Milene Gaudreault

From: Milene Gaudreault
Sent: November-24-14 1:55 PM
To: Kathy Renaud; Helene Bertrand
Cc: Barbara Bucknell; Helene Bertrand; Rachel Desjardins; Josee Phillips; Patricia Kosseim; Sophie Paluck-Bastien
Subject: RE: Request for BN - meet-and-greet with wireless industry

Hello,

Please use CTS-091166 for this request. A docket will follow.

Thank you.

Milène
(819) 994-5759

From: Patricia Kosseim
Sent: November-24-14 10:52 AM
To: Sophie Paluck-Bastien
Cc: Barbara Bucknell; Helene Bertrand; Rachel Desjardins; Josee Phillips; Milene Gaudreault; Kathy Renaud
Subject: RE: Request for BN - meet-and-greet with wireless industry

Merci Sophie.
Barb, please assign. Kathy, please log in and BF.
Merci.
Pat

From: Sophie Paluck-Bastien
Sent: November-24-14 10:50 AM
To: Patricia Kosseim
Cc: Barbara Bucknell; Helene Bertrand; Rachel Desjardins; Josee Phillips; Milene Gaudreault; Kathy Renaud
Subject: Request for BN - meet-and-greet with wireless industry

Bonjour Patricia,

The Commissioner has a meet-and-greet with the Canadian Wireless Telecommunications Association on December 10. (You and I will be accompanying him; it will be a very small delegation from their side, and they have suggested and the Commissioner has agreed that there should be an equally small delegation from our side.)

We require a BN for this meeting no later than 12:00 p.m. on Monday, December 8. The BN should include a summary of our process for issuing guidance documents and anything else you feel is appropriate.

Merci!

Sophie Paluck-Bastien
Conseillère spéciale :: Special Advisor
Secrétariat de la haute direction :: Executive Secretariat

Office of the Privacy Commissioner of Canada | Commissariat à la protection de la vie privée du Canada

Security Classification/Designation Classification/désignation sécuritaire	Total Pages Pages totales
Confidential	4

BRIEFING NOTE FOR THE COMMISSIONER | **NOTE D'INFORMATION POUR LE COMMISSAIRE**

Meeting with Canadian Wireless Technology Association (CWTA)

PURPOSE:

To provide background for your meet and greet meeting with CWTA on Dec. 10th, 2014

ISSUE:

- The CWTA are hoping to establish "first contact" and to understand better our process for issuing guidance documents (and presumably having the opportunity to comment on direction that may affect their industry)[1] – which is outlined in the discussion session below;
- Lawful access and transparency are also topics of interest; certain CWTA stakeholders (e.g. Rogers) have published statistics while others (esp. BCE and Blackberry) could take issue with recent calls for company reporting on government data requests and surveillance[2];
- Recall that our Office has been interacting on issues tied to CWTA members quite actively in the past year: *R. v. Spencer*, lawful access legislation and the issue of clarifying privacy policies and reporting public statistics in relation to requests from police and other agencies.[3]

[redacted]

DISCUSSION: s.16.1(1)(d) s.21(1)(a)

Overview

The CWTA's "primary role" is to represent the wireless industry's interests to government and regulators.[4] According to their corporate description, the CWTA is "an authority on wireless issues, developments and trends in Canada. It represents cellular, PCS [personal communications services], messaging, mobile radio, fixed wireless, and mobile satellite carriers as well as companies that develop and produce products and services for the industry."

[N.B. CWTA does not represent the full range of carriers or service providers for wireless in the Canadian marketplace, most notably TELUS, Wind Mobile, Mobilicity, Public Mobile and smaller ISPs].[5]

Current CWTA Staff

Bernard Lord is current President and CEO of the CWTA. Their Board of Directors includes executives from Ericsson, BCE, Blackberry, Rogers, Quebecor, Samsung, Google and Huawei. At present, the delegation slated to meet with you on December 10th will include Ken Englehart (Rogers, Regulatory Affairs), Anthony Hemond (Videotron, Consumer Affairs) and Kurt Eby (CWTA, Regulatory Affairs).

N.B. [redacted] = ajout de dernière minute à la délégation. -SPB
Suzanne Morin

1 It may be this relates to our CRTC Submission on the new *Wireless Code*, now that regulatory changes are being brought into effect – see Proceeding to establish a mandatory code for mobile wireless services - Submission of the Office of the Privacy Commissioner of Canada to the Canadian Radio-television and Telecommunication Commission (CRTC) – URL: https://www.priv.gc.ca/information/research-recherche/sub/sub_crtc_121204_e.asp

2 CBC, More transparency needed on digital privacy - Personal data has become 'precious coin of commerce' for the private sector, says Daniel Therrien (August 21, 2014) – URL: http://www.cbc.ca/news/politics/more-transparency-needed-on-digital-privacy-says-daniel-therrien-1.2743288

3 Please refer to BN on TSP handover and transparency - 7777-6-30554 – attached which discusses the background of this issue at length

4 Industry Canada Canadian Company Capabilities (CCC) database "CWTA Company Description" (Last Updated: 2014-03-18) – URL: http://www.ic.gc.ca/app/ccc/srch/nvgt.do?prtl=1&estblmntNo=123456183228&profile=cmpltPrfl&profileId=21&app=sold&lang=eng

5 Telus pulls out of wireless industry lobby group, Globe and Mail (Feb. 28, 2014) – URL: http://www.theglobeandmail.com/report-on-business/telus-pulls-out-of-key-industry-lobby-group/article17160276/; Small carriers leave CWTA, Toronto Star (April 20, 2013) – URL: http://www.thestar.com/business/2013/04/10/small_carriers_leave_canadian_wireless_telecommunications_association.html

Recent CWTA activities

According to the Office of the Commissioner of Lobbying (OCL) public registry, meetings at the ADM-level (Industry Canada, Spectrum and Telecom) and DG-level (Chief Consumer Office, CRTC) have been the Association's most recent interactions with government.

More precisely, the CWTA have been active in recent CRTC discussions around mobile device security, noting in a letter on Nov. 3, 2014 that their members have adopted self-regulation measures to reduce the impact of device theft.[6] On the Industry Canada mandate, the CWTA has been seeking clarity from government on a) regulations and legislative changes related to the CASL, b) new lawful access measures (under C-13), and c) the use of wireless radio communications jamming equipment (which were recently amended via amendments in Bill C-43).

We were asked to review C-43 by the INDU Committee but made no substantive privacy comment regarding the Telecommunications Act and Radio-communications Act amendments in Bill C-43.[7] Conversely, on Bill C-13, we provided a full-length submission and oral testimony which is accessible on our website.

Upcoming meeting

According to their most recent OCL Registration Summary it is the intention of the CWTA to discuss "oversight of compliance with the *Personal Information Protection and Electronic Documents Act.*" Note also that concern has been expressed in past by the CWTA regarding usage of terminology in OPC public discussions and documents. For example, as noted in a 2011 internal report, CWTA members "expressed frustration at the OPC's use of the terms "mobile" and "~~wireless~~ portable" interchangeably in various publications."

As a consequence, the Association has asked that we draw important distinctions between:

a) "wireless networks"—mobile phone networks transmitting wireless Internet and voice;
b) "Wi-Fi"—local area networks transmitting wireless Internet;
c) "mobile" devices—mobile phones, wireless Internet USB sticks that connect devices (like laptops and desktops) to mobile phone networks, and;
d) "portable" devices—laptops and other non-phone devices with wireless capability, wireless Internet USB sticks that connect devices (like laptops and desktops) to local area networks, and other non-Internet devices like USB memory sticks.

It will be important for you to bear these sensitivities in mind in the course of your discussions as this may be precisely a point the CWTA would like to reinforce (i.e. the issue of technical precision in the documentation that we make public).

The CWTA will also be invited to provide their views on the upcoming stakeholder consultation exercise around the new OPC Strategic Priorities. We have concluded internal discussions and analysis on these new priorities and will have distributed discussion papers and invitations by the time of the CWTA meeting and will look forward to discussions at the five consultation events planned for the New Year.

---

6 For example, a national outreach campaign and a "Protect your data" web site, which includes a national blacklist for lost and stolen devices; and the public IMEI [International Mobile Equipment Identifier] lookup tool – see CWTA Handset Security Update – Letter to CRTC (Nov. 3, 2014) – URL: http://cwta.ca/wordpress/wp-content/uploads/2011/09/CWTA-handset-security-update-2014-10-29.pdf

7 See (C-43) Legislative summary - RA and TA amendments - 7777-6-49820

Transparency around lawful access disclosures

Rogers Communications was the first major TSP in Canada to issue a public transparency report on government data requests after the controversy earlier this year around handover practices of subscriber information. The Rogers report separates data demands into six categories and figures: subscriber name and address look-ups (87, 856); court orders and warrants (74, 415); government requirements letters (2,556); emergency requests (9,339); child exploitation (711), and; MLAT requests (40), presenting a total of 174,917 separate inquiries to the company in the calendar year 2013 for Rogers Communications.[8]

By way of comparison, TELUS used a similar breakdown by providing statistics and descriptions for: a) name and address checks (40,900); court orders and subpoenas (4,315); government requirement letters (1,343); emergency calls (56,748); child exploitation (154), and; MLAT requests (2).[9]

Mr. Englehart has recently publically defended the company's move to provide public statistics, after Public Safety Canada documents were released to the media demonstrating government pushback at the decision by TELUS to report similar figures.[10] He was quoted as saying "I'm hopeful it won't bother the law enforcement people, but if it does, we thought that the needs of our customers came first."

ADVICE:

If asked directly for specific views on these reports, as in other venues, the move to greater transparency on data disclosures and government requests should be encouraged. You might also underscore the point that Industry Canada has itself directly confirmed that PIPEDA specifically (and privacy generally) are in no way an obstacle to reporting on these issues. Finally, many other firms operating both in Canada and globally have reporting for several years (e.g. Google, Apple, Facebook, Twitter, Yahoo, Vodaphone).

In other words, the precedent for public reporting of this sort is now well-established internationally and domestically, as we argued in our submissions to Parliament on both Bill S-4 (PIPEDA amendments) and Bill C-13 (lawful access). We have asked for annual public reporting and more clarity in terms of organizational practices and policy on both the government side (for investigative bodies) and commercial firms (in the same vein as the Rogers and TELUS reports).

As for a general description of the work process for Policy and Research before issuing OPC guidance, the basic steps are as follows:

1. Recognize significant bundling of relevant cases under PIPEDA, issues emerging in privacy research and/or Parliamentary work that draw attention to a systemic issue or legal ambiguity;
2. Scope out a basic position with broad application to relevant stakeholders;
3. Research issue and draft document;
4. Consult with relevant organizations, engage provincial Commissioners or international counterparts and/or industry associations;
5. Revise, submit for Legal review and seek approvals;
6. Translate and finalize format / layout with Communications;
7. Work with Outreach to launch at subject-appropriate venue.

8 Rogers 2013 Transparency Report – URL: http://www.rogers.com/cms/images/en/S35635%20Rogers-2013-Transparency-Report-EN.pdf
9 TELUS Transparency Report 2013 – URL: http://about.telus.com/servlet/JiveServlet/previewBody/5544-102-1-6081/TELUS%20Transparency%20Report%202013%20-English.pdf
10 "Feds were worries as telecom firm planned to go public on police access to Canadians' phone calls and emails, memo shows", National Post (December 1, 2014) – URL: http://news.nationalpost.com/2014/12/01/feds-were-worried-as-telecom-firms-planned-to-go-public-on-police-access-to-canadians-phone-calls-and-emails-memo-shows/

Significantly, at the time of this summer's controversy on the scale of government data requests, several TSPs called publically for guidance from our Office on the issue.[11] Mirko Bibic, Bell Canada's vice-president of regulatory affairs, stated before a Parliamentary committee that "what we need as an industry, and as a company, is guidance on what kind of specific information we can provide."

While a proposed factsheet on "Transparency and reporting under PIPEDA" was in draft stage in April 2014, this project was placed on hold pending the outcome of the *Spencer* case being decided by the Supreme Court of Canada and our submissions to Parliament on the latest lawful access legislation (C-13) and PIPEDA amendments (S-4). [redacted]

At this stage, however, with the SCC decision and C-13 debate settled for the moment, it may be time to take up this project again – either as an OPC discussion paper or formal industry guidance. Certainly, it is realistic to anticipate the privacy academic community will be vocal on the issue in the weeks ahead.12

CONSULTATION: CASL Working Group (Regan Morris), PIPEDA Investigations (Gillian Kular), Research (Arun Bauri)
DISTRIBUTION: Commissioner's Office, LSPR

s.16.1(1)(d)

Rédigé par / Prepared by	**Date**	**Révisions / Revisions**
Chris Prince	December 3, 2014	

Approuvé par / Approved by — **Date**

B Bucknell — Dec 4/14

Barbara Bucknell
Directrice intérimaire – Politiques, recherche et affaires parlementaires

Approved by – Approuvé par — **Date**

Patricia Kosseim — Dec. 4, 2014
Avocate générale principale et directrice générale

Approuvé par / Approved by — **Date**

☑ Je suis satisfait des mesures proposées. / I agree with the proposed recommendation(s).

☐ Je ne suis pas satisfait de ces recommandations pour les raisons suivantes. / I do not agree with the proposed recommendation(s) for the following reason(s):

Commentaires ou des instructions supplémentaires / Additional Comments or Instructions:

Daniel Therrien
Le commissaire à la protection de la vie privée

11 See "Bell seeks guidance on data sharing" *Chronicle-Herald* (May 1, 2014) – URL: http://thechronicleherald.ca/novascotia/1204370-bell-seeks-guidance-on-data-sharing and "Taxpayers paying for government telecom snooping" *The Star* (April 30, 2014) – URL: http://www.thestar.com/news/canada/2014/04/30/harper_says_telecoms_follow_rules_in_customer_data_disclosure.html

12 Citizen Lab, Early findings from AMI requests (October 6, 2014) – URL: https://citizenlab.org/2014/10/early-findings-ami-requests/; Hilts, Andrew and Parsons, Christopher A., Right to Information in Canada: Drawing Analogue Law into a Digital Present (2014). The Winston Report, Winter 2014. Available at SSRN: http://ssrn.com/abstract=2504109

Sophie Paluck-Bastien

From: Kurt Eby <keby@cwta.ca>
Sent: December-05-14 10:25 AM
To: Sophie Paluck-Bastien
Subject: RE: CWTA Meeting with Privacy Commissioner

Hi Sophie,
Suzanne Morin is now going to be attending the meeting as well as a representative of CWTA, not Bell. Can you please add her to the meeting invite using this address: [redacted]

Thanks!

Kurt

From: Sophie Paluck-Bastien [mailto:Sophie.Paluck-Bastien@priv.gc.ca]
Sent: December 02 2014 11:23 AM
To: Kurt Eby
Subject: RE: CWTA Meeting with Privacy Commissioner

Thank you!

From: Kurt Eby [mailto:keby@cwta.ca]
Sent: December-02-14 11:20 AM
To: Sophie Paluck-Bastien
Subject: RE: CWTA Meeting with Privacy Commissioner

Hi Sophie,
That's still accurate. We haven't changed the agenda, but I will let you k ow if someone raises any additional issues to discuss.

Kurt

On Dec 2, 2014 11:14 AM, Sophie Paluck-Bastien <Sophie.Paluck-Bastien@priv.gc.ca> wrote:

Hi Kurt,

When I originally chatted with Suzanne Morin about this meeting, I understood this would be a "first contact" meeting between the new Commissioner and the wireless industry. The purpose would be for the industry to give a general overview of their issues. Suzanne mentioned she might bring up the importance of the OPC consulting with the industry before issuing guidance that affects the industry, as well as the industry's position on lawful access.

Is this still accurate? Anything else you think might come up? You can give me a call if it's easier: 819-994-5825.

Thanks!

Sophie

From: Sophie Paluck-Bastien
Sent: December-01-14 12:40 PM
To: 'Kurt Eby'
Cc: Rachel Desjardins; Josee Phillips
Subject: RE: CWTA Meeting with Privacy Commissioner

Sounds good, Kurt, thanks!

From: Kurt Eby [mailto:keby@cwta.ca]
Sent: December-01-14 12:40 PM
To: Sophie Paluck-Bastien
Subject: CWTA Meeting with Privacy Commissioner

Hi Sophie,

I just wanted to confirm that we would still like to go ahead with our meeting with the Privacy Commissioner on December 10. Bill Abbott will be attending from Bell in place of Suzanne.

Thanks!

Kurt

Kurt Eby | Director, Regulatory Affairs and Government Relations

Canadian Wireless Telecommunications Association (CWTA)

80 Elgin Street, Suite 300, Ottawa, ON K1P 6R2

(613) 233-4888 x213 | Fax: (613) 233-2032 | keby@cwta.ca | cwta.ca

Sophie Paluck-Bastien

From: Sophie Paluck-Bastien
Sent: December-09-14 6:05 PM
To: Rachel Desjardins; Denis Phillion; Josee Phillips
Cc: Daniel Therrien
Subject: CWTA - participants

Veuillez noter que Suzanne Morin ET Bill Abbott seront à la rencontre avec le Commissaire demain.

(Il y a eu un malentendu de la part de Kurt Eby; il avait compris que c'était un ou l'autre mais c'est les deux.)

Sophie Paluck-Bastien

From: Kurt Eby <keby@cwta.ca>
Sent: November-24-14 12:06 PM
To: Josee Phillips; 'Morin, Suzanne [redacted]
Cc: Sophie Paluck-Bastien; Rachel Desjardins
Subject: RE: rencontre avec des représentants de l'industrie du sans-fils

Josée, s.19(1)
Certainly. That time should work for us, but I will canvass everyone to verify.

In the meantime, in addition to myself, the attendees are Suzanne Morin, Ken Engelhart and Anthony Hemond.

Kurt

-----Original Message-----
From: Josee Phillips [mailto:Josee.Phillips@priv.gc.ca]
Sent: November 24 2014 11:44 AM
To: Kurt Eby; 'Morin, Suzanne [redacted]
Cc: Sophie Paluck-Bastien; Rachel Desjardins
Subject: RE: rencontre avec des représentants de l'industrie du sans-fils

Good morning Kurt,
I would appreciate it if you could provide the names of the meeting attendees, as I need to provide the commissionaires with the names of all outside guests.

As for the exact time, we have blocked off from 2:00 to 3:00 p.m. in the Commissioner's agenda. Let me know if that works for you.

Thank you,
Josée Phillips
Adjointe à l'agenda / Scheduling Assistant Commissariat à la protection de la vie privée / Office of the Privacy Commissioner josee.phillips@priv.gc.ca

30, rue Victoria / 30 Victoria Street
Gatineau (Québec) K1A 1H3 / Gatineau, Quebec K1A 1H3 Téléphone /Telephone 819-994-5835

-----Original Message-----
From: Kurt Eby [mailto:keby@cwta.ca]
Sent: November-24-14 11:36 AM
To: Morin, Suzanne [redacted]; Rachel Desjardins
Cc: Josee Phillips; Sophie Paluck-Bastien
Subject: RE: rencontre avec des représentants de l'industrie du sans-fils

Good morning Rachel,
I can confirm that there will be four of us attending. I can provide names if you'd like.

Let me know when you have a preferred time for the afternoon of December 10.

Thanks,
Kurt

Kurt Eby | Director, Regulatory Affairs and Government Relations Canadian Wireless Telecommunications Association (CWTA)
80 Elgin Street, Suite 300, Ottawa, ON K1P 6R2
(613) 233-4888 x213 | Fax: (613) 233-2032 | keby@cwta.ca | cwta.ca

-----Original Message-----
From: Morin, Suzanne [redacted] [mailto:suzanne.morin@bellaliant.ca]
Sent: November 21 2014 2:09 PM
To: Rachel Desjardins
Cc: Josee Phillips; Sophie Paluck-Bastien; Kurt Eby; Morin, Suzanne [redacted]
Subject: RE: rencontre avec des représentants de l'industrie du sans-fils

s.19(1)

Allo Rachel,

Thank you so much for getting back to us so quickly with proposed dates and times. We would like to confirm the afternoon of Wednesday, December 10th. We will let you pick the time that is most convenient.

Also, I have copied Kurt Eby from the CWTA who will manage coordination with the OPC going forward for this meeting. He will confirm shortly the 3-4 attendees from our end.

Super bon weekend.

Suzanne

-----Original Message-----
From: Rachel Desjardins [mailto:Rachel.Desjardins@priv.gc.ca]
Sent: Friday, November 21, 2014 10:39 AM
To: Morin, Suzanne [redacted]
Cc: Josee Phillips; Sophie Paluck-Bastien
Subject: rencontre avec des représentants de l'industrie du sans-fils

Bonjour Suzanne,

Voici quelques options pour une rencontre d'une heure:
le 10 décembre en après-midi
le 12 décembre en avant midi
le 15 et 16 décembre en après-midi

J'attends de vos nouvelles ainsi que la confirmation de qui participera à cette rencontre.

