce qui suit :

1997, ch. 18, art. 46

Exigent circumstances

487.11 Either a peace officer or a public officer who has been appointed or designated to administer or enforce a federal or provincial law and whose duties include the enforcement of this or any other Act of Parliament may, in the course of their duties, exercise any of the powers described in section 487, 492.1 or 492.2 without a warrant if the conditions for obtaining a warrant exist but it would not be feasible to obtain a warrant because of exigent circumstances.

487.11 L'agent de la paix ou le fonctionnaire public nommé ou désigné pour l'exécution ou le contrôle d'application d'une loi fédérale ou provinciale et chargé notamment de faire observer la présente loi ou toute autre loi fédérale peut, pour l'accomplissement de ses fonctions, exercer sans mandat tous les pouvoirs prévus aux articles 487, 492.1 ou 492.2 lorsque l'urgence de la situation rend difficilement réalisable l'obtention du mandat, pourvu que les conditions d'obtention soient réunies.

Urgence de la situation

2004, c. 3, s. 8(1)

27. (1) The portion of subsection 487.3(1) of the Act before paragraph (*a*) is replaced by the following:

27. (1) Le passage du paragraphe 487.3(1) de la même loi précédant l'alinéa *a*) est remplacé par ce qui suit :

2004, ch. 3, par. 8(1)

Order denying access to information

487.3 (1) On application made at the time an application is made for a warrant under this or any other Act of Parliament, an order under any of sections 487.013 to 487.018 or an authorization under section 529 or 529.4, or at a later time, a justice, a judge of a superior court of criminal jurisdiction or a judge of the Court of Quebec may make an order prohibiting access to, and the disclosure of, any information relating to the warrant, order or authorization on the ground that

487.3 (1) Un juge de paix, un juge de la cour supérieure de juridiction criminelle ou un juge de la Cour du Québec peut interdire par ordonnance, sur demande présentée soit lors de la présentation de la demande en vue d'obtenir un mandat prévu par la présente loi ou toute autre loi fédérale, une autorisation prévue aux articles 529 ou 529.4, ou une ordonnance prévue à l'un des articles 487.013 à 487.018, soit par la suite, l'accès aux renseignements relatifs au mandat, à l'autorisation ou à l'ordonnance, et la communication de ces renseignements au motif que, à la fois :

Ordonnance interdisant l'accès aux renseignements

1997, c. 23, s. 14

(2) Paragraph 487.3(1)(*b*) of the English version of the Act is replaced by the following:

(*b*) the reason referred to in paragraph (*a*) outweighs in importance the access to the information.

(2) L'alinéa 487.3(1)*b*) de la version anglaise de la même loi est remplacé par ce qui suit :

(*b*) the reason referred to in paragraph (*a*) outweighs in importance the access to the information.

1997, ch. 23, art. 14

1993, c. 40, s. 18; 1999, c. 5, ss. 18 and 19

28. Sections 492.1 and 492.2 of the Act are replaced by the following:

28. Les articles 492.1 et 492.2 de la même loi sont remplacés par ce qui suit :

1993, ch. 40, art. 18; 1999, ch. 5, art. 18 et 19

Warrant for tracking device — transactions and things

492.1 (1) A justice or judge who is satisfied by information on oath that there are reasonable grounds to suspect that an offence has been or will be committed under this or any other Act of Parliament and that tracking the location of one or more transactions or the location or movement of a thing, including a vehicle, will assist in the investigation of the offence may issue a warrant authorizing a peace officer or a public officer to obtain that tracking data by means of a tracking device.

492.1 (1) S'il est convaincu, par une dénonciation sous serment, qu'il existe des motifs raisonnables de soupçonner qu'une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise et que la localisation du lieu d'une ou de plusieurs opérations ou du lieu ou des déplacements d'une chose, notamment un véhicule, sera utile à l'enquête relative à l'infraction, un juge de paix ou un juge peut délivrer un mandat autorisant un agent de la paix ou un fonctionnaire public à obtenir ces données de localisation au moyen d'un dispositif de localisation.

Mandat pour un dispositif de localisation : opération ou chose

Warrant for tracking device — individuals

(2) A justice or judge who is satisfied by information on oath that there are reasonable grounds to believe that an offence has been or will be committed under this or any other Act of Parliament and that tracking an individual's movement by identifying the location of a thing that is usually carried or worn by the individual will assist in the investigation of the offence may issue a warrant authorizing a peace officer or a public officer to obtain that tracking data by means of a tracking device.

(2) S'il est convaincu, par une dénonciation sous serment, qu'il existe des motifs raisonnables de croire qu'une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise et que la localisation des déplacements d'une personne physique par l'identification du lieu d'une chose qui est habituellement portée ou transportée par elle sera utile à l'enquête relative à l'infraction, un juge de paix ou un juge peut délivrer un mandat autorisant un agent de la paix ou un fonctionnaire public à obtenir ces données de localisation au moyen d'un dispositif de localisation.

Mandat pour un dispositif de localisation : personne physique

Scope of warrant

(3) The warrant authorizes the peace officer or public officer, or a person acting under their authority, to install, activate, use, maintain, monitor and remove the tracking device, including covertly.

(3) Le mandat autorise l'agent de la paix ou le fonctionnaire public, ou toute personne qui agit sous son autorité à installer, activer, employer, entretenir, surveiller et enlever le dispositif, notamment d'une manière secrète.

Portée du mandat

Conditions

(4) A warrant may contain any conditions that the justice or judge considers appropriate, including conditions to protect a person's interests.

(4) Le mandat peut être assorti de toutes conditions que le juge de paix ou le juge estime indiquées, notamment quant à la protection des droits de toute personne.

Conditions

Period of validity

(5) Subject to subsection (6), a warrant is valid for the period specified in it as long as that period ends no more than 60 days after the day on which the warrant is issued.

(5) Sous réserve du paragraphe (6), il est valide pour la période qui y est indiquée, laquelle ne peut dépasser soixante jours à compter de la date de délivrance. Période de validité

Period of validity — organized crime and terrorism offence

(6) A warrant is valid for the period specified in it as long as that period ends no more than one year after the day on which the warrant is issued, if the warrant relates to

(*a*) an offence under any of sections 467.11 to 467.13;

(*b*) an offence committed for the benefit of, at the direction of, or in association with a criminal organization; or

(*c*) a terrorism offence.

(6) Il est valide pour la période qui y est indiquée, laquelle ne peut dépasser un an à compter de la date de délivrance dans les cas où il vise :

a) soit une infraction prévue à l'un des articles 467.11 à 467.13;

b) soit une infraction commise au profit ou sous la direction d'une organisation criminelle, ou en association avec elle;

c) soit une infraction de terrorisme. Période de validité : organisation criminelle ou infraction de terrorisme

Removal after expiry of warrant

(7) On *ex parte* application supported by an affidavit, the justice or judge who issued a warrant or another justice or judge who has jurisdiction to issue such warrants may authorize the covert removal of the tracking device after the expiry of the warrant under any conditions that the justice or judge considers advisable in the public interest. The authorization is valid for the period specified in it as long as that period is not more than 90 days.

(7) Sur demande *ex parte*, accompagnée d'un affidavit, le juge de paix ou le juge qui a délivré le mandat ou un juge de paix ou juge compétent pour délivrer un tel mandat peut autoriser l'enlèvement en secret du dispositif de localisation après l'expiration du mandat, selon les conditions qu'il estime indiquées dans l'intérêt public. L'autorisation est valide pour une période, d'au plus quatre-vingt-dix jours, qui y est indiquée. Enlèvement après l'expiration du mandat

Definitions

(8) The following definitions apply in this section.

(8) Les définitions qui suivent s'appliquent au présent article. Définitions

"data" «*données*»

"data" means representations, including signs, signals or symbols, that are capable of being understood by an individual or processed by a computer system or other device.

« dispositif de localisation » Tout dispositif, notamment un programme d'ordinateur au sens du paragraphe 342.1(2), pouvant servir à obtenir ou à enregistrer des données de localisation ou à les transmettre par un moyen de télécommunication. « dispositif de localisation » "*tracking device*"

"judge" «*juge*»

"judge" means a judge of a superior court of criminal jurisdiction or a judge of the Court of Quebec.

« données » Représentations, notamment signes, signaux ou symboles, qui peuvent être compris par une personne physique ou traités par un ordinateur ou un autre dispositif. « données » "*data*"

"public officer" «*fonctionnaire public*»

"public officer" means a public officer who is appointed or designated to administer or enforce a federal or provincial law and whose duties include the enforcement of this or any other Act of Parliament.

« données de localisation » Données qui concernent le lieu d'une opération ou d'une chose ou le lieu où est située une personne physique. « données de localisation » "*tracking data*"

"tracking data" «*données de localisation*»

"tracking data" means data that relates to the location of a transaction, individual or thing.

« fonctionnaire public » Fonctionnaire public nommé ou désigné pour l'exécution ou le contrôle d'application d'une loi fédérale ou provinciale et chargé notamment de faire observer la présente loi ou toute autre loi fédérale. « fonctionnaire public » "*public officer*"

"tracking device" «*dispositif de localisation*»

"tracking device" means a device, including a computer program within the meaning of subsection 342.1(2), that may be used to obtain or record tracking data or to transmit it by a means of telecommunication.

«juge» Juge de la cour supérieure de juridiction criminelle ou juge de la Cour du Québec. «juge» *"judge"*

Warrant for transmission data recorder

492.2 (1) A justice or judge who is satisfied by information on oath that there are reasonable grounds to suspect that an offence has been or will be committed against this or any other Act of Parliament and that transmission data will assist in the investigation of the offence may issue a warrant authorizing a peace officer or a public officer to obtain the transmission data by means of a transmission data recorder.

492.2 (1) S'il est convaincu, par une dénonciation sous serment, qu'il existe des motifs raisonnables de soupçonner qu'une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise et que des données de transmission seront utiles à l'enquête relative à l'infraction, un juge de paix ou un juge peut délivrer un mandat autorisant un agent de la paix ou un fonctionnaire public à obtenir de telles données au moyen d'un enregistreur de données de transmission. Mandat pour un enregistreur de données de transmission

Scope of warrant

(2) The warrant authorizes the peace officer or public officer, or a person acting under their authority, to install, activate, use, maintain, monitor and remove the transmission data recorder, including covertly.

(2) Le mandat autorise l'agent de la paix ou le fonctionnaire public, ou toute personne qui agit sous son autorité, à installer, activer, employer, entretenir, surveiller et enlever l'enregistreur de données de transmission, notamment d'une manière secrète. Portée du mandat

Limitation

(3) No warrant shall be issued under this section for the purpose of obtaining tracking data.

(3) Aucun mandat ne peut être délivré en vertu du présent article pour obtenir des données de localisation. Limite

Period of validity

(4) Subject to subsection (5), a warrant is valid for the period specified in it as long as that period ends no more than 60 days after the day on which the warrant is issued.

(4) Sous réserve du paragraphe (5), il est valide pour la période qui y est indiquée, laquelle ne peut dépasser soixante jours à compter de la date de délivrance. Période de validité

Period of validity — organized crime or terrorism offence

(5) The warrant is valid for the period specified in it as long as that period ends no more than one year after the day on which the warrant is issued, if the warrant relates to

(5) Il est valide pour la période qui y est indiquée, laquelle ne peut dépasser un an à compter de la date de délivrance dans les cas où il vise : Période de validité : organisation criminelle ou infraction de terrorisme

(*a*) an offence under any of sections 467.11 to 467.13;

a) soit une infraction prévue à l'un des articles 467.11 à 467.13;

(*b*) an offence committed for the benefit of, at the direction of, or in association with a criminal organization; or

b) soit une infraction commise au profit ou sous la direction d'une organisation criminelle, ou en association avec elle;

(*c*) a terrorism offence.

c) soit une infraction de terrorisme.

Definitions

(6) The following definitions apply in this section.

(6) Les définitions qui suivent s'appliquent au présent article. Définitions

"data" «*données*»

"data" means representations, including signs, signals or symbols, that are capable of being understood by an individual or processed by a computer system or other device.

«données» Représentations, notamment signes, signaux ou symboles, qui peuvent être compris par une personne physique ou traités par un ordinateur ou un autre dispositif. «données» *"data"*

"judge" «*juge*»

"judge" means a judge of a superior court of criminal jurisdiction or a judge of the Court of Quebec.

"public officer" «*fonctionnaire public*»

"public officer" means a public officer who is appointed or designated to administer or enforce a federal or provincial law and whose duties include the enforcement of this or any other Act of Parliament.

"transmission data" «*données de transmission*»

"transmission data" means data that

(*a*) relates to the telecommunication functions of dialling, routing, addressing or signalling;

(*b*) is transmitted to identify, activate or configure a device, including a computer program as defined in subsection 342.1(2), in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and

(*c*) does not reveal the substance, meaning or purpose of the communication.

"transmission data recorder" «*enregistreur de données de transmission*»

"transmission data recorder" means a device, including a computer program within the meaning of subsection 342.1(2), that may be used to obtain or record transmission data or to transmit it by a means of telecommunication.

« données de transmission » *"transmission data"*

« données de transmission » Données qui, à la fois :

a) concernent les fonctions de composition, de routage, d'adressage ou de signalisation en matière de télécommunication;

b) soit sont transmises pour identifier, activer ou configurer un dispositif, notamment un programme d'ordinateur au sens du paragraphe 342.1(2), en vue d'établir ou de maintenir l'accès à un service de télécommunication afin de rendre possible une communication, soit sont produites durant la création, la transmission ou la réception d'une communication et indiquent, ou sont censées indiquer, le type, la direction, la date, l'heure, la durée, le volume, le point d'envoi, la destination ou le point d'arrivée de la communication;

c) ne révèlent pas la substance, le sens ou l'objet de la communication.

« enregistreur de données de transmission » *"transmission data recorder"*

« enregistreur de données de transmission » Tout dispositif, notamment un programme d'ordinateur au sens du paragraphe 342.1(2), pouvant servir à obtenir ou à enregistrer des données de transmission par un moyen de télécommunication.

« fonctionnaire public » *"public officer"*

« fonctionnaire public » Fonctionnaire public nommé ou désigné pour l'exécution ou le contrôle d'application d'une loi fédérale ou provinciale et chargé notamment de faire observer la présente loi ou toute autre loi fédérale.

« juge » *"judge"*

« juge » Juge de la cour supérieure de juridiction criminelle ou juge de la Cour du Québec.

29. Part XXVIII of the Act is amended by adding the following after Form 5:

29. La partie XXVIII de la même loi est modifiée par adjonction, après la formule 5, de ce qui suit :

FORM 5.001
(Subsection 487.012(1))

PRESERVATION DEMAND

Canada,

Province of .....

(*territorial division*)

To (*name of person*), of .....:

FORMULE 5.001
(paragraphe 487.012(1))

ORDRE DE PRÉSERVATION

Canada,

Province de .....

(*circonscription territoriale*)

À (*nom de la personne*), de ..... :

Because I have reasonable grounds to suspect that the computer data specified below is in your possession or control and that that computer data

will assist in the investigation of an offence that has been or will be committed under (*specify the provision of the Criminal Code or other Act of Parliament*),

(*or*)

will assist in the investigation of an offence that has been committed under (*specify the provision of the law of the foreign state*) that is being conducted by a person or authority, (*name of person or authority*), with responsibility in (*specify the name of the foreign state*) for the investigation of such offences,

you are required to preserve (*specify the computer data*) that is in your possession or control when you receive this demand until (*insert date*) unless, before that date, this demand is revoked or a document that contains that data is obtained under a warrant or an order.

This demand is subject to the following conditions:

If you contravene this demand without lawful excuse, you may be subject to a fine.

You are required to destroy the computer data that would not be retained in the ordinary course of business, and any document that is prepared for the purpose of preserving the computer data, in accordance with section 487.0194 of the *Criminal Code*. If you contravene that provision without lawful excuse, you may be subject to a fine, to imprisonment or to both.

.....

(*Signature of peace officer or public officer*)

Attendu que j'ai des motifs raisonnables de soupçonner que les données informatiques précisées ci-dessous sont en votre possession ou à votre disposition et qu'elles

seront utiles à l'enquête relative à l'infraction prévue à (*préciser la disposition du Code criminel ou de l'autre loi fédérale*) qui a été ou sera commise,

(*ou*)

seront utiles à l'enquête relative à l'infraction prévue à (*préciser la disposition de la loi de l'État étranger*) qui a été commise et que l'enquête est menée par une personne ou un organisme, (*indiquer le nom de la personne ou de l'organisme*), chargé au (*ou* en *ou* à) (*indiquer le nom de l'État étranger*) des enquêtes relatives à de telles infractions,

En conséquence, vous êtes tenu(e) de préserver (*préciser les données informatiques*) qui sont en votre possession ou à votre disposition au moment où vous recevez le présent ordre jusqu'au (*indiquer la date*) à moins que l'ordre ne soit annulé ou qu'un document comportant ces données n'ait été obtenu en exécution d'un mandat ou d'une ordonnance avant cette date.

Le présent ordre est assorti des conditions suivantes :

Sachez que la contravention du présent ordre, sans excuse légitime, peut entraîner une amende.

Vous êtes tenu(e) de détruire les données informatiques qui ne sont pas conservées dans le cadre normal de votre activité commerciale et tout document établi en vue de les préserver, conformément à l'article 487.0194 du *Code criminel*. Sachez que la contravention de cette disposition, sans excuse légitime, peut entraîner une peine d'emprisonnement et une amende, ou l'une de ces peines.

.....

(*Signature de l'agent de la paix ou du fonctionnaire public*)

FORM 5.002
(Subsection 487.013(2))

INFORMATION TO OBTAIN A PRESERVATION ORDER

Canada,

Province of .....

(*territorial division*)

This is the information of (*name of peace officer or public officer*), of ..... ("the informant").

The informant says that they have reasonable grounds to suspect that an offence has been or will be committed under (*specify the provision of the Criminal Code or other Act of Parliament*) (*or* has been committed under (*specify the provision of the law of the foreign state*)) and that (*specify the computer data*) is in the possession or control of (*name of the person*) and will assist in the investigation of the offence.

