

**SECRET**

DATE:

File No.: NS 6952-O3 / 395254

RDIMS No.: Dragon 7092

**MEMORANDUM FOR THE SENIOR ASSISTANT DEPUTY MINISTER****UPDATE ON ENHANCEMENTS TO THE LAWFUL INTERCEPTION  
CONDITION OF LICENCE FORBEARANCE PROGRAM**

(Information only)

**ISSUE**

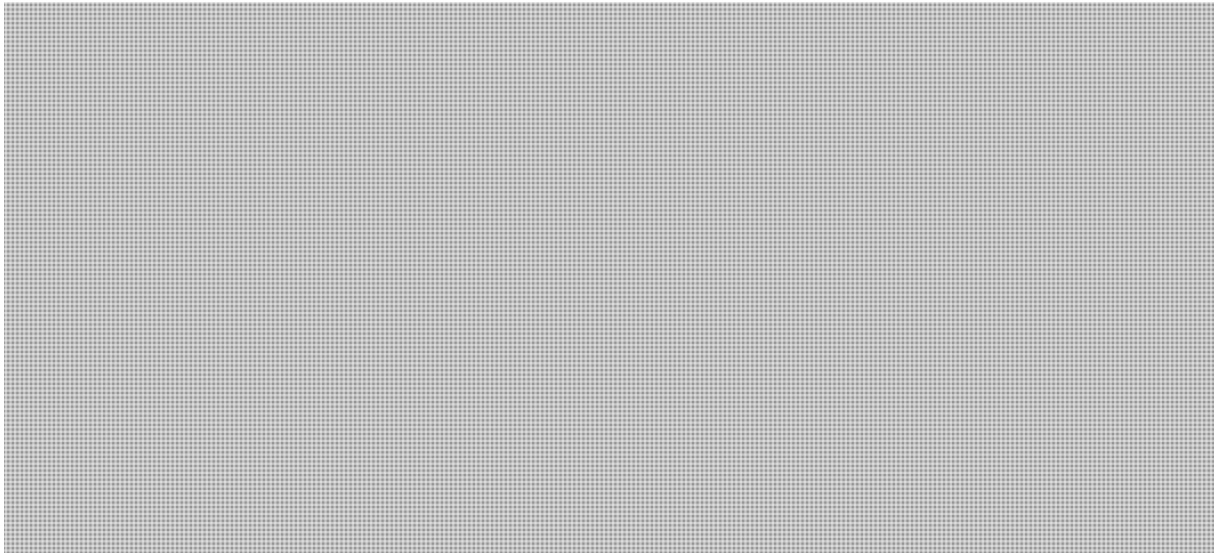
To provide an update on ongoing efforts to enhance to the lawful interception condition of licence forbearance program.

**BACKGROUND**

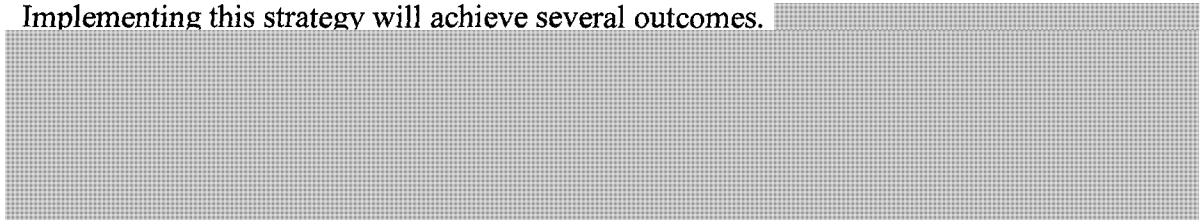
Under the *Radiocommunication Act* (RA), the Minister of Industry has the authority to grant wireless licences to telecommunication service providers (TSPs). TSPs must comply with the conditions of their licence in order to deliver wireless services in Canada. Certain, but not all, licences have an applicable lawful interception condition, which requires TSPs to have and maintain lawful interception capabilities as outlined in the *Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications* (SGES).

As part of this condition, the Minister of Industry, in consultation with Public Safety Canada (PS), has the power to grant forbearance to any licence holder from complying with all or part of the SGES. As such, when TSPs cannot meet the SGES requirements, they apply to Industry Canada (IC) for forbearance. The forbearance allows TSPs to continue to provide services while [REDACTED] to develop technical solutions to eventually meet the SGES requirements. PS has been coordinating PS Portfolio advice to IC for each of these requests on a case by case basis.

Last spring, the Investigative Technologies and Telecommunications Policy (ITTP) Division undertook to review and enhance the lawful interception condition of licence forbearance program (**ANNEX A**). The objective is to ensure that the lawful interception capabilities of public safety agencies are maximized within the existing regulatory framework.



Implementing this strategy will achieve several outcomes.



Several of these instruments have already been operationalized, while others require further analysis and consultation. Attached at **ANNEX B** is a brief report on the progress of these initiatives.

**CONSIDERATIONS**



PS will continue to provide leadership on the forbearance file, and will develop and manage most of the proposed enhancements.



the upcoming 700MHz auction, will allow for the TSP engagement process to remain manageable.