Salutations,

Rachel Desjardins
Gestionnaire, Secrétariat de la haute direction/ Manager, Executive Secretariat 30, rue Victoria / 30 Victoria Street

Gatineau (Québec) / Gatineau, Quebec K1A 1H3
Tel : 819-994-5828
Fax : 819-994-6441

Sophie Paluck-Bastien

From: Rachel Desjardins
Sent: November-21-14 10:39 AM
To: 'Morin, Suzanne [redacted]
Cc: Josee Phillips; Sophie Paluck-Bastien
Subject: rencontre avec des représentants de l'industrie du sans-fils

Bonjour Suzanne,

Voici quelques options pour une rencontre d'une heure: le 10 décembre en après-midi
le 12 décembre en avant midi
le 15 et 16 décembre en après-midi

J'attends de vos nouvelles ainsi que la confirmation de qui participera à cette rencontre.

Salutations,

Rachel Desjardins
Gestionnaire, Secrétariat de la haute direction/ Manager, Executive Secretariat 30, rue Victoria / 30 Victoria Street
Gatineau (Québec) / Gatineau, Quebec K1A 1H3
Tel : 819-994-5828
Fax : 819-994-6441

-----Original Message-----
From: Morin, Suzanne [redacted] [mailto:suzanne.morin@bellaliant.ca]
Sent: November-18-14 3:25 PM
To: Josee Phillips
Cc: Rachel Desjardins
Subject: RE: Lundi s.19(1)

Merci Josée.

Rachel, j'attends de tes nouvelles.

Sincèrement,

Suzanne
613-785-8231 (b)
[redacted]

-----Original Message-----
From: Josee Phillips [mailto:Josee.Phillips@priv.gc.ca]
Sent: Tuesday, November 18, 2014 2:43 PM
To: Morin, Suzanne [redacted]
Cc: Rachel Desjardins
Subject: RE: Lundi

Bonjour Suzanne,

Puisque nous n'avons toujours pas reçu la confirmation de la date de comparution devant le parlement, je suis incapable de fixer votre rencontre avec le commissaire.

Je serais à l'extérieur du bureau pour les prochains jours mais Rachel communiquera avec vous dès que possible.

Merci.
Josée Phillips
Adjointe à l'agenda / Scheduling Assistant Commissariat à la protection de la vie privée / Office of the Privacy Commissioner josee.phillips@priv.gc.ca

30, rue Victoria / 30 Victoria Street
Gatineau (Québec) K1A 1H3 / Gatineau, Quebec K1A 1H3 Téléphone /Telephone 819-994-5835

-----Original Message-----
From: Sophie Paluck-Bastien
Sent: November-18-14 8:48 AM
To: 'Morin, Suzanne [redacted]
Cc: Josee Phillips
Subject: RE: Lundi

s.19(1)

Ça marche. You can reach Josée at 819-994-5835.

À bientôt!

-----Original Message-----
From: Morin, Suzanne [redacted] [mailto:suzanne.morin@bellaliant.ca]
Sent: November-17-14 8:49 PM
To: Sophie Paluck-Bastien
Cc: Josee Phillips; Morin, Suzanne [redacted]
Subject: Re: Lundi

Merci Sophie.

Josée, peut être on pourrait se parler brièvement demain. S'il vous plaît laisser moi savoir à quel numéro je peux vous rejoindre.

Sophie, je crois que la rencontre dont nous avons discuté est relié à certains sujets beaucoup plus spécifiques, et une rencontre en petit nombre est plus adéquat.

Cependant, je sais que les entreprises principales dans le secteur des télécommunications sont intéressées à rencontrer le Commissaire et plusieurs individus de son équipe directement afin de discuter de façon beaucoup plus général de notre industrie comme nous avions toujours fait avec le OPC, et nous pensions de faire cette demande dans le nouvel an. En plus, pour cette rencontre nous aimerions non seulement partager des informations sur notre industrie mais en plus aborder des sujets très spécifiques qui nous préoccupe ou qui intéresse le OPC en particulier. Je crois que ces entreprises de télécommunications devraient inclure au moins Bell, Rogers, Telus, et MTS. Alors si vous êtes d'accord je vous reviens bientôt, et entre temps, si le OPC reçoit des demandes spécifiques des télécommunications vous pouvez bien leur dire de me contacter.

Sincèrement,

Suzanne

Sent from my BlackBerry 10 smartphone.
Original Message
From: Sophie Paluck-Bastien
Sent: Monday, November 17, 2014 16:38
To: Morin, Suzanne [redacted]
Cc: Josee Phillips
Subject: RE: Lundi

Absolument. Je mets Josée Phillips dans le loop; c'est elle qui est responsable du calendrier de M. Therrien. Vous pouvez communiquer directement avec elle pour fixer une date et une heure qui convienne à tous. (N.B. Josée : Ce sera une très petite délégation de notre côté.)

Une petite question : Nous recevons énormément de demandes de rencontre de la part d'entreprises réglementées par le fédéral. Si quelqu'un d'autre des télécoms demande à rencontrer M. Therrien dans les prochaines semaines, est-ce qu'on pourrait leur offrir de communiquer avec vous pour faire partie de votre délégation? Est-ce qu'ils communiqueraient avec toi directement, avec ITAC ou avec CWTA?

À bientôt!

-----Original Message-----
From: Morin, Suzanne [redacted] [mailto:suzanne.morin@bellaliant.ca]
Sent: November-17-14 1:56 PM
To: Sophie Paluck-Bastien
Subject: RE: Lundi

Allo Sophie,

Suivant notre brève conversation, j'ai eu la chance de réfléchir et discuter avec certains collègues et voulais savoir si on va organiser un rendez-vous?

A bientôt.

s.19(1)

Suzanne

-----Original Message-----
From: Morin, Suzanne [redacted]
Sent: Tuesday, November 04, 2014 10:11 AM
To: 'Sophie Paluck-Bastien'
Subject: RE: Lundi

Alors, est-ce que 11h00 demain fonctionne? Si oui, je peux t'appeler, cependant je n'ai pas ton numéro à Gatineau.

Suzanne Morin
General Counsel Regulatory & Privacy Chief Bell Aliant Regional Communications
160 Elgin Street, 19th Floor -- Ottawa, Ontario K2P 2C4
(w) 613-785-8231
[redacted]

-----Original Message-----
From: Sophie Paluck-Bastien [mailto:Sophie.Paluck-Bastien@priv.gc.ca]

Sent: Tuesday, November 04, 2014 8:45 AM
To: Morin, Suzanne [redacted]
Subject: Re: Lundi

Ça marche.

Original Message
From: Morin, Suzanne [redacted]
Sent: Monday, November 3, 2014 8:28 PM
To: Sophie Paluck-Bastien
Subject: Re: Lundi

Allo Sophie, mes excuses pour le délai. Il semble que venir à Gatineau sera très difficile pour moi cette semaine. Peut être on pourra parler brièvement au téléphone mercredi et si nécessaire je pourrai traverser le pont la semaine prochaine.

Sent from my BlackBerry 10 smartphone.
Original Message
From: Sophie Paluck-Bastien
Sent: Monday, November 3, 2014 06:43
To: Morin, Suzanne [redacted]
Subject: Re: Lundi

s.19(1)

Bonjour Suzanne,

Andréa m'a dit que tu me ferais peut-être signe bientôt. Malheureusement, je ne serai pas au bureau aujourd'hui, mais ça me ferait plaisir de te rencontrer plus tard cette semaine. Je suis libre demain en début d'après-midi et mercredi n'importe quand après 11 h.

Sophie
Original Message
From: Morin, Suzanne [redacted]
Sent: Sunday, November 2, 2014 9:47 AM
To: Sophie Paluck-Bastien
Subject: Lundi

Allo Sophie,

J'espère que tout va bien. Je parlais avec Andréa hier à la conférence et je voulais faire un suivis avec toi. C'est peut-être dernière minute mais je rencontre Barb avec un groupe d'industrie pour discuter de S-4 de 1:30-2:30, et je voulais savoir si tu avais 10-15 après pour se rencontrer. C'est tellement plus difficile maintenant que vous êtes à Gatineau.

Sinon, peut-être on peut trouver un autre temps cette semaine.

A bientôt,

Suzanne

Sophie Paluck-Bastien

From: Morin, Suzanne [redacted] <suzanne.morin@bellaliant.ca>
Sent: November-18-14 11:37 AM
To: Sophie Paluck-Bastien
Subject: RE: Lundi

C'est super!

-----Original Message-----
From: Sophie Paluck-Bastien [mailto:Sophie.Paluck-Bastien@priv.gc.ca]
Sent: Tuesday, November 18, 2014 8:48 AM
To: Morin, Suzanne [redacted]
Cc: Josee Phillips
Subject: RE: Lundi

s.19(1)

Ça marche. You can reach Josée at 819-994-5835.

À bientôt!

-----Original Message-----
From: Morin, Suzanne [redacted] [mailto:suzanne.morin@bellaliant.ca]
Sent: November-17-14 8:49 PM
To: Sophie Paluck-Bastien
Cc: Josee Phillips; Morin, Suzanne [redacted]
Subject: Re: Lundi

Merci Sophie.

Josée, peut être on pourrait se parler brièvement demain. S'il vous plaît laisser moi savoir à quel numéro je peux vous rejoindre.

Sophie, je crois que la rencontre dont nous avons discuté est relié à certains sujets beaucoup plus spécifiques, et une rencontre en petit nombre est plus adéquat.

Cependant, je sais que les entreprises principales dans le secteur des télécommunications sont intéressées à rencontrer le Commissaire et plusieurs individus de son équipe directement afin de discuter de façon beaucoup plus général de notre industrie comme nous avions toujours fait avec le OPC, et nous pensions de faire cette demande dans le nouvel an. En plus, pour cette rencontre nous aimerions non seulement partager des informations sur notre industrie mais en plus aborder des sujets très spécifiques qui nous préoccupe ou qui intéresse le OPC en particulier. Je crois que ces entreprises de télécommunications devraient inclure au moins Bell, Rogers, Telus, et MTS. Alors si vous êtes d'accord je vous reviens bientôt, et entre temps, si le OPC reçoit des demandes spécifiques des télécommunications vous pouvez bien leur dire de me contacter.

Sincèrement,

Suzanne

Sent from my BlackBerry 10 smartphone.
Original Message

From: Sophie Paluck-Bastien
Sent: Monday, November 17, 2014 16:38
To: Morin, Suzanne [redacted]
Cc: Josee Phillips
Subject: RE: Lundi

Absolument. Je mets Josée Phillips dans le loop; c'est elle qui est responsable du calendrier de M. Therrien. Vous pouvez communiquer directement avec elle pour fixer une date et une heure qui convienne à tous. (N.B. Josée : Ce sera une très petite délégation de notre côté.)

Une petite question : Nous recevons énormément de demandes de rencontre de la part d'entreprises réglementées par le fédéral. Si quelqu'un d'autre des télécoms demande à rencontrer M. Therrien dans les prochaines semaines, est-ce qu'on pourrait leur offrir de communiquer avec vous pour faire partie de votre délégation? Est-ce qu'ils communiqueraient avec toi directement, avec ITAC ou avec CWTA?

À bientôt!

-----Original Message-----
From: Morin, Suzanne [redacted] [mailto:suzanne.morin@bellaliant.ca]
Sent: November-17-14 1:56 PM
To: Sophie Paluck-Bastien
Subject: RE: Lundi

Allo Sophie,

Suivant notre brève conversation, j'ai eu la chance de réfléchir et discuter avec certains collègues et voulais savoir si on va organiser un rendez-vous?

A bientôt.

Suzanne s.19(1)

-----Original Message-----
From: Morin, Suzanne [redacted]
Sent: Tuesday, November 04, 2014 10:11 AM
To: 'Sophie Paluck-Bastien'
Subject: RE: Lundi

Alors, est-ce que 11h00 demain fonctionne? Si oui, je peux t'appeler, cependant je n'ai pas ton numéro à Gatineau.

Suzanne Morin
General Counsel Regulatory & Privacy Chief Bell Aliant Regional Communications
160 Elgin Street, 19th Floor -- Ottawa, Ontario K2P 2C4
(w) 613-785-8231
[redacted]

-----Original Message-----
From: Sophie Paluck-Bastien [mailto:Sophie.Paluck-Bastien@priv.gc.ca]
Sent: Tuesday, November 04, 2014 8:45 AM
To: Morin, Suzanne [redacted]
Subject: Re: Lundi

Ça marche.

Original Message
From: Morin, Suzanne [redacted]
Sent: Monday, November 3, 2014 8:28 PM
To: Sophie Paluck-Bastien
Subject: Re: Lundi

Allo Sophie, mes excuses pour le délai. Il semble que venir à Gatineau sera très difficile pour moi cette semaine. Peut être on pourra parler brièvement au téléphone mercredi et si nécessaire je pourrai traverser le pont la semaine prochaine.

Sent from my BlackBerry 10 smartphone.
Original Message
From: Sophie Paluck-Bastien
Sent: Monday, November 3, 2014 06:43
To: Morin, Suzanne [redacted]
Subject: Re: Lundi

s.19(1)

Bonjour Suzanne,

Andréa m'a dit que tu me ferais peut-être signe bientôt. Malheureusement, je ne serai pas au bureau aujourd'hui, mais ça me ferait plaisir de te rencontrer plus tard cette semaine. Je suis libre demain en début d'après-midi et mercredi n'importe quand après 11 h.

Sophie
Original Message
From: Morin, Suzanne [redacted]
Sent: Sunday, November 2, 2014 9:47 AM
To: Sophie Paluck-Bastien
Subject: Lundi

Allo Sophie,

J'espère que tout va bien. Je parlais avec Andréa hier à la conférence et je voulais faire un suivis avec toi. C'est peut-être dernière minute mais je rencontre Barb avec un groupe d'industrie pour discuter de S-4 de 1:30-2:30, et je voulais savoir si tu avais 10-15 après pour se rencontrer. C'est tellement plus difficile maintenant que vous êtes à Gatineau.

Sinon, peut-être on peut trouver un autre temps cette semaine.

A bientôt,

Suzanne

Sent from my BlackBerry 10 smartphone.

▶ [CWIA meeting]

KE, BA, KE, AH, DT, SM, PK, MMC

■ NOTES

1 R v. Spencer
2 Lawful access generally
3 warrantless disclosures
4 future relationship
5 transparency reports

1)
Canadian Coalition Against Child Exploitation
R v Plant
immediate impact of Spencer is no longer using CCACE letters.

Other industries, other offences, bigger impact.

police asking for more info if they have to go through the trouble of asking for a warrant.

if there's any discrepancy within the industry, it's on CWIA.

■ ACTION

NOTES

ACTION

2)

[redacted]

had never received request for transparency reports or figures from OPC until 2011.

Solicitor General Enforcement Regulations may limit what can be disclosed (e.g. wiretaps).

request good will "others involved in request"

[redacted]

3)

[redacted]

[redacted]

s.19(1)
s.20(1)(c)

s.19(1)
s.20(1)(c)

NOTES

need to explain what CEA asks for and why, to dispell myths.

no metadata is being provided w/o warrant.

[redacted]

4)
We'd like to come back in and better explain the industry

We'd like to collaborate on transparency reports.

some have included 911 calls in their transparency requests
some count one thing as one request, others as 100.

ACTION

OPC to organize stakeholder groups to come up w/ model transparency report.

the facts would put ppl's mind at ease.

don't have to do individual reports, could be industry report.

companies will need time to upgrade their systems.

→ inconsistencies in gvt depts reports for requests, we're visiting dept's

→ Open to get back to you on transparency reports

1. Spencer
2. LA & interaction w/ OPC
3. warrantless discl.
4. Relationship ; rebuilding trust
5. transparency reporting

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

---

① Spencer
- Coalition v. child exploitation
- C-can protocol & LE requests — Rv Ward
→ only C-porn ∴ vy narrow
- OPC attended C-can mtgs
- Spencer = Shaw & carry tech plate
- all cos. stopped after Spencer
- was faster but child porn = crime ∴ warrant possible ; is heavy more impact for other crime
- distinction b/w C-can & LA jurisp ?

② OPC
- Industry offered to meet Asst Cr. Comm Cdn.
  % LA up date ; explained 1.1 M
- [redacted]
- required approach to narrow ; 'Our :
- [redacted]

(2) suite
- Sol Gen "rqx" re licence conditions restrict
- involvement of non-OPC in ATIP request
- "we've been asking for years" statement by Intern Com. after ATIP info provided

(3) [redacted]

→ # metadata → Engelhart [illegible] his media interviews clarified [illegible]

Engelhart (Rogers): nothing w/o warrant due to obiter in Spencer
easy to get prod. orders

(4) Future mtgs
OLA transparency reports → more consistency

Spencer
[redacted]
- one of which not giving metadata w/o warrants to NS

s.19(1)
s.20(1)(c)

Regan Morris

From: Regan Morris
Sent: November-27-14 10:17 AM
To: Christopher Prince; Arun Bauri; Gillian Kular
Subject: RE: CWTA meeting note (background)
Attachments: CWTA meeting note (background)_7A2DA008 - RM's comments.doc

Hi Chris,

Here you go small suggested revision to the paragraph discussing OPC's role under CASL. While the CWTA may be interested in CASL generally, I'm not sure they will be interested in the OPC's specific slice of responsibility.

What about OBA and related issues like geo-location tracking? Could these come up?

[redacted]

s.23

Regan

From: Christopher Prince
Sent: November-26-14 3:10 PM
To: Arun Bauri; Gillian Kular; Regan Morris
Subject: CWTA meeting note (background)

Hi all,

I've been asked to prepare this for an upcoming meeting with between the Commissioner and the Wireless Technology Association.

Wondering if you could have a quick glance see if I've missed anything?

Thanks!

CWTA meeting note (background) -
http://officium/_layouts/OPC.Officium/Utilities/OfficiumIDLookup.aspx?id=7777-6-52597

BRIEFING NOTE FOR THE COMMISSIONER

NOTE D'INFORMATION POUR LE COMMISSAIRE

Meeting with Canadian Wireless Technology Association (CWTA)

PURPOSE:

To provide background for your meet and greet meeting with CWTA on Dec. 10th, 2014

ISSUE:

- The CWTA has expressed an interest in understanding the OPC process for issuing guidance documents (and presumably having the opportunity to comment on direction that may affect their industry) - this may be related to our CRTC Submission on the new Wireless Code, now that regulatory changes are being brought into effect[1];
- It may also be reasonable to assume the CWTA may take issue with recent calls by the Commissioner – both in public and before Parliament - for additional transparency and public reporting by industry players in connection with hand-over of subscriber data to government[2];
- Recall that our Office has been interacting on issues tied to CWTA members quite actively in the past year: *R. v. Spencer*, lawful access legislation and the issue of clarifying privacy policies and reporting public statistics in relation to requests from police and other agencies.[3]
- N.B. PIPEDA Investigations has dozens of active complaints on the issue of access to personal information held by TSPs and their disclosures to authorities – this should **not** be a topic of discussion at this time.

DISCUSSION:

Overview

The CWTA's "primary role" is to represent the wireless industry's interests to government and regulators.[4] According to their own corporate description, the CWTA is "an authority on wireless issues, developments and trends in Canada. It represents cellular, PCS, messaging, mobile radio, fixed wireless, and mobile satellite carriers as well as companies that develop and produce products and services for the industry." It is important to note, however, that the CWTA does not speak for all the major carriers in the Canadian wireless marketplace, most notably TELUS, Wind Mobile, Mobilicity and Public Mobile.[5]

Current CWTA Staff and Activities

Bernard Lord is the current President and Chief Executive Officer of the CWTA. Their Board of Directors includes representatives from Ericsson, BCE, Blackberry, Rogers, Quebecor, Samsung, Google and Huawei. You will likely be meeting with Caitlin Carrol, Manager, Research and Analysis, Kurt Eby, Director, Regulatory Affairs and/or Ursula Grant, Director, Industry Affairs. Exact attendance was not conveyed in the request for a meeting. According to the Office of the Registrar of Lobbyist public registry, meetings at the ADM-level (Industry Canada, Spectrum and Telecom) and DG-level (Chief Consumer Office, CRTC) have been the Association's most recent interactions with government.