The informant also says that a peace officer or public officer intends to apply or has applied for a warrant or order in connection with the investigation to obtain a document that contains the computer data (*and, if applicable,* and that (*name of person or authority*) is conducting the investigation and has responsibility for the investigation of such offences in (*insert the name of the foreign state*)).

The reasonable grounds are: (*including, if applicable, whether a preservation demand was made under section 487.012 of the Criminal Code*)

The informant therefore requests that (*name of the person*) be ordered to preserve (*specify the computer data*) that is in their possession or control when they receive the order for 90 days after the day on which the order is made.

Sworn before me on (*date*), at (*place*).

.....
(*Signature of informant*)

.....
(*Signature of justice or judge*)

FORMULE 5.002
(paragraphe 487.013(2))

DÉNONCIATION EN VUE D'OBTENIR UNE ORDONNANCE DE PRÉSERVATION

Canada,

Province de .....

(*circonscription territoriale*)

La présente constitue la dénonciation de (*nom de l'agent de la paix ou du fonctionnaire public*), de ....., ci-après appelé(e) « le dénonciateur ».

Le dénonciateur déclare qu'il a des motifs raisonnables de soupçonner qu'une infraction prévue à (*préciser la disposition du Code criminel ou de l'autre loi fédérale*) a été ou sera commise (*ou* qu'une infraction à (*préciser la disposition de la loi de l'État étranger*) a été commise) et que (*préciser les données informatiques*) sont en la possession de (*nom de la personne*) ou à sa disposition et seront utiles à l'enquête relative à l'infraction.

Le dénonciateur déclare qu'il a l'intention de demander ou a demandé la délivrance d'un mandat ou d'une ordonnance en vue d'obtenir un document comportant les données informatiques relativement à l'enquête (*et, le cas échéant,* et que (*indiquer le nom de la personne ou de l'organisme*) mène l'enquête et est chargé au (*ou* en *ou* à) (*indiquer le nom de l'État étranger*) des enquêtes relatives à de telles infractions).

Les motifs raisonnables sont les suivants : (*préciser, le cas échéant, si un ordre en vertu de l'article 487.012 du Code criminel a été donné*)

En conséquence, le dénonciateur demande d'ordonner à (*nom de la personne*) de préserver, pendant les quatre-vingt-dix jours qui suivent la date à laquelle l'ordonnance a été rendue, (*préciser les données informatiques*) qui sont en sa possession ou à sa disposition au moment où il ou elle reçoit l'ordonnance.

Fait sous serment devant moi ce (*date*), à (*lieu*).

.....
(*Signature du dénonciateur*)

.....
(*Signature du juge de paix ou du juge*)

FORM 5.003
(Subsection 487.013(4))

PRESERVATION ORDER

Canada,

Province of .....

(*territorial division*)

To (*name of person*), of .....:

Whereas I am satisfied by information on oath of (*name of peace officer or public officer*), of .....,

(*a*) that there are reasonable grounds to suspect that an offence has been or will be committed under (*specify the provision of the Criminal Code or other Act of Parliament*) (*or* has been committed under (*specify the provision of the law of the foreign state*)) and that (*specify the computer data*) is in your possession or control and will assist in the investigation of the offence; and

(*b*) that a peace officer or public officer intends to apply or has applied for a warrant or order to obtain a document that contains the computer data (*and, if applicable,* and that (*name of person or authority*) is conducting the investigation and has responsibility for the investigation of such offences in (*insert the name of the foreign state*));

Therefore, you are required to preserve the specified computer data that is in your possession or control when you receive this order until (*insert date*) unless, before that date, this order is revoked or a document that contains that data is obtained under a warrant or an order.

This order is subject to the following conditions:

FORMULE 5.003
(paragraphe 487.013(4))

ORDONNANCE DE PRÉSERVATION

Canada,

Province de .....

(*circonscription territoriale*)

À (*nom de la personne*), de .....:

Attendu que je suis convaincu, en me fondant sur une dénonciation sous serment par (*nom de l'agent de la paix ou du fonctionnaire public*), de .....:

a) qu'il existe des motifs raisonnables de soupçonner qu'une infraction prévue à (*préciser la disposition du Code criminel ou de l'autre loi fédérale*) a été ou sera commise (*ou* qu'une infraction prévue à (*préciser la disposition de la loi de l'État étranger*) a été commise) et que (*préciser les données informatiques*) sont en votre possession ou à votre disposition et seront utiles à l'enquête relative à l'infraction;

b) qu'un agent de la paix ou un fonctionnaire public a l'intention de demander ou a demandé la délivrance d'un mandat ou d'une ordonnance en vue d'obtenir un document comportant les données informatiques (*et, le cas échéant,* et que (*indiquer le nom de la personne ou de l'organisme*) mène l'enquête et est chargé au (*ou* en *ou* à) (*indiquer le nom de l'État étranger*) des enquêtes relatives à de telles infractions),

En conséquence, vous êtes tenu(e) de préserver les données informatiques précisées qui sont en votre possession ou à votre disposition au moment où vous recevez la présente ordonnance jusqu'au (*indiquer la date*) à moins que l'ordonnance ne soit révoquée ou qu'un docu-

If you contravene this order without lawful excuse, you may be subject to a fine, to imprisonment or to both.

You are required to destroy the computer data that would not be retained in the ordinary course of business, and any document that is prepared for the purpose of preserving the computer data, in accordance with section 487.0194 of the *Criminal Code*. If you contravene that provision without lawful excuse, you may be subject to a fine, to imprisonment or to both.

Dated (*date*), at (*place*).

.....
(*Signature of justice or judge*)

FORM 5.004
(Subsections 487.014(2), 487.015(2), 487.016(2), 487.017(2) and 487.018(3))

INFORMATION TO OBTAIN A PRODUCTION ORDER

Canada,

Province of .....

(*territorial division*)

This is the information of (*name of peace officer or public officer*), of ..... ("the informant").

The informant says that they have reasonable grounds to suspect (*or, if the application is for an order under section 487.014 of the Criminal Code,* reasonable grounds to believe)

(*a*) that an offence has been or will be committed under (*specify the provision of the Criminal Code or other Act of Parliament*); and

(*b*) (*if the application is for an order under section 487.014 of the Criminal Code*) that (*specify the document or data*) is in the

ment comportant ces données n'ait été obtenu en exécution d'un mandat ou d'une ordonnance avant cette date.

La présente ordonnance est assortie des conditions suivantes :

Sachez que la contravention de la présente ordonnance, sans excuse légitime, peut entraîner une peine d'emprisonnement et une amende, ou l'une de ces peines.

Vous êtes tenu(e) de détruire les données informatiques qui ne sont pas conservées dans le cadre normal de votre activité commerciale et tout document établi en vue de les préserver, conformément à l'article 487.0194 du *Code criminel*. Sachez que la contravention de cette disposition, sans excuse légitime, peut entraîner une peine d'emprisonnement et une amende, ou l'une de ces peines.

Fait le (*date*), à (*lieu*).

.....
(*Signature du juge de paix ou du juge*)

FORMULE 5.004
(paragraphes 487.014(2), 487.015(2), 487.016(2), 487.017(2) et 487.018(3))

DÉNONCIATION EN VUE D'OBTENIR UNE ORDONNANCE DE COMMUNICATION

Canada,

Province de .....

(*circonscription territoriale*)

La présente constitue la dénonciation de (*nom de l'agent de la paix ou du fonctionnaire public*), de ....., ci-après appelé(e) « le dénonciateur ».

Le dénonciateur déclare qu'il a des motifs raisonnables de soupçonner (*ou, si la demande vise à obtenir une ordonnance en vertu de l'article 487.014 du Code criminel,* de croire) que les conditions suivantes sont réunies :

a) une infraction prévue à (*préciser la disposition du Code criminel ou de l'autre loi fédérale*) a été ou sera commise;

possession or control of (*name of the person*) and will afford evidence respecting the commission of the offence.

(*or*)

(*b*) (*if the application is for an order under section 487.015 of the Criminal Code*) that the identification of a device or person involved in the transmission of (*specify the communication*) will assist in the investigation of the offence and that (*specify the transmission data*) that is in the possession or control of one or more persons whose identity is unknown will enable that identification.

(*or*)

(*b*) (*if the application is for an order under section 487.016 of the Criminal Code*) that (*specify the transmission data*) is in the possession or control of (*name of the person*) and will assist in the investigation of the offence.

(*or*)

(*b*) (*if the application is for an order under section 487.017 of the Criminal Code*) that (*specify the tracking data*) is in the possession or control of (*name of the person*) and will assist in the investigation of the offence.

(*or*)

(*b*) (*if the application is for an order under section 487.018 of the Criminal Code*) that (*specify the data*) is in the possession or control of (*name of the financial institution, person or entity*) and will assist in the investigation of the offence.

The reasonable grounds are:

The informant therefore requests

(*if the application is for an order under section 487.014 of the Criminal Code*) that (*name of the person*) be ordered to produce a document that is a copy of (*specify the document*) that is in their possession or control when they receive the order (*and/or* to prepare and produce a document containing (*specify the data*) that is in their possession or control when they receive the order).

(*or*)

b) (*si la demande vise à obtenir une ordonnance en vertu de l'article 487.014 du Code criminel, préciser les données*) sont en la possession de (*nom de la personne*) ou à sa disposition et fourniront une preuve concernant la perpétration de l'infraction.

(*ou*)

b) (*si la demande vise à obtenir une ordonnance en vertu de l'article 487.015 du Code criminel*) l'identification de tout dispositif ayant servi à la transmission de (*préciser la communication*) ou de toute personne y ayant participé sera utile à l'enquête relative à l'infraction et que (*préciser les données de transmission*) sont en la possession ou à la disposition d'une ou de plusieurs personnes — dont l'identité n'est pas connue — et permettront cette identification.

(*ou*)

b) (*si la demande vise à obtenir une ordonnance en vertu de l'article 487.016 du Code criminel, préciser les données de transmission*) sont en la possession de (*nom de la personne*) ou à sa disposition et seront utiles à l'enquête relative à l'infraction.

(*ou*)

b) (*si la demande vise à obtenir une ordonnance en vertu de l'article 487.017 du Code criminel, préciser les données de localisation*) sont en la possession de (*nom de la personne*) ou à sa disposition et seront utiles à l'enquête relative à l'infraction.

(*ou*)

b) (*si la demande vise à obtenir une ordonnance en vertu de l'article 487.018 du Code criminel, préciser les données*) sont en la possession de (*nom de l'institution financière, de la personne ou de l'entité*) ou à sa disposition et seront utiles à l'enquête relative à l'infraction.

Les motifs raisonnables sont les suivants :

En conséquence, le dénonciateur demande

(*si la demande vise à obtenir une ordonnance en vertu de l'article 487.014 du Code criminel*) d'ordonner à (*nom de la personne*) de com-

(*if the application is for an order under section 487.015 of the Criminal Code*) that a person who is served with the order in accordance with subsection 487.015(4) of the *Criminal Code* be ordered to prepare and produce a document containing (*specify the transmission data*) that is in their possession or control when they are served with the order.

(*or*)

(*if the application is for an order under section 487.016 of the Criminal Code*) that (*name of the person*) be ordered to prepare and produce a document containing (*specify the transmission data*) that is in their possession or control when they receive the order.

(*or*)

(*if the application is for an order under section 487.017 of the Criminal Code*) that (*name of the person*) be ordered to prepare and produce a document containing (*specify the tracking data*) that is in their possession or control when they receive the order.

(*or*)

(*if the application is for an order under section 487.018 of the Criminal Code*) that (*name of the financial institution, person or entity*) be ordered to prepare and produce a document setting out (*specify the data*) that is in their possession or control when they receive the order.

Sworn before me on (*date*), at (*place*).

.....
(*Signature of informant*)

.....
(*Signature of justice or judge*)

muniquer un document qui est la copie de (*indiquer le document*) qui est en sa possession ou à sa disposition au moment où il ou elle reçoit l'ordonnance (*ou* d'établir et de communiquer un document comportant (*indiquer les données*) qui sont en sa possession ou à sa disposition au moment où il ou elle reçoit l'ordonnance).

(*ou*)

(*si la demande vise à obtenir une ordonnance en vertu de l'article 487.015 du Code criminel*) d'ordonner à toute personne à qui l'ordonnance est signifiée conformément au paragraphe 487.015(4) du *Code criminel* d'établir et de communiquer un document comportant (*préciser les données de transmission*) qui sont en sa possession ou à sa disposition au moment où l'ordonnance lui est signifiée.

(*ou*)

(*si la demande vise à obtenir une ordonnance en vertu de l'article 487.016 du Code criminel*) d'ordonner à (*nom de la personne*) d'établir et de communiquer un document comportant (*préciser les données de transmission*) qui sont en sa possession ou à sa disposition au moment où il ou elle reçoit l'ordonnance.

(*ou*)

(*si la demande vise à obtenir une ordonnance en vertu de l'article 487.017 du Code criminel*) d'ordonner à (*nom de la personne*) d'établir et de communiquer un document comportant (*préciser les données de localisation*) qui sont en sa possession ou à sa disposition au moment où il ou elle reçoit l'ordonnance.

(*ou*)

(*si la demande vise à obtenir une ordonnance en vertu de l'article 487.018 du Code criminel*) d'ordonner à (*nom de l'institution financière, de la personne ou de l'entité*) d'établir et de communiquer un document énonçant (*préciser les données*) qui sont en sa possession ou à sa disposition au moment où il ou elle reçoit l'ordonnance.

Fait sous serment devant moi ce (*date*), à (*lieu*).

.....
(*Signature du dénonciateur*)

..... 5
(*Signature du juge de paix ou du juge*)

FORM 5.005
(Subsection 487.014(3))

PRODUCTION ORDER FOR DOCUMENTS

Canada,

Province of .....

(*territorial division*)

To (*name of person*), of .....:

Whereas I am satisfied by information on oath of (*name of peace officer or public officer*), of ....., that there are reasonable grounds to believe that an offence has been or will be committed under (*specify the provision of the Criminal Code or other Act of Parliament*) and that (*specify the document or data*) is in your possession or control and will afford evidence respecting the commission of the offence;

Therefore, you are ordered to

produce a document that is a copy of (*specify the document*) that is in your possession or control when you receive this order

(*and/or*)

prepare and produce a document containing (*specify the data*) that is in your possession or control when you receive this order.

The document must be produced to (*name of peace officer or public officer*) within (*time*) at (*place*) in (*form*).

This order is subject to the following conditions:

You have the right to apply to revoke or vary this order.

If you contravene this order without lawful excuse, you may be subject to a fine, to imprisonment or to both.

FORMULE 5.005
(paragraphe 487.014(3))

ORDONNANCE DE COMMUNICATION : DOCUMENTS

Canada,

Province de .....

(*circonscription territoriale*)

À (*nom de la personne*), de ..... :

Attendu que je suis convaincu, en me fondant sur une dénonciation sous serment par (*nom de l'agent de la paix ou du fonctionnaire public*), de ....., qu'il existe des motifs raisonnables de croire qu'une infraction prévue à (*préciser la disposition du Code criminel ou de l'autre loi fédérale*) a été ou sera commise et que (*préciser le document ou les données*) sont en votre possession ou à votre disposition et fourniront une preuve concernant la perpétration de l'infraction,

En conséquence, vous êtes tenu(e)

de communiquer un document qui est la copie de (*préciser le document*) qui est en votre possession ou à votre disposition au moment où vous recevez la présente ordonnance,

(*et/ou*)

d'établir et de communiquer un document comportant (*préciser les données*) qui sont en votre possession ou à votre disposition au moment où vous recevez la présente ordonnance.

Le document doit être communiqué à (*nom de l'agent de la paix ou du fonctionnaire public*), dans un délai de (*indiquer le délai*), à (*lieu*), et être présenté (*indiquer la forme*).

La présente ordonnance est assortie des conditions suivantes :

Dated (*date*), at (*place*).

.....
(*Signature of justice or judge*)

FORM 5.006
(Subsection 487.015(3))

PRODUCTION ORDER TO TRACE A COMMUNICATION

Canada,

Province of .....

(*territorial division*)

Whereas I am satisfied by information on oath of (*name of peace officer or public officer*), of ....., that there are reasonable grounds to suspect that an offence has been or will be committed under (*specify the provision of the Criminal Code or other Act of Parliament*), that the identification of a device or person involved in the transmission of (*specify the communication*) will assist in the investigation of the offence and that one or more persons whose identity was unknown when the application was made have possession or control of (*specify the transmission data*) that will enable that identification;

Therefore, on being served with this order in accordance with subsection 487.015(4) of the *Criminal Code*, you are ordered to prepare and produce a document containing (*specify the transmission data*) that is in your possession or control when you are served with this order.

The document must be produced to (*name of peace officer or public officer*) as soon as feasible at (*place*) in (*form*).

This order is subject to the following conditions:

You have the right to apply to revoke or vary this order.

Vous avez le droit de demander la révocation ou la modification de la présente ordonnance.

Sachez que la contravention de la présente ordonnance, sans excuse légitime, peut entraîner une peine d'emprisonnement et une amende, ou l'une de ces peines.

Fait le (*date*), à (*lieu*).

.....
(*Signature du juge de paix ou du juge*)

FORMULE 5.006
(paragraphe 487.015(3))

ORDONNANCE DE COMMUNICATION EN VUE DE RETRACER UNE COMMUNICATION

Canada,

Province de .....

(*circonscription territoriale*)

Attendu que je suis convaincu, en me fondant sur une dénonciation sous serment par (*nom de l'agent de la paix ou du fonctionnaire public*), de ....., qu'il existe des motifs raisonnables de soupçonner qu'une infraction prévue à (*préciser la disposition du Code criminel ou de l'autre loi fédérale*) a été ou sera commise, que l'identification de tout dispositif ayant servi à la transmission de (*préciser la communication*) ou de toute personne y ayant participé sera utile à l'enquête relative à l'infraction et que (*préciser les données de transmission*) sont en la possession ou à la disposition d'une ou de plusieurs personnes — dont l'identité n'était pas connue au moment de la présentation de la demande — et permettront cette identification,

En conséquence, sur signification de la présente ordonnance conformément au paragraphe 487.015(4) du *Code criminel*, vous êtes tenu(e) d'établir et de communiquer un document comportant (*préciser les données de transmission*) qui sont en votre possession ou à votre disposition au moment où l'ordonnance vous est signifiée.