**SECRET**

-3-

Over the past several years, IC officials have had difficulties in monitoring TSPs' compliance with the lawful interception condition of licence. While IC will remain responsible for the condition of licence and for granting forbearance to TSPs, PS direct engagement with licence holders to assess their compliance level will reduce the burden on IC and provide the Portfolio with valuable information on the interception capacity currently available. PS will keep IC aware of any engagements with TSPs [REDACTED]

[REDACTED]

[REDACTED]

**NEXT STEPS**

We will continue to work with [REDACTED] IC to refine and implement the forbearance strategy. We will keep you informed of progress.

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

Michael MacDonald  
Director General  
National Security Operations Directorate

Prepared by: Shawn Plunkett

**SECRET**

## **ANNEX B – Strategy Implementation Tools**

### **Operationalized**

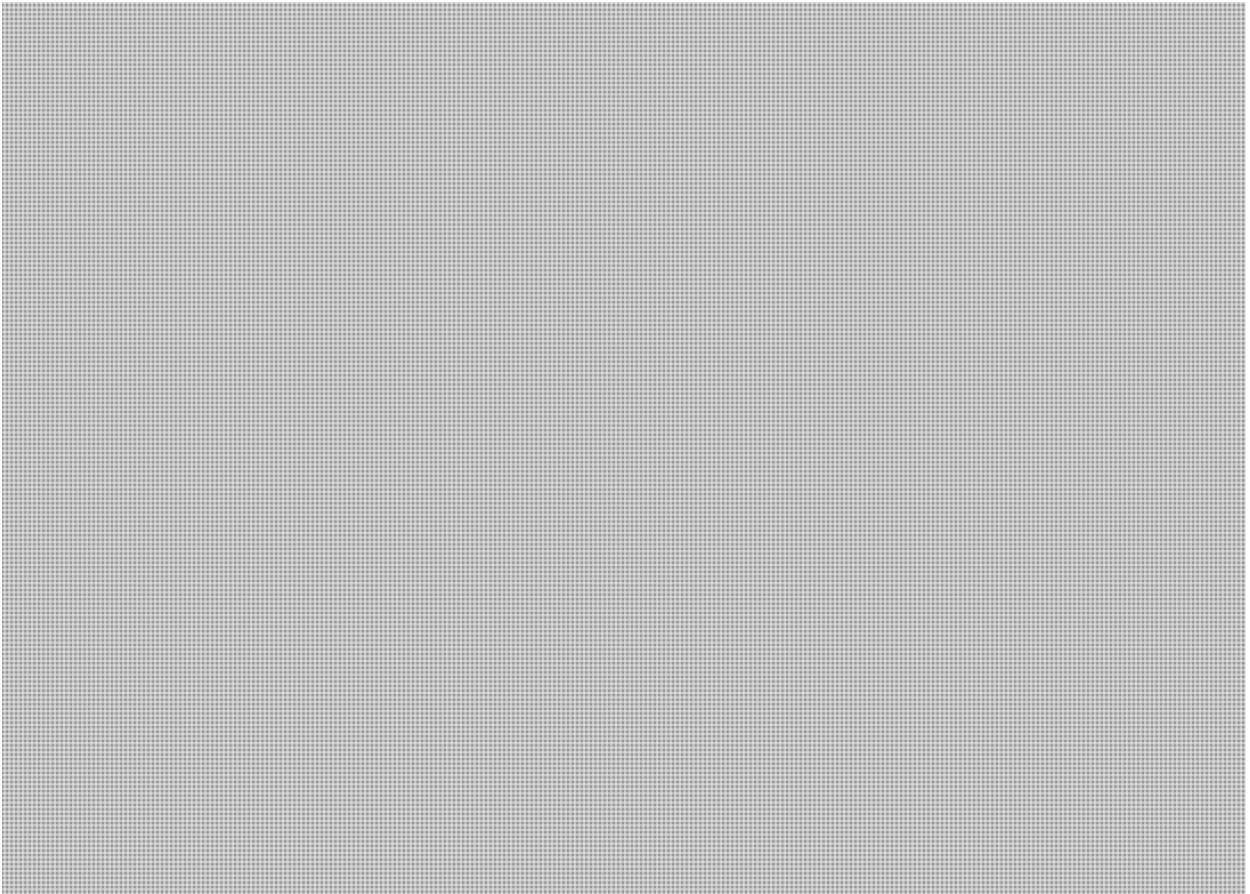
**Forbearance Formal Updates:** To ensure that TSPs that were granted forbearance continue to work towards developing a lawful interception solution, IC, on the recommendation of ITTP, has been requesting that companies provide a mid term update on their progress as a condition of their forbearance. This allows the PS Portfolio to better monitor progress [REDACTED]

**Forbearance Quarterly Reports:** So far, 5 forbearance quarterly reports have been submitted to the Director General of National Security Operations. These quarterly reports focus on progress made by companies with forbearance to develop interception solutions and provide updates on the implementation of the forbearance [REDACTED]

**Updated Tracking Report:** Sections have been added to the forbearance tracking report, including area of non compliance, schedule for compliance, and next steps. These new fields give a better overview of where potential challenges lie with respect to compliance.