---

1 Proceeding to establish a mandatory code for mobile wireless services - Submission of the Office of the Privacy Commissioner of Canada to the Canadian Radio-television and Telecommunication Commission (CRTC) – URL: https://www.priv.gc.ca/information/research-recherche/sub/sub_crtc_121204_e.asp

2 CBC, More transparency needed on digital privacy - Personal data has become 'precious coin of commerce' for the private sector, says Daniel Therrien (August 21, 2014) – URL: http://www.cbc.ca/news/politics/more-transparency-needed-on-digital-privacy-says-daniel-therrien-1.2743288

3 BN on TSP handover and transparency - 7777-6-30554

4 Industry Canada Canadian Company Capabilities (CCC) database "CWTA Company Description" (Last Updated: 2014-03-18) – URL: http://www.ic.gc.ca/app/ccc/srch/nvgt.do?prtl=1&estblmntNo=123456183228&profile=cmpltPrfl&profileId=21&app=sold&lang=eng

5 Telus pulls out of wireless industry lobby group, Globe and Mail (Feb. 28, 2014) – URL: http://www.theglobeandmail.com/report-on-business/telus-pulls-out-of-key-industry-lobby-group/article17160276/

More precisely, the CWTA have been active in recent CRTC discussion around mobile device security, noting in a letter on Nov. 3, 2014 that their members have adopted self-regulation measures to reduce the impact of device theft in Canada – for example, a national outreach campaign and a "Protect your data" web site, which includes a national blacklist for lost and stolen devices; and the public IMEI lookup tool.[6]

On the Industry Canada side, the CWTA have been seeking clarity from government on regulations and legislative changes related to the CASL and the use of wireless radio communications jamming equipment (which were recently amended via amendments in Bill C-43).[7]

Upcoming meeting

According to their most recent OCL Registration Summary it is the intention of the CWTA to lobby you specifically to provide "ongoing input with respect to Office of the Privacy Commissioner of Canada oversight of compliance with the Personal Information Protection and Electronic Documents Act."

It is also reasonable to assume they may also be interested in discussing the OPC's role ~~of~~ under CASL ~~regulations and enforcement~~ with respect to address harvesting and spyware in the context of providing wireless services in Canada.[8]

Comment [RM1]: Personally, I'm doubtful that the OPC's specific mandate under CASL would be of interest to CWTA.

Concern has also been expressed via the CWTA to our Office in the past specifically regarding characterisations in our discussion documents. For example, as noted in a 2011 internal report, "CWTA members have expressed frustration at the OPC's use of the terms "mobile" and "wireless" interchangeably in various publications."

As a consequence, the Association has asked that we bear in mind the important distinctions between:

- "wireless networks"—mobile phone networks transmitting wireless Internet and voice;
- "Wi-Fi"—local area networks transmitting wireless Internet;
- "mobile" devices—mobile phones, wireless Internet USB sticks that connect devices (like laptops and desktops) to mobile phone networks;
- "portable" devices—laptops and other non-phone devices with wireless capability, wireless Internet USB sticks that connect devices (like laptops and desktops) to local area networks, and other non-Internet devices like USB memory sticks.

It will be important for you to bear these distinctions in mind in the course of your discussions. The CWTA will also be invited to provide their views on the upcoming stakeholder consultation exercise around the new OPC Strategic Priorities.

6 CWTA Handset Security Update – Letter to CRTC (Nov. 3, 2014) – URL: http://cwta.ca/wordpress/wp-content/uploads/2011/09/CWTA-handset-security-update-2014-10-29.pdf
7 See (C-43) Legislative summary - RA and TA amendments - 7777-6-49820
8 Office of the Commissioner of Lobbying of Canada, 12-Month Lobbying Summary - In-house Organization Canadian Wireless Telecommunications Association (Last updated: 2014-11-19) – URL: https://ocl-cal.gc.ca/app/secure/orl/lrrs/do/clntSmmry?clientNumber=228021&sMdKy=1369059633220

Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

Security Classification/Designation Classification/désignation sécuritaire	Total Pages Pages totales
Confidential	3

BRIEFING NOTE FOR THE COMMISSIONER

NOTE D'INFORMATION POUR LE COMMISSAIRE

CONSULTATION: CASL Working Group (Regan Morris), PIPEDA Investigations (Gillian Kular), Research (Arun Bauri)
DISTRIBUTION: Commissioner`s Office, LSPR

Prepared by - Rédigé par	Date	Original dated - Date de l'original	Revision dated - Date de la révision	Revision dated - Date de la révision
C. Prince		2014-11-26		
Approved by (Signature) – Approuvé par (Signature)	Date			Date
Barbara Bucknell				

Kathy Renaud

From: Kathy Renaud
Sent: Thursday, December 04, 2014 12:59 PM
To: LSPRTA - SJPRAT
Subject: CWTA meeting note (background)

Good afternoon,

Please find below the link to a document that was submitted to the Commissioner's office.

Thanks,

Kathy

CWTA meeting note (background) -
http://officium/_layouts/OPC.Officium/Utilities/OfficiumIDLookup.aspx?id=7777-6-53278

BRIEFING NOTE FOR THE COMMISSIONER

NOTE D'INFORMATION POUR LE COMMISSAIRE

Meeting with Canadian Wireless Technology Association (CWTA)

PURPOSE:

To provide background for your meet and greet meeting with CWTA on Dec. 10th, 2014

ISSUE:

- The CWTA are hoping to establish "first contact" and to understand better our process for issuing guidance documents (and presumably having the opportunity to comment on direction that may affect their industry)[1] – which is outlined in the discussion session below;
- Lawful access and transparency are also topics of interest; certain CWTA stakeholders (e.g. Rogers) have published statistics while others (esp. BCE and Blackberry) could take issue with recent calls for company reporting on government data requests and surveillance[2];
- Recall that our Office has been interacting on issues tied to CWTA members quite actively in the past year: *R. v. Spencer*, lawful access legislation and the issue of clarifying privacy policies and reporting public statistics in relation to requests from police and other agencies.[3]

DISCUSSION:

s.16.1(1)(d)
s.21(1)(a)

Overview

The CWTA's "primary role" is to represent the wireless industry's interests to government and regulators.[4] According to their corporate description, the CWTA is "an authority on wireless issues, developments and trends in Canada. It represents cellular, PCS [personal communications services], messaging, mobile radio, fixed wireless, and mobile satellite carriers as well as companies that develop and produce products and services for the industry."

[N.B. CWTA does not represent the full range of carriers or service providers for wireless in the Canadian marketplace, most notably TELUS, Wind Mobile, Mobilicity, Public Mobile and smaller ISPs].[5]

Current CWTA Staff

Bernard Lord is current President and CEO of the CWTA. Their Board of Directors includes executives from Ericsson, BCE, Blackberry, Rogers, Quebecor, Samsung, Google and Huawei. At present, the delegation slated to meet with you on December 10th will include Ken Englehart (Rogers, Regulatory Affairs), Anthony Hemond (Videotron, Consumer Affairs) and Kurt Eby (CWTA, Regulatory Affairs).

---

1 It may be this relates to our CRTC Submission on the new *Wireless Code*, now that regulatory changes are being brought into effect – see Proceeding to establish a mandatory code for mobile wireless services - Submission of the Office of the Privacy Commissioner of Canada to the Canadian Radio-television and Telecommunication Commission (CRTC) – URL: https://www.priv.gc.ca/information/research-recherche/sub/sub_crtc_121204_e.asp

2 CBC, More transparency needed on digital privacy - Personal data has become 'precious coin of commerce' for the private sector, says Daniel Therrien (August 21, 2014) – URL: http://www.cbc.ca/news/politics/more-transparency-needed-on-digital-privacy-says-daniel-therrien-1.2743288

3 Please refer to BN on TSP handover and transparency - 7777-6-30554 – attached which discusses the background of this issue at length

4 Industry Canada Canadian Company Capabilities (CCC) database "CWTA Company Description" (Last Updated: 2014-03-18) – URL: http://www.ic.gc.ca/app/ccc/srch/nvgt.do?prtl=1&estblmntNo=123456183228&profile=cmpltPrfl&profileId=21&app=sold&lang=eng

5 Telus pulls out of wireless industry lobby group, Globe and Mail (Feb. 28, 2014) – URL: http://www.theglobeandmail.com/report-on-business/telus-pulls-out-of-key-industry-lobby-group/article17160276/; Small carriers leave CWTA, Toronto Star (April 20, 2013) – URL: http://www.thestar.com/business/2013/04/10/small_carriers_leave_canadian_wireless_telecommunications_association.html

Recent CWTA activities

According to the Office of the Commissioner of Lobbying (OCL) public registry, meetings at the ADM-level (Industry Canada, Spectrum and Telecom) and DG-level (Chief Consumer Office, CRTC) have been the Association's most recent interactions with government.

More precisely, the CWTA have been active in recent CRTC discussions around mobile device security, noting in a letter on Nov. 3, 2014 that their members have adopted self-regulation measures to reduce the impact of device theft.[6] On the Industry Canada mandate, the CWTA has been seeking clarity from government on a) regulations and legislative changes related to the CASL, b) new lawful access measures (under C-13), and c) the use of wireless radio communications jamming equipment (which were recently amended via amendments in Bill C-43).

We were asked to review C-43 by the INDU Committee but made no substantive privacy comment regarding the Telecommunications Act and Radio-communications Act amendments in Bill C-43.[7] Conversely, on Bill C-13, we provided a full-length submission and oral testimony which is accessible on our website.

Upcoming meeting

According to their most recent OCL Registration Summary it is the intention of the CWTA to discuss "oversight of compliance with the *Personal Information Protection and Electronic Documents Act.*" Note also that concern has been expressed in past by the CWTA regarding usage of terminology in OPC public discussions and documents. For example, as noted in a 2011 internal report, CWTA members "expressed frustration at the OPC's use of the terms "mobile" and "wireless" interchangeably in various publications."

As a consequence, the Association has asked that we draw important distinctions between:

a) "wireless networks"—mobile phone networks transmitting wireless Internet and voice;
b) "Wi-Fi"—local area networks transmitting wireless Internet;
c) "mobile" devices—mobile phones, wireless Internet USB sticks that connect devices (like laptops and desktops) to mobile phone networks, and;
d) "portable" devices—laptops and other non-phone devices with wireless capability, wireless Internet USB sticks that connect devices (like laptops and desktops) to local area networks, and other non-Internet devices like USB memory sticks.

It will be important for you to bear these sensitivities in mind in the course of your discussions as this may be precisely a point the CWTA would like to reinforce (i.e. the issue of technical precision in the documentation that we make public).

The CWTA will also be invited to provide their views on the upcoming stakeholder consultation exercise around the new OPC Strategic Priorities. We have concluded internal discussions and analysis on these new priorities and will have distributed discussion papers and invitations by the time of the CWTA meeting and will look forward to discussions at the five consultation events planned for the New Year.

---

6 For example, a national outreach campaign and a "Protect your data" web site, which includes a national blacklist for lost and stolen devices; and the public IMEI [International Mobile Equipment Identifier] lookup tool – see CWTA Handset Security Update – Letter to CRTC (Nov. 3, 2014) – URL: http://cwta.ca/wordpress/wp-content/uploads/2011/09/CWTA-handset-security-update-2014-10-29.pdf

7 See (C-43) Legislative summary - RA and TA amendments - 7777-6-49820

Transparency around lawful access disclosures

Rogers Communications was the first major TSP in Canada to issue a public transparency report on government data requests after the controversy earlier this year around handover practices of subscriber information. The Rogers report separates data demands into six categories and figures: subscriber name and address look-ups (87, 856); court orders and warrants (74, 415); government requirements letters (2,556); emergency requests (9,339); child exploitation (711), and; MLAT requests (40), presenting a total of 174,917 separate inquiries to the company in the calendar year 2013 for Rogers Communications.[8]

By way of comparison, TELUS used a similar breakdown by providing statistics and descriptions for: a) name and address checks (40,900); court orders and subpoenas (4,315); government requirement letters (1,343); emergency calls (56,748); child exploitation (154), and; MLAT requests (2).[9]

Mr. Englehart has recently publically defended the company's move to provide public statistics, after Public Safety Canada documents were released to the media demonstrating government pushback at the decision by TELUS to report similar figures.[10] He was quoted as saying "I'm hopeful it won't bother the law enforcement people, but if it does, we thought that the needs of our customers came first."

ADVICE:

If asked directly for specific views on these reports, as in other venues, the move to greater transparency on data disclosures and government requests should be encouraged. You might also underscore the point that Industry Canada has itself directly confirmed that PIPEDA specifically (and privacy generally) are in no way an obstacle to reporting on these issues. Finally, many other firms operating both in Canada and globally have reporting for several years (e.g. Google, Apple, Facebook, Twitter, Yahoo, Vodaphone).

In other words, the precedent for public reporting of this sort is now well-established internationally and domestically, as we argued in our submissions to Parliament on both Bill S-4 (PIPEDA amendments) and Bill C-13 (lawful access). We have asked for annual public reporting and more clarity in terms of organizational practices and policy on both the government side (for investigative bodies) and commercial firms (in the same vein as the Rogers and TELUS reports).

As for a general description of the work process for Policy and Research before issuing OPC guidance, the basic steps are as follows:

1. Recognize significant bundling of relevant cases under PIPEDA, issues emerging in privacy research and/or Parliamentary work that draw attention to a systemic issue or legal ambiguity;
2. Scope out a basic position with broad application to relevant stakeholders;
3. Research issue and draft document;
4. Consult with relevant organizations, engage provincial Commissioners or international counterparts and/or industry associations;
5. Revise, submit for Legal review and seek approvals;
6. Translate and finalize format / layout with Communications;
7. Work with Outreach to launch at subject-appropriate venue.

8 Rogers 2013 Transparency Report – URL: http://www.rogers.com/cms/images/en/S35635%20Rogers-2013-Transparency-Report-EN.pdf
9 TELUS Transparency Report 2013 – URL: http://about.telus.com/servlet/JiveServlet/previewBody/5544-102-1-6081/TELUS%20Transparency%20Report%202013%20-English.pdf
10 "Feds were worries as telecom firm planned to go public on police access to Canadians' phone calls and emails, memo shows", National Post (December 1, 2014) – URL: http://news.nationalpost.com/2014/12/01/feds-were-worried-as-telecom-firms-planned-to-go-public-on-police-access-to-canadians-phone-calls-and-emails-memo-shows/

Significantly, at the time of this summer's controversy on the scale of government data requests, several TSPs called publically for guidance from our Office on the issue.[11] Mirko Bibic, Bell Canada's vice-president of regulatory affairs, stated before a Parliamentary committee that "what we need as an industry, and as a company, is guidance on what kind of specific information we can provide."

While a proposed factsheet on "Transparency and reporting under PIPEDA" was in draft stage in April 2014, this project was placed on hold pending the outcome of the *Spencer* case being decided by the Supreme Court of Canada and our submissions to Parliament on the latest lawful access legislation (C-13) and PIPEDA amendments (S-4).

At this stage, however, with the SCC decision and C-13 debate settled for the moment, it may be time to take up this project again – either as an OPC discussion paper or formal industry guidance. Certainly, it is realistic to anticipate the privacy academic community will be vocal on the issue in the weeks ahead.[12]

CONSULTATION: CASL Working Group (Regan Morris), PIPEDA Investigations (Gillian Kular), Research (Arun Bauri)
DISTRIBUTION: Commissioner`s Office, LSPR

s.16.1(1)(d)

Rédigé par / Prepared by	**Date**	**Révisions / Revisions**
Chris Prince	December 3, 2014	

Approuvé par / Approved by — **Date**

Barbara Bucknell
Directrice intérimaire – Politiques, recherche et affaires parlementaires

Approved by – Approuvé par — **Date**

Patricia Kosseim
Avocate générale principale et directrice générale

Approuvé par / Approved by — **Date**

☐ Je suis satisfait des mesures proposées. / I agree with the proposed recommendation(s).

☐ Je ne suis pas satisfait de ces recommandations pour les raisons suivantes. / I do not agree with the proposed recommendation(s) for the following reason(s):

Commentaires ou des instructions supplémentaires / Additional Comments or Instructions:

Daniel Therrien
Le commissaire à la protection de la vie privée

11 See "Bell seeks guidance on data sharing" *Chronicle-Herald* (May 1, 2014) – URL: http://thechronicleherald.ca/novascotia/1204370-bell-seeks-guidance-on-data-sharing and "Taxpayers paying for government telecom snooping" *The Star* (April 30, 2014) – URL: http://www.thestar.com/news/canada/2014/04/30/harper_says_telecoms_follow_rules_in_customer_data_disclosure.html

12 Citizen Lab, Early findings from AMI requests (October 6, 2014) – URL: https://citizenlab.org/2014/10/early-findings-ami-requests/; Hilts, Andrew and Parsons, Christopher A., Right to Information in Canada: Drawing Analogue Law into a Digital Present (2014). The Winston Report, Winter 2014. Available at SSRN: http://ssrn.com/abstract=2504109

Kathy Renaud

From: Arun Bauri
Sent: Wednesday, November 26, 2014 3:29 PM
To: Christopher Prince
Subject: other CWTA stuff

I believe the CWTA also funded this report - http://officium/_layouts/OPC.Officium/Utilities/OfficiumIDLookup.aspx?id=7777-6-38625. Im not sure about the focus of the meeting, it may be related to Spencer, but they also have interest in the GPEN Sweep, m-payments, OBA , and not sure to the extent though they would be interested in the Bell OBA issue (because it doesn't just relate to internet, but extends to wireless as well).

OPC Factsheet: Openness and Accountability (April 2014)

Overview

The issue of information disclosure practices between governments and companies continue to play out prominently in the headlines.

The appropriate legal framework for allowing state investigators access to certain information held by telecommunications companies has seized the attention of citizens, legislators, privacy officials, academics, civil society and the media. Similarly, there are legal questions as to allowance made to encourage such companies to provide personal information to government agencies.

As a consequence, how often such companies provide personal information to government with or without court oversight, in what circumstances and subject to rules are now a subject of much public discussion. Statistical or general information about state access to such information would help Canadians better understand the extent of the information-sharing practices between telecommunications companies and government agencies.

Indeed, our Office has called for legislative changes that would see companies publicly reporting on disclosures of information to national security entities without court oversight. However, we continue to hear the argument that the federal law governing the collection, use and disclosure of personal information in the private-sector, PIPEDA, itself bars the disclosure of such general information.

The purpose of this factsheet is to clarify that, while there may be other relevant reasons for companies not to disclose information relating to government requests for information, PIPEDA itself is **not** a bar to companies providing the public with such information as long as it does not contain personally identifiable information.

On general transparency

Many transparency reports now being issued by various online companies already cover government requests for data by country - including Canada and the U.S. This is an encouraging development for privacy rights and consumer awareness.

Our Office has been raising the importance of transparency, most recently, in our January 2014 Special Report to Parliament: *Checks and Controls*.[i] Similarly, in our Case for Reforming PIPEDA paper issued last year, we recommended that organizations should be required to be more transparent, especially where the use of generic "lawful authority" by government investigators is used to request data on Canadian clients.[ii] The OPC has similarly urged Parliament to require greater

transparency on the part of both government agencies and commercial practices in connection with use of various investigative techniques and lawful access tools.[iii]

Indeed, openness is one of the fundamental privacy principles enshrined under Schedule 1 of PIPEDA. Under the "Openness" Principle, commercial organizations should "make readily available to individuals specific information about policies and practices relating to the management of personal information."

When organizations are ambiguous about how, when and with what frequency they receive and respond to state requests for personal information - as a matter of general policy - this can undermine consumer trust in the businesses and services they enjoy.

Privacy should not be used as cover against unwanted publicity or to avoid issues of accountability.[iv] Where no personal information is revealed or capable of being adduced through general transparency reports, privacy laws do not restrict organizations from providing such information to the public.

There may be certain legislative provisions in Canada that permit police investigators and national security authorities to shield certain activities from view for security or confidentiality reasons.[v] However, use of these exceptional provisions need to be justified in their own right.

On the specific non-disclosure provisions in PIPEDA

PIPEDA does provide a scheme for preventing an individual from knowing whether certain personal information was disclosed to a government institution in certain cases, or from being provided with access to such personal information.

Paragraphs 9(2.1) to 9(2.4) of PIPEDA set out the particular circumstances in which an organization are prevented from revealing to an individual, following a request for access to his or her personal information, the fact that information was disclosed to certain government agencies, and the procedures that must be followed in such cases.

These provisions allow the government agency in question to object to the organization responding to an access request for personal information in certain cases where investigations or intelligence-gathering would be compromised.

That being said, there is nothing in these provisions, or in PIPEDA, that otherwise prevent organizations from disclosing statistical or aggregate information on lawful access requests made by law enforcement or national security agencies.[vi]

Conclusion

While there may be other reasons why an organization may take the position that it cannot share such aggregate information, PIPEDA is not itself a bar.

The aim of PIPEDA is to protect personal information entrusted to private-sector organizations.

It does not otherwise prevent organizations from being transparent with providing general or statistical information about how many times they have received and have provided information to law enforcement or national security agencies, provided they do not in so doing disclose personal information.