Le document doit être communiqué à (*nom de l'agent de la paix ou du fonctionnaire public*), dans les meilleurs délais, à (*lieu*), et être présenté (*indiquer la forme*).

If you contravene this order without lawful excuse, you may be subject to a fine, to imprisonment or to both.

Dated (*date*), at (*place*).

.....
(*Signature of justice or judge*)

Served on (*name of person*) on (*date*), at (*place*).

.....
(*Signature of peace officer or public officer*)

.....
(*Signature of person served*)

FORM 5.007
(Subsections 487.016(3) and 487.017(3))

PRODUCTION ORDER FOR TRANSMISSION DATA OR TRACKING DATA

Canada,

Province of .....

(*territorial division*)

To (*name of person*), of .....:

Whereas I am satisfied by information on oath of (*name of peace officer or public officer*), of ....., that there are reasonable grounds to suspect that an offence has been or will be committed under (*specify the provision of the Criminal Code or other Act of Parliament*) and that (*if the order is made under section 487.016 of the Criminal Code, specify the transmission data*) (*or, if the order is made under section 487.017 of the Criminal Code, specify the tracking data*) is in your possession or control and will assist in the investigation of the offence;

La présente ordonnance est assortie des conditions suivantes :

Vous avez le droit de demander la révocation ou la modification de la présente ordonnance.

Sachez que la contravention de la présente ordonnance, sans excuse légitime, peut entraîner une peine d'emprisonnement et une amende, ou l'une de ces peines.

Fait le (*date*), à (*lieu*).

.....
(*Signature du juge de paix ou du juge*)

Signifiée à (*nom de la personne*), le (*date*), à (*lieu*).

.....
(*Signature de l'agent de la paix ou du fonctionnaire public*)

.....
(*Signature de la personne à qui l'ordonnance est signifiée*)

FORMULE 5.007
(paragraphes 487.016(3) et 487.017(3))

ORDONNANCE DE COMMUNICATION : DONNÉES DE TRANSMISSION OU DONNÉES DE LOCALISATION

Canada,

Province de .....

(*circonscription territoriale*)

À (*nom de la personne*), de ..... :

Attendu que je suis convaincu, en me fondant sur une dénonciation sous serment par (*nom de l'agent de la paix ou du fonctionnaire public*), de ....., qu'il existe des motifs raisonnables de soupçonner qu'une infraction prévue à (*préciser la disposition du Code criminel ou de l'autre loi fédérale*) a été ou sera commise et que (*si l'ordonnance a été rendue en vertu de l'article 487.016 du Code criminel, préciser les données de transmission*) (*ou, si l'ordonnance a été rendue en vertu de l'article 487.017 du Code criminel, préciser les données de localisation*) sont en votre possession ou à votre disposition et seront utiles à l'enquête relative à l'infraction,

Therefore, you are ordered to prepare and produce a document containing the data specified that is in your possession or control when you receive this order.

The document must be produced to (*name of peace officer or public officer*) within (*time*) at (*place*) in (*form*).

This order is subject to the following conditions:

You have the right to apply to revoke or vary this order.

If you contravene this order without lawful excuse, you may be subject to a fine, to imprisonment or to both.

Dated (*date*), at (*place*).

.....
(*Signature of justice or judge*)

En conséquence, vous êtes tenu(e) d'établir et de communiquer un document comportant ces données qui sont en votre possession ou à votre disposition au moment où vous recevez la présente ordonnance.

Le document doit être communiqué à (*nom de l'agent de la paix ou du fonctionnaire public*), dans un délai de (*indiquer le délai*), à (*lieu*), et être présenté (*indiquer la forme*).

La présente ordonnance est assortie des conditions suivantes :

Vous avez le droit de demander la révocation ou la modification de la présente ordonnance.

Sachez que la contravention de la présente ordonnance, sans excuse légitime, peut entraîner une peine d'emprisonnement et une amende, ou l'une de ces peines.

Fait le (*date*), à (*lieu*).

.....
(*Signature du juge de paix ou du juge*)

FORM 5.008
(Subsection 487.018(4))

PRODUCTION ORDER FOR FINANCIAL DATA

Canada,

Province of .....

(*territorial division*)

To (*name of financial institution, person or entity*), of .....:

Whereas I am satisfied by information on oath of (*name of peace officer or public officer*), of ....., that there are reasonable grounds to suspect that an offence has been or will be committed under (*specify the provision of the Criminal Code or other Act of Parliament*) and that (*specify the data*) is in your possession or control and will assist in the investigation of the offence;

Therefore, you are ordered to prepare and produce a document setting out (*specify the data*) that is in your possession or control when you receive this order.

FORMULE 5.008
(paragraphe 487.018(4))

ORDONNANCE DE COMMUNICATION : DONNÉES FINANCIÈRES

Canada,

Province de .....

(*circonscription territoriale*)

À (*nom de l'institution financière, de la personne ou de l'entité*), de ..... :

Attendu que je suis convaincu, en me fondant sur une dénonciation sous serment par (*nom de l'agent de la paix ou du fonctionnaire public*), de ....., qu'il existe des motifs raisonnables de soupçonner qu'une infraction prévue à (*préciser la disposition du Code criminel ou de l'autre loi fédérale*) a été ou sera commise et que (*préciser les données*) sont en votre possession ou à votre disposition et seront utiles à l'enquête relative à l'infraction,

The document must be produced to (*name of the peace officer or public officer*) within (*time*) at (*place*) in (*form*).

This order is subject to the following conditions:

You have the right to apply to revoke or vary this order.

If you contravene this order without lawful excuse, you may be subject to a fine, to imprisonment or to both.

Dated (*date*), at (*place*).

.....
(*Signature of justice or judge*)

FORM 5.0081
(Subsection 487.019(3))

INFORMATION TO REVOKE OR VARY AN ORDER MADE UNDER ANY OF SECTIONS 487.013 TO 487.018 OF THE CRIMINAL CODE

Canada,

Province of .....

(*territorial division*)

This is the information of (*name of peace officer or public officer*), of ..... ("the informant").

The informant says that on or after (*insert date*) the informant became aware of the following facts that justify the revocation (*or* variation) of an order made on (*insert date*) under (*specify the provision of the Criminal Code*):

.....

The informant therefore requests that the order be revoked (*or* be varied as follows: .....).

En conséquence, vous êtes tenu(e) d'établir et de communiquer un document énonçant (*préciser les données*) qui sont en votre possession ou à votre disposition au moment où vous recevez la présente ordonnance.

Le document doit être communiqué à (*nom de l'agent de la paix ou du fonctionnaire public*), dans un délai de (*indiquer le délai*), à (*lieu*), et être présenté (*indiquer la forme*).

La présente ordonnance est assortie des conditions suivantes :

Vous avez le droit de demander la révocation ou la modification de la présente ordonnance.

Sachez que la contravention de la présente ordonnance, sans excuse légitime, peut entraîner une peine d'emprisonnement et une amende, ou l'une de ces peines.

Fait le (*date*), à (*lieu*).

.....
(*Signature du juge de paix ou du juge*)

FORMULE 5.0081
(paragraphe 487.019(3))

DÉNONCIATION EN VUE D'OBTENIR LA RÉVOCATION OU LA MODIFICATION D'UNE ORDONNANCE RENDUE EN VERTU DE L'UN DES ARTICLES 487.013 À 487.018 DU CODE CRIMINEL

Canada,

Province de .....

(*circonscription territoriale*)

La présente constitue la dénonciation de (*nom de l'agent de la paix ou du fonctionnaire public*), de ....., ci-après appelé(e) « le dénonciateur ».

Le dénonciateur déclare que le ou vers le (*insérer la date*) il a pris connaissance des faits énoncés ci-dessous qui justifient que l'ordonnance rendue en vertu de (*préciser la disposition du Code criminel*) le (*insérer la date*) soit révoquée (*ou* modifiée) :

.....,

Sworn before me on (*date*), at (*place*).

.....
(*Signature of informant*)

.....
(*Signature of justice or judge*)

FORM 5.009
(Subsection 487.0191(2))

INFORMATION TO OBTAIN A NON-DISCLOSURE ORDER

Canada,

Province of .....

(*territorial division*)

This is the information of (*name of peace officer or public officer*), of ..... ("the informant").

The informant says that they have reasonable grounds to believe that the disclosure of the existence (*or* any of the contents *or* any of the following portion or portions) of (*identify the preservation demand made under section 487.012 of the Criminal Code, the preservation order made under section 487.013 of that Act or the production order made under any of sections 487.014 to 487.018 of that Act, as the case may be*) during (*identify the period*) would jeopardize the conduct of the investigation of the offence to which it relates:

(*specify portion or portions*)

The reasonable grounds are:

The informant therefore requests an order prohibiting (*name of the person, financial institution or entity*) from disclosing the existence (*or* any of the contents *or* any of the specified portion or portions) of the demand (*or* the order) during a period of (*identify the period*) after the day on which the order is made.

En conséquence, le dénonciateur demande que l'ordonnance soit révoquée (*ou* modifiée de la façon suivante : .....).

Fait sous serment devant moi ce (*date*), à (*lieu*).

.....
(*Signature du dénonciateur*)

.....
(*Signature du juge de paix ou du juge*)

FORMULE 5.009
(paragraphe 487.0191(2))

DÉNONCIATION EN VUE D'OBTENIR UNE ORDONNANCE DE NON-DIVULGATION

Canada,

Province de .....

(*circonscription territoriale*)

La présente constitue la dénonciation de (*nom de l'agent de la paix ou du fonctionnaire public*), de ....., ci-après appelé(e) « le dénonciateur ».

Le dénonciateur déclare qu'il a des motifs raisonnables de croire que la divulgation de l'existence (*ou* d'une partie quelconque *ou* d'une partie quelconque du ou des passages — précisés ci-dessous —) de (*indiquer l'ordre de préservation donné en vertu de l'article 487.012 du Code criminel, l'ordonnance de préservation rendue en vertu de l'article 487.013 de cette loi ou l'ordonnance de communication rendue en vertu de l'un des articles 487.014 à 487.018 de cette loi, selon le cas*) pendant (*indiquer la période*) compromettrait le déroulement de l'enquête relative à l'infraction visée :

(*préciser le ou les passages*)

Les motifs raisonnables sont les suivants :

En conséquence, le dénonciateur demande d'ordonner à (*nom de la personne, de l'institution financière ou de l'entité*) de ne pas divulguer l'existence (*ou* une partie quelconque *ou* une partie quelconque du ou des passages

Sworn before me on (*date*), at (*place*).

.....
(*Signature of informant*)

.....
(*Signature of justice or judge*)

FORM 5.0091
(Subsection 487.0191(3))

NON-DISCLOSURE ORDER

Canada,

Province of .....

(*territorial division*)

To (*name of person, financial institution or entity*), of .....:

Whereas I am satisfied by information on oath of (*name of peace officer or public officer*), of ....., that there are reasonable grounds to believe that the disclosure of the existence (*or* any of the contents *or* any of the portion or portions, specified in the information,) of (*identify the preservation demand made under section 487.012 of the Criminal Code, the preservation order made under section 487.013 of that Act or the production order made under any of sections 487.014 to 487.018 of that Act, as the case may be*) during (*identify the period*) would jeopardize the conduct of the investigation of the offence to which it relates;

Therefore, you are prohibited from disclosing the existence (*or* any of the contents *or* any of the following portion or portions) of the demand (*or* the order) during a period of (*identify the period*) after the day on which this order is made.

(*specify portion or portions*)

You have the right to apply to revoke or vary this order.

If you contravene this order without lawful excuse, you may be subject to a fine, to imprisonment or to both.

précisés) de l'ordre (*ou* de l'ordonnance) pendant (*indiquer la période*) après la date à laquelle l'ordonnance est rendue.

Fait sous serment devant moi ce (*date*), à (*lieu*).

.....
(*Signature du dénonciateur*)

.....
(*Signature du juge de paix ou du juge*)

FORMULE 5.0091
(paragraphe 487.0191(3))

ORDONNANCE DE NON-DIVULGATION

Canada,

Province de .....

(*circonscription territoriale*)

À (*nom de la personne, de l'institution financière, ou de l'entité*), de .....:

Attendu que je suis convaincu, en me fondant sur une dénonciation sous serment par (*nom de l'agent de la paix ou du fonctionnaire public*), de ....., qu'il existe des motifs raisonnables de croire que la divulgation de l'existence (*ou* d'une partie quelconque *ou* d'une partie quelconque du ou des passages — précisés dans la dénonciation —) de (*indiquer l'ordre de préservation donné en vertu de l'article 487.012 du Code criminel, l'ordonnance de préservation rendue en vertu de l'article 487.013 de cette loi ou l'ordonnance de communication rendue en vertu de l'un des articles 487.014 à 487.018 de cette loi, selon le cas*) pendant (*indiquer la période*) compromettrait le déroulement de l'enquête relative à l'infraction visée,

En conséquence, vous êtes tenu(e) de ne pas divulguer l'existence (*ou* une partie quelconque *ou* une partie quelconque du ou des passages précisés ci-dessous) de l'ordre (*ou* de l'ordonnance) pendant (*indiquer la période*) après la date à laquelle la présente ordonnance est rendue :

(*préciser le ou les passages*)

Dated (*date*), at (*place*).

.....
(*Signature of justice or judge*)

Vous avez le droit de demander la révocation ou la modification de la présente ordonnance.

Sachez que la contravention de la présente ordonnance, sans excuse légitime, peut entraîner une peine d'emprisonnement et une amende, ou l'une de ces peines.

Fait le (*date*), à (*lieu*).

.....
(*Signature du juge de paix ou du juge*)

R.S., c. C-34; R.S., c. 19 (2nd Supp.), s. 19

COMPETITION ACT

LOI SUR LA CONCURRENCE

L.R., ch. C-34; L.R., ch. 19 (2e suppl.), art. 19

R.S., c. 19 (2nd Supp.), s. 20(3)

30. (1) The definition "record" in subsection 2(1) of the *Competition Act* is replaced by the following:

30. (1) La définition de « document », au paragraphe 2(1) de la *Loi sur la concurrence*, est remplacée par ce qui suit :

L.R., ch. 19 (2e suppl.), par. 20(3)

"record" « *document* »

"record" means a medium on which information is registered or marked;

« document » Tout support sur lequel sont enregistrés ou inscrits des renseignements.

« document » "*record*"

(2) Subsection 2(1) of the Act is amended by adding the following in alphabetical order:

(2) Le paragraphe 2(1) de la même loi est modifié par adjonction, selon l'ordre alphabétique, de ce qui suit :

"computer system" « *ordinateur* »

"computer system" has the same meaning as in subsection 342.1(2) of the *Criminal Code*;

« données » Représentations, notamment signes, signaux ou symboles, qui peuvent être compris par une personne physique ou traités par un ordinateur ou un autre dispositif.

« données » "*data*"

"data" « *données* »

"data" means representations, including signs, signals or symbols, that are capable of being understood by an individual or processed by a computer system or other device;

« ordinateur » S'entend au sens du paragraphe 342.1(2) du *Code criminel*.

« ordinateur » "*computer system*"

"information" « *renseignement* »

"information" includes data;

« renseignement » S'entend notamment de données.

« renseignement » "*information*"

31. The Act is amended by adding the following after section 14:

31. La même loi est modifiée par adjonction, après l'article 14, de ce qui suit :

Application of *Criminal Code* — preservation demand and orders for preservation or production of data

14.1 (1) Sections 487.012, 487.013, 487.015, 487.016 and 487.018 of the *Criminal Code*, which apply to the investigation of offences under any Act of Parliament, also apply, with any modifications that the circumstances require,

(*a*) to an investigation in relation to a contravention of an order made under section 32, 33 or 34 or Part VII.1 or VIII; or

(*b*) to an investigation in relation to whether grounds exist for the making of an order under Part VII.1 or VIII.

14.1 (1) Les articles 487.012, 487.013, 487.015, 487.016 et 487.018 du *Code criminel*, qui s'appliquent à l'enquête relative à une infraction à une loi fédérale, s'appliquent aussi, avec les adaptations nécessaires, à l'une ou l'autre des enquêtes suivantes :

a) celle relative à la contravention à une ordonnance rendue en vertu des articles 32, 33 ou 34 ou des parties VII.1 ou VIII;

b) celle relative à l'existence de motifs justifiant que soit rendue une ordonnance en vertu des parties VII.1 ou VIII.

Application du *Code criminel* : ordres de préservation et ordonnances de préservation ou de communication

Clarification

(2) The provisions of the *Criminal Code* referred to in subsection (1) apply whether or not an inquiry has been commenced under section 10.

Précision

(2) Les dispositions du *Code criminel* s'appliquent que l'enquête visée à l'article 10 ait commencé ou non.

R.S., c. 19 (2nd Supp.), s. 24

32. Subsection 16(6) of the Act is repealed.

32. Le paragraphe 16(6) de la même loi est abrogé.

L.R., ch. 19 (2e suppl.), art. 24

R.S., c. 19 (2nd Supp.), s. 24

33. Subsection 20(2) of the Act is replaced by the following:

33. Le paragraphe 20(2) de la même loi est remplacé par ce qui suit :

L.R., ch. 19 (2e suppl.), art. 24

Copies

(2) Copies of any records referred to in subsection (1), made by any process of reproduction, on proof orally or by affidavit that they are true copies, are admissible in evidence in any proceedings under this Act and have the same probative force as the original.

Copies

(2) Les copies d'un document visé au paragraphe (1) obtenues au moyen de tout procédé de reproduction sont, lorsqu'il est démontré au moyen d'un témoignage oral ou d'un affidavit qu'il s'agit de copies conformes, admissibles en preuve dans toute procédure prévue par la présente loi et leur force probante est la même que celle des documents originaux.