**Forbearance Working Group:** In fall 2012, ITTP launched a forbearance working group, in which representatives from [REDACTED] PS meet bimonthly to discuss both policy and operational issues related to the forbearance program.

### **In Progress**





Public Safety  
Canada

Sécurité publique  
Canada

**SECRET**

Subject to ATI exemption 21(1)(a,b)

**BUILDING A SAFE AND RESILIENT CANADA**



# **Strategy for Enhancing the Lawful Interception Condition Forbearance Program:**

## **SGES Compliance**

May 2013

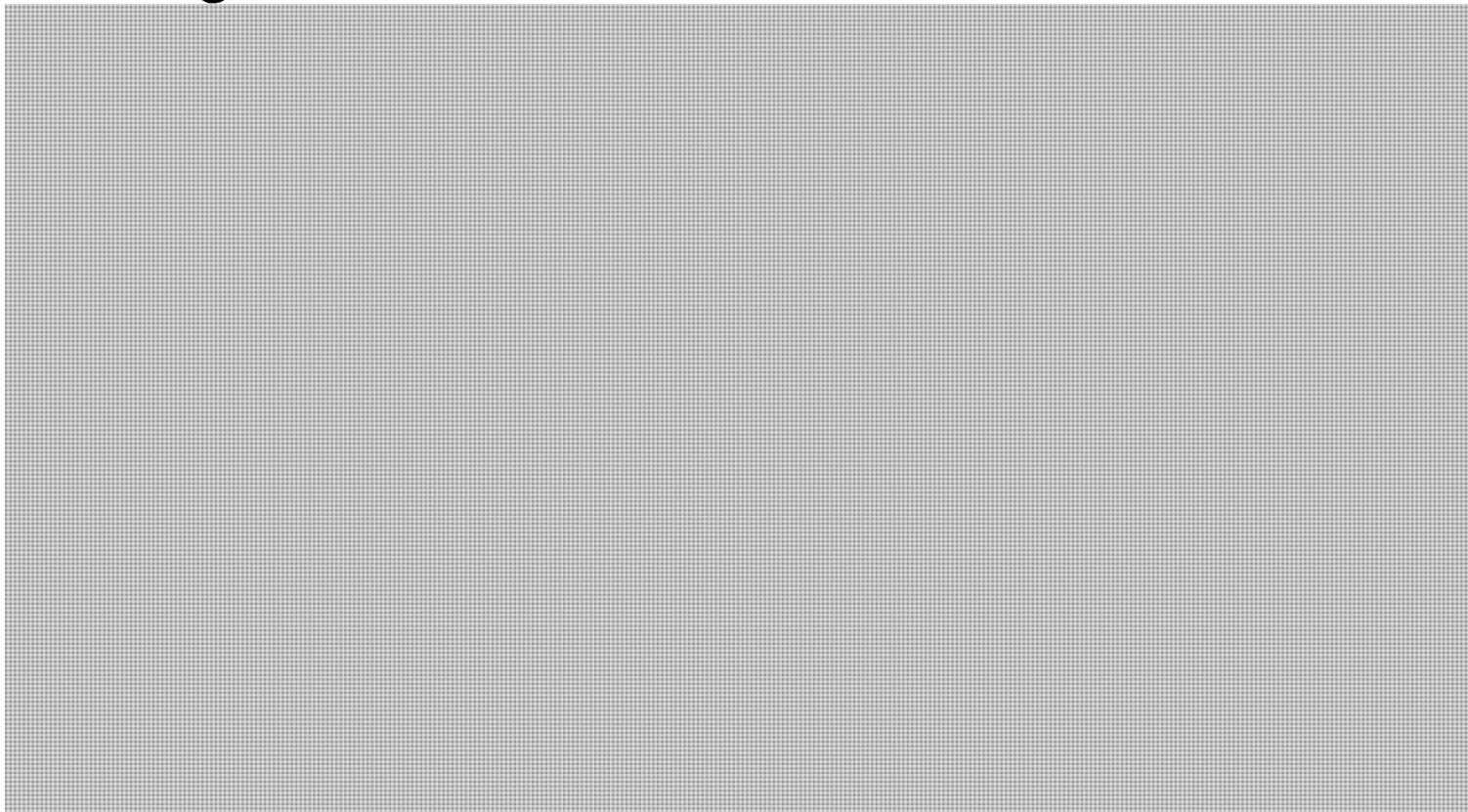
**Canada**

# Overview



BUILDING A SAFE AND RESILIENT CANADA

- Strengthen the forbearance program along



# Rationale



BUILDING A SAFE AND RESILIENT CANADA

- Problem Definition:



# Opportunity

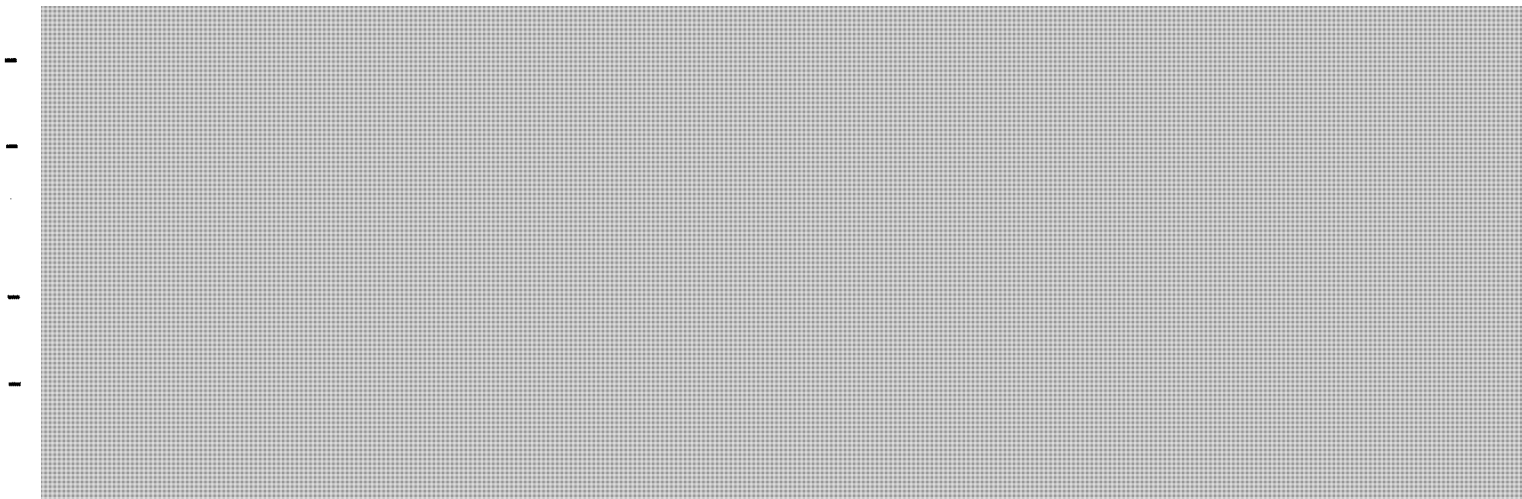


BUILDING A SAFE AND RESILIENT CANADA

s.21(1)(a)

s.21(1)(b)

- We need to make the most of all existing regulatory measures related to lawful interception
- PS will continue to process forbearance requests, but also will identify opportunities to improve the program





# Engaging Licence Holders

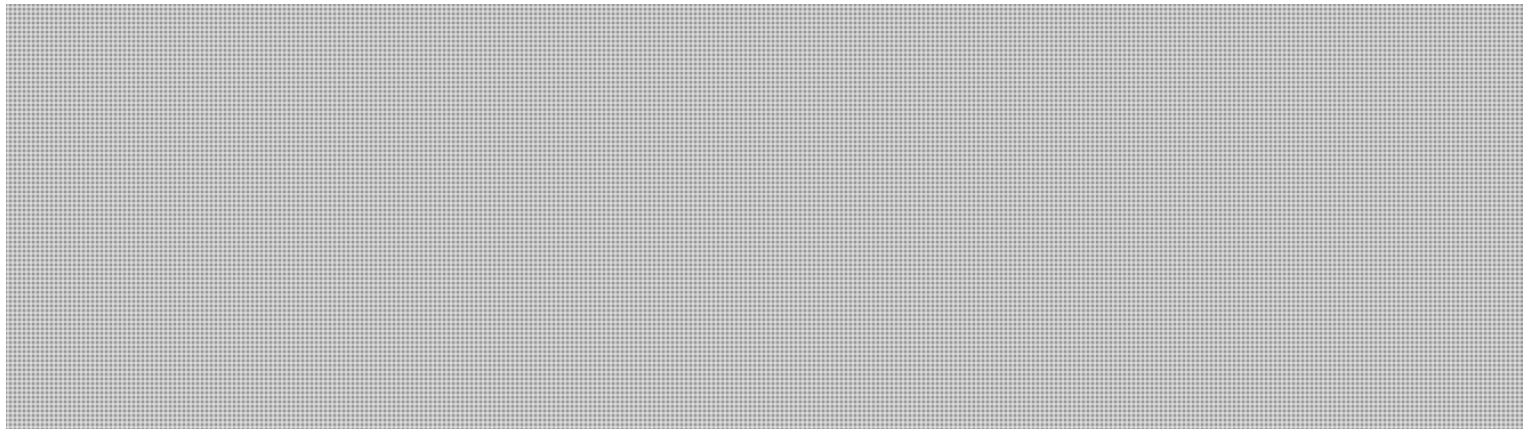


BUILDING A SAFE AND RESILIENT CANADA

s.21(1)(a)

s.21(1)(b)

- Industry Canada (IC) is responsible for administering and ensuring compliance with the lawful interception condition of licence
- With a view to strengthening compliance with the SGES, PS discussed potential approaches with IC
- The preferred approach that emerged involves:



# Proposed Approach



BUILDING A SAFE AND RESILIENT CANADA

- We are proposing a 4 step approach:
  - 1) Internally Clarify Operational Requirements
  - 2) Undertake a Risk Assessment (Triage)
  - 3) Proactively Engage Licence Holders
    - Self Assessment by licence holders
    - Identification of items for further action
  - 4) Assessment, Monitoring, Reporting