---

[i] See "Augment existing review and reporting mechanisms" from *Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance* (January 2014) – URL: http://www.priv.gc.ca/information/sr-rs/201314/sr_cic_e.asp#section6-1

[ii] See "Lawful authority disclosures and lack of transparency" from *The Case for Reforming the Personal Information Protection and Electronic Documents Act* (May 2013) - URL: http://www.priv.gc.ca/parl/2013/pipeda_r_201305_e.asp#toc4e

[iii] *OPC Submission to the House of Commons Standing Committee on Justice and Human Rights on Bill C-13, An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act* (June 2014) – URL: https://www.priv.gc.ca/parl/2014/parl_sub_140609_e.asp and OPC Submission to the Senate Standing Committee on Transport and Communications on Bill S-4, An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act (June 2014) – URL: https://www.priv.gc.ca/parl/2014/parl_sub_140604_sen_e.asp

[iv] For elaboration of this idea, see the OPC Fact Sheet entitle *The Privacy Act is not an excuse to promote secrecy* (April 2006) - URL: http://www.priv.gc.ca/resource/fs-fi/02_05_d_29_e.asp

[v] Where genuine security or confidentiality obligations are justified, organizations should be as clear and specific as possible with the public about limitations placed upon them. The *Criminal Code, Canada Evidence Act* and *Security of Information Act* may well place limits on the level of detail organizations are able to provide proactively or upon individual request. Besides specific legal provisions that may have been triggered by investigators in specific instances there may also be other statutes, regulations and/or licensing agreements that compel secrecy and seek to limit publication of details. For instance, use of certain surveillance technology and access to specific commercial analysis tools stipulate confidentiality obligations as a condition of sale contracts or in ongoing tech support through end-user agreements.

[vi] However, to be clear, this is meant to be an iterative process related to specific, individualized requests for information (section 9(2.1)). It is also important to note the trigger for non-disclosure must be enunciated and documented by government authorities. It can be challenged. It is meant to be a documented, iterative process (section 9(2.2)) between the commercial firm and the government institution (section 9(2.3)). This section is not a blanket secrecy clause, and whenever these provisions are used, our Office must be notified (section 9(2.4)(b).

Kathy Renaud

From: Christopher Prince
Sent: Wednesday, December 10, 2014 11:04 AM
To: Sophie Paluck-Bastien; Patricia Kosseim
Cc: Rachel Desjardins; Josee Phillips; Daniel Therrien
Subject: RE: Meeting with CWTA

Just printing now

-----Original Message-----
From: Sophie Paluck-Bastien
Sent: Wednesday, December 10, 2014 11:04 AM
To: Christopher Prince; Patricia Kosseim
Cc: Rachel Desjardins; Josee Phillips; Daniel Therrien
Subject: RE: Meeting with CWTA

The Commissioner will be back from his speaking engagement before lunch. Can we expect to receive it by then?

-----Original Message-----
From: Christopher Prince
Sent: December-10-14 9:59 AM
To: Daniel Therrien; Patricia Kosseim
Cc: Sophie Paluck-Bastien; Rachel Desjardins; Josee Phillips
Subject: RE: Meeting with CWTA

Absolutely - just making a quick revision or two to update; will provide Charter and draft factsheet momentarily.

-----Original Message-----
From: Daniel Therrien
Sent: Wednesday, December 10, 2014 7:40 AM
To: Christopher Prince; Patricia Kosseim
Cc: Sophie Paluck-Bastien; Rachel Desjardins; Josee Phillips
Subject: RE: Meeting with CWTA

Thanks. May I see these options before today's meeting, please?

From: Christopher Prince
Sent: Monday, December 08, 2014 5:54 PM
To: Daniel Therrien; Patricia Kosseim
Cc: Sophie Paluck-Bastien; Rachel Desjardins; Josee Phillips
Subject: Re: Meeting with CWTA

Commissioner,

I have outlined some options in a project Charter which Barbara was intending to share at the next HIF meeting; a copy for reference is also with Patricia should this be front and centre at the upcoming discussion. Hopefully those possibilities should help, if Rogers or Videotron have specific approaches in mind.

Chris

From: Daniel Therrien
Sent: Monday, December 08, 2014 05:25 PM
To: Christopher Prince; Patricia Kosseim
Cc: Sophie Paluck-Bastien; Rachel Desjardins; Josee Phillips
Subject: Meeting with CWTA

Chris,

Thanks for the note for this meeting. At the end you make the point that the association wants guidance on the issue of transparency reports. We have certainly encouraged transparency reports and I will continue in that vein. We will also ask government departments to provide us with information that will allow us to assess whether the information they seek and obtain is obtained lawfully, including pursuant to the Privacy Act and Spencer. What else can we say to private sector organizations that would constitute guidance ?

Sent from my BlackBerry 10 smartphone on the Rogers network.

Kathy Renaud

From: Christopher Prince
Sent: Monday, November 24, 2014 12:39 PM
To: Barbara Bucknell
Cc: Kathy Renaud
Subject: RE: Request for BN - meet-and-greet with wireless industry

Can do

-----Original Message-----
From: Barbara Bucknell
Sent: Monday, November 24, 2014 12:36 PM
To: Christopher Prince
Cc: Kathy Renaud
Subject: FW: Request for BN - meet-and-greet with wireless industry
Importance: High

Hi Chris,

Please prepare the BN requested below. You may need to consult with others within P/R, and elsewhere within the office, to prepare the note.

Please note the date it is due to the Cr's office. I will need to see it two days before that day, Dec. 4.

Thanks!

b

Barbara Bucknell

Directrice, Politiques et recherche (intérimaire)/Director, Policy and Research (Acting)

Commissariat à la protection de la vie privée du Canada/Office of the Privacy Commissioner of Canada

819-994-5965

barbara.bucknell@priv.gc.ca <mailto:barbara.bucknell@priv.gc.ca>

From: Patricia Kosseim

Sent: November-24-14 10:52 AM
To: Sophie Paluck-Bastien
Cc: Barbara Bucknell; Helene Bertrand; Rachel Desjardins; Josee Phillips; Milene Gaudreault; Kathy Renaud
Subject: RE: Request for BN - meet-and-greet with wireless industry

Merci Sophie.

Barb, please assign. Kathy, please log in and BF.

Merci.

Pat

From: Sophie Paluck-Bastien
Sent: November-24-14 10:50 AM
To: Patricia Kosseim
Cc: Barbara Bucknell; Helene Bertrand; Rachel Desjardins; Josee Phillips; Milene Gaudreault; Kathy Renaud
Subject: Request for BN - meet-and-greet with wireless industry

Bonjour Patricia,

The Commissioner has a meet-and-greet with the Canadian Wireless Telecommunications Association on December 10. (You and I will be accompanying him; it will be a very small delegation from their side, and they have suggested and the Commissioner has agreed that there should be an equally small delegation from our side.)

We require a BN for this meeting no later than 12:00 p.m. on Monday, December 8. The BN should include a summary of our process for issuing guidance documents and anything else you feel is appropriate.

Merci!

Sophie Paluck-Bastien

Conseillère spéciale :: Special Advisor

Secrétariat de la haute direction :: Executive Secretariat

Commissariat à la protection de la vie privée du Canada :: Office of the Privacy Commissioner of Canada

819-994-5825

sophie.paluck-bastien@priv.gc.ca <mailto:sophie.paluck-bastien@priv.gc.ca>

Helene Bertrand

Subject: Rencontre avec des représentants de l'industrie du sans-fils
Location: BoardroomJ, 30 Victoria Street, Gatineau

Start: Wed 12/10/2014 2:00 PM
End: Wed 12/10/2014 3:00 PM
Show Time As: Tentative

Recurrence: (none)

Meeting Status: Tentatively accepted

Organizer: Daniel Therrien
Required Attendees: Sophie Paluck-Bastien; Patricia Kosseim; 'Anthony.Hemond@quebecor.com'; 'ken.engelhart@rci.rogers.com'; Kurt Eby (keby@cwta.ca); 'Bill.Abbott@bellalliant.ca';

s.19(1)

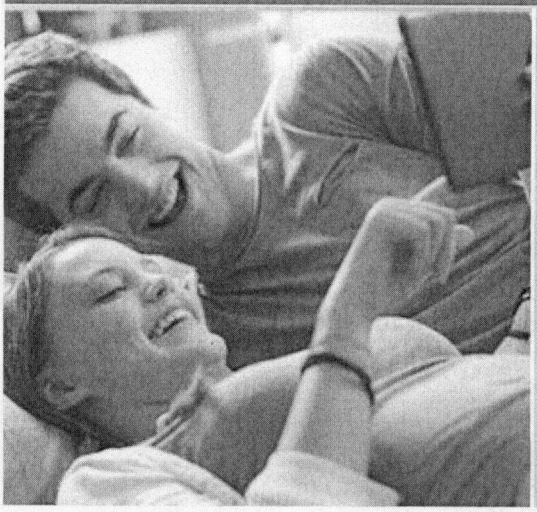
OPC contact: Josée Phillips – 819-994-5835

CTS-091166

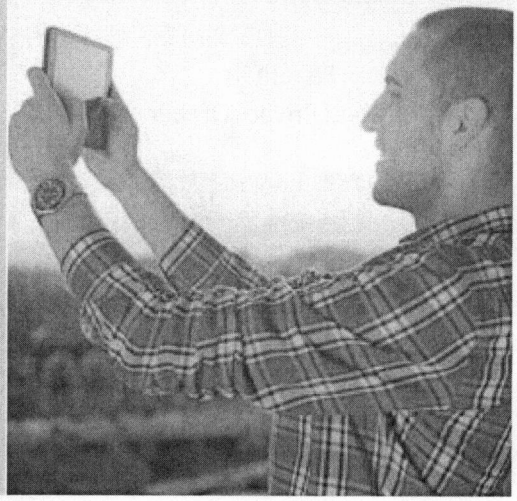
ROGERS COMMUNICATIONS

REQUESTS FOR CUSTOMER INFORMATION |

2013 TRANSPARENCY REPORT



ROGERS



INTRODUCTION

As a communications company, government and law enforcement agencies approach Rogers looking for information about our customers. This report is designed to provide more details on the number and types of requests we received in 2013.

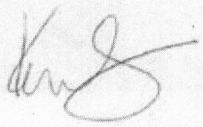
We fully comply with Canadian privacy law and take active steps to safeguard our customers' information. At the same time we are compelled by law to respond to federal, provincial and municipal government and law enforcement agencies when they have a legally valid request – like a search warrant or court order.

The requests we receive are to respond to warrants and orders from law enforcement agencies. In addition, we receive requests from government departments who are authorized to request information to enforce laws like the Income Tax Act. We also assist police services in emergency life threatening situations.

About half of the requests we receive are to confirm a customer's name and address, which we respond to so police do not issue a warrant to the wrong person. Otherwise, we only provide customer information when forced by law or in emergencies after the request has been thoroughly vetted. If we consider an order to be too broad, we push back and, if necessary, go to court to oppose the request.

Our customers' privacy is important to us and that is why we are issuing this report. We believe more transparency is helpful and encourage the Government of Canada to issue its own report on these requests.

Sincerely,



Ken Engelhart
Chief Privacy Officer

WHY AND HOW WE RESPOND

Canadian law governs how we protect private customer information and how government and law enforcement agencies can compel us to provide it to them:

- The *Criminal Code* and other laws allow government and law enforcement agencies to require us to provide customer information.
- The *Personal Information Protection and Electronic Documents Act (PIPEDA)* covers both how we protect customers' information and how we disclose it.
- The CRTC Confidential Customer Information Rules (CRTC Rules) set out circumstances under which customer information – other than name, address and listed numbers, which can always be provided – may be disclosed to third parties including law enforcement agencies.

Our Privacy Policy and Terms of Service outline how we safeguard customers' information under these laws and rules. We only give out private customer information when required by law or in emergencies and after the request has been thoroughly vetted. See Type of Requests below and our Frequently Asked Questions (FAQs) for more information.

BREAKDOWN OF 2013 REQUESTS

The statistics below represent the total number of requests we received last year. If we consider an order to be too broad, we push back and, if necessary, go to court to oppose the request.

Customer name/address checks	87,856
Court order / warrant	74,415
Government requirement letter (compelled to provide under a federal/provincial law)	2,556
Emergency requests from police in life threatening situations	9,339
Child sexual exploitation emergency assistance requests	711
Court order to comply with an international Mutual Legal Assistance Treaty request	40
Total	**174,917**

Notes:

1. These statistics include the following scenarios: (a) The information requested was provided; (b) Partial information was provided; (c) No information was provided because it doesn't exist or the person is not a Rogers customer; and (d) We rejected the request or successfully fought it in court.
2. These statistics do not include informal requests such as phone calls from law enforcement looking for information they would require a warrant for. These requests are rejected because there is no legal authority and no formal response is provided

WE RECEIVED SIX TYPES OF REQUESTS

1. **Customer name/address checks:**
   Legal authority: *PIPEDA* and CRTC Rules permit confirming basic information like name, address and listed phone number. **Details:** These requests are to confirm a customer's name and address, which we respond to so police do not issue a warrant to the wrong person. **Examples of info provided:** When provided with a name and address we will confirm whether or not the person is a Rogers customer and when provided with a listed phone number we'll provide the name and address of a customer. IP address is not provided.

2. **Court order/warrant:**
   Legal authority: Issued under the *Criminal Code* or other laws. **Details:** A court order or warrant includes production orders, summons, subpoenas and search warrants issued by a judge or other judicial officer. It compels us to provide customer information to police or other authorities or to attend court to provide evidence/testimony about customer information. **Examples of info provided:** Customer account information like name and address, payment history, billing records, or call records.

3. **Government requirement order:**
   Legal authority: Issued under laws such as the Customs Act or Income Tax Act. **Details:** An order that compels us to provide customer information to the requesting agency. **Examples of info provided:** Customer account information like payment history, billing records, or call records.

4. **Emergency requests from police in life threatening situations:**
   Legal authority: The *Criminal Code* and *PIPEDA*. **Details:** We assist police services in emergency life threatening situations such as missing persons cases and individuals in distress. **Examples of info provided:** Helping locate someone with a cell phone and providing contact details for someone who has contacted emergency services and may be unable to communicate.

5. **Child sexual exploitation emergency assistance requests:**
   Legal authority: The *Criminal Code* and *PIPEDA*. **Details:** We assist police during child exploitation investigations. **Examples of info provided:** Confirming a customer's name and address when provided with an IP address so that police can get a search or arrest warrant to stop the sexual exploitation of a child.

6. **Court order to comply with a Mutual Legal Assistance Treaty request:**
Legal authority: Issued under *Mutual Legal Assistance in Criminal Matters Act.* **Details:** We don't respond to requests from foreign agencies, but we do advise them to have their country's justice authority contact the Department of Justice Canada. If that country has a treaty or convention with Canada, the request is processed by Canadian authorities and an order may be issued by a Canadian court to gather evidence. We're compelled to provide customer information to the police or other authority in Canada conducting the investigation. **Examples of info provided:** Customer account information like payment history, billing records, or call records.

FREQUENTLY ASKED QUESTIONS

1. **Which agencies have requested information?**
We get requests from many different agencies, including:
   - > Federal agencies like the Royal Canadian Mounted Police, Canadian Security Intelligence Service, Canada Border Services Agency, and Canada Revenue Agency
   - > Provincial and municipal agencies like police forces and coroners

2. **Do you provide metadata or direct access to customer databases?**
No, we do not provide metadata without a warrant, or direct access to our customer databases. We only provide the information we are required to provide and this information is retrieved by our staff.

3. **How many times did you provide info? Do you ever reject law enforcement requests?**
Our statistics represent the total number of requests we received last year. If we consider an order to be too broad, we push back and, if necessary, go to court to oppose the request.

4. **How much do you charge for requests?**
For most court-ordered responses for customer information, we assume all costs associated with providing a response. In some cases, we charge a minimal fee to recover our costs based on the work required to comply with requests.

5. **Do you fight for customers' privacy rights?**
Absolutely, if we consider an order to be too broad, we push back and, if necessary, go to court to oppose the request. Our customers' privacy is important to us and that's why we're issuing this report. We believe more transparency is helpful and encourage the Government of Canada to issue its own report on these requests.

6. **How long do you keep customer information?**
We only keep information for as long as it's required for business purposes or as required by law. For example, we are required by law to keep customer bills for seven years. We don't keep our customers' communications like text messages and emails because our customers' privacy is important and we don't need this information.

HELPFUL LINKS

- > **Canada's** *Personal Information Protection and Electronic Documents Act*
- > **Rogers'** Terms of Service and Privacy Policy
- > **Public Safety Canada's** Annual Report on the Use of Electronic Surveillance

TELUS Transparency Report 2013

TELUS is a national telecommunications company, and as such, law enforcement agencies and government organizations regularly contact us to request specific information about our customers. This transparency report, our first, was created to provide TELUS customers and the general public with information regarding the numbers and types of information requests we received in 2013, and to provide insight into our internal practices and overall approach to complying with or challenging these requests. This report covers TELUS' telecommunications businesses, including wireline, wireless and Internet. We plan to issue this report annually.

The discussions taking place in Canada regarding transparency reporting will help to shape the future privacy landscape in Canada. Respecting our customers' privacy is an important principle of TELUS' Customers First philosophy, and with this in mind we are pleased to contribute to the evolution of the privacy dialogue with the release of this report.

One noteworthy fact this report brings to light is that more than half of all requests we received last year were in emergency situations where someone's life, health or security was threatened. We will, for example, work with agencies such as the Coast Guard and Search and Rescue, providing them the location of a device belonging to a customer who is lost while boating or hiking. Another specific example of an emergency situation occurred in July 2014, where a police agency in Alberta contacted us minutes after a car was stolen with a young child still in the back seat. We were able to help track the location of a wireless device left in the car, and within an hour the car was located and the child was found unharmed.

We handled almost 57,000 such calls last year – an average of almost 156 a day. While customer privacy is of critical importance, it is equally important we acknowledge the crucial role information plays in helping Canadians in a crisis.

TELUS®

Approximate Numbers of Requests from Government Organizations in 2013*

Court Orders/ Subpoenas** Court Orders 3,922 Subpoenas 393	4,315
Court Orders to comply with a Mutual Legal Assistance Treaty (MLAT) request	2
Customer Name and Address Checks	40,900
Emergency Calls	56,748
Internet Child Exploitation Emergency Assistance Requests	154
Legislative Demands	1,343
TOTAL	103,462

* TELUS has calculated these numbers based on how requests are recorded in our systems. We note that this may or may not be consistent with how other telecommunication services providers calculate the number of requests they receive in these categories.

** TELUS measures the number of requests in this category based on numbers of court orders or subpoenas received, rather than the number of impacted subscribers. Most court orders and subpoenas request information with respect to more than one TELUS subscriber.

The types of requests TELUS receives

Court Order/ Subpoena	**Description:** An order or subpoena is a legal demand signed by a judge directing TELUS to provide customer information. The information may be associated with any of our TELUS services, including wireline, wireless or Internet. Most orders and subpoenas require TELUS to provide historic information, such as telephone records. A small minority of the court orders require TELUS to provide real-time information; for example, the content of a telephone call (by means of a wiretap) or the location of a cell phone. Court orders obtained by law enforcement agencies are often referred to as "warrants". Of the 4,315 orders and subpoenas received in 2013, TELUS provided partial or no information in approximately 40% of the instances*. This was largely due to our limited retention periods which resulted in the requested information no longer being available. In many cases, TELUS challenged an order on the ground that it was either defective or overreaching. Most challenges involved asking a law enforcement agency to reduce the amount of customer information to be provided by TELUS pursuant to the order, so that the agency would receive only the information actually required for its purposes. In some cases, TELUS has gone to court to challenge orders which we believed to be overreaching. *This estimate was derived by sampling records maintained by TELUS' Corporate Security department. **Applicable law:** Criminal Code of Canada.
Court orders to comply with a Mutual Legal Assistance Treaty (MLAT) request	**Description:** These requests take the form of a court order issued by a Canadian court pursuant to the Mutual Legal Assistance in Criminal Matters Act. Typically, these are requests for aid from a law enforcement agency in another country related to a criminal investigation, and require an order from a Canadian court. We don't respond to requests that come directly from foreign agencies, but will provide information if ordered to by a Canadian court. **Applicable law:** The Mutual Legal Assistance in Criminal Matters Act.