2002, c. 16, s. 3

34. The definition "data" in section 30 of the Act is repealed.

34. La définition de « données », à l'article 30 de la même loi, est abrogée.

2002, ch. 16, art. 3

1999, c. 2, s. 12(1)

35. Paragraph 52(2)(*d*) of the Act is replaced by the following:

(*d*) made in the course of in-store or door-to-door selling to a person as ultimate user, or by communicating orally by any means of telecommunication to a person as ultimate user, or

35. L'alinéa 52(2)*d*) de la même loi est remplacé par ce qui suit :

d) sont données, au cours d'opérations de vente en magasin, par démarchage ou par communication orale faite par tout moyen de télécommunication, à un usager éventuel;

1999, ch. 2, par. 12(1)

1999, c. 2, s. 13

36. (1) Subsection 52.1(1) of the Act is replaced by the following:

36. (1) Le paragraphe 52.1(1) de la même loi est remplacé par ce qui suit :

1999, ch. 2, art. 13

Definition of "telemarketing"

52.1 (1) In this section, "telemarketing" means the practice of communicating orally by any means of telecommunication for the purpose of promoting, directly or indirectly, any business interest or the supply or use of a product.

Définition de « télémarketing »

52.1 (1) Au présent article, « télémarketing » s'entend de la pratique qui consiste à communiquer oralement par tout moyen de télécommunication pour promouvoir, directement ou indirectement, soit la fourniture ou l'usage d'un produit, soit des intérêts commerciaux quelconques.

1999, c. 2, s. 13

(2) Paragraph 52.1(2)(*a*) of the Act is replaced by the following:

(*a*) disclosure is made, in a fair and reasonable manner at the beginning of each communication, of the identity of the person on behalf of whom the communication is made, the nature of the business interest or product being promoted and the purposes of the communication;

(2) L'alinéa 52.1(2)*a*) de la même loi est remplacé par ce qui suit :

a) à la divulgation, d'une manière juste et raisonnable, au début de chaque communication, de l'identité de la personne pour le compte de laquelle la communication est effectuée, de la nature du produit ou des intérêts commerciaux dont la promotion est faite et du but de la communication;

1999, ch. 2, art. 13

1999, c. 2, s. 13

(3) Subsection 52.1(5) of the Act is replaced by the following:

Time of disclosure

(5) The disclosure of information referred to in paragraph (2)(*b*) or (*c*) or (3)(*b*) or (*c*) must be made during the course of a communication unless it is established by the accused that the information was disclosed within a reasonable time before the communication, by any means, and the information was not requested during the communication.

1999, c. 2, s. 22

37. Paragraph 74.03(1)(*d*) of the Act is replaced by the following:

(*d*) made in the course of in-store or door-to-door selling to a person as ultimate user, or by communicating orally by any means of telecommunication to a person as ultimate user, or

R.S., c. 30 (4th Supp.)

MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS ACT

38. The definitions "data" and "record" in subsection 2(1) of the *Mutual Legal Assistance in Criminal Matters Act* are replaced by the following:

"data" *« données »*

"data" means representations, including signs, signals or symbols, that are capable of being understood by an individual or processed by a computer system or other device;

"record" *« document »*

"record" means a medium on which data is registered or marked;

39. Section 12 of the Act is amended by adding the following after subsection (1):

Commissioner of Competition

(1.1) The judge may, in addition to or instead of a peace officer, authorize the Commissioner of Competition appointed under subsection 7(1) of the *Competition Act* or his or her authorized representative named in the warrant to execute the search warrant, in which case the Commissioner or his or her representative, as the case may be, has, in relation to the warrant, all of the powers and duties that are set out for a peace officer in this section and sections 13 and 14.

2000, c. 24, s. 61

40. Section 13.1 of the Act is repealed.

1999, ch. 2, art. 13

(3) Le paragraphe 52.1(5) de la même loi est remplacé par ce qui suit :

Moment de la divulgation

(5) La divulgation de renseignements visée aux alinéas (2)*b*) ou *c*) ou (3)*b*) ou *c*) doit être faite au cours d'une communication, sauf si l'accusé établit qu'elle a été faite dans un délai raisonnable antérieur à la communication, par n'importe quel moyen, et que les renseignements n'ont pas été demandés au cours de la communication.

1999, ch. 2, art. 22

37. L'alinéa 74.03(1)*d*) de la même loi est remplacé par ce qui suit :

d) sont données, au cours d'opérations de vente en magasin, par démarchage ou par communication orale faite par tout moyen de télécommunication, à un usager éventuel;

L.R., ch. 30 (4e suppl.)

LOI SUR L'ENTRAIDE JURIDIQUE EN MATIÈRE CRIMINELLE

38. Les définitions de « document » et « données », au paragraphe 2(1) de la *Loi sur l'entraide juridique en matière criminelle*, sont respectivement remplacées par ce qui suit :

« document » *"record"*

« document » Tout support sur lequel sont enregistrées ou inscrites des données.

« données » *"data"*

« données » Représentations, notamment signes, signaux ou symboles, qui peuvent être compris par une personne physique ou traités par un ordinateur ou un autre dispositif.

39. L'article 12 de la même loi est modifié par adjonction, après le paragraphe (1), de ce qui suit :

Commissaire de la concurrence

(1.1) Il peut également, en lieu et place ou en sus de l'agent de la paix, autoriser le commissaire de la concurrence nommé en vertu du paragraphe 7(1) de la *Loi sur la concurrence* ou son représentant autorisé qui est nommé dans le mandat à exécuter celui-ci et, le cas échéant, le commissaire ou son représentant a, eu égard au mandat, les attributions conférées à l'agent de la paix par le présent article et les articles 13 et 14.

2000, ch. 24, art. 61

40. L'article 13.1 de la même loi est abrogé.

41. The Act is amended by adding the following after section 16:

Other warrants

16.1 (1) A judge of the province to whom an application is made under subsection 11(2) may, in the manner provided for by the *Criminal Code*, issue a warrant, other than a warrant referred to in section 12, to use any device or investigative technique or do anything described in the warrant that would, if not authorized, constitute an unreasonable search or seizure in respect of a person or a person's property.

Criminal Code applies

(2) Subject to subsection (3), a warrant issued under subsection (1) may be obtained, issued and executed in the manner provided for by the *Criminal Code*, with any necessary modifications.

Exception — certain warrants

(3) Subsections 12(3) and (4) and sections 14 to 16 apply in respect of a warrant issued under subsection (1) — other than a warrant issued in the manner provided for by section 492.1 or 492.2 of the *Criminal Code* — and prevail over any provisions of the *Criminal Code* that are inconsistent with them.

Sending abroad — certain warrants

16.2 (1) If a judge referred to in subsection 16.1(1) issues a warrant in the manner provided for under section 492.1 or 492.2 of the *Criminal Code*, the judge must also order

(*a*) that the peace officer who executes the warrant send a record containing the data obtained under the warrant directly to the state or entity that made the request under subsection 11(1); or

(*b*) that sections 20 and 21 apply to the warrant with any necessary modifications.

Report

(2) The peace officer who executes the warrant must

(*a*) make a report concerning the execution of the warrant to the judge who issued the warrant or to another judge of the same court, accompanied by a general description of the data obtained under the warrant and, if the judge requires it, a record containing the data; and

(*b*) send a copy of the report to the Minister without delay.

41. La même loi est modifiée par adjonction, après l'article 16, de ce qui suit :

Autres mandats

16.1 (1) Tout juge d'une province auquel une requête est présentée en application du paragraphe 11(2) peut, de la manière prévue au *Code criminel*, délivrer un mandat, autre qu'un mandat visé à l'article 12, autorisant l'utilisation d'un dispositif ou d'une technique ou méthode d'enquête ou tout acte qui y est mentionné qui, sans cette autorisation, donnerait lieu à une fouille, perquisition ou saisie abusives à l'égard d'une personne ou d'un bien.

Application du *Code criminel*

(2) Sous réserve du paragraphe (3), le mandat peut être obtenu, délivré et exécuté de la manière prévue au *Code criminel*, avec les adaptations nécessaires.

Exception relative à certains mandats

(3) Les paragraphes 12(3) et (4) et les articles 14 à 16 s'appliquent à tout mandat délivré en vertu du paragraphe (1) — autre que celui délivré de la manière prévue aux articles 492.1 ou 492.2 du *Code criminel* —, et l'emportent sur toute disposition incompatible du *Code criminel*.

Transmission à l'étranger relative à certains mandats

16.2 (1) Un juge visé au paragraphe 16.1(1) qui délivre un mandat de la manière prévue aux articles 492.1 ou 492.2 du *Code criminel* ordonne aussi, selon le cas :

a) que l'agent de la paix qui exécute le mandat transmette directement à l'État ou à l'entité requérant visé au paragraphe 11(1) un document comportant les données obtenues;

b) que les articles 20 et 21 s'appliquent au mandat, avec les adaptations nécessaires.

Rapport

(2) L'agent de la paix qui exécute le mandat :

a) remet au juge ou à un autre juge du même tribunal un rapport d'exécution comportant une description générale des données obtenues en vertu du mandat et, si le juge l'exige, un document comportant les données;

b) envoie sans délai une copie du rapport au ministre.

Timing of report and sending abroad

(3) If the judge makes an order under paragraph (1)(*a*), the peace officer must make the report to the judge and send a record containing the data to the state or entity that made the request no later than five days after the day on which all of the data is obtained under the warrant.

Délai : rapport et transmission à l'étranger

(3) Dans le cas d'une ordonnance rendue en vertu de l'alinéa (1)*a*), l'agent de la paix est tenu de remettre le rapport au juge et de transmettre le document comportant les données à l'État ou à l'entité requérant au plus tard cinq jours après la date à laquelle elles ont toutes été obtenues en vertu du mandat.

42. The heading before section 17 of the Act is replaced by the following:

42. L'intertitre précédant l'article 17 de la même loi est remplacé par ce qui suit :

PRODUCTION ORDERS

ORDONNANCES DE COMMUNICATION

43. The Act is amended by adding the following after section 22:

43. La même loi est modifiée par adjonction, après l'article 22, de ce qui suit :

Application of *Criminal Code*

22.01 The *Criminal Code* applies, with any necessary modifications, in respect of an order made under subsection 22.03(1) in the manner provided for under any of sections 487.015 to 487.018 and 487.0191 of the *Criminal Code*, except to the extent that that Act is inconsistent with this Act.

Application du *Code criminel*

22.01 Le *Code criminel* s'applique, avec les adaptations nécessaires, aux ordonnances rendues en vertu du paragraphe 22.03(1) de la manière prévue à l'un des articles 487.015 à 487.018 et 487.0191 du *Code criminel*, sauf incompatibilité avec la présente loi.

Approval of request to obtain production

22.02 (1) If the Minister approves a request of a state or entity to obtain an order under this Act made in the manner provided for under any of sections 487.015 to 487.018 of the *Criminal Code* to require the production of a record containing data, the Minister must provide a competent authority with any documents or information necessary to apply for the order.

Autorisation

22.02 (1) Le ministre, s'il autorise la demande présentée par un État ou une entité en vue d'obtenir une ordonnance rendue sous le régime de la présente loi de la manière prévue à l'un des articles 487.015 à 487.018 du *Code criminel* pour exiger la communication d'un document comportant les données, fournit à l'autorité compétente les documents ou les renseignements nécessaires pour lui permettre de présenter une requête à cet effet.

Application for orders

(2) The competent authority must apply *ex parte* for an order made in the manner provided for under any of sections 487.015 to 487.018 and 487.0191 of the *Criminal Code* to a justice as defined in section 2 of the *Criminal Code*, a judge of a superior court of criminal jurisdiction as defined in that section or a judge of the Court of Quebec.

Requête

(2) L'autorité compétente présente une requête *ex parte*, en vue de l'obtention de l'ordonnance rendue de la manière prévue à l'un des articles 487.015 à 487.018 et 487.0191 du *Code criminel*, à un juge de paix au sens de l'article 2 du *Code criminel*, à un juge de la cour supérieure de juridiction criminelle au sens de cet article ou à un juge de la Cour du Québec.

Production and non-disclosure orders

22.03 (1) The justice or judge to whom the application is made may make an order in the manner provided for under any of sections 487.015 to 487.018 and 487.0191 of the *Criminal Code* if the conditions set out in that section have been met.

Ordonnance de communication et de non-divulgation

22.03 (1) Le juge de paix ou le juge saisi de la requête peut rendre l'ordonnance de la manière prévue à l'un des articles 487.015 à 487.018 et 487.0191 du *Code criminel* si les conditions énoncées dans l'article visé sont réunies.

Condition in order

(2) An order made in the manner provided for under any of sections 487.015 to 487.018 of the *Criminal Code* must require that a record containing the data be given to a designated person.

Précision

(2) L'ordonnance rendue de la manière prévue à l'un des articles 487.015 à 487.018 du *Code criminel* exige que soit présenté à une personne désignée le document comportant les données.

Sending abroad

22.04 (1) If the justice or judge makes an order in the manner provided for under any of sections 487.015 to 487.018 of the *Criminal Code*, the justice or judge must also order

(*a*) that the person designated in the order send a record containing the data directly to the state or entity that made the request under subsection 22.02(1); or

(*b*) that sections 20 and 21 apply to the order with any necessary modifications.

Transmission à l'étranger

22.04 (1) Le juge de paix ou le juge qui rend une ordonnance de la manière prévue à l'un des articles 487.015 à 487.018 du *Code criminel* ordonne aussi, selon le cas :

a) que la personne désignée dans l'ordonnance transmette directement à l'État ou à l'entité requérant visé au paragraphe 22.02(1) un document comportant les données obtenues;

b) que les articles 20 et 21 s'appliquent à l'ordonnance, avec les adaptations nécessaires.

Report

(2) The person designated in the order must

(*a*) make a report concerning the execution of the order to the justice or judge who made it — or to another justice for the same territorial division or another judge in the judicial district where the order was made — accompanied by a general description of the data contained in the record obtained under the order and, if the justice or judge requires it, a record containing the data; and

(*b*) send a copy of the report to the Minister without delay.

Rapport

(2) La personne désignée dans l'ordonnance :

a) remet au juge de paix ou au juge — ou à un autre juge de paix de la même circonscription territoriale ou à un autre juge du district judiciaire où l'ordonnance a été rendue — un rapport d'exécution comportant une description générale des données contenues dans le document obtenu en vertu de l'ordonnance et, si le juge de paix ou le juge l'exige, un document comportant les données;

b) envoie sans délai une copie du rapport au ministre.

Timing of report and sending abroad

(3) If the justice or judge makes an order under paragraph (1)(*a*), the person designated in the order must make the report to the justice or judge and send a record containing the data to the state or entity that made the request no later than five days after the day on which such a record is obtained under the order.

Délai : rapport et transmission à l'étranger

(3) Dans le cas d'une ordonnance rendue en vertu de l'alinéa (1)*a*), la personne désignée dans l'ordonnance est tenue de remettre le rapport au juge de paix ou au juge et de transmettre un document comportant les données à l'État ou à l'entité requérant au plus tard cinq jours après la date à laquelle il a été obtenu en vertu de l'ordonnance.

Offence

22.05 Section 487.0198 of the *Criminal Code* applies to everyone who is subject to an order made under subsection 22.03(1) in the manner provided for under any of sections 487.015 to 487.018 of the *Criminal Code*.

Infraction

22.05 L'article 487.0198 du *Code criminel* s'applique aux ordonnances rendues en vertu du paragraphe 22.03(1) de la manière prévue à l'un des articles 487.015 à 487.018 du *Code criminel*.

VIDEO LINK

TÉMOIN VIRTUEL

44. The Act is amended by adding the following after section 22.4:

44. La même loi est modifiée par adjonction, après l'article 22.4, de ce qui suit :

ARREST WARRANT

MANDAT D'ARRESTATION

45. The Act is amended by adding the following after section 23:

45. La même loi est modifiée par adjonction, après l'article 23, de ce qui suit :

EXAMINATION OF PLACE OR SITE

EXAMEN D'UN LIEU OU D'UN EMPLACEMENT

1999, c. 18, s. 120

46. Subsection 36(2) of the Act is replaced by the following:

46. Le paragraphe 36(2) de la même loi est remplacé par ce qui suit :

1999, ch. 18, art. 120

Probative value

(2) For the purpose of determining the probative value of a record or a copy of a record admitted in evidence under this Act, the trier of fact may examine the record or copy, receive evidence orally or by affidavit, or by a certificate or other statement pertaining to the record in which a person attests that the certificate or statement is made in conformity with the laws that apply to a state or entity, whether or not the certificate or statement is in the form of an affidavit attested to before an official of the state or entity, including evidence as to the circumstances in which the data contained in the record or copy was written, stored or reproduced, and draw any reasonable inference from the form or content of the record or copy.

(2) Le juge des faits peut, afin de décider de la force probante d'un document — ou de sa copie — admis en preuve en vertu de la présente loi, procéder à son examen ou recevoir une déposition verbale, un affidavit ou un certificat ou autre déclaration portant sur le document, fait, selon le signataire, conformément aux lois de l'État ou entité, qu'il soit fait en la forme d'un affidavit rempli devant un agent de l'État ou entité ou non, y compris une déposition quant aux circonstances de la rédaction, de l'enregistrement, de la mise en mémoire ou de la reproduction des données contenues dans le document ou la copie, et tirer de sa forme ou de son contenu toute conclusion fondée.

Force probante

1999, c. 18, s. 127

47. (1) Subsection 44(1) of the French version of the Act is replaced by the following:

47. (1) Le paragraphe 44(1) de la version française de la même loi est remplacé par ce qui suit :

1999, ch. 18, art. 127

Documents protégés

44. (1) Sous réserve du paragraphe 38(2), les documents transmis au ministre par un État ou entité en conformité avec une demande canadienne sont protégés. Jusqu'à ce qu'ils aient été, en conformité avec les conditions attachées à leur transmission au ministre, rendus publics ou révélés au cours ou aux fins d'une déposition devant un tribunal, il est interdit de communiquer à quiconque ces documents, leur teneur ou des données qu'ils contiennent.

44. (1) Sous réserve du paragraphe 38(2), les documents transmis au ministre par un État ou entité en conformité avec une demande canadienne sont protégés. Jusqu'à ce qu'ils aient été, en conformité avec les conditions attachées à leur transmission au ministre, rendus publics ou révélés au cours ou aux fins d'une déposition devant un tribunal, il est interdit de communiquer à quiconque ces documents, leur teneur ou des données qu'ils contiennent.