# Operational Requirements



BUILDING A SAFE AND RESILIENT CANADA

s.21(1)(a)

s.21(1)(b)

- **Step 1 – Clarify Operational Requirements**



Public Safety  
Canada

Sécurité publique  
Canada

# Risk Assessment



BUILDING A SAFE AND RESILIENT CANADA

s.21(1)(a)

s.21(1)(b)

- **Step 2 – Undertake a Risk Assessment**

- 
- 
- 
- 
- 



# Engagement

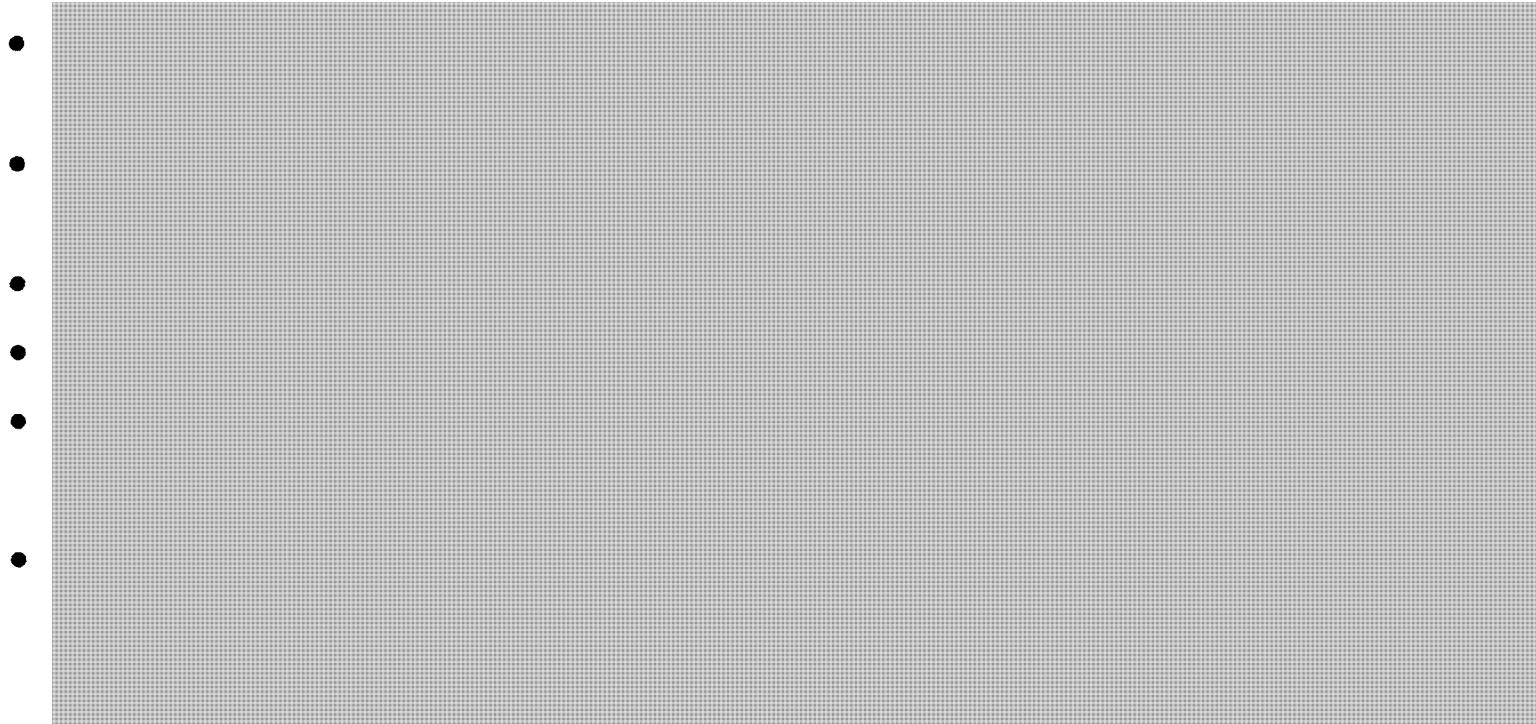


BUILDING A SAFE AND RESILIENT CANADA

s.21(1)(a)

s.21(1)(b)

- **Step 3 – Pro Actively Engage Licence Holders**



# Program Management



BUILDING A SAFE AND RESILIENT CANADA

s.21(1)(a)

s.21(1)(b)

- **Step 4 – Program Management - Assessment, Monitoring, Reporting**
- *Objective:* The forbearance program is managed in an effective and efficient manner



Public Safety  
Canada

Sécurité publique  
Canada



# Timelines

BUILDING A SAFE AND RESILIENT CANADA

s.21(1)(a)

s.21(1)(b)

- Step 1 – Operational Requirements

- [Redacted]
- [Redacted]

- Step 2 – Risk Assessment

- [Redacted]
- [Redacted]

- Step 3 – Engagement

- [Redacted]
- [Redacted]

- Step 4 – Program Management

- [Redacted]
- [Redacted]



# Resource Impacts



BUILDING A SAFE AND RESILIENT CANADA

s.21(1)(a)

s.21(1)(b)