Customer Name and Address Checks	**Description:** Requests to provide basic customer information, such as customer name and address. These are usually done in order to identify an individual associated with a telephone number. Previously, it was understood that such disclosure was permitted under Canadian law and TELUS' service terms. However, in light of the recent decision of the Supreme Court of Canada in the case of R. v. Spencer, TELUS has changed its practice and now requires a court order for customer name and address information, except in an emergency or where the information is published in a directory. **Applicable law:** Personal Information Protection and Electronic Documents Act (PIPEDA), CRTC rules with respect to customer confidentiality; see also applicable TELUS Service Terms and customer Privacy Commitment.
Emergency Calls	**Description:** These are usually urgent requests for help locating or assisting an individual where their life, health or security is at risk. For example, TELUS will provide police or other emergency responders with location information for a wireless device belonging to someone who is lost or in danger. In these cases we only provide the information needed to respond to the emergency. TELUS is the incumbent local exchange carrier (the traditional home phone service provider) in British Columbia, Alberta and Eastern Quebec and is responsible for providing technical support for 911 services in those areas. TELUS handles a large number of calls from 911 call centers (32,618 in 2013) and local police and other emergency responders (24,130 in 2013) in order to support 911 and emergency services. **Applicable law:** PIPEDA and CRTC rules with respect to customer confidentiality.
Internet Child Exploitation Emergency Assistance Requests	**Description:** In response to police requests, TELUS disclosed the name and address of a customer using an IP address to help the police investigate a case of online child sexual exploitation. Previously, it was understood that such disclosure without a court order was permitted under Canadian law and TELUS' service terms. However, the Supreme Court of Canada in the Spencer case (referred to above) has ruled that such disclosure requires a court order, except in an emergency. Accordingly, TELUS has amended its practices in this regard. **Applicable law:** PIPEDA, Criminal Code of Canada.
Legislative Demands	**Description:** A request for information by a government body, where TELUS is required by applicable legislation to provide the information. For example, pursuant to the Income Tax Act, the Canada Revenue Agency may require TELUS to disclose certain customer information. **Applicable law:** Any federal or provincial legislation that authorizes a government body to request information from TELUS

When does TELUS fulfil requests for customer information?

TELUS will provide customer information to law enforcement agencies or other government organizations where authorized or permitted by our service terms, customer Privacy Commitment, a valid court order or other applicable laws.

More than half of the disclosure requests we received in 2013 related to emergency situations. The information provided ranged from simply providing the street address of a customer who called 911, to more complex information requests such as locating a wireless device belonging to someone who was lost or in difficulty.

When will TELUS challenge a court order?

TELUS will challenge any court order that we believe goes beyond what a judge is authorized to order under applicable legislation, such as the Criminal Code. For example, TELUS recently challenged a general court order obtained by a law enforcement agency requiring the provision of text message data on a nearly real-time basis, and successfully pursued the matter all the way to the Supreme Court of Canada. The resulting Supreme Court decision enhanced the privacy rights of TELUS customers and other Canadians.

What is the process for responding to information requests?

TELUS has a process for carefully assessing information requests received from law enforcement agencies and other government organizations:

- A request is received and logged by TELUS' Corporate Security department.
- A specially trained and authorized TELUS Security team representative reviews the request to ensure it has been correctly prepared and is legally valid. In the case of emergency calls, this involves obtaining confirmation that the situation involves an imminent risk to an individual's life, health or security.
- If the representative has any concerns, those concerns are brought to the attention of a supervisor, TELUS' legal department, or the agency or organization, as appropriate, for resolution.
- Once the representative is satisfied that the request is valid, they will take appropriate steps to properly respond to the information request. For example, this could include searching relevant TELUS databases for the requested information.

Frequently Asked Questions

1. **How long does TELUS keep my information?**

   TELUS keeps customer information only as long as necessary to comply with the law and to fulfill our business purposes. For example, TELUS retains copies of customer bills for approximately seven years to satisfy legal requirements. TELUS also retains call detail records for billable calls made by our customers on our network for a period of up to 14 months for network management and billing purposes. As another example, TELUS retains logs of Internet Protocol (IP) addresses for a period of 90 days for network management purposes.

2. **What legislation applies to the protection of customer privacy?**

   TELUS' telecommunications businesses are governed by the federal Personal Information Protection and Electronic Documents Act (PIPEDA) and by rules prescribed by the CRTC with respect to customer confidentiality.

   This report covers TELUS' telecommunications businesses, including wireline, wireless and Internet.

3. **Does TELUS charge for providing information in response to requests?**

   TELUS is allowed to recover some costs for complying with certain types of information requests, but not others. TELUS bears most of the cost of complying with the types of requests referred to in this report.

4. **How do you strike the right balance between protecting your customers' privacy rights and fulfilling these information requests?**

   We take great care to safeguard personal information and ensure that our customers' privacy and confidentiality are preserved wherever possible. While some people may think that telecommunications companies hand over customer information to law enforcement agencies and government organizations without question, TELUS challenges information requests when we believe the request goes beyond what is lawful. We only release confidential customer information when we are satisfied it is appropriate to do so.

TELUS®

5. **What is the difference between a court order and a subpoena?**

A court order requires TELUS to provide customer information or to assist the police in conducting some activity; for example, intercepting a communication or tracking the location of a cell phone. A subpoena requires a representative of TELUS to bring some customer records to court and, if necessary, to provide oral testimony with respect to those records.

6. **Why have you decided to release a Transparency Report?**

The discussions taking place in Canada regarding transparency reporting will help to shape the future privacy landscape in Canada. Respecting our customers' privacy is an important principle of TELUS' Customers First philosophy, and with this in mind we are pleased to contribute to the evolution of the privacy dialogue with the release of this report.

7. **Will you be producing Transparency Reports in the future?**

We plan on releasing Transparency Reports annually.

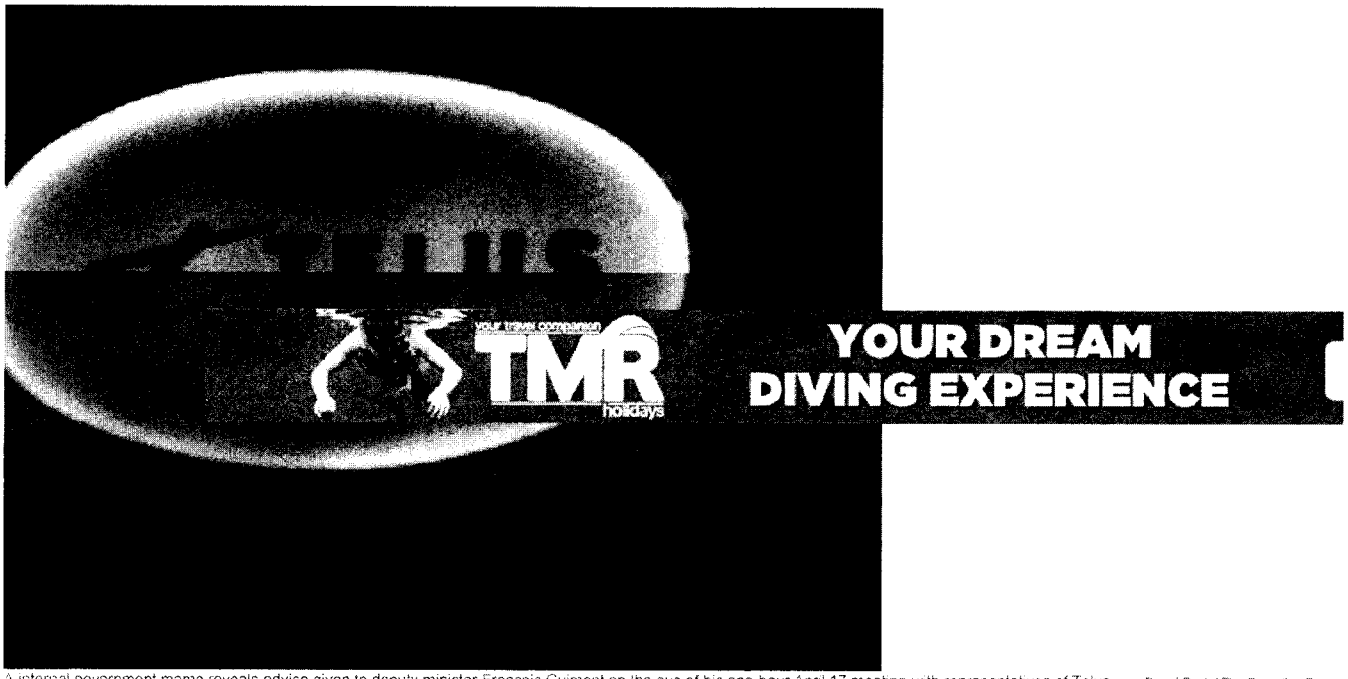
For more information about TELUS' privacy practices, visit our website at
http://about.telus.com/community/english/privacy

For more information about our Corporate Social Responsibility Report 2013, visit
http://csr.telus.com/en/

TELUS
the future is friendly®

Feds were worried as telecom firm planned to go public on police access to Canadians' phone calls and emails, memo shows

NP JIM BRONSKILL, CANADIAN PRESS | December 1, 2014 | Last Updated: Dec 1 11:03 AM ET
More from Canadian Press



A internal government memo reveals advice given to deputy minister Francois Guimont on the eve of his one-hour April 17 meeting with representatives of Telus Corp. to discuss specifically what information the company was allowed to tell the public about electronic surveillance activities Darryl Dyck / The Canadian Press

OTTAWA — A move by telecommunications firms to be more forthcoming with the public about their role in police and spy surveillance could divulge "sensitive operational details," a senior Public Safety official warned in a classified memo.

Company efforts to reveal more about police and intelligence requests — even the disclosure of broad numbers — would require "extensive consultations with all relevant stakeholders," wrote Lynda Clairmont, senior assistant deputy minister for national and cybersecurity.

Clairmont's note, released under the Access to Information Aet, provided advice to deputy minister Francois Guimont on the eve of his one-hour April 17 meeting with representatives of Telus Corp. to discuss specifically what information the company was allowed to tell the public about electronic surveillance activities.

Telus released a so-called "transparency report" five months later, revealing it had received more than 103,000 official requests for information about subscribers in 2013.

Rogers Communications published a similar report in June — three months before Telus — becoming the first of the major Canadian telecom firms to issue one. Bell Canada, the other major company, has yet to release a report.

In shadow of NSA revelations, Rogers, TekSavvy open up on government data requests

In the wake of blockbuster revelations by former NSA contractor Edward Snowden, Canada's telecommunications companies are starting to pull back the curtains on their relationships with government authorities around the sharing of customer information.

Follow

The internal Public Safety memo sheds new light on behind-the-scenes tensions between government officials and industry amid pressure from privacy advocates and civil libertarians for details of the scope and nature of law enforcement access to Canadians' subscriber information, phone calls and email messages.

The demand for more transparency was fuelled by leaks from former American intelligence contractor Edward Snowden, whose significant disclosures revealed the U.S. National Security Agency had access to a huge volume of telecommunications data.

The revelations prompted a flurry of questions about the activities of the NSA's Canadian counterpart, the Communications Security Establishment, as well as the Canadian Security Intelligence Service and the RCMP.

We recognize that transparency is key to giving Parliament and Canadians confidence in our ability

Rogers Communications Inc. on Thursday released what it called its 2013 Transparency Report, a brief four-page document detailing the number and types of requests the company has received, and the legal framework governing its response.

The Rogers report comes on the heels of similar disclosure from independent communications provider TekSavvy Solutions Inc. Other providers are expected to follow suit later this year.

Rogers said it received a total of 174,917 requests for information last year, or the equivalent of about 1.75% of the company's roughly 10 million individual customers.

Read more ...

The Public Safety Department is committed to protecting the security of Canadians while respecting their privacy, Clairmont wrote in her April 16 memo to Guimont, stamped "Secret/Canadian Eyes Only."

"We recognize that transparency is key to giving Parliament and Canadians confidence in our ability to meet both these objectives, but must continue to ensure that sensitive operational details remain protected."

There was a need to evaluate whether such details could be revealed even through "mass aggregate reporting of data," she added.

A month before Telus's scheduled meeting with Guimont, the company said it was prohibited from disclosing certain information by a governing docume

Related

Byron Holland: Rise of the surveillance state

In a letter to Christopher Parsons of the University of Toronto's Citizen Lab, a digital rights body, Telus privacy officer Heather Hawley said the company would ask the government to "clarify and limit the scope of current confidentiality requirements and to consider measures to facilitate greater transparency."

Neither Telus and Public Safety would make anyone available to answer questions about their discussions.

Rogers spokesman Kevin Spafford said the company did not talk with the government about its June transparency report before it was published.

The report said Rogers received almost 175,000 requests for customer information from government and police agencies last year. Of those, 74,415 were made under a warrant or court order, including production orders, summons, subpoenas and search warrants issued by a judge or other judicial officer.

In deciding what to disclose in its transparency report, the company abided by just one restriction, Ken Engelhart, chief privacy officer for Rogers, said at the time.

"The only legal restraint is that you can't even give a number of wireless interceptions that you do — that's like a wiretap, but it's a wireless tap," Engelhart said in an interview.

It was important to get a transparency report out, he continued.

"I'm hopeful it won't bother the law enforcement people, but if it does, we thought that the needs of our customers came first."

Stephen Harper thanks Muslims for condemning attacks

Newsbite: December 4, 2014

Newsbite: December 3, 2014

Newsbite: December 2, 2014

Find National Post on Facebook

Most Popular

Stephanie Moseley shot dead by rapper husband in L.A....

'Calgary's worst driver?' Watch woman hit car as she...

The university sexual assault overcorrection: How...

Discovery's 'Eaten Alive' guy isn't actually eaten alive...

Topics: **Canada**, **Canadian Politics**, **News**, **Government Surveillance**, **Public Safety**, **Telecom**

Comments for this thread are now closed.

RCMP drops some internet-related probes following Supreme Court ruling

Justice department 'examining the need for potential remedies'

By Jim Bronskill, The Canadian Press Posted: Nov 21, 2014 7:57 AM ET Last Updated: Nov 21, 2014 1:45 PM ET

The RCMP has abandoned some investigations because of a key Supreme Court ruling that said police require a warrant or other legal tool to obtain basic internet subscriber information, an internal government memo says.

- **Online privacy decision means 'back to the drawing board' for Tories**
- **Daniel Therrien grilled on views about police powers in cyberbullying bill**
- **Stockwell Day calls for changes to cybercrime bill**

The Mounties and Canada's spy and border agencies are "very concerned" about increased paperwork and delays now involved in obtaining such information, the newly disclosed memo says.

In addition, the Justice Department is "examining the need for potential remedies" following the landmark June ruling.

The Public Safety Canada note is perhaps the first concrete indication from federal police and intelligence officials of how the Supreme Court decision is affecting their work.

A copy of the memo was released to The Canadian Press under the Access to Information Act.

Basic subscriber information includes a person's name, phone number and internet protocol (IP) address, but not the actual content of messages or their metadata, such as time stamps and routing codes.

Before the Supreme Court decision, law-enforcement agencies submitted hundreds of thousands of warrantless requests for such data annually to telecommunications companies, and they complied in about 95 per cent of cases.

Telcos have 'erred on the side of caution': memo

At least two major telecommunication firms, Rogers and Telus, have since stopped routinely disclosing basic customer information without a warrant or production order.

The memo says telecom companies "have erred on the side of caution" by requiring warrants for all basic subscriber information requests except listed landlines and emergency demands.

The RCMP, Canada Border Services Agency and Canadian Security Intelligence Service "are very concerned about the potentially unsustainable resource and operational fallout" from the June ruling, the memo adds.

Prior to the court decision, the RCMP and border agency estimate, it took about five minutes to complete the less than one page of documentation needed to ask for subscriber information, and the company usually turned it over immediately or within one day.

The agencies say that following the Supreme Court ruling about 10 hours are needed to complete the 10-to-20 pages of documentation for a request, and an answer can take up to 30 days.

Banks, car rental companies also review ruling

Applying for a production order requires that all the elements of an offence under the Criminal Code have been met but — posing a Catch-22 — basic subscriber information is often needed to meet that threshold, the memo says.

For instance, a child could receive a "creepy" email from someone, but that might not be enough to fulfil the requirements of a child-luring offence.

"Evidence is limited at this early stage, but some cases have already been abandoned by the RCMP as a result of not having enough information to get a production order to obtain (basis subscriber information)," the memo says.

Other concerns outlined in the note:

- Some telecom providers keep internet protocol logs for 30 days or less, and they may be erased by the time a company processes a production order;
- Banks, hotels, and car rental companies are reviewing the Supreme Court decision and "a few have signalled less voluntary co-operation" in future.

Still, the federal privacy commissioner said Thursday there appears to be wide variation in how the Supreme Court ruling is being interpreted.

Privacy watchdog calls for clarity

As a result, Canadians are still in the dark about what may happen to their personal information, Therrien told a Senate committee studying the government's cyberbullying bill.

Complicating matters is an immunity provision of the bill that would protect companies from legal liability should they voluntarily disclose personal information in response to requests without a warrant.

Therrien urged Parliament to put an end to the ambiguity and clarify what — if anything — remains of the common-law policing powers to obtain information without a warrant.

The Public Safety memo says the department and other federal agencies continue to "document the resource and investigative impacts" of the court decision.

"Justice Canada is gathering information and examining the need for potential remedies."

Office of the Privacy Commissioner of Canada

Appearances before Parliamentary Committees

Appearance before the House of Commons Standing Committee on Finance on Part IV, Bill C-43 (*Economic Action Plan 2014, No 2*)

November 24, 2014
Ottawa, Ontario

Opening Statement by Daniel Therrien
Privacy Commissioner of Canada

(Check against delivery)

Good afternoon, Mister Chair, and Members of the Committee.

Thank you for the invitation to present my views on the possible privacy implications of Part IV, Bill C-43, the *Economic Action Plan 2014, No. 2*.

I have provided written submissions on various parts of the Bill, and would like to summarize my comments as follows:

With respect to Division 17, which contains amendments to the *DNA Identification Act*, I agree that society is well served by intensifying humanitarian efforts to locate missing persons and identify human remains. Creating a DNA databank is a reasonable way of achieving these objectives.

However, I have some reservations about the extent to which the Bill permits the cross matching of the proposed new indices for these humanitarian purposes with the existing crime scene index (CSI) and convicted offender index (COI), which serve law enforcement purposes.

When families provide the personal effects of the missing person or their own biological samples, they are doing so to find their missing loved one or to achieve a sense of closure.

While the Bill recognizes that the profiles of relatives can only be compared to the missing persons and human remains indices for these purposes, the profiles of missing persons should likewise be similarly restricted and not linked to the CSI and COI to serve law enforcement purposes. If, however, the profiles of missing persons are to be matched against the CSI or COI, and any resulting matches to be used for law enforcement purposes, the relative who provided the personal effect of the missing person should be informed of, and consent to this matching.

I am also concerned about provisions that would increase information sharing with foreign states. This again involves the cross matching of missing persons profiles with domestic and foreign crime scene profiles, potentially leading to the investigation of an offence in a foreign state that may not be one under Canadian law. I would therefore recommend that these provisions to increase such sharing be removed from the Bill.

Regarding Division 24, concerning amendments to the *Immigration and Refugee Protection Act* and the Temporary Foreign Workers program, I am primarily concerned with expanded use and sharing of the Social Insurance Number (SIN), and enhanced authority for information sharing with the provinces. While it is appropriate for Employment and Social Development Canada to use the SIN for employment-related purposes, the Bill is vague on the specifics of how the SIN will be handled, and it is not clear whether the SIN could be collected and shared beyond the employment context. I would wish to be consulted on the

content of the regulations, which will include details on the use of the SIN and enhanced authority to share information with provincial governments. I would also recommend that any SIN-related privacy issues be identified in comprehensive Privacy Impact Assessments, and that any associated privacy risks be mitigated to the extent possible.

In terms of Divisions 6, 10, and 11, in my view, there do not appear to be significant privacy issues of concern raised in these sections. Indeed, one amendment would allow the CRTC to impose on persons who provide telecommunications services (other than Canadian carriers) conditions to protect the privacy of persons using those services. I view this as a positive move from a privacy perspective.

Divisions 9, 18, 27 and 28 appear to implicate some personal information. However, it is not evident that they raise any significant privacy issues.

And with that, I welcome your questions.

Date Modified: 2014-11-24

Office of the Privacy Commissioner of Canada

Appearances before Parliamentary Committees

Bill C-13, the *Protecting Canadians from Online Crime Act*

Submission to the Standing Senate Committee on Legal and Constitutional Affairs

November 19, 2014

The Honourable Bob Runciman, Senator
Chair, Standing Senate Committee on Legal and Constitutional Affairs
The Senate of Canada
Ottawa, Ontario
Canada, K1A 0A4

Dear Mr. Chair:

Thank you for the invitation from the Committee to present the views of the Office of the Privacy Commissioner of Canada (OPC) in connection with Bill C-13, the *Protecting Canadians from Online Crime Act*. As the debates both in Parliament and among Canadians attest, the Bill engages complex legal, technical and privacy issues. We hope this submission will assist your study of the legislation.