Documents protégés

(2) Subsection 44(2) of the English version of the Act is replaced by the following:

(2) Le paragraphe 44(2) de la version anglaise de la même loi est remplacé par ce qui suit :

Privilege

(2) No person in possession of a record mentioned in subsection (1) or of a copy of such a record, or who has knowledge of any data contained in the record, shall be required, in

(2) No person in possession of a record mentioned in subsection (1) or of a copy of such a record, or who has knowledge of any data contained in the record, shall be required, in

Privilege

connection with any legal proceedings, to produce the record or copy or to give evidence relating to any data that is contained in it.

connection with any legal proceedings, to produce the record or copy or to give evidence relating to any data that is contained in it.

PART 3

COORDINATING AMENDMENTS AND COMING INTO FORCE

COORDINATING AMENDMENTS

PARTIE 3

DISPOSITIONS DE COORDINATION ET ENTRÉE EN VIGUEUR

DISPOSITIONS DE COORDINATION

2010, c. 23

48. (1) In this section, "other Act" means *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act.*

48. (1) Au présent article, « autre loi » s'entend de la *Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications.*

2010, ch. 23

(2) If subsection 30(1) of this Act comes into force before subsection 70(1) of the other Act, then that subsection 70(1) is repealed.

(2) Si le paragraphe 30(1) de la présente loi entre en vigueur avant le paragraphe 70(1) de l'autre loi, ce paragraphe 70(1) est abrogé.

(3) If subsection 70(1) of the other Act comes into force on the same day as subsection 30(1) of this Act, then that subsection 70(1) is deemed to have come into force before that subsection 30(1).

(3) Si l'entrée en vigueur du paragraphe 70(1) de l'autre loi et celle du paragraphe 30(1) de la présente loi sont concomitantes, ce paragraphe 70(1) est réputé être entré en vigueur avant ce paragraphe 30(1).

(4) If subsection 70(2) of the other Act comes into force before subsection 30(2) of this Act, then that subsection 30(2) is replaced by the following:

(4) Si le paragraphe 70(2) de l'autre loi entre en vigueur avant le paragraphe 30(2) de la présente loi, ce paragraphe 30(2) est remplacé par ce qui suit :

(2) The definition "data" in subsection 2(1) of the Act is replaced by the following:

(2) La définition de « données », au paragraphe 2(1) de la même loi, est remplacée par ce qui suit :

"data" « *données* »

"data" means representations, including signs, signals or symbols, that are capable of being understood by an individual or processed by a computer system or other device;

« données » Représentations, notamment signes, signaux ou symboles, qui peuvent être compris par une personne physique ou traités par un ordinateur ou un autre dispositif.

« données » "*data*"

(5) If subsection 30(2) of this Act comes into force before subsection 70(2) of the other Act, then that subsection 70(2) is replaced by the following:

(5) Si le paragraphe 30(2) de la présente loi entre en vigueur avant le paragraphe 70(2) de l'autre loi, ce paragraphe 70(2) est remplacé par ce qui suit :

(2) Subsection 2(1) of the Act is amended by adding the following in alphabetical order:

"electronic message" means a message sent by any means of telecommunication, including a text, sound, voice or image message;

"locator" means a name or information used to identify a source of data on a computer system, and includes a URL;

"sender information" means the part of an electronic message — including the data relating to source, routing, addressing or signalling — that identifies or purports to identify the sender or the origin of the message;

"subject matter information" means the part of an electronic message that purports to summarize the contents of the message or to give an indication of them;

(2) Le paragraphe 2(1) de la même loi est modifié par adjonction, selon l'ordre alphabétique, de ce qui suit :

« localisateur » Toute chaîne de caractères normalisés ou tout renseignement servant à identifier une source de données dans un ordinateur, notamment l'adresse URL.

« message électronique » Message envoyé par tout moyen de télécommunication, notamment un message alphabétique, sonore, vocal ou image.

« objet » Partie du message électronique qui contient des renseignements censés résumer le contenu du message ou donner une indication à l'égard de ce contenu.

« renseignements sur l'expéditeur » Partie du message électronique, notamment les données liées à la source, au routage, à l'adressage ou à la signalisation, qui contient ou qui est censée contenir l'identité de l'expéditeur ou l'origine du message.

"electronic message" « *message électronique* »

"locator" « *localisateur* »

"sender information" « *renseignements sur l'expéditeur* »

"subject matter information" « *objet* »

« localisateur » "*locator*"

« message électronique » "*electronic message*"

« objet » "*subject matter information*"

« renseignements sur l'expéditeur » "*sender information*"

(6) If subsection 70(2) of the other Act comes into force on the same day as subsection 30(2) of this Act, then that subsection 70(2) is deemed to have come into force before that subsection 30(2) and subsection (4) applies as a consequence.

(6) Si l'entrée en vigueur du paragraphe 70(2) de l'autre loi et celle du paragraphe 30(2) de la présente loi sont concomitantes, ce paragraphe 70(2) est réputé être entré en vigueur avant ce paragraphe 30(2), le paragraphe (4) s'appliquant en conséquence.

(7) If section 71 of the other Act comes into force before section 32 of this Act, then that section 32 is repealed.

(7) Si l'article 71 de l'autre loi entre en vigueur avant l'article 32 de la présente loi, cet article 32 est abrogé.

(8) If section 32 of this Act comes into force before section 71 of the other Act, then that section 71 is repealed.

(8) Si l'article 32 de la présente loi entre en vigueur avant l'article 71 de l'autre loi, cet article 71 est abrogé.

(9) If section 71 of the other Act comes into force on the same day as section 32 of this Act, then that section 71 is deemed to have come into force before that section 32 and subsection (7) applies as a consequence.

(9) Si l'entrée en vigueur de l'article 71 de l'autre loi et celle de l'article 32 de la présente loi sont concomitantes, cet article 71 est réputé être entré en vigueur avant cet article 32, le paragraphe (7) s'appliquant en conséquence.

(10) If section 72 of the other Act comes into force before section 33 of this Act, then that section 33 is repealed.

(10) Si l'article 72 de l'autre loi entre en vigueur avant l'article 33 de la présente loi, cet article 33 est abrogé.

(11) If section 33 of this Act comes into force before section 72 of the other Act, then that section 72 is repealed.

(11) Si l'article 33 de la présente loi entre en vigueur avant l'article 72 de l'autre loi, cet article 72 est abrogé.

(12) If section 72 of the other Act comes into force on the same day as section 33 of this Act, then that section 72 is deemed to have come into force before that section 33 and subsection (10) applies as a consequence.

(12) Si l'entrée en vigueur de l'article 72 de l'autre loi et celle de l'article 33 de la présente loi sont concomitantes, cet article 72 est réputé être entré en vigueur avant cet article 33, le paragraphe (10) s'appliquant en conséquence.

(13) If section 35 of this Act comes into force before subsection 74(2) of the other Act, then that subsection 74(2) is repealed.

(13) Si l'article 35 de la présente loi entre en vigueur avant le paragraphe 74(2) de l'autre loi, ce paragraphe 74(2) est abrogé.

(14) If subsection 74(2) of the other Act comes into force on the same day as section 35 of this Act, then that subsection 74(2) is deemed to have come into force before that section 35.

(14) Si l'entrée en vigueur du paragraphe 74(2) de l'autre loi et celle de l'article 35 de la présente loi sont concomitantes, ce paragraphe 74(2) est réputé être entré en vigueur avant cet article 35.

(15) If subsection 36(1) of this Act comes into force before subsection 76(1) of the other Act, then that subsection 76(1) is repealed.

(15) Si le paragraphe 36(1) de la présente loi entre en vigueur avant le paragraphe 76(1) de l'autre loi, ce paragraphe 76(1) est abrogé.

(16) If subsection 76(1) of the other Act comes into force on the same day as subsection 36(1) of this Act, then that subsection 76(1) is deemed to have come into force before that subsection 36(1).

(16) Si l'entrée en vigueur du paragraphe 76(1) de l'autre loi et celle du paragraphe 36(1) de la présente loi sont concomitantes, ce paragraphe 76(1) est réputé être entré en vigueur avant ce paragraphe 36(1).

(17) If subsection 76(2) of the other Act comes into force before subsection 36(2) of this Act, then that subsection 36(2) is repealed.

(17) Si le paragraphe 76(2) de l'autre loi entre en vigueur avant le paragraphe 36(2) de la présente loi, ce paragraphe 36(2) est abrogé.

(18) If subsection 36(2) of this Act comes into force before subsection 76(2) of the other Act, then that subsection 76(2) is repealed.

(18) Si le paragraphe 36(2) de la présente loi entre en vigueur avant le paragraphe 76(2) de l'autre loi, ce paragraphe 76(2) est abrogé.

(19) If subsection 76(2) of the other Act comes into force on the same day as subsection 36(2) of this Act, then that subsection 76(2) is deemed to have come into force before that subsection 36(2) and subsection (17) applies as a consequence.

(19) Si l'entrée en vigueur du paragraphe 76(2) de l'autre loi et celle du paragraphe 36(2) de la présente loi sont concomitantes, ce paragraphe 76(2) est réputé être entré en vigueur avant ce paragraphe 36(2), le paragraphe (17) s'appliquant en conséquence.

(20) If subsection 76(3) of the other Act comes into force before subsection 36(3) of this Act, then that subsection 36(3) is repealed.

(20) Si le paragraphe 76(3) de l'autre loi entre en vigueur avant le paragraphe 36(3) de la présente loi, ce paragraphe 36(3) est abrogé.

(21) If subsection 36(3) of this Act comes into force before subsection 76(3) of the other Act, then that subsection 76(3) is repealed.

(21) Si le paragraphe 36(3) de la présente loi entre en vigueur avant le paragraphe 76(3) de l'autre loi, ce paragraphe 76(3) est abrogé.

(22) If subsection 76(3) of the other Act comes into force on the same day as subsection 36(3) of this Act, then that subsection 76(3) is deemed to have come into force before that subsection 36(3) and subsection (20) applies as a consequence.

(22) Si l'entrée en vigueur du paragraphe 76(3) de l'autre loi et celle du paragraphe 36(3) de la présente loi sont concomitantes, ce paragraphe 76(3) est réputé être entré en vigueur avant ce paragraphe 36(3), le paragraphe (20) s'appliquant en conséquence.

(23) If section 37 of this Act comes into force before section 78 of the other Act, then that section 78 is repealed.

(23) Si l'article 37 de la présente loi entre en vigueur avant l'article 78 de l'autre loi, cet article 78 est abrogé.

(24) If section 78 of the other Act comes into force on the same day as section 37 of this Act, then that section 78 is deemed to have come into force before that section 37.

(24) Si l'entrée en vigueur de l'article 78 de l'autre loi et celle de l'article 37 de la présente loi sont concomitantes, cet article 78 est réputé être entré en vigueur avant cet article 37.

Bill C-12

49. If Bill C-12, introduced in the 1st session of the 41st Parliament and entitled the *Safeguarding Canadians' Personal Information Act*, receives royal assent, then, on the first day on which both section 8 of that Act and section 23 of the *Investigating and Preventing Criminal Electronic Communications Act*, as enacted by section 2 of this Act, are in force, that section 23 is replaced by the following:

Projet de loi C-12

49. En cas de sanction du projet de loi C-12, déposé au cours de la 1re session de la 41e législature et intitulé *Loi protégeant les renseignements personnels des Canadiens*, dès le premier jour où l'article 8 de cette loi et l'article 23 de la *Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention*, édictée par l'article 2 de la présente loi, sont tous deux en vigueur, cet article 23 est remplacé par ce qui suit :

Deemed nature of information

23. Personal information, as defined in subsection 2(1) of the *Personal Information Protection and Electronic Documents Act*, that is provided under subsection 16(1) or 17(1) is deemed, for the purposes of section 7.5 and subsections 9(2.1) to (2.4) of that Act, to be disclosed under subparagraph 7(3)(*c.1*)(i) or (ii), and not under paragraph 7(3)(*i*), of that Act. This section operates despite the other provisions of Part 1 of that Act.

Dérogation

23. Pour l'application de l'article 7.5 et des paragraphes 9(2.1) à (2.4) de la *Loi sur la protection des renseignements personnels et les documents électroniques*, les renseignements personnels au sens du paragraphe 2(1) de cette loi qui sont fournis au titre des paragraphes 16(1) ou 17(1) sont réputés être communiqués au titre des sous-alinéas 7(3)*c.1*)(i) ou (ii) de cette loi et non de son alinéa 7(3)*i*). Le présent article s'applique malgré les autres dispositions de la partie 1 de la même loi.

COMING INTO FORCE

ENTRÉE EN VIGUEUR

Order in council

50. (1) Subject to subsection (2), the provisions of this Act, other than sections 3 to 5, 9, 13, 14, 48 and 49, come into force on a day or days to be fixed by order of the Governor in Council.

Décret

50. (1) Sous réserve du paragraphe (2), les dispositions de la présente loi, à l'exception des articles 3 à 5, 9, 13, 14, 48 et 49, entrent en vigueur à la date ou aux dates fixées par décret.

Order in council

(2) The provisions of the *Investigating and Preventing Criminal Electronic Communications Act*, as enacted by section 2, come into force on a day or days to be fixed by order of the Governor in Council.

Décret

(2) Les dispositions de la *Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention*, édictée par l'article 2, entrent en vigueur à la date ou aux dates fixées par décret.

SCHEDULE
(Section 2)

SCHEDULE 1
(Subsections 5(1) and (4) and 14(2))

EXCLUSIONS FROM THE APPLICATION OF THE ACT

PART 1

1. A telecommunications service intended principally for the use of its provider and the provider's household or employees and not by the public.

2. A telecommunications service intended principally for the sale or purchase of goods or services other than telecommunications services to the public.

3. A telecommunications service provided by a financial institution, as defined in section 2 of the *Bank Act*, that enables the business of banking, the trust, loan or insurance business, the business of a cooperative credit society or the business of dealing in securities or other business primarily related to the business of providing financial services.

PART 2

1. Telecommunications service providers whose principal function is operating a registered charity within the meaning of the *Income Tax Act*, other than any service provider in a class listed in Schedule 2, or operating an educational institution other than a post-secondary institution, or operating a hospital, a place of worship, a retirement home or a telecommunications research network, only in respect of telecommunications services that they provide ancillary to their principal function.

2. Telecommunications service providers that are also broadcasting undertakings, as defined in subsection 2(1) of the *Broadcasting Act*, only in respect of broadcasting.

ANNEXE
(article 2)

ANNEXE 1
(paragraphes 5(1) et (4) et 14(2))

NON-APPLICATION DE LA LOI

PARTIE 1

1. Services de télécommunication destinés principalement à leur fournisseur, aux membres de sa famille ou à ses employés, et non au public.

2. Services de télécommunication destinés principalement à la vente ou à l'achat par le public de biens ou de services, autres que des services de télécommunication.

3. Services de télécommunication fournis par une institution financière, au sens de l'article 2 de la *Loi sur les banques*, qui permettent à quiconque de se livrer à des activités bancaires ou à des activités fiduciaires, de prêt ou d'assurance, aux activités d'une société coopérative de crédit ou de faire le commerce des valeurs mobilières, ou encore, de toute autre manière, de se livrer à des activités ayant principalement trait à la prestation de services financiers.

PARTIE 2

1. Télécommunicateurs dont l'activité principale consiste à exploiter un organisme de bienfaisance enregistré, au sens de la *Loi de l'impôt sur le revenu* — sauf s'ils appartiennent à l'une ou l'autre des catégories figurant à l'annexe 2 — un établissement d'enseignement autre qu'un établissement d'enseignement postsecondaire, un hôpital, un lieu de culte, une maison de retraite ou un réseau de recherche sur les télécommunications, uniquement pour ce qui est des services de télécommunication qu'ils fournissent de façon accessoire à leur activité principale.

2. Télécommunicateurs qui sont également des entreprises de radiodiffusion au sens du paragraphe 2(1) de la *Loi sur la radiodiffusion*, uniquement pour ce qui est de leur activité de radiodiffusion.

SCHEDULE 2
(Subsections 5(2) to (4) and 14(2) and Schedule 1)

PARTIAL APPLICATION OF THE ACT

PART 1

1. Telecommunications service providers that transmit communications on behalf of other telecommunications service providers, that do not modify particular communications transmitted and that do not authenticate the end users of the telecommunications services of those other service providers, only in respect of the telecommunications services provided to the other service providers.

PART 2

1. Telecommunications service providers whose principal business or function is operating a post-secondary educational institution, a library, a community centre, a restaurant or an establishment that provides lodgings or residential accommodations, such as a hotel, an apartment building or a condominium, only in respect of telecommunications services that they provide ancillary to their principal business or function.

ANNEXE 2
(paragraphes 5(2) à (4) et 14(2) et annexe 1)

APPLICATION PARTIELLE DE LA LOI

PARTIE 1

1. Télécommunicateurs qui transmettent des communications pour le compte d'autres télécommunicateurs et qui ne modifient pas les communications transmises et n'authentifient pas les utilisateurs finaux des services de télécommunication des autres télécommunicateurs, uniquement pour ce qui est des services de télécommunication fournis à ces télécommunicateurs.

PARTIE 2

1. Télécommunicateurs dont l'entreprise ou l'activité principale consiste à exploiter un établissement d'enseignement postsecondaire, une bibliothèque, un centre communautaire, un restaurant, un établissement qui offre des services d'hébergement ou de logement, notamment un hôtel, un immeuble d'habitation ou un immeuble d'habitation en copropriété, uniquement pour ce qui est des services de télécommunication qu'ils fournissent de façon accessoire à leur activité principale.