•

•

•





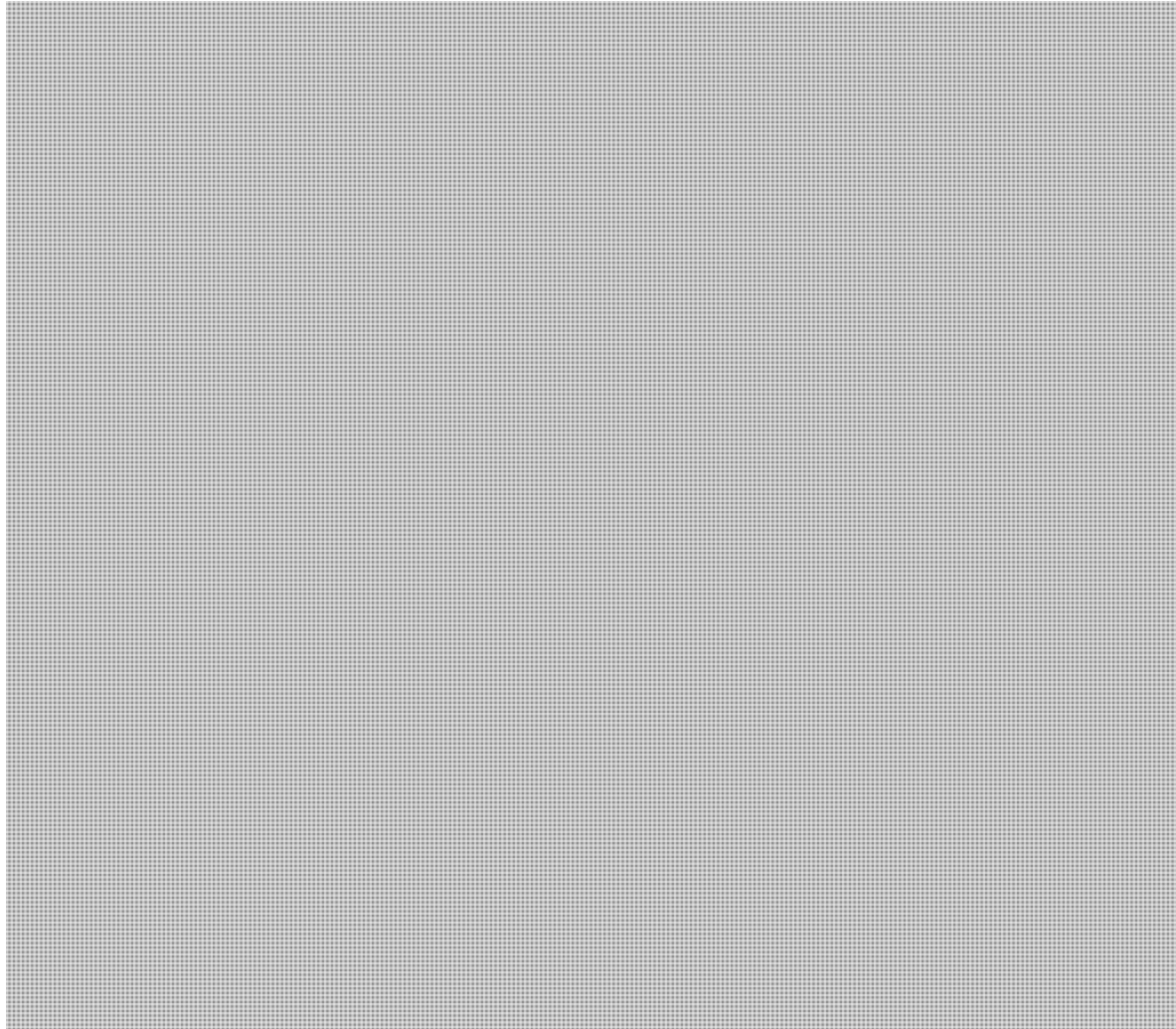
# Draft Business Process



BUILDING A SAFE AND RESILIENT CANADA

s.21(1)(a)

s.21(1)(b)



Public Safety  
Canada

Sécurité publique  
Canada

# Benefits



BUILDING A SAFE AND RESILIENT CANADA

s.21(1)(a)