General background

We regard the first aim of the Bill as commendable, specifically the sections treating the serious issues of online bullying, harassment and non-consensual circulation of intimate images. Stalking through social networks, cyber-bullying and other forms of Internet exploitation are demeaning forms of abuse that affect Canadians, especially young people. Clearly, Internet bullying and online shaming can have lasting privacy repercussions for victims. Parents, teachers and police have called for reform, and rightly so.

As a consequence, we believe that the criminalization of the distribution of intimate images without consent and extending *Criminal Code* provisions to cover new channels of communication will send an important signal that such offensive actions will not be tolerated. Canadians surely have a legal right to be free from harassment, bullying and personal invasion in the physical world. In a digital era, government must work to ensure these rights are equally respected online.

Summary of privacy issues

In our submission, the main privacy issues that arise in the context of Bill C-13 relate to the other provisions that propose to expand the investigatory powers afforded to peace officers and public officers under the *Criminal Code*. Given our advisory function to Parliament, we would like to highlight four specific privacy issues stemming from these aspects of the Bill that merit close scrutiny:

- The thresholds for the use of the new powers and procedures;
- The range of departments, agencies and officials who can use these powers;
- The transparency and accountability framework governing their use; and,

- The need for legal clarity (following the Supreme Court of Canada decision in *R. v. Spencer*) on warrantless requests, voluntary disclosure, and legal immunity.

Thresholds for the use of the new powers and procedures

One aim of the Bill is to amend various legal thresholds for the use of the new investigative powers and procedures. What follows is a list of the new powers, their duration and the legal threshold for their authorization:

Investigative Power	**Example of data *obtained***	**Threshold**
Preservation demand - 21 days (s. 487.012)	No data	suspicion
Preservation order – three months (s. 487.013)	No data	suspicion
General production order (s. 487.014)	Any stored data	belief
Production order to trace specified communication (s. 487.015)	Email, Internet Protocol (IP) and MAC addresses	suspicion
Production order – transmission data (s. 487.016)	IP addresses, website domains / pages visited, file sharing and other protocols, packet numbers, search engine search terms and email addresses	suspicion
Production order – tracking data (s. 487.017)	Location information, GPS coordinates	suspicion
Production order – financial data (s. 487.018)	Account holder information, types of accounts, date of account, current address	suspicion
Warrant for tracking device – transactions and things (s. 492.1 (1))	Locations of credit or bank card usage, movements of vehicles	suspicion
Warrant for tracking device – individuals (s. 492.1(2))	Location of tracked individual (via personal mobile device)	belief
Warrant for transmission data recorder (s. 492.2)	See above	suspicion

The bulk of the new powers may be used where investigators have a mere *suspicion* of wrongdoing, as opposed to a higher threshold of reasonable *belief* that the search will provide evidence of a specific crime. The difference between these two thresholds represents a marked difference in privacy protection.

The potential level of government intrusion must be matched by commensurate judicial scrutiny and an appropriate legal standard for authorization. There should be evidence of a higher probability of wrongdoing before information about individuals' private communications or their digital activities are compelled. Downgrading to a "reasonable suspicion" standard should be a necessary and proportionate response to a demonstrated problem, and in our view, a more compelling case for the use of a reduced legal threshold must be presented and thoroughly examined.

Courts have upheld the lower reasonable suspicion standard only in limited situations where privacy interests are reduced or where state objectives of public importance are predominant. The government defends the lower thresholds in Bill C-13 in part based on the argument that the information sought is not very sensitive and triggers a lower expectation of privacy. With respect, we think that argument does not give appropriate weight to the teachings of the Supreme Court of Canada in the recent *R. v. Spencer* decision. In that case, the Supreme Court clearly held that the protection of privacy interests requires us to look not only at the specific information being sought – no matter how seemingly innocuous – but also at what the information may further reveal.

The powers provided under Bill C-13 will allow access to potentially sensitive personal information for all manner of investigation and enforcement action. Electronic surveillance and data analyses have become increasingly powerful in the digital era, given that every transaction, every message, every online search, every call and movement across the Internet leaves a recorded trace and is, therefore, potentially subject to scrutiny. While others have argued that the higher threshold should be reserved for the content of communications, we would stress that various forms of transaction and transmission data could be just as sensitive and revealing depending on the context.

As the Supreme Court noted in *Spencer*, "the Internet has exponentially increased both the quality and quantity of information that is stored about Internet users," and that such information can "provide detailed information about users' interests." To underscore this point, we include a technical and legal overview of ***Metadata and Privacy***, a report published by my office last month, which demonstrates the various forms of personal data that could be derived from metadata obtained at the lower legal threshold being proposed by the Bill. An accompanying infographic and link to the full report can be found in the Annex to this submission.

Some witnesses who have appeared before this Committee have argued that they require a lower threshold for authorization in order to access information at the early stages of an investigation. Indeed, the "reasonable suspicion" standard requires less groundwork for investigators and fewer facts to be put before court officers reviewing requests for surveillance. But would having a higher threshold, as some have suggested, impede effective investigation and prosecution of online crime, and carve out a crime-friendly Internet landscape? We do not believe so. Again, in *Spencer*, the Court rejected that argument noting that the police, in that case, had ample information to obtain a production order for what they needed even at the early stages of the investigation.

If the "reasonable suspicion" standard is kept, there are no legal limitations at this point to prevent the various authorities who can avail themselves of these new powers from using the evidence gathered for broad surveillance or fishing expeditions. For example, once public officials have information based on mere suspicion for purposes of investigating a specific crime, there is currently no legal limitation to prevent this open-ended category of public officers from using potentially sensitive information for a multitude of other, much less compelling circumstances. In short, the proper thresholds do not depend, as the Supreme Court has said, on whether privacy shelters legal or illegal activity, or on the legal or illegal nature of the information being sought. The issue, therefore, is not one of concealing illegal use of the Internet for cyberbullying or child pornography at all costs. Rather, it is a matter of preserving the privacy interests of all Canadians generally "with respect to computers which they use in their home for private purposes."

Fundamentally, it is our view that reasonable suspicion is too low a threshold for allowing a wide assortment of public officers, and for a multitude of purposes, to access personal information that can be so revealing. Therefore, I recommend it be replaced by a "reasonable grounds to believe" threshold with respect to the new productions orders and warrants. Alternatively, if the "reasonable grounds to suspect" standard is maintained, the Bill should clarify that the use of evidence gathered pursuant to such a court order should be limited to investigating only the alleged crime specified in the court application and not for other purposes.

Recommendation: While "reasonable suspicion" may be acceptable for preservation of data, the traditional standard of "reasonable grounds to believe" should continue to prevail as the appropriate judicial threshold for the authorization of the new production orders and warrants being proposed. Alternatively, should the Committee support the lower standard of reasonable suspicion, we recommend limiting the use of information obtained through those powers to the investigation of the alleged crime specified in the court application and not for other purposes.

Range of departments, agencies and officials who can use new powers

A second aspect of the Bill that merits serious scrutiny is the wide range of governmental authorities and governmental bodies – well beyond police - that will be able to use the new investigative powers. A very broad range of actors - at all levels of government - will be able to avail themselves of the new investigative powers including demanding the preservation of data, seeking production of personal records

or private communications, or requesting warrants to collect tracking data associated with vehicles, transactions or individuals.

The language in proposed section 487.011 of the *Criminal Code* defines a public officer as anyone "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." That means that, in addition to police officers, the Bill will empower mayors, wardens, reeves, sheriffs, certain airline pilots, customs officers, fisheries officers, and any federal or provincial officer whose duties include the enforcement of a federal or provincial law.

While police organizations and security agencies have some form of oversight and reporting requirements, other actors falling under the definition of "public officer" are not subject to dedicated review or required to report on the use of surveillance powers. Given these gaps in accountability and oversight, we would urge caution in providing such a wide range of actors with such significant search powers, especially where, in our view, a demonstrable case has not yet been made.

Recommendation: Use of the proposed search powers should be limited to traditional "peace officers" engaged in criminal investigations. Alternatively, the open-ended category of public officers should be replaced by a closed list of designated public officers who would be afforded these new powers in respect of specific legislative duties.

Transparency and accountability for the use of the powers

In our view, the lack of provisions requiring transparency or regular public reporting on the use of the new powers is a concern. On the commercial side, many Internet service and telecommunications companies have begun voluntarily reporting on a regular basis, aggregate data on the numbers and categories of instances where they have shared information with law enforcement agencies. Companies, like government institutions, also need to concern themselves with openness, transparency and public trust.

In terms of reporting to Parliament and the public on how surveillance measures are used, Canada already has a model precedent to consider with respect to federal law enforcement. Since 1977, the *Annual Report on the Use of Electronic Surveillance* tabled annually in Parliament (pursuant to section 195 of the *Criminal Code*) has provided a model for reporting on sensitive investigations. These provisions were updated and extended by new legislation as recently as March 2013 pursuant to directions set out by the Supreme Court of Canada.

Annual reporting on the new powers would mesh with the existing process to provide a measure of transparency and accountability. Reported statistics would also provide Parliamentarians and the public with insight into the usage, results and overall effectiveness of such powers. Finally, they would also support the statutory review of the provisions by a House of Commons Committee as is being proposed under section 487.021.

Recommendation: The new powers listed in sections 487.011 to 487.02 as well as warrantless requests should be subject to regular public reporting as required under section 195 of the *Criminal Code* for other forms of electronic surveillance

Legal clarity (post-Spencer) on government requests, voluntary disclosure, and legal immunity

A final concern of our Office relates to the Bill's proposed new section 487.0195 of the *Criminal Code*. This immunity provision would protect from legal liability those persons who voluntarily disclose personal information in response to government requests without a warrant. Where the state seeks access to personal information held by organizations, including Internet service providers, *R. v. Spencer* clearly

limited warrantless searches to situations where there are exigent circumstances, a reasonable law, or where the information does not attract a reasonable expectation of privacy.

Carrying out a "reasonable expectation of privacy" analysis is complex, highly contextual and difficult for organizations and individuals to undertake in each individual case. This will place an unfairly heavy burden on organizations especially where they might lack the time, knowledge or resources to challenge or refuse such requests. In our view, the immunity provision will exacerbate ongoing confusion with respect to organizations' obligations under paragraph 7(3)(*c.1*) of the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Even after the Supreme Court of Canada's decision in *R. v. Spencer*, companies and government are still debating the concept of "lawful authority" for the purposes of 7(3)(*c.1*) of PIPEDA.[1]

As a result, Canadians remain in the dark as to what may happen to their personal information. The government claims that nothing in Bill C-13 needs to be changed as a result of *R. v. Spencer*, leaving Canadians to wonder what impact the ruling has, if any. In response to various MP questions regarding warrantless requests made to third party organizations over the past few years, several departments and agencies provided little or no data. While some telecommunications companies have announced that they would no longer provide personal information to law enforcement absent judicial authorization, a reasonable law or exigent circumstances, other companies provided no such assurance.

We would therefore urge the Committee to put an end to this state of ambiguity and clarify what, if anything, remains of the common law policing powers to obtain information without a warrant post-*Spencer*. This would provide clarity to individuals, private-sector organizations and law enforcement officials as to when the state can obtain personal information via warrantless access. Bill C-13 should be amended to state explicitly that discretionary disclosures to law enforcement following a request should be permissible only under a reasonable law, with judicial authorization or in exigent circumstances.

While some may argue that this would remove an important investigative tool for law enforcement to gather information outside these situations, we see no need to maintain a tool that permits disclosure of personal information below what is already a low threshold of reasonable suspicion. Alternatively, to achieve greater certainty for Canadians about what can or cannot be done with their personal information, Parliament could prescribe limited circumstances under which personal information which does not attract a reasonable expectation of privacy could be disclosed.

Recommendation: The proposed section 487.0195 should be amended to state explicitly that personal information may only be disclosed to law enforcement in the presence of a reasonable law, judicial authorization or exigent circumstances. Alternatively, Parliament could prescribe limited circumstances under which personal information which does not attract a reasonable expectation of privacy could be disclosed.

Conclusion

In sum, it is important to remember that these new investigative tools would sweep up vast amounts of potentially sensitive personal information by an open-ended group of authorities for a wide range of purposes, without any public reporting requirements. Thank you once again for the opportunity to present the Committee with our views on the proposal. We look forward to the discussion and any questions of your Members in connection with the current study.

Sincerely,

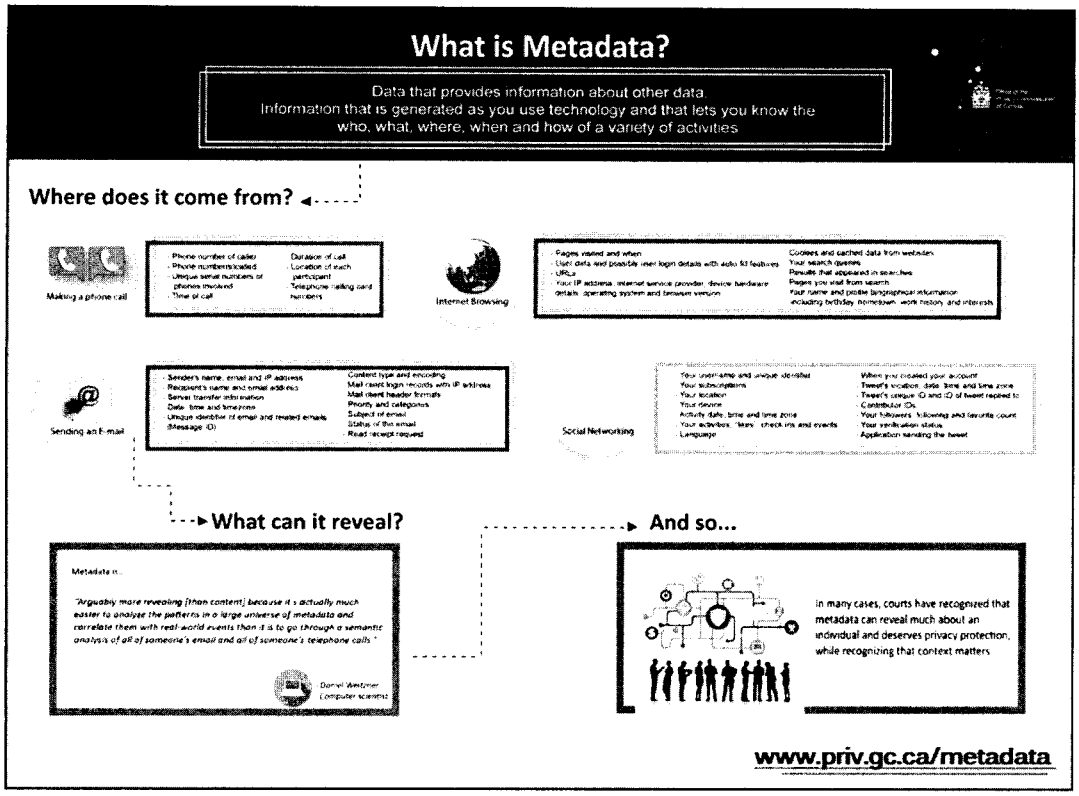
Original signed by

Daniel Therrien
Privacy Commissioner

Encl.

c.c Shayla Anwar, Clerk

Annex – Forms and examples of metadata subject to access and surveillance through new warrant provisions in Bill C-31



[text version]

PDF Version

---

[1] Under this provision, an organization may disclose personal information to a government institution or part of a government institution without the knowledge or consent of the individual if the government institution has requested it; has identified its "lawful authority" to obtain the information; and has indicated the information is for the purpose of law enforcement (among others).

Date Modified: 2014-11-20

Date Dec. 10, 2014

Meeting w CTWA

(Suzanne Morin, (Quebecor) Antony, (CWTA) Kurt & Ken E. (Rogers)
Bill Abbott (Bell)

1) R. v. Spencer

2) Lawful Access

3) Warrantless Disclosure.

4) Future relp w OPC

5) Transparency Reporting.

s.19(1)

[redacted]

1) CdN Coalition A/ Child Exploitation
CCASE was created to facilitate rapid investigations; created protocol form - ONLY for child exploitation cases. (couple years after R v. Plant)

R v. Spencer → case used the older protocol. Newer protocol explicitly states that PIPEDA

is NOT the lawful authority.

Now, since R. v. Spencer, have all stopped & no longer respond to CCASE letters).

Also since Spencer, police can/should get a warrant in these cases - But since they hv to so anyway, they ask for a lot more than they would otherwise without a warrant.

other info → more than CNA
+ payment info
+ other phone #'s.

Everyone has stopped using the CCASE letter.

May hv stopped CNA requests, but not necy all - not sure.

Law is clear; we follow the law

Date

2) Past rel'ns w OPC

↳ Telco's came to meet w OPC to discuss Lawful access requests. Came together as an industry & respon

1.1 million requests in 2010

↳ pro-active discussions on part of industry.

Comr interested in better understd the practice & preparing posn on previous legl proposals

Subst Lawful access bills have gotten narrower as a result of

[redacted]

In 2011, industry responded to OPC's request in the aggregate thru advice of counsel.

s.19(1)
s.20(1)(c)

Page

s.19(1)
s.20(1)(c)

Date

Asked once, met and responded right away.

[redacted]

⊛ Com'R will ask for greater clarity on b/2 of individuals, and for orgNs b/c to comply w law, without imputing bad faith

[redacted]

s.19(1)
s.20(1)(c)

Date

[redacted]

Have stopped CCASE requests.

[redacted]

But these hv stopped post Spencer

s.19(1)
s.20(1)(c)

Date

No metadata being provided by indy to law enforcement in Cda.

Yes to a warrant, No otherwise

[redacted]

s.19(1)
s.20(1)(c)

Date

[redacted]

Con'R
↳ some legal reqt's to disclose
↳ some non-sensitive
↳ no meta-data to natNL security w/out a warrant

Wd transparency reports help clarify all this?

[redacted]

s.19(1)
s.20(1)(c)

Date

What can we do to make things better?

Possible area of collaboration = transparency reporting.

if you understd the industry - they seem normal.

[redacted]

Transparency Report - maybe we cd work together on, and invite sent to join discussion.

↳ Stakeholder roundtable to discuss elements of a transparency report. std.

Page

Date

Guidelines → ed help industry stdz and adapt their systems to be able report on responses to requests.

C.R

- open in principle to the idea & we'll get back to you on this.

We are working on encouraging transparency on public sector side.

We are also supporting telco's recent transparency reports.

Page

Kathy Renaud

From: Melanie Millar-Chapman
Sent: Wednesday, December 10, 2014 3:54 PM
To: Christopher Prince; Arun Bauri
Cc: Barbara Bucknell
Subject: rough notes on mtg with telcos, etc.
Attachments: lawful access - Dec 10 2014.docx

Attending: Daniel Therrien; Sophie Paluck-Bastien; Patricia Kosseim; 'Anthony.Hemond@quebecor.com'; 'ken.engelhart@rci.rogers.com'; 'Kurt Eby (keby@cwta.ca)'; 'Bill.Abbott@bellalliant.ca'; [redacted] and me

s.19(1)

Mtg with Can Wireless orgs – Dec 10th

Prep – we are told of 2 items they will raise:

- A template for reporting that they provide consistent info that we like so they can use (categories for warrants – now that C-13 has received royal assent – we should ask for breakdowns – they may pushback on cost of tracking this, which ones made in the context of child exploitation, customer name and address checks – what are the scenarios for them to confirm name and address (Spencer) or simply whether this person is a customer, also – we should get confirmation about what they. [redacted]
- Suggest a forum for industry and gov for us to convene? Cssr would want civil society – [redacted]

Meeting Notes

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

Suzanne – 5 things:

1 Spencer – history and what's changed

2 lawful access generally and higher level interactions

3 warrantless disclosures

4 rebuilding trust – relationship w

5 transparency reporting

**

s.19(1)
s.20(1)(c)

1 Spencer – history and what's changed

Suzanne – [redacted]

Bill - [redacted]

Cssr comment – I hear that you are feeling that your industry is feeling some pain because of Spencer, but it is a good dev from a privacy perspective. He hears that companies have stopped pre-Spencer actions.

s.19(1)
s.20(1)(c)

Fall out from Spencer seems to rule out name and address requests. If there's any discrepancy in the marketplace, it is probably that.