Published under authority of the Speaker of the House of Commons

Available from:
Publishing and Depository Services
Public Works and Government Services Canada
Ottawa, Ontario K1A 0S5
Telephone: 613-941-5995 or 1-800-635-7943
Fax: 613-954-5779 or 1-800-565-7757
publications@tpsgc-pwgsc.gc.ca
http://publications.gc.ca

Publié avec l'autorisation du président de la Chambre des communes

Disponible auprès de :
Les Éditions et Services de dépôt
Travaux publics et Services gouvernementaux Canada
Ottawa (Ontario) K1A 0S5
Téléphone : 613-941-5995 ou 1-800-635-7943
Télécopieur : 613-954-5779 ou 1-800-565-7757
publications@tpsgc-pwgsc.gc.ca
http://publications.gc.ca

EXPLANATORY NOTES

Criminal Code

Clause 6: (1) Relevant portion of subsection 164.1(1):

164.1 (1) If a judge is satisfied by information on oath that there are reasonable grounds to believe that there is material — namely child pornography within the meaning of section 163.1, a voyeuristic recording within the meaning of subsection 164(8) or data within the meaning of subsection 342.1(2) that makes child pornography or a voyeuristic recording available — that is stored on and made available through a computer system within the meaning of subsection 342.1(2) that is within the jurisdiction of the court, the judge may order the custodian of the computer system to

(2) Existing text of subsection 164.1(5):

(5) If the court is satisfied, on a balance of probabilities, that the material is child pornography within the meaning of section 163.1, a voyeuristic recording within the meaning of subsection 164(8) or data within the meaning of subsection 342.1(2) that makes child pornography or the voyeuristic recording available, it may order the custodian of the computer system to delete the material.

(3) Existing text of subsection 164.1(7):

(7) If the court is not satisfied that the material is child pornography within the meaning of section 163.1, a voyeuristic recording within the meaning of subsection 164(8) or data within the meaning of subsection 342.1(2) that makes child pornography or the voyeuristic recording available, the court shall order that the electronic copy be returned to the custodian and terminate the order under paragraph (1)(*b*).

Clause 7: (1) and (2) Relevant portion of the definition:

"offence" means an offence contrary to, any conspiracy or attempt to commit or being an accessory after the fact in relation to an offence contrary to, or any counselling in relation to an offence contrary to

(*a*) any of the following provisions of this Act, namely,

...

(lviii) section 342.2 (possession of device to obtain computer service),

...

(lxvii) section 372 (false messages),

Clause 8: New.

Clause 9: Existing text of section 184.4:

184.4 A peace officer may intercept, by means of any electro-magnetic, acoustic, mechanical or other device, a private communication where

(*a*) the peace officer believes on reasonable grounds that the urgency of the situation is such that an authorization could not, with reasonable diligence, be obtained under any other provision of this Part;

(*b*) the peace officer believes on reasonable grounds that such an interception is immediately necessary to prevent an unlawful act that would cause serious harm to any person or to property; and

NOTES EXPLICATIVES

Code criminel

Article 6: (1) Texte du passage visé du paragraphe 164.1(1):

164.1 (1) Le juge peut, s'il est convaincu par une dénonciation sous serment qu'il y a des motifs raisonnables de croire qu'il existe une matière — constituant de la pornographie juvénile au sens de l'article 163.1, un enregistrement voyeuriste au sens du paragraphe 164(8) ou des données au sens du paragraphe 342.1(2) rendant la pornographie juvénile ou l'enregistrement voyeuriste accessible — qui est emmagasinée et rendue accessible au moyen d'un ordinateur au sens de ce paragraphe, situé dans le ressort du tribunal, ordonner au gardien de l'ordinateur:

(2) Texte du paragraphe 164.1(5):

(5) Si le tribunal est convaincu, selon la prépondérance des probabilités, que la matière constitue de la pornographie juvénile au sens de l'article 163.1, un enregistrement voyeuriste au sens du paragraphe 164(8) ou des données au sens du paragraphe 342.1(2) qui rendent la pornographie juvénile ou l'enregistrement voyeuriste accessible, il peut ordonner au gardien de l'ordinateur de l'effacer.

(3) Texte du paragraphe 164.1(7):

(7) Si le tribunal n'est pas convaincu que la matière constitue de la pornographie juvénile au sens de l'article 163.1, un enregistrement voyeuriste au sens du paragraphe 164(8) ou des données au sens du paragraphe 342.1(2) qui rendent la pornographie juvénile ou l'enregistrement voyeuriste accessible, il doit ordonner que la copie électronique soit remise au gardien de l'ordinateur et mettre fin à l'ordonnance visée à l'alinéa (1)*b*).

Article 7: (1) et (2) Texte du passage visé de la définition:

« infraction » Infraction, complot ou tentative de commettre une infraction, complicité après le fait ou le fait de conseiller à une autre personne de commettre une infraction en ce qui concerne:

a) l'une des dispositions suivantes de la présente loi:

[...]

(lviii) l'article 342.2 (possession de moyens permettant d'utiliser un service d'ordinateur),

[...]

(lxvii) l'article 372 (faux messages),

Article 8: Nouveau.

Article 9: Texte de l'article 184.4:

184.4 L'agent de la paix peut intercepter, au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, une communication privée si les conditions suivantes sont réunies:

a) il a des motifs raisonnables de croire que l'urgence de la situation est telle qu'une autorisation ne peut, avec toute la diligence raisonnable, être obtenue sous le régime de la présente partie;

b) il a des motifs raisonnables de croire qu'une interception immédiate est nécessaire pour empêcher un acte illicite qui causerait des dommages sérieux à une personne ou un bien;

(*c*) either the originator of the private communication or the person intended by the originator to receive it is the person who would perform the act that is likely to cause the harm or is the victim, or intended victim, of the harm.

Clause 10: New.

Clause 11: New.

Clause 12: New.

Clause 13: (1) Existing text of subsection 195(1):

195. (1) The Minister of Public Safety and Emergency Preparedness shall, as soon as possible after the end of each year, prepare a report relating to

(*a*) authorizations for which he and agents to be named in the report who were specially designated in writing by him for the purposes of section 185 made application, and

(*b*) authorizations given under section 188 for which peace officers to be named in the report who were specially designated by him for the purposes of that section made application,

and interceptions made thereunder in the immediately preceding year.

(2) Relevant portion of subsection 195(2):

(2) The report referred to in subsection (1) shall, in relation to authorizations and interceptions made thereunder, set out

(3) New.

(4) Relevant portion of subsection 195(3):

(3) The report referred to in subsection (1) shall, in addition to the information referred to in subsection (2), set out

(5) Existing text of subsection 195(5):

(5) The Attorney General of each province shall, as soon as possible after the end of each year, prepare and publish or otherwise make available to the public a report relating to

(*a*) authorizations for which he and agents specially designated in writing by him for the purposes of section 185 made application, and

(*b*) authorizations given under section 188 for which peace officers specially designated by him for the purposes of that section made application,

and interceptions made thereunder in the immediately preceding year setting out, with such modifications as the circumstances require, the information described in subsections (2) and (3).

Clause 14: New.

Clause 15: Existing text of subsection 318(4):

(4) In this section, "identifiable group" means any section of the public distinguished by colour, race, religion, ethnic origin or sexual orientation.

Clause 16: Existing text of the definition:

"identifiable group" has the same meaning as in section 318;

c) l'auteur de la communication ou la personne à laquelle celui-ci la destine est soit la victime ou la personne visée, soit la personne dont les actes sont susceptibles de causer les dommages.

Article 10 : Nouveau.

Article 11 : Nouveau.

Article 12 : Nouveau.

Article 13 : (1) Texte du paragraphe 195(1) :

195. (1) Le ministre de la Sécurité publique et de la Protection civile établit, chaque année, aussitôt que possible, un rapport relatif :

a) aux autorisations dont lui-même et les mandataires, dont le nom doit apparaître au rapport, spécialement désignés par lui, par écrit, pour l'application de l'article 185 ont fait la demande;

b) aux autorisations données en vertu de l'article 188 qui ont été demandées par des agents de la paix, dont le nom doit apparaître au rapport, spécialement désignés par lui pour l'application de cet article,

et aux interceptions faites en vertu de ces autorisations au cours de l'année précédente.

(2) Texte du passage visé du paragraphe 195(2) :

(2) Le rapport mentionné au paragraphe (1) indique, en ce qui concerne les autorisations et les interceptions faites en vertu de celles-ci :

(3) Nouveau.

(4) Texte du passage visé du paragraphe 195(3) :

(3) Le rapport mentionné au paragraphe (1) contient, outre les renseignements mentionnés au paragraphe (2) :

(5) Texte du paragraphe 195(5) :

(5) Le procureur général de chaque province établit et publie chaque année, aussitôt que possible, ou autrement met à la disposition du public, un rapport relatif :

a) aux autorisations dont lui-même et les mandataires spécialement désignés par lui, par écrit, pour l'application de l'article 185 ont fait la demande;

b) aux autorisations données en vertu de l'article 188 qui ont été demandées par des agents de la paix spécialement désignés par lui pour l'application de cet article,

et aux interceptions faites en vertu de ces autorisations au cours de l'année précédente, contenant les renseignements visés aux paragraphes (2) et (3), compte tenu des adaptations de circonstance.

Article 14 : Nouveau.

Article 15 : Texte du paragraphe 318(4) :

(4) Au présent article, « groupe identifiable » désigne toute section du public qui se différencie des autres par la couleur, la race, la religion, l'origine ethnique ou l'orientation sexuelle.

Article 16 : Texte de la définition :

« groupe identifiable » A le sens que lui donne l'article 318.

Clause 17: (1) Relevant portion of subsection 320.1(1):

320.1 (1) If a judge is satisfied by information on oath that there are reasonable grounds for believing that there is material that is hate propaganda within the meaning of subsection 320(8) or data within the meaning of subsection 342.1(2) that makes hate propaganda available, that is stored on and made available to the public through a computer system within the meaning of subsection 342.1(2) that is within the jurisdiction of the court, the judge may order the custodian of the computer system to

(2) Existing text of subsection 320.1(5):

(5) If the court is satisfied, on a balance of probabilities, that the material is available to the public and is hate propaganda within the meaning of subsection 320(8) or data within the meaning of subsection 342.1(2) that makes hate propaganda available, it may order the custodian of the computer system to delete the material.

(3) Existing text of subsection 320.1(7):

(7) If the court is not satisfied that the material is available to the public and is hate propaganda within the meaning of subsection 320(8) or data within the meaning of subsection 342.1(2) that makes hate propaganda available, the court shall order that the electronic copy be returned to the custodian and terminate the order under paragraph (1)(*b*).

Clause 18: (1) Relevant portion of subsection 326(1):

326. (1) Every one commits theft who fraudulently, maliciously, or without colour of right,

...

(*b*) uses any telecommunication facility or obtains any telecommunication service.

(2) Existing text of subsection 326(2):

(2) In this section and section 327, "telecommunication" means any transmission, emission or reception of signs, signals, writing, images or sounds or intelligence of any nature by wire, radio, visual or other electromagnetic system.

Clause 19: Existing text of section 327:

327. (1) Every one who, without lawful excuse, the proof of which lies on him, manufactures, possesses, sells or offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for obtaining the use of any telecommunication facility or service, under circumstances that give rise to a reasonable inference that the device has been used or is or was intended to be used to obtain the use of any telecommunication facility or service without payment of a lawful charge therefor, is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years.

(2) Where a person is convicted of an offence under subsection (1) or paragraph 326(1)(*b*), any instrument or device in relation to which the offence was committed or the possession of which constituted the offence, on such conviction, in addition to any punishment that is imposed, may be ordered forfeited to Her Majesty, whereupon it may be disposed of as the Attorney General directs.

(3) No order for forfeiture shall be made under subsection (2) in respect of telephone, telegraph or other communication facilities or equipment owned by a person engaged in providing telephone, telegraph or other communication service to the public or forming part of the telephone, telegraph or other

Article 17: (1) Texte du passage visé du paragraphe 320.1(1):

320.1 (1) Le juge peut, s'il est convaincu par une dénonciation sous serment qu'il y a des motifs raisonnables de croire qu'il existe une matière — qui constitue de la propagande haineuse au sens du paragraphe 320(8) ou contient des données, au sens du paragraphe 342.1(2), qui rendent la propagande haineuse accessible — qui est emmagasinée et rendue accessible au public au moyen d'un ordinateur au sens du paragraphe 342.1(2) situé dans le ressort du tribunal, ordonner au gardien de l'ordinateur:

(2) Texte du paragraphe 320.1(5):

(5) Si le tribunal est convaincu, selon la prépondérance des probabilités, que la matière est accessible au public et constitue de la propagande haineuse au sens du paragraphe 320(8) ou contient des données, au sens du paragraphe 342.1(2), qui rendent la propagande haineuse accessible, il peut ordonner au gardien de l'ordinateur de l'effacer.

(3) Texte du paragraphe 320.1(7):

(7) Si le tribunal n'est pas convaincu que la matière est accessible au public et constitue de la propagande haineuse au sens du paragraphe 320(8) ou contient des données, au sens du paragraphe 342.1(2), qui rendent la propagande haineuse accessible, il doit ordonner que la copie électronique soit remise au gardien de l'ordinateur et mettre fin à l'ordonnance visée à l'alinéa (1)*b*).

Article 18: (1) Texte du passage visé du paragraphe 326(1):

326. (1) Commet un vol quiconque, frauduleusement, malicieusement ou sans apparence de droit:

[...]

b) soit se sert d'installations ou obtient un service en matière de télécommunication.

(2) Texte du paragraphe 326(2):

(2) Au présent article et à l'article 327, « télécommunication » désigne toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de renseignements de toute nature par fil, radioélectricité, optique ou autres systèmes électromagnétiques.

Article 19: Texte de l'article 327:

327. (1) Quiconque, sans excuse légitime, dont la preuve lui incombe, fabrique, possède, vend ou offre en vente ou écoule des instruments ou des pièces particulièrement utiles pour utiliser des installations ou obtenir un service en matière de télécommunication, dans des circonstances qui permettent raisonnablement de conclure qu'ils ont été utilisés, sont destinés ou ont été destinés à l'être à cette fin, sans acquittement des droits exigibles, est coupable d'un acte criminel et passible d'un emprisonnement maximal de deux ans.

(2) Lorsqu'une personne est déclarée coupable d'une infraction prévue au paragraphe (1) ou à l'alinéa 326(1)*b*), tout instrument au moyen duquel l'infraction a été commise ou dont la possession a constitué l'infraction peut, après cette déclaration de culpabilité et en plus de toute peine qui est imposée, être par ordonnance confisqué au profit de Sa Majesté, après quoi il peut en être disposé conformément aux instructions du procureur général.

(3) Aucune ordonnance de confiscation ne peut être rendue en vertu du paragraphe (2) relativement à des installations ou du matériel de communications téléphoniques, télégraphiques ou autres qui sont la propriété d'une personne fournissant au public un service de communications téléphoniques,

communication service or system of such a person by means of which an offence under subsection (1) has been committed if such person was not a party to the offence.

Clause 20: (1) Existing text of subsection 342.1(1):

342.1 (1) Every one who, fraudulently and without colour of right,

(*a*) obtains, directly or indirectly, any computer service,

(*b*) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,

(*c*) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (*a*) or (*b*) or an offence under section 430 in relation to data or a computer system, or

(*d*) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (*a*), (*b*) or (*c*)

is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

(2) and (3) Existing text of the definitions:

"computer password" means any data by which a computer service or computer system is capable of being obtained or used;

"computer program" means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

"computer service" includes data processing and the storage or retrieval of data;

"computer system" means a device that, or a group of interconnected or related devices one or more of which,

(*a*) contains computer programs or other data, and

(*b*) pursuant to computer programs,

(i) performs logic and control, and

(ii) may perform any other function;

"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system;

(4) New.

Clause 21: (1) Existing text of subsections 342.2(1) and (2):

342.2 (1) Every person who, without lawful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for committing an offence under section 342.1, under circumstances that give rise to a reasonable inference that the instrument, device or component has been used or is or was intended to be used to commit an offence contrary to that section,

(*a*) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or

(*b*) is guilty of an offence punishable on summary conviction.

télégraphiques ou autres ou qui font partie du service ou réseau de communications téléphoniques, télégraphiques ou autres d'une telle personne et au moyen desquels une infraction prévue au paragraphe (1) a été commise, si cette personne n'a pas participé à l'infraction.

Article 20 : (1) Texte du paragraphe 342.1(1) :

342.1 (1) Quiconque, frauduleusement et sans apparence de droit :

a) directement ou indirectement, obtient des services d'ordinateur;

b) au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, directement ou indirectement, intercepte ou fait intercepter toute fonction d'un ordinateur;

c) directement ou indirectement, utilise ou fait utiliser un ordinateur dans l'intention de commettre une infraction prévue à l'alinéa *a*) ou *b*) ou une infraction prévue à l'article 430 concernant des données ou un ordinateur;

d) a en sa possession ou utilise un mot de passe d'ordinateur qui permettrait la perpétration des infractions prévues aux alinéas *a*), *b*) ou *c*), ou en fait le trafic ou permet à une autre personne de l'utiliser,

est coupable d'un acte criminel et passible d'un emprisonnement maximal de dix ans ou d'une infraction punissable sur déclaration de culpabilité par procédure sommaire.

(2) et (3) Texte des définitions :

« données » Représentations d'informations ou de concepts qui sont préparés ou l'ont été de façon à pouvoir être utilisés dans un ordinateur.

« mot de passe » Donnée permettant d'utiliser un ordinateur ou d'obtenir des services d'ordinateur.

« ordinateur » Dispositif ou ensemble de dispositifs connectés ou reliés les uns aux autres, dont l'un ou plusieurs d'entre eux :

a) contiennent des programmes d'ordinateur ou d'autres données;

b) conformément à des programmes d'ordinateur :

(i) soit exécutent des fonctions logiques et de commande,

(ii) soit peuvent exécuter toute autre fonction.

« programme d'ordinateur » Ensemble de données qui représentent des instructions ou des relevés et qui, lorsque traités par l'ordinateur, lui font remplir une fonction.

« service d'ordinateur » S'entend notamment du traitement des données de même que de la mémorisation et du recouvrement ou du relevé des données.

(4) Nouveau.

Article 21 : (1) Texte des paragraphes 342.2(1) et (2) :

342.2 (1) Quiconque, sans justification ou excuse légitime, fabrique, possède, vend, offre en vente ou écoule des instruments, ou des pièces de ceux-ci, particulièrement utiles à la commission d'une infraction prévue à l'article 342.1, dans des circonstances qui permettent de conclure raisonnablement qu'ils ont été utilisés, sont destinés ou étaient destinés à la commission d'une telle infraction, est coupable :

a) soit d'un acte criminel et passible d'un emprisonnement maximal de deux ans;

b) soit d'une infraction punissable sur déclaration de culpabilité par procédure sommaire.