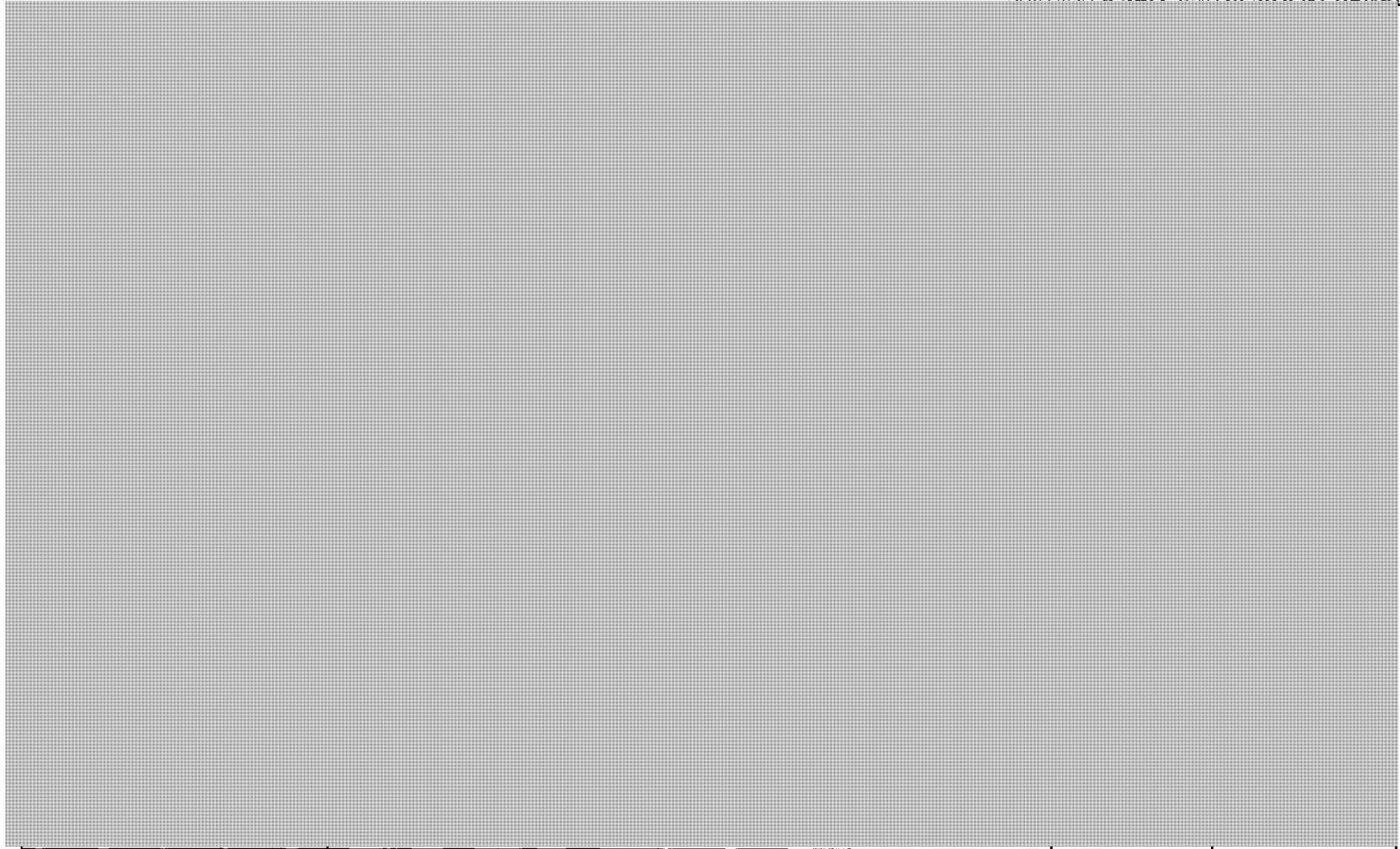
s.21(1)(b)

- Short term investments in outlining operational requirements, [REDACTED] and program management will reap benefits
- A stronger, more structured program will lead to resource savings:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]



# Work plan



# Forbearance Strengthening



BUILDING A SAFE AND RESILIENT CANADA

## Questions?



Public Safety  
Canada

Sécurité publique  
Canada



Public Safety      Sécurité publique  
Canada              Canada

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

Ottawa, Canada  
K1A 0P8

**SECRET//CEO**

DATE:

File No.: NS 6950  
RDIMS No.: Dragon 19748

**MEMORANDUM FOR THE DEPUTY MINISTER**

**STATUS OF LAWFUL ACCESS POLICY DEVELOPMENT  
AND MEDIUM TERM WAY FORWARD**

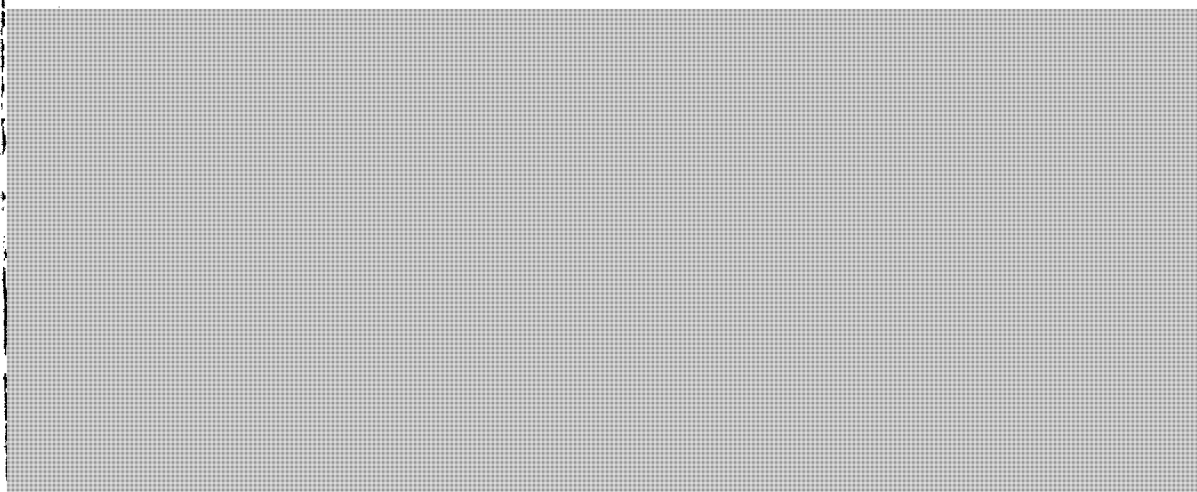
(Information Only)

**ISSUE**

To update you on the current and medium term vision for policy development related to lawful access issues.