Bill –

2 lawful access generally and higher level interactions w OPC

Suzanne -

Bill -

Suzanne -

Suzanne –

Ken –

Cssr – I have tried to explain my perspective on Spencer and for Canadians – there should be more clarity – I will look for you to respond to the needs of individuals

3 warrantless disclosures

Suzanne –

s.19(1)
s.20(1)(c)

Ken –

Bill –

Ken –

Suzanne –

Bill –

4 rebuilding trust – relationship w OPC

Suzanne -

5 transparency reporting

Suzanne –

[redacted]

Ken – [redacted]

Cssr – we can address some of these issues in principle. He has makde a formal request for rcmp to improve its record keeping. We have encouraged telcos to issue transparency reports but we have not given any guidance on what this should look like. We will take this into consideration.

s.19(1)
s.20(1)(c)

Kathy Renaud

From: Christopher Prince
Sent: Monday, December 01, 2014 10:17 AM
To: Barbara Bucknell
Subject: RE: CWTA meeting note (background)

Will need to update note with new details from Sophie and this story

http://www.leaderpost.com/Revealing+sensitive+surveillance+details+worried+Ottawa+memo/10429152/story.html

-----Original Message-----
From: Christopher Prince
Sent: Monday, December 01, 2014 9:57 AM
To: Sophie Paluck-Bastien
Cc: Barbara Bucknell; Josee Phillips; Rachel Desjardins
Subject: RE: CWTA meeting note (background)

Perfect Sophie - that's very helpful - will add in. Thanks.

-----Original Message-----
From: Sophie Paluck-Bastien
Sent: Monday, December 01, 2014 9:29 AM
To: Christopher Prince
Cc: Barbara Bucknell; Josee Phillips; Rachel Desjardins
Subject: RE: CWTA meeting note (background)

Hi Chris,

It's a first contact with the industry. They want to brief the Commissioner on their issues. The delegation at this point will consist of Kurt Eby of CWTA, Ken Englehart of Rogers and Anthony Hemond of Videotron.

One issue they will bring up is consultation with industry before issuing guidance. The other issue is lawful access and transparency reports.

I suggest:
1- a brief overview of our dealings with wireless telecom, especially wrt lawful access (I remember you had prepared something for Chantal to back up the "we've been asking for years" statement),
2- our process for issuing guidance.

Of course, you can add anything else that you feel is relevant or helpful.

Thanks!

-----Original Message-----
From: Rachel Desjardins
Sent: November-27-14 11:29 AM
To: Christopher Prince
Cc: Barbara Bucknell; Sophie Paluck-Bastien; Josee Phillips
Subject: RE: CWTA meeting note (background)

Chris: Sophie is back on Monday and will respond to you then. She is the most knowledgeable on this file.

Thanks..
R.

-----Original Message-----
From: Christopher Prince
Sent: November-27-14 10:26 AM
To: Rachel Desjardins
Cc: Barbara Bucknell
Subject: CWTA meeting note (background)

Good morning Rachel,

Sorry to trouble you on this but I was wondering if anyone might be able to shed some light on the upcoming meeting with CWTA.

I am trying to prep a general note but there are dozens of potential issues for discussion with the telecom folks - - - has anyone in the Secretariat been in touch with them about what they'd like to discuss?

Sophie mentioned they wanted to hear about how we draw up guidance - but I'm just wondering if that's it - I don't want to overload the note with unneeded detail.

Chris

-----Original Message-----
From: Christopher Prince
Sent: Thursday, November 27, 2014 10:22 AM
To: Sophie Paluck-Bastien
Subject: CWTA meeting note (background)

Questions arising from Legal and Investigations on upcoming CWTA meeting - do we have actual agenda or sense what they want to present? OBA, CASL, location-based services, access complaints?

Or was it strictly our process for release of guidance?

-----Original Message-----
From: Regan Morris
Sent: Thursday, November 27, 2014 10:17 AM
To: Christopher Prince; Arun Bauri; Gillian Kular
Subject: RE: CWTA meeting note (background)

Hi Chris,

Here you go small suggested revision to the paragraph discussing OPC's role under CASL. While the CWTA may be interested in CASL generally, I'm not sure they will be interested in the OPC's specific slice of responsibility.

What about OBA and related issues like geo-location tracking? Could these come up?

s.23

Regan

From: Christopher Prince
Sent: November-26-14 3:10 PM
To: Arun Bauri; Gillian Kular; Regan Morris
Subject: CWTA meeting note (background)

Hi all,

I've been asked to prepare this for an upcoming meeting with between the Commissioner and the Wireless Technology Association.

Wondering if you could have a quick glance see if I've missed anything?

Thanks!

CWTA meeting note (background) - http://officium/_layouts/OPC.Officium/Utilities/OfficiumIDLookup.aspx?id=7777-6-52597

Kathy Renaud

From: Christopher Prince
Sent: Wednesday, December 10, 2014 1:17 PM
To: Patricia Kosseim; Melanie Millar-Chapman
Cc: Leslie Fournier-Dupelle
Subject: BN on TSP handover and transparency
Attachments: BN on TSP handover and transparency.doc

As requested, additional documentation

Chris Prince
Conseiller en politiques/Strategic Policy Analyst
Télé/Phone: 819-994-5914
Christopher.Prince@priv.gc.ca
Commissariat à la protection de la vie privé du Canada/ Office of the Privacy Commissioner of Canada
30, rue Victoria / 30 Victoria Street
Gatineau (Québec) K1A 1H3

BRIEFING NOTE **NOTE D'INFORMATION**

Government requests for personal information to telecommunications service providers (TSP)

Purpose:

To present an overview of the following issues:

1) How *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies when authorities *compel* personal data from firms
2) How PIPEDA provisions allow organizations to disclose data to authorities upon request;
3) OPC research on how Canadian TSP's treat government requests for data;
4) Media coverage of OPC research findings on the issue;
5) External calls for improved transparency;
6) How companies in Canada have begun to issue transparency reports, what these documents detail and the implications for privacy;
7) The potential impact of Bills S-4 and C-13 on lawful access.

Issues:

1) *How PIPEDA applies when authorities compel personal data from firms*

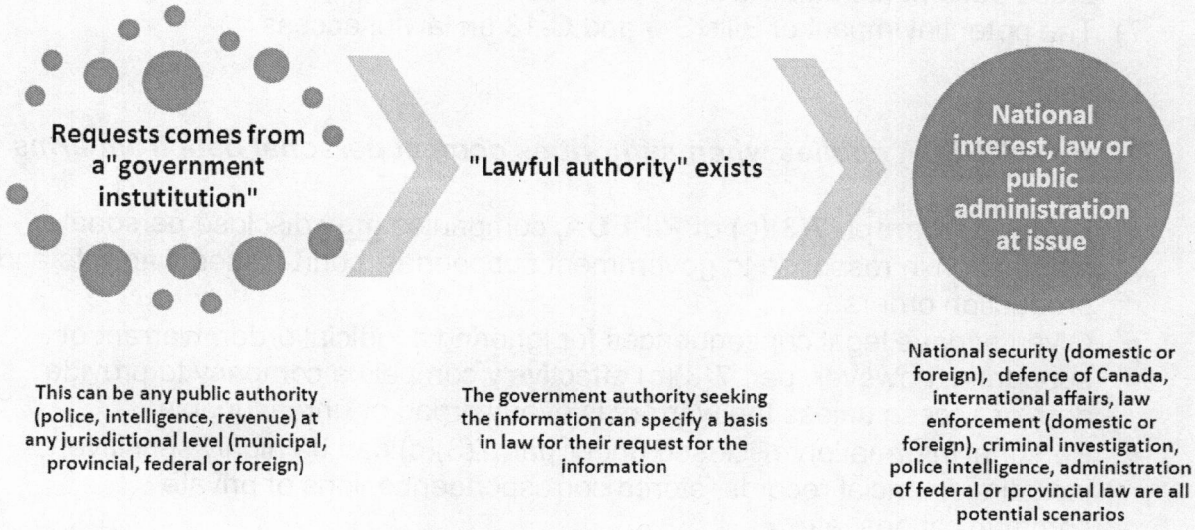
- **Under paragraph 7(3)(c) of PIPEDA,** companies **may** disclose personal information in response to government subpoenas, court-issued warrants and production orders.[1]
- Given serious legal consequences for ignoring a judicial order, warrant or subpoena, however, par. 7(3)(c) effectively compels a company to provide data or access unless the warrant is overly broad or unreasonable.
- Personal information disclosed under par. 7(3)(c) can be highly sensitive, including financial records, stored correspondence, logs of private communications, etc.
- As an indicator of scale, one major provider (TELUS) stated in 2011 that they processed roughly 10,000 search warrants and production orders in the preceding three years from various agencies and levels of government.[2]
- By contrast, from 2009 to 2011, 355 wiretap authorizations for real-time interception of private communications were issued by courts to federal law enforcement.[3]

2) *How PIPEDA provisions allow organizations to disclose data to authorities upon request*

Under paragraph 7(3)(c.1) of PIPEDA, an organization **may** disclose personal information without the knowledge or consent of the individual if:

I. A "government institution" has made a request for the information;
II. Government has specified "lawful authority" to obtain the information, and;
III. The government requestor has indicated:

(i) It suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;
(ii) The disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law; or
(iii) The disclosure is requested for the purpose of administering any law of Canada or a province.



Basically, **PIPEDA 7(3)(c.1)** provides the discretion for companies to disclose personal information sought by any government institution[4] - without knowledge or consent - where there is a "lawful authority" to obtain the information in the situations listed.[5]

7(3)(c.1) has been a primary avenue for government agencies to acquire information from commercial firms.[6] Unlike disclosures via 7(3)(c), companies have more latitude to comply or refuse requests under 7(3)(c.1), especially if investigators are at the "pre-warrant" stage or requests seem overbroad. Border

security officers, intelligence and police often use 7(3)(c.1) to confirm information on persons of interest or verify intelligence obtained from other sources.[7]

As currently set out in PIPEDA, however, companies retain a discretion to refuse such requests; many do so where they believe confidential information should be sought via a judicial process.[8] The recent decision by the SCC in *Spencer* will clearly buttress that response, by finding that 7(3)(c.1) of PIPEDA does not provide the lawful authority needed to obtain the data sought.[9] The implications of the *Spencer* decision go far beyond the specific facts of the case and the particular *Criminal Code* offences at issue.[10] For a full discussion, please refer here to D. Caron's note (RDIMS 423828) summarizing the decision and its legal implications (p. 5-6).

From a policy perspective, the recent SCC decision sets a clear limit on the types of information that government investigators (subject to the Charter) can obtain from commercial firms as sources. Subscriber information in the hands of a commercial firm has been found definitively to carry a reasonable expectation of privacy - given it can both identify a specific individual and link them to online activities. Such records cannot be obtained by government investigators without prior judicial authorization, unless there are clear exigent circumstances or through a reasonable law that provides the authority to access such information.

As a specific example of how **7(3)(c.1)** was used for online investigations and intelligence-gathering, the RCMP, police and telecommunications service providers (TSPs) jointly developed a standard letter specifically for use by investigators in online child exploitation cases to be provided to firms requesting personal information.[11]

In summary, while the scope of private data and communications handed over to government authorities may be greater under **7(3)(c)**, there is independent review and recourse through the courts. By contrast, the total volume of requests and disclosures under **7(3)(c.1)** is much higher because:

a) Any "government institution" at any level may make a request;
b) Requests can relate to "enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any law, or, gathering intelligence for the purpose of enforcing any such law" - which sets broad parameters for requests across a range of police officers, public officials or security bodies[12], and;
c) Requests may relate to "administering any law of Parliament or a province" which is also very broad.

The impact of the SCC decision in *Spencer* last week, therefore, will go far beyond police investigation or general government intelligence work.[13]

3) *OPC research on how Canadian TSPs treat government requests for data*

The OPC has an extended history in the debate around lawful access (see Annex to this note) and since PIPEDA came into force in 2001 we've consulted at length on when it is reasonable for TSPs to provide personal information to authorities or to volunteer that information. We have exchanged views (with government and companies) on use of electronic surveillance, data handover and lawful access on dozens of separate occasions.[14] An attempt to clarify these exchanges was made in early 2011 when the previous Commissioner requested we seek specific details from the main TSPs operating in Canada.[15]

This research was undertaken as we believed the issues of lawful access and PIPEDA reform were likely to escalate with new legislation and Parliamentary debate.[16] In the letters, sent to thirteen major companies providing services in Canada, we posed the following questions:

1. *Approximately how many data requests from government authorities does your organization receive annually, on average? Similarly, approximately how many users or accounts are subject to disclosure to authorities in response to a valid request?*
2. *Do you make these figures available to the public in any form?*
3. *Do you keep internal, aggregate statistics on the types of requests you receive (such as production orders and emergency requests) and the kinds of information requested (e.g. subscriber records, non-content or transactional data, communications content, location information customer look-ups, location data, emergency requests, wiretap requests, production orders)? If so, would you be willing to provide a copy of this information?*
4. *If your enterprise uses Deep Packet Inspection equipment or software, have you used it in response to a request from federal authorities?*
5. *Do you notify your customers, when the law allows, that their information has been requested, thus giving them an opportunity to contest the request in court?*

6. *Do you currently seek reimbursement for the cost of complying with these requests? If so, do federal authorities pay their bills in a prompt manner? If not, what steps if any have you taken in order to obtain payment (such as terminating wiretaps and withholding data)?*

7. *Do you make a schedule of these tariffs or fees available to the public?*

These letters were signed and sent in June 2011.[17] Following discussions with various firms, an aggregated response from nine of the companies was provided in December 2011 through an intermediary legal firm. The details of the report provided a firm evidentiary basis for various legislative reform positions and transparency calls made by the OPC issued thereafter. From our perspective, the crux of the report (lost in much of the media discussion) was to refute the assertion made in previous years by various proponents of lawful access legislation that Canadian TSPs did not consistently assist investigators.

When asked approximately how many requests from government the firms received, they stated that they had received nearly **1.2 million requests** in 2011. These requests led to disclosures on at least **780,000 separate individual**s (only three of the nine respondents' tracked disclosures, as opposed to requests). Figures detailed related to disclosures made under both 7(3)(c) [court authorized] and 7(3)(c.1) [without warrant]. These figures encompassed all levels of government (federal, provincial, municipal) and all functions (tax compliance, immigration agencies, etc.).[18]

Subsequent reporting by firms and academic research has confirmed that the nature of these requests vary greatly: from confirming a last known name and address for an account (i.e. locating individuals), to reverse look-ups on unknown phone numbers (i.e. return of missing property), to linking IP addresses with suspect activity (e.g. copyright violations).[19] Either way, we believe the vast majority of the transactions described by the TSPs in their report fall under sections 7(3)(c.1)(ii) and (iii) of PIPEDA.

4) Media coverage of OPC research findings on the issue

- While the 2011 report provided us with some clarity around government data requests made to telecommunications firms – and informed OPC positions on various lawful access and privacy law reform matters – these details were provided to us on the basis of commercial sensitivity and confidentiality.[20]
- However, in early 2014, the letter (and related material) was the subject of a specific Access to Information request.[21]

- As is standard practice, our ATI unit consulted the law firm to ensure their clients had no objection to its release. It was subsequently provided to the requestor by our ATIP unit.
- After an appearance before Parliament (on changes to Bell Canada's Privacy Policy) on April 29, 2014, media asked the Interim Commissioner about the scale of disclosures to government by TSPs. The issue had already been the subject of media coverage for several months, given widespread reports of government surveillance in Canada and other countries.
- Given the questions to the Interim Commissioner were about the same matter as the letter released under ATI, the Interim Commissioner referenced the response from industry and we proceeded to make the letter available to the media when it was requested. Given the volume of requests, we also had the letter translated and posted on the OPC website.
- Dozens of media requests, interviews, articles and op-ed pieces on the issue of warrantless disclosure and government surveillance followed (May-June), given Parliament was also examining Bills S-4 and C-13. PCO has now formally queried departments about the practice. As well, several Written Questions on the issue have been tabled in the House for government response.[22]
- The matter also figured prominently in Question Period over several days in May and a court challenge to the provisions under PIPEDA 7(3)(c.1) was filed three weeks later by the CCLA in the Ontario Superior Court.[23]

5) *OPC recommendations and external calls for improved transparency*

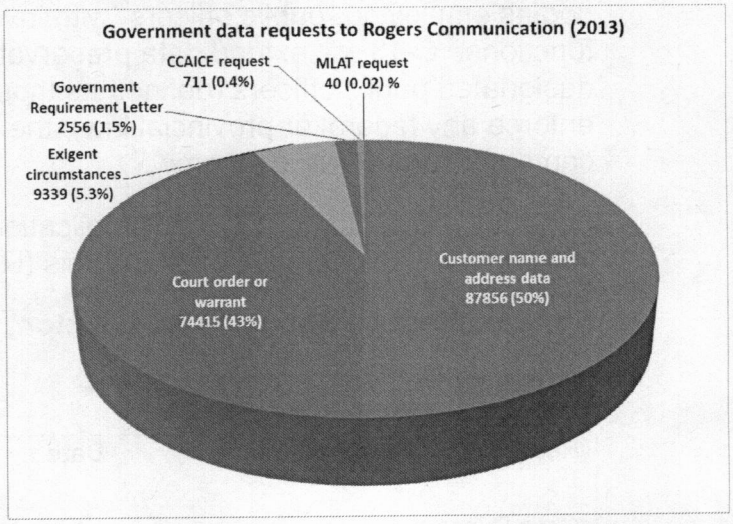
In the specific context of surveillance and intelligence-gathering, since 2005, the OPC has been calling for greater openness and transparency from both government and commercial firms. We have made these recommendations in formal submissions on legislative review (2005, 2009, 2013 and 2014), open letters to responsible Ministers (2011), Federal/provincial/territorial joint resolutions (2009), discussion papers on legal reform (2013) and special reports to Parliament (2014).[24]

At the same time, civil society groups, academics and privacy advocates have been exerting pressure for organizations and government to make more information available on surveillance and lawful access. In January 2014, Christopher Parsons coordinated a joint letter from academics and researchers seeking aggregate data on surveillance carried out through TSPs, though that effort produced only limited responses from companies.[25]

Next, the Citizen Lab, Digital Stewardship Initiative and Open Media have developed a specialized application (AMI: https://openmedia.ca/myinfo) for individuals seeking to access their personal information when held by TSPs. CIPPIC (University of Ottawa), the Surveillance Studies Centre (Queen's) and the New Transparency Project have all been actively developing educational reports, editorial pieces and recommendations to government.

6) *Canadian companies begin to issue transparency reports*

As of June 2013, some TSPs have issued reports on government requests and court orders (Tek Savvy, Rogers) or announced they plan to do so in the near future (TELUS). These reports demonstrate, even with the status quo, information on hundreds of thousands of individuals is sought by various levels of government. For example, Rogers is Canada's largest wireless firm, with 9.5M subscribers. In 2013, Rogers received nearly 175,000 government requests. Half of these were warrantless requests for subscriber name and address; another 43% were court orders or warrants. They do not provide precise statistics on request responses – but plan to report more details in future reports.



By contrast, niche firms like Tek Savvy who have also started to report are much smaller operations and provide only internet access. It does not represent a statistically significant data set and they received only 53 government requests in all of 2012 and 2013.

Both reports are useful, however, in that they provide public clarity, in accessible language on the legal process and transparency on how the companies retain data, triage requests from government and challenge these in court. For example, both clearly state requests received come from investigators and officers from a wide range of public agencies, including the RCMP, CSIS, CBSA and CRA, as well as provincial and municipal police or coroners.

7) *The projected impact of Bills S-4 and C-13 upon warrantless access*

As we have stated for some time, the 7(3)(c.1) regime is troubling from a privacy standpoint as there are no public reporting requirements, no notice provisions

and no clearly established rules as to what personal information can or should be provided to government institutions. We also understand that there is significant inconsistency (from industry to industry, jurisdiction to jurisdiction) in terms of what firms will provide from their data holdings at government requests under 7(3)(c.1).

Investigators tend to seek out as much corroborating information as they can obtain under 7(3)(c.1) at the pre-warrant stage, in advance of formal application for a court order or some other form of judicial authorization.[26] C-13 does not provide clarity on these points. S-4 is silent on the issue. Each of the bills in mid-review before Parliament and amendments may flow from the wider public debate now taking place.

In addition, as noted in our C-13 submission, parts of the CBSA, CRA, Correctional Services Canada, DND, DFO and Canada Post are all federal bodies employing "public officers" with investigative duties and enforcement functions. C-13 will extend data preservation and access powers to any designated public officers (defined as those investigators who administer or enforce any federal or provincial law); the figures on court orders cited above, it can be assumed, will only grow.

[redacted]

Consultation: C. Baggaley, V. Lockton, D. Caron s.23

Distribution: P&P, LSRTA

Rédigé par / Prepared by	**Date**	**Revisions**
Chris Prince	June 11, 2014	June 13, 2014 June 16, 2014 June 20, 2014
Approuvé par / Approved by	**Date**	
Barbara Bucknell *Directrice, Politiques et recherche (intérimaire) / Director, Policy and Research (Acting)*		

ANNEX – LAWFUL ACCESS CHRONOLOGY

1970: House of Commons Standing Committee on Justice and Legal Affairs urges Government to ensure a) only specified crimes should be subject to electronic

surveillance, b) stringent controls and limits on use of electronic surveillance, c) set applications to use electronic intercept devices, and, d) that judicial authorization be required, along with an annual report to Parliament by the Attorney General on the use of surveillance.