(2) Where a person is convicted of an offence under subsection (1), any instrument or device, in relation to which the offence was committed or the possession of which constituted the offence, may, in addition to any other punishment that may be imposed, be ordered forfeited to Her Majesty, whereupon it may be disposed of as the Attorney General directs.

(2) New.

Clause 22: Existing text of sections 371 and 372:

371. Every one who, with intent to defraud, causes or procures a telegram, cablegram or radio message to be sent or delivered as being sent by the authority of another person, knowing that it is not sent by his authority and with intent that the message should be acted on as being sent by his authority, is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.

372. (1) Every one who, with intent to injure or alarm any person, conveys or causes or procures to be conveyed by letter, telegram, telephone, cable, radio or otherwise information that he knows is false is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years.

(2) Every one who, with intent to alarm or annoy any person, makes any indecent telephone call to that person is guilty of an offence punishable on summary conviction.

(3) Every one who, without lawful excuse and with intent to harass any person, makes or causes to be made repeated telephone calls to that person is guilty of an offence punishable on summary conviction.

Clause 23: (1) Existing text of subsection 430(1.1):

(1.1) Every one commits mischief who wilfully

(*a*) destroys or alters data;

(*b*) renders data meaningless, useless or ineffective;

(*c*) obstructs, interrupts or interferes with the lawful use of data; or

(*d*) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.

(2) Relevant portion of subsection 430(5):

(5) Every one who commits mischief in relation to data

(3) Relevant portion of subsection 430(5.1):

(5.1) Every one who wilfully does an act or wilfully omits to do an act that it is his duty to do, if that act or omission is likely to constitute mischief causing actual danger to life, or to constitute mischief in relation to property or data,

(4) Existing text of subsection 430(8):

(8) In this section, "data" has the same meaning as in section 342.1.

Clause 24: Existing text of sections 487.011 to 487.02:

487.011 The following definitions apply in sections 487.012 to 487.017.

"data" has the same meaning as in subsection 342.1(2).

(2) Lorsqu'une personne est déclarée coupable d'une infraction prévue au paragraphe (1), tout instrument au moyen duquel l'infraction a été commise ou dont la possession a constitué l'infraction peut, en plus de toute peine applicable en l'espèce, être par ordonnance confisqué au profit de Sa Majesté, après quoi il peut en être disposé conformément aux instructions du procureur général.

(2) Nouveau.

Article 22 : Texte des articles 371 et 372 :

371. Est coupable d'un acte criminel et passible d'un emprisonnement maximal de cinq ans quiconque, avec l'intention de frauder, fait en sorte ou obtient qu'un télégramme, un câblogramme ou un message radiophonique soit expédié ou livré comme si l'envoi en était autorisé par une autre personne, sachant que cette autre personne n'en a pas autorisé l'envoi, et dans le dessein qu'il soit donné suite au message comme s'il était expédié avec l'autorisation de cette personne.

372. (1) Est coupable d'un acte criminel et passible d'un emprisonnement maximal de deux ans quiconque, avec l'intention de nuire à quelqu'un ou de l'alarmer, transmet ou fait en sorte ou obtient que soit transmis, par lettre, télégramme, téléphone, câble, radio ou autrement, des renseignements qu'il sait être faux.

(2) Est coupable d'une infraction punissable sur déclaration de culpabilité par procédure sommaire quiconque, avec l'intention d'alarmer ou d'ennuyer quelqu'un, lui tient au cours d'un appel téléphonique des propos indécents.

(3) Est coupable d'une infraction punissable sur déclaration de culpabilité par procédure sommaire quiconque, sans excuse légitime et avec l'intention de harasser quelqu'un, lui fait ou fait en sorte qu'il lui soit fait des appels téléphoniques répétés.

Article 23 : (1) Texte du paragraphe 430(1.1) :

(1.1) Commet un méfait quiconque volontairement, selon le cas :

a) détruit ou modifie des données;

b) dépouille des données de leur sens, les rend inutiles ou inopérantes;

c) empêche, interrompt ou gêne l'emploi légitime des données;

d) empêche, interrompt ou gêne une personne dans l'emploi légitime des données ou refuse l'accès aux données à une personne qui y a droit.

(2) Texte du passage visé du paragraphe 430(5) :

(5) Quiconque commet un méfait à l'égard de données est coupable :

(3) Texte du passage visé du paragraphe 430(5.1) :

(5.1) Quiconque volontairement accomplit un acte ou volontairement omet d'accomplir un acte qu'il a le devoir d'accomplir, si cet acte ou cette omission est susceptible de constituer un méfait qui cause un danger réel pour la vie des gens ou de constituer un méfait à l'égard de biens ou de données est coupable :

(4) Texte du paragraphe 430(8) :

(8) Au présent article, « données » s'entend au sens de l'article 342.1.

Article 24 : Texte des articles 487.011 à 487.02 :

487.011 Les définitions qui suivent s'appliquent aux articles 487.012 à 487.017.

« document » Tout support sur lequel est enregistré ou marqué quelque chose qui peut être lu ou compris par une personne, un ordinateur ou un autre dispositif.

"document" means any medium on which is recorded or marked anything that is capable of being read or understood by a person or a computer system or other device.

487.012 (1) A justice or judge may order a person, other than a person under investigation for an offence referred to in paragraph (3)(*a*),

(*a*) to produce documents, or copies of them certified by affidavit to be true copies, or to produce data; or

(*b*) to prepare a document based on documents or data already in existence and produce it.

(2) The order shall require the documents or data to be produced within the time, at the place and in the form specified and given

(*a*) to a peace officer named in the order; or

(*b*) to a public officer named in the order, who has been appointed or designated to administer or enforce a federal or provincial law and whose duties include the enforcement of this or any other Act of Parliament.

(3) Before making an order, the justice or judge must be satisfied, on the basis of an *ex parte* application containing information on oath in writing, that there are reasonable grounds to believe that

(*a*) an offence against this Act or any other Act of Parliament has been or is suspected to have been committed;

(*b*) the documents or data will afford evidence respecting the commission of the offence; and

(*c*) the person who is subject to the order has possession or control of the documents or data.

(4) The order may contain any terms and conditions that the justice or judge considers advisable in the circumstances, including terms and conditions to protect a privileged communication between a lawyer and their client or, in the province of Quebec, between a lawyer or a notary and their client.

(5) The justice or judge who made the order, or a judge of the same territorial division, may revoke, renew or vary the order on an *ex parte* application made by the peace officer or public officer named in the order.

(6) Sections 489.1 and 490 apply, with any modifications that the circumstances require, in respect of documents or data produced under this section.

(7) Every copy of a document produced under this section, on proof by affidavit that it is a true copy, is admissible in evidence in proceedings under this or any other Act of Parliament and has the same probative force as the original document would have if it had been proved in the ordinary way.

(8) Copies of documents produced under this section need not be returned.

487.013 (1) A justice or judge may order a financial institution, as defined in section 2 of the *Bank Act*, or a person or entity referred to in section 5 of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, unless they are under investigation for an offence referred to in paragraph (4)(*a*), to produce in writing the account number of a person named in the order or the name of a person whose account number is specified in the order, the status and type of the account, and the date on which it was opened or closed.

(2) For the purpose of confirming the identity of the person named in the order or whose account number is specified in the order, the production order may require the financial institution, person or entity to produce that person's date of birth, current address and any previous addresses.

« données » S'entend au sens du paragraphe 342.1(2).

487.012 (1) Sauf si elle fait l'objet d'une enquête relative à l'infraction visée à l'alinéa (3)*a*), un juge de paix ou un juge peut ordonner à une personne :

a) de communiquer des documents — originaux ou copies certifiées conformes par affidavit — ou des données;

b) de préparer un document à partir de documents ou données existants et de le communiquer.

(2) L'ordonnance précise le moment, le lieu et la forme de la communication ainsi que la personne à qui elle est faite — agent de la paix ou fonctionnaire public nommé ou désigné pour l'application ou l'exécution d'une loi fédérale ou provinciale et chargé notamment de faire observer la présente loi ou toute autre loi fédérale.

(3) Le juge de paix ou le juge ne rend l'ordonnance que s'il est convaincu, à la suite d'une dénonciation par écrit faite sous serment et présentée *ex parte*, qu'il existe des motifs raisonnables de croire que les conditions suivantes sont réunies :

a) une infraction à la présente loi ou à toute autre loi fédérale a été ou est présumée avoir été commise;

b) les documents ou données fourniront une preuve touchant la perpétration de l'infraction;

c) les documents ou données sont en la possession de la personne en cause ou à sa disposition.

(4) L'ordonnance peut être assortie des conditions que le juge de paix ou le juge estime indiquées, notamment pour protéger les communications privilégiées entre l'avocat — et, dans la province de Québec, le notaire — et son client.

(5) Le juge de paix ou le juge qui a rendu l'ordonnance — ou un juge de la même circonscription territoriale — peut, sur demande présentée *ex parte* par l'agent de la paix ou le fonctionnaire public nommé dans l'ordonnance, la modifier, la renouveler ou la révoquer.

(6) Les articles 489.1 et 490 s'appliquent, avec les adaptations nécessaires, aux documents ou données communiqués sous le régime du présent article.

(7) La copie d'un document communiquée sous le régime du présent article est, à la condition d'être certifiée conforme à l'original par affidavit, admissible en preuve dans toute procédure sous le régime de la présente loi ou de toute autre loi fédérale et a la même valeur probante que l'original aurait eue s'il avait été déposé en preuve de la façon normale.

(8) Il n'est pas nécessaire de retourner les copies de documents qui ont été communiquées sous le régime du présent article.

487.013 (1) Un juge de paix ou un juge peut ordonner à une institution financière au sens de l'article 2 de la *Loi sur les banques* ou à une personne ou entité visée à l'article 5 de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*, sauf si elles font l'objet d'une enquête relative à l'infraction visée à l'alinéa (4)*a*), de communiquer par écrit soit le numéro de compte de la personne nommée dans l'ordonnance, soit le nom de la personne dont le numéro de compte est mentionné dans l'ordonnance, ainsi que l'état du compte, sa catégorie et la date à laquelle il a été ouvert ou fermé.

(2) En vue de confirmer l'identité de la personne nommée dans l'ordonnance ou celle de la personne dont le numéro de compte est mentionné dans l'ordonnance, il peut être exigé dans celle-ci que l'institution financière, la personne ou l'entité en cause donne la date de naissance, l'adresse actuelle ou une adresse antérieure de la personne concernée.

(3) The order shall require the information to be produced within the time, at the place and in the form specified and given

(*a*) to a peace officer named in the order; or

(*b*) to a public officer named in the order, who has been appointed or designated to administer or enforce a federal or provincial law and whose duties include the enforcement of this or any other Act of Parliament.

(4) Before making an order, the justice or judge must be satisfied, on the basis of an *ex parte* application containing information on oath in writing, that there are reasonable grounds to suspect that

(*a*) an offence against this Act or any other Act of Parliament has been or will be committed;

(*b*) the information will assist in the investigation of the offence; and

(*c*) the institution, person or entity that is subject to the order has possession or control of the information.

(5) The order may contain any terms and conditions that the justice or judge considers advisable in the circumstances, including terms and conditions to protect a privileged communication between a lawyer and their client or, in the province of Quebec, between a lawyer or a notary and their client.

(6) The justice or judge who made the order, or a judge of the same territorial division, may revoke, renew or vary the order on an *ex parte* application made by the peace officer or public officer named in the order.

487.014 (1) For greater certainty, no production order is necessary for a peace officer or public officer enforcing or administering this or any other Act of Parliament to ask a person to voluntarily provide to the officer documents, data or information that the person is not prohibited by law from disclosing.

(2) A person who provides documents, data or information in the circumstances referred to in subsection (1) is deemed to be authorized to do so for the purposes of section 25.

487.015 (1) A person named in an order made under section 487.012 and a financial institution, person or entity named in an order made under section 487.013 may, before the order expires, apply in writing to the judge who issued the order, or a judge of the same territorial division as the judge or justice who issued the order, for an exemption from the requirement to produce any document, data or information referred to in the order.

(2) A person, financial institution or entity may only make an application under subsection (1) if they give notice of their intention to do so to the peace officer or public officer named in the order, within 30 days after it is made.

(3) The execution of a production order is suspended in respect of any document, data or information referred to in the application for exemption until a final decision is made in respect of the application.

(4) The judge may grant the exemption if satisfied that

(*a*) the document, data or information would disclose information that is privileged or otherwise protected from disclosure by law;

(*b*) it is unreasonable to require the applicant to produce the document, data or information; or

(*c*) the document, data or information is not in the possession or control of the applicant.

(3) L'ordonnance précise le moment, le lieu et la forme de la communication ainsi que la personne à qui elle est faite — agent de la paix ou fonctionnaire public nommé ou désigné pour l'application ou l'exécution d'une loi fédérale ou provinciale et chargé notamment de faire observer la présente loi ou toute autre loi fédérale.

(4) Le juge de paix ou le juge ne rend l'ordonnance que s'il est convaincu, à la suite d'une dénonciation par écrit faite sous serment et présentée *ex parte*, qu'il existe des motifs raisonnables de soupçonner que les conditions suivantes sont réunies :

a) une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise;

b) les renseignements demandés seront utiles à l'enquête relative à l'infraction;

c) les renseignements sont en la possession de l'institution financière, de la personne ou de l'entité en cause ou à sa disposition.

(5) L'ordonnance peut être assortie des conditions que le juge de paix ou le juge estime indiquées, notamment pour protéger les communications privilégiées entre l'avocat — et, dans la province de Québec, le notaire — et son client.

(6) Le juge de paix ou le juge qui a rendu l'ordonnance — ou un juge de la même circonscription territoriale — peut, sur demande présentée *ex parte* par l'agent de la paix ou le fonctionnaire public nommé dans l'ordonnance, la modifier, la renouveler ou la révoquer.

487.014 (1) Il demeure entendu qu'une ordonnance de communication n'est pas nécessaire pour qu'un agent de la paix ou un fonctionnaire public chargé de l'application ou de l'exécution de la présente loi ou de toute autre loi fédérale demande à une personne de lui fournir volontairement des documents, données ou renseignements qu'aucune règle de droit n'interdit à celle-ci de communiquer.

(2) La personne qui fournit des documents, données ou renseignements dans les circonstances visées au paragraphe (1) est, pour l'application de l'article 25, réputée être autorisée par la loi à le faire.

487.015 (1) Toute personne visée par l'ordonnance rendue en vertu de l'article 487.012 ou toute institution financière, personne ou entité visée par l'ordonnance rendue en vertu de l'article 487.013 peut, avant l'expiration de l'ordonnance, demander par écrit au juge qui l'a rendue ou à un autre juge de la circonscription territoriale du juge ou du juge de paix qui l'a rendue de l'exempter de l'obligation de communiquer la totalité ou une partie des documents, données ou renseignements demandés.

(2) La personne, l'institution financière ou l'entité ne peut présenter une demande en vertu du paragraphe (1) qu'à la condition d'avoir donné, dans les trente jours suivant celui où l'ordonnance est rendue, un préavis de son intention à l'agent de la paix ou au fonctionnaire public nommé dans l'ordonnance.

(3) L'exécution de l'ordonnance de communication visée par la demande d'exemption est suspendue à l'égard des documents, données ou renseignements mentionnés dans la demande jusqu'à ce qu'une décision définitive ait été rendue sur celle-ci.

(4) Le juge peut accorder l'exemption s'il est convaincu que, selon le cas :

a) la communication révélerait des renseignements protégés par le droit applicable en matière de divulgation ou de privilèges;

b) il serait déraisonnable d'obliger l'intéressé à communiquer les documents, données ou renseignements;

c) les documents, données ou renseignements ne sont ni en la possession de l'intéressé ni à sa disposition.

487.016 No person is excused from complying with an order made under section 487.012 or 487.013 on the ground that the document, data or information referred to in the order may tend to incriminate them or subject them to any proceeding or penalty, but no document prepared by an individual under paragraph 487.012(1)(*b*) may be used or received in evidence against that individual in any criminal proceedings subsequently instituted against them, other than a prosecution under section 132, 136 or 137.

487.017 A financial institution, person or entity who does not comply with a production order made under section 487.012 or 487.013 is guilty of an offence and liable on summary conviction to a fine not exceeding $250,000 or imprisonment for a term not exceeding six months, or to both.

487.02 Where an authorization is given under section 184.2, 184.3, 186 or 188, a warrant is issued under this Act or an order is made under subsection 492.2(2), the judge or justice who gives the authorization, issues the warrant or makes the order may order any person to provide assistance, where the person's assistance may reasonably be considered to be required to give effect to the authorization, warrant or order.

Clause 25: Existing text of the heading:

OTHER PROVISIONS RESPECTING SEARCH WARRANTS

Clause 26: Existing text of section 487.11:

487.11 A peace officer, or a public officer who has been appointed or designated to administer or enforce any federal or provincial law and whose duties include the enforcement of this or any other Act of Parliament, may, in the course of his or her duties, exercise any of the powers described in subsection 487(1) or 492.1(1) without a warrant if the conditions for obtaining a warrant exist but by reason of exigent circumstances it would be impracticable to obtain a warrant.

Clause 27: (1) and (2) Relevant portion of subsection 487.3(1):

487.3 (1) A judge or justice may, on application made at the time of issuing a warrant under this or any other Act of Parliament or a production order under section 487.012 or 487.013, or of granting an authorization to enter a dwelling-house under section 529 or an authorization under section 529.4 or at any time thereafter, make an order prohibiting access to and the disclosure of any information relating to the warrant, production order or authorization on the ground that

...

(*b*) the ground referred to in paragraph (*a*) outweighs in importance the access to the information.

Clause 28: Existing text of sections 492.1 and 492.2:

492.1 (1) A justice who is satisfied by information on oath in writing that there are reasonable grounds to suspect that an offence under this or any other Act of Parliament has been or will be committed and that information that is relevant to the commission of the offence, including the whereabouts of any person, can be obtained through the use of a tracking device, may at any time issue a warrant authorizing a peace officer or a public officer who has been appointed or designated to administer or enforce a federal or provincial law and whose duties include the enforcement of this Act or any other Act of Parliament and who is named in the warrant

(*a*) to install, maintain and remove a tracking device in or on any thing, including a thing carried, used or worn by any person; and

487.016 Nul n'est dispensé de se conformer à une ordonnance rendue en vertu des articles 487.012 ou 487.013 du fait que les documents, les données ou les renseignements demandés peuvent tendre à l'incriminer ou à l'exposer à quelque procédure ou pénalité; toutefois, les documents qu'une personne physique prépare dans le cas visé à l'alinéa 487.012(1)*b*) ne peuvent être utilisés ou admis contre elle dans le cadre de poursuites criminelles intentées contre elle par la suite, sauf en ce qui concerne les poursuites prévues aux articles 132, 136 ou 137.