1972: Department of Communications and Department of Justice issues their *Privacy and Computers: A Report of a Task Force* (Information Canada, Ottawa)

1974: passage of the *Protection of Privacy Act* (added the "invasion of privacy" sections to *Criminal Code*, prior to which there was no legislation regulating use of electronic surveillance by Canadian authorities). In revising Part VI of the *Criminal Code*, these sections protect the privacy of Canadians by making it an offence to intercept private communications except where permitted by law.

1976: As a requirement under the new *Criminal Code* provisions, the Solicitor General of Canada tables the first *Annual Report on the Use of Electronic Surveillance* in Parliament.

1977: *Canadian Human Rights Act* is enacted, establishing Canada's first Privacy Commissioner.

1980: The Organisation for Economic Co-operation and Development (OECD) releases *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.*

1983: The federal *Privacy Act* comes into force and Canada adopts the OECD 1980 *Guidelines on protecting privacy and transborder data.*

1987: Commons Standing Committee on Justice and Legal Affairs issues its report *Open and Shut: Enhancing the Right to Know and the Right to Privacy*, with over a hundred recommendations for amendments.

1992: US FBI issues *International User Requirements for Interception of Telecommunications* (also known as the Quantico Standards)

1994: Privy Council Office begins informal consultations on new *Telecommunications Interception Standards.* US Congress passes the *Communications Assistance for Law Enforcement Act* (CALEA) which places the Quantico Standards into a legal framework.

1995: The Solicitor General issues *Enforcement Standards for Lawful Interception of Telecommunications* (also referred to Sol-Gen 21 standard) based on the *International User Requirements for Interception of Telecommunications.* Industry Canada expresses discomfort with this unilateral approach, arguing for consultation, legislation and

subsequent regulations. The issued Sol-Gen Standards apply only to cellular and wireless companies, not all telecommunication service providers.

1996: In an omnibus crime bill, *the Criminal Law Improvement Act* (C-17) proposes to amend section 487 of the *Criminal Code* to allow authorities an array of wider search powers of all networked computer systems. Introduced by Allan Rock, Minister of Justice, these provisions fall off in the course of Committee study.

1998: The Information Policy and Planning Branch of Industry Canada issues *Lawful Access: A Baseline Information Study* which usefully summarizes the legal debate, industry challenges and recent trends in the use of electronic surveillance. *Personal Information Protection and Electronic Documents Act* (PIPEDA) first introduced in the House of Commons (later to fall off agenda with Parliament's prorogation).

1999: Justice Canada consults with OPC on technical matters in a briefing: *How Does the Internet Work - Background for Lawful Access* - headed by their Technology & Analysis Criminal Law Policy Section. Justice also beings a comprehensive legal review to weigh security needs versus legal issues, privacy considerations, industry competitiveness, etc. PIPEDA reintroduced and enacted into law.

2000: The *Regulation of Investigatory Powers Act* (RIPA) is tabled in the UK to 'make provision for and about the interception of, communications, the acquisition and disclosure of data relating to communications, the carrying out of surveillance and the use of covert human intelligence sources.

2001: PIPEDA comes into fully into force across federally regulated industry. Canada (along with 28 other countries) signs the Council of *Europe's Convention on Cybercrime*, which incorporates many of the key elements of the FBI *International User Requirements* (including revising procedures for searching / seizing computer data, production orders, preservation of data in computer systems, disclosure of traffic data, interception of electronic communications and provisions for mutual assistance / exchange of information). New legal tools to deal with cybercrime figure prominently in the Speech from the Throne. *USA PATRIOT Act* passed in the United States, significantly altered interception laws by extending the period of their applicability and placing less specific constraints on their use; Canada passes its *Anti-Terrorism Act* while the UK passes the *Anti-terrorism, Crime and Security Act.*

2002: Solicitor General, Industry and Justice Canada jointly issue *Lawful Access Consultation Document.* Immediate response from media, industry, legal community, civil society and the general public is largely negative. Justice re-establishes formal consultations with the OPC. Civil society groups are also consulted in all day session.

2003: Civil society groups, IT associations and legal associations across Quebec form the *Collectif sur la surveillance électronique* to condemn the government's lawful access

initiative, arguing it is disproportionate, dilutes existing legal thresholds for interception, infringes upon rights to privacy and free expression, and that illegal racial or religious profiling could result. Members of the NDP and the BQ also publically oppose the proposal.

2004: Justice consults with OPC as it conclude *Lawful Access Legal Review*, proposing two pieces of legislation to ensure a) all TSPs have technical capacity to provide for interception (Public Safety to lead) and b) *Criminal Code* is amended to allow preservation / production orders and real-time search of traffic data (CNA). PIPEDA comes fully into force.

2005: Justice continues consultation with OPC through set of three briefings: *Transmission data: considerations for criminal law policy, Emails: considerations for Criminal Law Policy and Lawful Access Legal Review* for follow-up consultations. In the fall, Public Safety Minister Anne McLellan tables Bill C-74, the *Modernization of Investigative Techniques Act* (MITA). In the UK, the *Prevention of Terrorism Act* is passed, allowing the Home Secretary to issue data retention directives to all communications providers for the purpose of protecting national security or preventing or detecting crime that relates to national security. Under this policy, communications data must be retained and made accessible to authorities for up to one year.

2006: MITA dies on the order paper with the 2006 election call. In the European Union, *Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publically available electronic communications services* are issued (also referred to as the *EC Data Retention Directive*).

2007: Public Safety Canada *launches Customer Name and Address (CNA) consultation paper*; OPC issues formal response. The US Congress amended *the Foreign Intelligence Surveillance Act* (FISA) permitting interception of communications transiting the United States, even those involved US citizens, as long as one party is outside of the country.

2008: Public Safety Canada arranges meeting with OPC officials to discuss forthcoming CNA legislative amendments. Legislation does not appear.

2009: Early February, in statements before committee, Minister for Public Safety indicates new lawful access legislation is about to be introduced. Following media coverage, the Minister corrects those comments. In April, the UK government launches its consultation on its Interception Modernisation Programme, entitled *Protecting the Public in a Changing Communications Environment*. In mid-June, just before summer recess, Bill C-46 (IP21C) and C-47 (TALEA) are introduced. OPC works with P/T Offices to produce Joint Resolution on issue and writes an open letter to Parliament and the Ministers. In December, Bills C-46 and 47 died on the Order Paper.

2010: In November 2010, Bills C-50, *Improving Access to Investigative Tools for Serious Crimes Act, C-51; the Investigative Powers for the 21st Century Act and C-52, Investigating and Regulating Criminal Electronic Communications Act* were tabled, but died on the Order Paper.

2011: In Feb. 2011, the OPC appears in the Senate on Bill C-22, *An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service*

2012: Bill C-30, introduced in February 2012, combined the previous three Bills; given public concerns expressed immediately after release, government announced that it would be referred to Committee for study before second reading.

2013: Bill C-30 withdrawn by Minister of Justice in February 2013. In December, the OPC appears on Bill C-55 which imposes new measures for annual reporting on the use of warrantless electronic surveillance. Bill C-13 is introduced in November – without warrantless subscriber data provisions or universal intercept requirements.

2014: In Jan, the OPC tables a special report to Parliament (*Checks and Controls*) calling for more transparency by authorities using invasive surveillance. In April, the OPC releases the telecomm letter detailing government requests and provision of data on subscribers. In June, the OPC appears (with newly appointed Commissioner) before Parliament on Bill C-13.

---

[1] PIPEDA offers no statutory definition of "government institution" nor has the term been set out in subsequent regulation. See BN 372321 PIPEDA 7(3)(c) for additional background. Consequently court instruments can be legal orders issued in Canada or foreign requests - as with the SWIFT case, or those given local force under Mutual Legal Assistance Treaties – just as 7(3)(c.1) requests may come from authorities outside Canada. Canadian firms have had to deal delicately with such requests in the past, e.g. BN on RIM international lawful access dispute (282238)

[2] See *R. v. Telus Communications Company, 2011 ONSC 1143, par. 2* – URL: http://www.canlii.org/en/on/onsc/doc/2011/2011onsc1143/2011onsc1143.html. TELUS currently holds 25-30% of the Canadian wireless market.

[3] There are public reporting requirements in place specifically for wiretap warrants issued under Part VI of the *Criminal Code*; these are prepared by Public Safety Canada and tabled annually in Parliament. They have provided trend data since 1977. Unfortunately, there are no public reporting requirements for other forms of court authorization such as production orders, general warrants, tracking devices or number recorders - compliance with which would fall under 7(3)(c).

s.23

[redacted]

[6] The clause was specifically inserted in the final phases of Parliament's consideration of PIPEDA at the request of government agencies to ensure access to commercial data could be maintained. This includes international efforts undertaken by a Canadian government institution, as "lawful authority" need **not** be from a Canadian source (a court or an

express statutory power can be exerted). See *Executive Summary - Privacy Commissioner of Canada v. SWIFT* - April 2, 2007 – URL: http://www.priv.gc.ca/cf-dc/2007/swift_exec_070402_e.asp

[7] For example, as they assemble a warrant application (in particular the targeting component), see RDIMS 187422 *Legal Opinion – Response to Eastlink*

[8] Again, under this provision, an organization may disclose personal information for the purpose of enforcing a law, conducting an investigation or gathering intelligence. See C. Prince, Summary of lawful authority under PIPEDA 7(3)(c.1) (RDIMS 251915)

[9] That is the crucial distinction between (c) and (c.1) - the latter gives organizations far more discretion — precisely because the government institution is not compelling production with a warrant or a court order than can have serious legal consequences for the organization if refuted. See for example RDIMS 152794 - *OPC submission on the 2005 "Lawful Access" Consultations*

[10] Some key policy principles and privacy lessons reinforced by Justice Cromwell's ruling include: A) Lawful access and government searches cannot be regulated solely on the basis of the data viewed in isolation– what the gathered information can in turn reveal must also be considered as a critical factor [par. 16]; B) The invasiveness of a search must be determined by the potential impact upon the individual – not the illicit nature of the material sought or crime thwarted [par.18, 36]; C) These points underscore why judicial authorities (considering surveillance applications) and lawmakers (examining investigative powers) must also bear in mind: when an invasive technique becomes unreasonable (*Plant*), why informational privacy must be protected given new technologies (*Tessling*), ohow privacy rights persist even in public spaces (*Kang-Brown*), and how courts define a "search" for the purposes of section 8 of the Charter (*Gomboc*) [par. 27-32]; D) contemporary conceptions of informational privacy as protected by the Charter must include elements of secrecy, control and anonymity [par. 38] ; E)Much of the information citizens exchange in both the real world and online is done with the specific understanding these ideas and opinions will not be recorded and linked specifically to them [par. 42-43, 45]; F) While neither PIPEDA nor the *Criminal Code* provided any lawful authority to obtain the subscriber data at issue, online policing and investigation remains possible – the Court simply reasserted that investigators must seek court authorization before conducting searches or surveillance, or that there must be a reasonable law that authorizes the request [par. 49-51, 66, 70-71].

[11] Under the so-called CCAICE protocol, companies provide subscriber information to investigators with a standard one-page letter. CCAICE is the Canadian Coalition Against Internet Child Exploitation. See S. Morin, "Business Disclosure of personal information to law enforcement agencies: PIPEDA and the CNA letter of request protocol" (May 2011) URL - http://www.cba.org/cba/newsletters-sections/pdf/2011-11-privacy1.pdf

[12] There are separate PIPEDA 7(3)(c.2) disclosures specific to the financial services industry – however these are related specifically to disclosures to FINTRAC for purposes of detecting money-laundering and terrorist-financing; review of this activity is already the subject of our bi-annual audit. Additional reporting on this clause would not likely be helpful.

[13] Colin Freeze, "Canadian agencies' warrantless snooping on shaky legal ground, critics warn " *Globe and Mail* (Jun. 19, 2014) - URL: http://www.theglobeandmail.com/news/politics/canadian-agencies-warrantless-snooping-on-shaky-legal-ground-critics-warn/article19255174/

[14] **2002** – Letter to Industry, Solicitor General and Justice Canada on lawful access and subscriber data (38249); **2004** – OPC response to Eastlink on treatment of subscriber data (187422); **2005** - ISP meeting regarding disclosures of subscriber data (161884); 2006 - EAC discussion on ISP disclosures w/o warrant (164040); Letter to CRCVC on ISP disclosure w/o warrant (179050); **2008** – Meeting - Public Safety Canada on lawful access and subscriber data (214055); meeting - Bell Aliant on subscriber data (208777); **2009** – Meeting - CACP, RCMP, CSIS on subscriber data access (278870); Discussion - civil society on lawful access and subscriber data (253487); Discussion - EAC on lawful access and subscriber data (253390); Meeting - Canadian Bar Association on lawful access and subscriber data (254735); Meeting - MySpace (256971); Lawful access / ITAC meeting (248714); Meeting - telecom industry on lawful access and subscriber data (249393); **2010** - Meeting - M. Mourani (MP) on lawful access and subscriber data (267849); Meeting - Public Safety on lawful access and subscriber data (289770); Meeting - PSC on lawful access and subscriber data (290664); **2011** - Discussion of law enforcement access to digital profile data (298983); Letter to TSP CEOs on data requests from government (312071); meeting – EAC on lawful access issues (321250); Letter to Public Safety on lawful access and subscriber data access (328966); **2012** - Meeting - CACP on lawful access and subscriber data access (361807); Meeting - CACP on C-30 subscriber data (367683); FPT debrief on C-30 and data access (367732); **2013** - Meeting - Assistant Commissioner and RCMP Deputy Commissioner (394734); Meeting - Justice Canada on lawful access and subscriber data (379241); Meeting - Pierre-Yves Borduas on RCMP lawful access audit (416322); Meeting - Ian Kerr on RCMP lawful access audit (416356); Meeting - D. McArthur on RCMP lawful access audit (416307); Meeting - L. Austin on RCMP lawful access audit (416703); meeting with M. Geist on RCMP lawful access audit (418665)

[15] Briefing note – law enforcement access to digital profile data (RDIMS 298983, April 2011)

[16] Lawful access legislation (Bills C-50, *Improving Access to Investigative Tools for Serious Crimes Act, C-51; the Investigative Powers for the 21st Century Act and C-52, Investigating and Regulating Criminal Electronic Communications Act)* had been tabled two months prior on which we expected to be called to appear. We were also called before the Senate on legislation (Bill C-22, *An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service)* compelling TSP cooperation for certain investigations. We were also anticipating an eventual

review of PIPEDA and preparing for an appearance on legislative amendments to clarify 'lawful authority' (in Bill C-29). See 2010 Library of Parliament Legislative Summary on Bill C-29 "Exceptions to Consent Requirements" in PIPEDA – URL: http://www.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?Language=E&ls=c29&Parl=40&Ses=3&source=library_prb#a5.

[17] Letter to TSP CEO on data requests from Government (RDIMS 312071, June 2011)

[18] Media coverage of the report from the firms has been extensive but in some instances misleading, insofar as most commentators assume all the government's requests originate from federal agencies, and that all requests are necessarily responded to. Neither of those interpretations bears out. The firms have also faced some criticism for failing to be more transparent, now that many U.S. TSPs have begun issuing quarterly transparency reports. Another of the rationales for our sending the letter and posing the question "Like some organizations, do you make these figures available to the public in any form?" was that we anticipated these calls for reporting in Canada.

[19] Micheal Geist, Internet data routinely handed over without a warrant, The Toronto Star (Mar 28 2014) – URL - http://www.thestar.com/business/tech_news/2014/03/28/internet_data_routinely_handed_over_without_a_warrant_geist.html; Colin Freeze, "Border agency asked for Canadians' telecom info 18,849 times in one year", *Globe and Mail* URL - http://www.theglobeandmail.com/news/politics/telecoms-routinely-give-customer-information-to-canada-border-service-agency/article17691103/

[20] Gowling Lafleur Henderson LLP - Response to Request for General Information from Canadian Wireless Telecommunications Association (RDIMS 336134, December 2011) – URL: http://www.priv.gc.ca/media/nr-c/2014/let_140430_e.asp

[21] Michael Geist, "Canadian Telcos Asked to Disclose Data Every 27 Seconds" (April 30, 2014) – URL: http://www.michaelgeist.ca/content/view/7116/125/

[22] These are detailed formal queries by MPs for information through a Parliamentary process – one for which government departments are legally obliged to respond to in 45 sitting days. This can often be reliable channel for seeking information than the ATI process. For example, on June 20, 2016, the following questions was tabled (Q-630): "With regard to requests by government agencies to telecommunications service providers (TSPs) to provide information about customers' usage of communications devices and services: (a) between 2001 and 2013, how many such requests were made; (b) of the total referred to in (a), how many requests were made by the (i) RCMP, (ii) Canadian Security Intelligence Service, (iii) Competition Bureau, (iv) Canada Revenue Agency, (v) Canada Border Services Agency, (vi) Communications Security Establishment Canada; (c) for the requests referred to in (a), how many of each of the following types of information were requested, (i) geolocation of device, broken down by real-time and historical data, (ii) call detail records, as obtained by number recorders or by disclosure of stored data, (iii) text message content, (iv) voicemail, (v) cell tower logs, (vi) real-time interception of communications (i.e. wire-tapping), (vii) subscriber information, (viii) transmission data (e.g. duration of interaction, port numbers, communications routing data, etc.), (ix) data requests (e.g. web sites visited, IP address logs), (x) any other kinds of data requests pertaining to the operation of TSPs' networks and businesses, broken down by type; (d) for each of the request types referred to in (c), what are all of the data fields that are disclosed as part of responding to a request; (e) of the total referred to in (a), how many of the requests were made (i) for real-time disclosures, (ii) retroactively, for stored data, (iii) in exigent circumstances, (iv) in non-exigent circumstances, (v) subject to a court order; (f) of the total referred to in (a), (i) how many of the requests did TSPs fulfill, (ii) how many requests did they deny and for what reasons; (g) do the government agencies that request information from TSPs notify affected TSP subscribers that information pertaining to their telecommunications service has been requested or accessed by the government, (i) if so, how many subscribers are notified per year, (ii) by which government agencies; (h) for each type of request referred to in (c), broken down by agency, (i) how long is the information obtained by such requests retained by government agencies, (ii) what is the average time period for which government agencies request such information (e.g. 35 days of records), (iii) what is the average amount of time that TSPs are provided to fulfill such requests, (iv) what is the average number of subscribers who have their information disclosed to government agencies; (i) what are the legal standards that agencies use to issue the requests for information referred to in (c); (j) how many times were the requests referred to in (c) based specifically on grounds of (i) terrorism, (ii) national security, (iii) foreign intelligence, (iv) child exploitation; (k) what is the maximum number of subscribers that TSPs are required by government agencies to monitor for each of the information types identified in (c); (l) has the government ever ordered (e.g. through ministerial authorization or a court order) the increase of one of the maximum numbers referred to in (k); (m) do TSPs ever refuse to comply with requests for information identified in (c) and, if so, (i) why were such requests refused, (ii) how do government agencies respond when a TSP refuses to comply; (n) between 2001 and 2013, did government agencies provide money or other forms of compensation to TSPs in exchange for the information referred to in (a) and, if so, (i) how much money have government agencies paid, (ii) are there different levels of compensation for exigent or non-exigent requests; (o) for the requests referred to in (a), how many users, accounts, IP addresses and individuals were subject to disclosure; (p) for the requests referred to in (a), how many were made without a warrant; (q) do the government agencies that request information from TSPs keep internal aggregate statistics on these type of requests and the kind of information requested; and (r) do the government agencies that request information from TSPs notify individuals when the law allows or after investigations are complete that their information has been requested or disclosed?"

[23] Canadian Civil Liberties Association (CCLA) and Christopher Parsons, *Notice of Application on May 13th, 2014 to the Ontario Superior Court* – URL: http://ccla.org/wordpress/wp-content/uploads/2014/05/Notice-of-Application-re-PIPEDA-Issued.pdf

[24] OPC, "Lawful Access Proposals" – URL: https://www.priv.gc.ca/a-z/index_e.asp?let=L

[25] Christopher Parsons, "Towards Transparency in Canadian Telecommunications" (Jan. 22, 2014) – URL: Towards Transparency in Canadian Telecommunications

[26] That is because, after an affidavit is made to a court and an authorization or warrant issued, information gathered subsequent to legal process is subject to full disclosure to defendants (in compliance with the 1991 SCC ruling in *Stinchcombe*) – URL: http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/808/index.do