487.017 La personne, l'institution financière ou l'entité qui omet de se conformer à une ordonnance rendue en vertu des articles 487.012 ou 487.013 commet une infraction et encourt, sur déclaration de culpabilité par procédure sommaire, une amende maximale de 250 000 $ et un emprisonnement maximal de six mois, ou l'une de ces peines.

487.02 Le juge ou le juge de paix qui a accordé une autorisation en vertu des articles 184.2, 184.3, 186 ou 188, décerné un mandat en vertu de la présente loi ou rendu une ordonnance en vertu du paragraphe 492.2(2) peut ordonner à toute personne de prêter son assistance si celle-ci peut raisonnablement être jugée nécessaire à l'exécution des actes autorisés, du mandat ou de l'ordonnance.

Article 25 : Texte de l'intertitre :

AUTRES DISPOSITIONS : MANDAT DE PERQUISITION

Article 26 : Texte de l'article 487.11 :

487.11 L'agent de la paix ou le fonctionnaire public nommé ou désigné pour l'application ou l'exécution d'une loi fédérale ou provinciale et chargé notamment de faire observer la présente loi ou toute autre loi fédérale peut, pour l'accomplissement de ses fonctions, exercer, sans mandat, tous les pouvoirs prévus aux paragraphes 487(1) ou 492.1(1) lorsque l'urgence de la situation rend difficilement réalisable l'obtention du mandat, sous réserve que les conditions de délivrance de celui-ci soient réunies.

Article 27 : (1) et (2) Texte du passage visé du paragraphe 487.3(1) :

487.3 (1) Le juge ou le juge de paix peut, sur demande présentée lors de la délivrance du mandat, en vertu de la présente loi ou d'une autre loi fédérale, de la délivrance d'une ordonnance de communication prévue aux articles 487.012 ou 487.013 ou de celle de l'autorisation prévue aux articles 529 ou 529.4, ou par la suite, interdire, par ordonnance, l'accès à l'information relative au mandat, à l'ordonnance de communication ou à l'autorisation et la communication de cette information pour le motif que, à la fois :

[...]

b) la raison visée à l'alinéa *a*) l'emporte sur l'importance de l'accès à l'information.

Article 28 : Texte des articles 492.1 et 492.2 :

492.1 (1) Le juge de paix qui est convaincu, à la suite d'une dénonciation par écrit faite sous serment, qu'il existe des motifs raisonnables de soupçonner qu'une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise et que des renseignements utiles à cet égard, notamment sur le lieu où peut se trouver une personne, peuvent être obtenus au moyen d'un dispositif de localisation peut décerner un mandat autorisant un agent de la paix ou, dans le cas d'un fonctionnaire public nommé ou désigné pour l'application ou l'exécution d'une loi fédérale ou provinciale et chargé notamment de faire observer la présente loi ou toute autre loi fédérale, celui qui y est nommé :

a) à installer un dispositif de localisation dans ou sur toute chose, notamment une chose transportée, utilisée ou portée par une personne, à l'entretenir et à l'enlever;

(*b*) to monitor, or to have monitored, a tracking device installed in or on any thing.

(2) A warrant issued under subsection (1) is valid for the period, not exceeding sixty days, mentioned in it.

(3) A justice may issue further warrants under this section.

(4) For the purposes of this section, "tracking device" means any device that, when installed in or on any thing, may be used to help ascertain, by electronic or other means, the location of any thing or person.

(5) On *ex parte* application in writing supported by affidavit, the justice who issued a warrant under subsection (1) or a further warrant under subsection (3) or any other justice having jurisdiction to issue such warrants may authorize that the tracking device be covertly removed after the expiry of the warrant

(*a*) under any terms or conditions that the justice considers advisable in the public interest; and

(*b*) during any specified period of not more than sixty days.

492.2 (1) A justice who is satisfied by information on oath in writing that there are reasonable grounds to suspect that an offence under this or any other Act of Parliament has been or will be committed and that information that would assist in the investigation of the offence could be obtained through the use of a number recorder, may at any time issue a warrant authorizing a peace officer or a public officer who has been appointed or designated to administer or enforce a federal or provincial law and whose duties include the enforcement of this Act or any other Act of Parliament and who is named in the warrant

(*a*) to install, maintain and remove a number recorder in relation to any telephone or telephone line; and

(*b*) to monitor, or to have monitored, the number recorder.

(2) When the circumstances referred to in subsection (1) exist, a justice may order that any person or body that lawfully possesses records of telephone calls originated from, or received or intended to be received at, any telephone give the records, or a copy of the records, to a person named in the order.

(3) Subsections 492.1(2) and (3) apply to warrants and orders issued under this section, with such modifications as the circumstances require.

(4) For the purposes of this section, "number recorder" means any device that can be used to record or identify the telephone number or location of the telephone from which a telephone call originates, or at which it is received or is intended to be received.

Clause 29: New.

Competition Act

Clause 30: (1) Existing text of the definition:

"record" includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine readable record, and any other documentary material, regardless of physical form or characteristics, and any copy or portion thereof;

(2) New.

Clause 31: New.

b) à surveiller ou faire surveiller ce dispositif.

(2) Le mandat est valide pour la période, d'au plus soixante jours, qui y est indiquée.

(3) Le juge de paix peut décerner de nouveaux mandats en vertu du présent article.

(4) Pour l'application du présent article, « dispositif de localisation » s'entend d'un dispositif qui, lorsqu'il est placé dans ou sur une chose, peut servir à localiser une chose ou une personne par des moyens électroniques ou autres.

(5) Sur demande écrite *ex parte*, accompagnée d'un affidavit, le juge de paix qui a décerné le mandat visé aux paragraphes (1) ou (3) ou un juge de paix compétent pour décerner un tel mandat peut permettre que le dispositif de localisation soit enlevé secrètement après l'expiration du mandat :

a) selon les modalités qu'il estime opportunes;

b) au cours de la période, d'au plus soixante jours, qu'il spécifie.

492.2 (1) Le juge de paix qui est convaincu, à la suite d'une dénonciation par écrit faite sous serment, qu'il existe des motifs raisonnables de soupçonner qu'une infraction à la présente loi ou à toute autre loi fédérale a été ou sera commise et que des renseignements utiles à l'enquête relative à l'infraction pourraient être obtenus au moyen d'un enregistreur de numéro peut décerner un mandat autorisant un agent de la paix ou, dans le cas d'un fonctionnaire public nommé ou désigné pour l'application ou l'exécution d'une loi fédérale ou provinciale et chargé notamment de faire observer la présente loi ou toute autre loi fédérale, celui qui y est nommé :

a) à placer sous enregistreur de numéro un téléphone ou une ligne téléphonique, à entretenir l'enregistreur et à les en dégager;

b) à surveiller ou faire surveiller l'enregistreur.

(2) Dans les circonstances visées au paragraphe (1), le juge peut ordonner à la personne ou à l'organisme qui possède légalement un registre des appels provenant d'un téléphone ou reçus ou destinés à être reçus à ce téléphone de donner le registre ou une copie de celui-ci à toute personne nommée dans l'ordonnance.

(3) Les paragraphes 492.1(2) et (3) s'appliquent, avec les adaptations nécessaires, aux mandats décernés et aux ordonnances rendues en vertu du présent article.

(4) Pour l'application du présent article, « enregistreur de numéro » s'entend d'un dispositif qui peut enregistrer ou identifier le numéro ou la localisation du téléphone d'où provient un appel ou auquel l'appel est reçu ou destiné à être reçu.

Article 29 : Nouveau.

Loi sur la concurrence

Article 30 : (1) Texte de la définition :

« document » Les éléments d'information, quels que soient leur forme et leur support, notamment la correspondance, les notes, livres, plans, cartes, dessins, diagrammes, illustrations ou graphiques, photographies, films, microformules, enregistrements sonores, magnétoscopiques ou informatisés, ou toute reproduction totale ou partielle de ces éléments d'information.

(2) Nouveau.

Article 31 : Nouveau.

Clause 32: Existing text of subsection 16(6):

(6) In this section, "computer system" and "data" have the meanings set out in subsection 342.1(2) of the *Criminal Code*.

Clause 33: Existing text of subsection 20(2):

(2) Copies of any records referred to in subsection (1), including copies by any process of photographic reproduction, on proof orally or by affidavit that they are true copies, are admissible in evidence in any proceedings under this Act and have the same probative force as the original.

Clause 34: Existing text of the definition:

"data" means representations, in any form, of information or concepts.

Clause 35: Relevant portion of subsection 52(2):

(2) For the purposes of this section, a representation that is

...

(*d*) made in the course of in-store, door-to-door or telephone selling to a person as ultimate user, or

...

is deemed to be made to the public by and only by the person who causes the representation to be so expressed, made or contained, subject to subsection (2.1).

Clause 36: (1) Existing text of subsection 52.1(1):

52.1 (1) In this section, "telemarketing" means the practice of using interactive telephone communications for the purpose of promoting, directly or indirectly, the supply or use of a product or for the purpose of promoting, directly or indirectly, any business interest.

(2) Relevant portion of subsection 52.1(2):

(2) No person shall engage in telemarketing unless

(*a*) disclosure is made, in a fair and reasonable manner at the beginning of each telephone communication, of the identity of the person on behalf of whom the communication is made, the nature of the product or business interest being promoted and the purposes of the communication;

(3) Existing text of subsection 52.1(5):

(5) The disclosure of information referred to in paragraph (2)(*b*) or (*c*) or (3)(*b*) or (*c*) must be made during the course of a telephone communication unless it is established by the accused that the information was disclosed within a reasonable time before the communication, by any means, and the information was not requested during the telephone communication.

Clause 37: Relevant portion of subsection 74.03(1):

74.03 (1) For the purposes of sections 74.01 and 74.02, a representation that is

...

(*d*) made in the course of in-store, door-to-door or telephone selling to a person as ultimate user, or

...

Article 32 : Texte du paragraphe 16(6) :

(6) Pour l'application du présent article, « données » et « ordinateur » s'entendent au sens du paragraphe 342.1(2) du *Code criminel*.

Article 33 : Texte du paragraphe 20(2) :

(2) Les copies d'un document visé au paragraphe (1), y compris les copies obtenues au moyen d'un procédé photographique quelconque, sont, lorsqu'il est démontré au moyen d'un témoignage oral ou d'un affidavit qu'il s'agit de copies conformes, admissibles en preuve dans toute procédure prévue à la présente loi et leur force probante est la même que celle des documents originaux.

Article 34 : Texte de la définition :

« données » Toute forme de représentation d'informations ou de notions.

Article 35 : Texte du passage visé du paragraphe 52(2) :

(2) Pour l'application du présent article, sauf le paragraphe (2.1), sont réputées n'être données au public que par la personne de qui elles proviennent les indications qui, selon le cas :

[...]

d) sont données, au cours d'opérations de vente en magasin, par démarchage ou par téléphone, à un utilisateur éventuel;

Article 36 : (1) Texte du paragraphe 52.1(1) :

52.1 (1) Dans le présent article, « télémarketing » s'entend de la pratique de la communication téléphonique interactive pour promouvoir directement ou indirectement soit la fourniture ou l'utilisation d'un produit, soit des intérêts commerciaux quelconques.

(2) Texte du passage visé du paragraphe 52.1(2) :

(2) La pratique du télémarketing est subordonnée :

a) à la divulgation, d'une manière juste et raisonnable, au début de chaque communication téléphonique, de l'identité de la personne pour le compte de laquelle la communication est effectuée, de la nature du produit ou des intérêts commerciaux dont la promotion est faite et du but de la communication;

(3) Texte du paragraphe 52.1(5) :

(5) La divulgation de renseignements visée aux alinéas (2)*b*) ou *c*) ou (3)*b*) ou *c*) doit être faite au cours d'une communication téléphonique, sauf si l'accusé établit que la divulgation a été faite dans un délai raisonnable antérieur à la communication, par n'importe quel moyen, et que les renseignements n'ont pas été demandés au cours de la communication.

Article 37 : Texte du passage visé du paragraphe 74.03(1) :

74.03 (1) Pour l'application des articles 74.01 et 74.02, sous réserve du paragraphe (2), sont réputées n'être données au public que par la personne de qui elles proviennent les indications qui, selon le cas :

[...]

d) sont données, au cours d'opérations de vente en magasin, par démarchage ou par téléphone, à un usager éventuel;

is deemed to be made to the public by and only by the person who causes the representation to be so expressed, made or contained, subject to subsection (2).

Mutual Legal Assistance in Criminal Matters Act

Clause 38: Existing text of the definitions:

"data" means representations, in any form, of information or concepts;

"record" means any material on which data are recorded or marked and which is capable of being read or understood by a person or a computer system or other device;

Clause 39: New.

Clause 40: Existing text of section 13.1:

13.1 (1) A judge of the province to whom an application is made under subsection 11(2) may, in a manner provided for by the *Criminal Code*, issue a warrant, other than a warrant referred to in section 12, to use any device or other investigative technique or do anything described in the warrant that would, if not authorized, constitute an unreasonable search or seizure in respect of a person or a person's property.

(2) A warrant issued under subsection (1) may be obtained, issued and executed in the manner prescribed by the *Criminal Code*, with any modifications that the circumstances may require.

(3) Despite subsection (2), subsections 12(3) and (4) and sections 14 to 16 apply in respect of a warrant issued under subsection (1), and any sections of the *Criminal Code* inconsistent with those provisions do not apply.

Clause 41: New.

Clause 42: Existing text of the heading:

EVIDENCE FOR USE ABROAD

Clause 43: New.

Clause 44: New.

Clause 45: New.

Clause 46: Existing text of subsection 36(2):

(2) For the purpose of determining the probative value of a record or a copy of a record admitted in evidence under this Act, the trier of fact may examine the record or copy, receive evidence orally or by affidavit, or by a certificate or other statement pertaining to the record in which a person attests that the certificate or statement is made in conformity with the laws that apply to a state or entity, whether or not the certificate or statement is in the form of an affidavit attested to before an official of the state or entity, including evidence as to the circumstances in which the information contained in the record or copy was written, stored or reproduced, and draw any reasonable inference from the form or content of the record or copy.

Clause 47: (1) and (2) Existing text of section 44:

44. (1) Subject to subsection 38(2), a record sent to the Minister by a state or entity in accordance with a Canadian request is privileged and no person shall disclose to anyone the record or its purport or the contents of the record or

Loi sur l'entraide juridique en matière criminelle

Article 38 : Texte des définitions :

« document » Tout support où sont enregistrées ou sur lequel sont inscrites des données et qui peut être lu ou compris par une personne, un système informatique ou un autre dispositif.

« données » Toute forme de représentation d'informations ou de notions.

Article 39 : Nouveau.

Article 40 : Texte de l'article 13.1 :

13.1 (1) Un juge d'une province auquel une requête est présentée en application du paragraphe 11(2) peut, de la manière prévue au *Code criminel*, décerner un mandat, autre qu'un mandat visé à l'article 12, autorisant l'utilisation d'un dispositif ou d'une technique ou méthode d'enquête ou tout acte qui y est mentionné, qui, sans cette autorisation, donnerait lieu à une fouille, une perquisition ou une saisie abusive à l'égard d'une personne ou d'un bien.

(2) Un mandat décerné en vertu du paragraphe (1) peut être obtenu, décerné et exécuté de la manière prévue au *Code criminel*, avec les adaptations nécessaires.

(3) Par dérogation au paragraphe (2), les paragraphes 12(3) et (4) et les articles 14 à 16 s'appliquent au mandat décerné en vertu du paragraphe (1), et toute disposition du *Code criminel* incompatible avec ces dispositions ne s'applique pas.

Article 41 : Nouveau.

Article 42 : Texte de l'intertitre :

ÉLÉMENTS DE PREUVE DESTINÉS À L'ÉTRANGER

Article 43 : Nouveau.

Article 44 : Nouveau.

Article 45 : Nouveau.

Article 46 : Texte du paragraphe 36(2) :

(2) Le juge des faits peut, afin de décider de la force probante d'un document — ou de sa copie — admis en preuve en vertu de la présente loi, procéder à son examen ou recevoir une déposition verbale, un affidavit ou un certificat ou autre déclaration portant sur le document, fait, selon le signataire, conformément aux lois de l'État ou entité, qu'il soit fait en la forme d'un affidavit rempli devant un agent de l'État ou entité ou non, y compris une déposition quant aux circonstances de la rédaction, de l'enregistrement, de la mise en mémoire ou de la reproduction des renseignements contenus dans le document ou la copie, et tirer de sa forme ou de son contenu toute conclusion fondée.

Article 47 : (1) et (2) Texte de l'article 44 :

44. (1) Sous réserve du paragraphe 38(2), les documents transmis au ministre par un État ou entité en conformité avec une demande canadienne sont protégés. Jusqu'à ce qu'ils aient été, en conformité avec les conditions attachées

any part of it before the record, in compliance with the conditions on which it was so sent, is made public or disclosed in the course or for the purpose of giving evidence.

(2) No person in possession of a record mentioned in subsection (1) or of a copy thereof, or who has knowledge of any information contained in the record, shall be required, in connection with any legal proceedings, to produce the record or copy or to give evidence relating to any information that is contained therein.

à leur transmission au ministre, rendus publics ou révélés au cours ou aux fins d'une déposition devant un tribunal, il est interdit de communiquer à quiconque ces documents, leur teneur ou des renseignements qu'ils contiennent.

(2) Les personnes en possession de l'original ou de la copie d'un document étranger visé au paragraphe (1), ou qui ont connaissance de son contenu, ne peuvent être tenues, dans des procédures judiciaires, de déposer l'original ou la copie ou de rendre témoignage sur son contenu.