**BACKGROUND**

Lawful access refers to the lawful interception of communications and the search and seizure of digital data. It covers a range of tools and techniques used by law enforcement and intelligence agencies. The information collected and analyzed is vital to conducting investigations and prosecuting serious offences, as 80-95% of major crimes leave behind electronic evidence.



.../2

CONSIDERATIONS

[REDACTED]

This work is led by the Investigative Technologies and Telecommunications Policy (ITTP) Division.

Strengthening existing tools

[REDACTED]

[REDACTED]

As the Minister of Industry is responsible for spectrum licencing, we will continue to engage with Industry Canada to ensure that national security perspectives are considered when regulating the telecommunications sector.

[REDACTED]

New approaches

PS will also evaluate new approaches to lawful access structures and tools. These will be drawn from international best practices, as well as research and analysis on the challenges and opportunities presented by [REDACTED]

**NEXT STEPS**

ITTP will continue to evaluate policy development opportunities related to both existing tools and new approaches. This work will include careful consideration of jurisdictional/legal issues, privacy concerns, and the evolving public debate on privacy.

A key component of the work program will be communication and engagement with the public, in line with the Department's recently published Citizen Engagement Framework. Lawful access is a complex topic in a sensitive domain, and occupies a debated space between the security of a nation's citizens and their individual privacy. Education, awareness, and information sharing are critical as more and more Canadians become savvy about technology and engage in the virtual world. ITTP will redouble efforts to enhance the public business case for lawful intercept capability, and will explore the merits of citizen engagement as a way to seek views on the appropriate balance between security and privacy, as well as to address misinformation regarding lawful access in the public environment.

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Mr. Michael MacDonald, Director General, National Security Operations, at 613-993-4595.

Lynda Clairmont  
National and Cyber Security

Encl.: (1)

Prepared by: Maciek Hawrylak



Public Safety / Sécurité publique  
Canada / Canada

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

Ottawa, Canada  
K1A 0P8

s.20(1)(c)

s.21(1)(a)

s.23

*Thks Lynda -*

**CONFIDENTIAL**

DATE:

File No.: NS 6950-O1 / 404717  
RDIMS No.: Dragon 24838

**MEMORANDUM FOR THE DEPUTY MINISTER**

**NEXT STEPS IN TRANSPARENCY  
REPORTING FOR DIGITAL INFORMATION REQUESTS**

SEP 04 2014

(Decision sought)

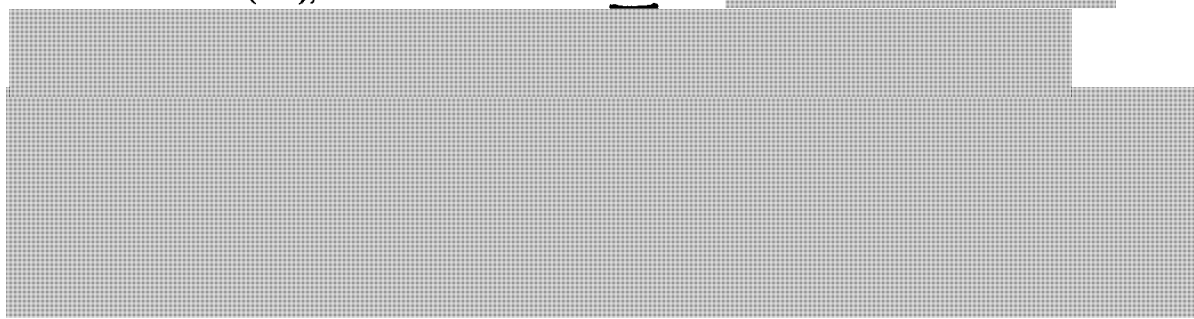
**ISSUE**

Seeking authorization to conduct closed consultations regarding proposed transparency guidance for telecommunications service provider (TSP) reporting of government lawful access and basic subscriber information requests.

**BACKGROUND**

The term "lawful access" refers to the use of electronic surveillance tools such as wiretaps and retrieving stored data, while "basic information requests" refers to obtaining discrete identifiers such as the name, phone number, and address of a TSP subscriber.

Transparency pertaining to lawful access and basic subscriber information requests is of growing interest in Canada. There has been a growing push from the Canadian public, media, civil society, industry, and other groups to be more open on matters of electronic surveillance in the wake of the unauthorized disclosures of former National Security Agency contractor Edward Snowden and the release of transparency reports by TSPs in the United States (US), such as Verizon and Microsoft.

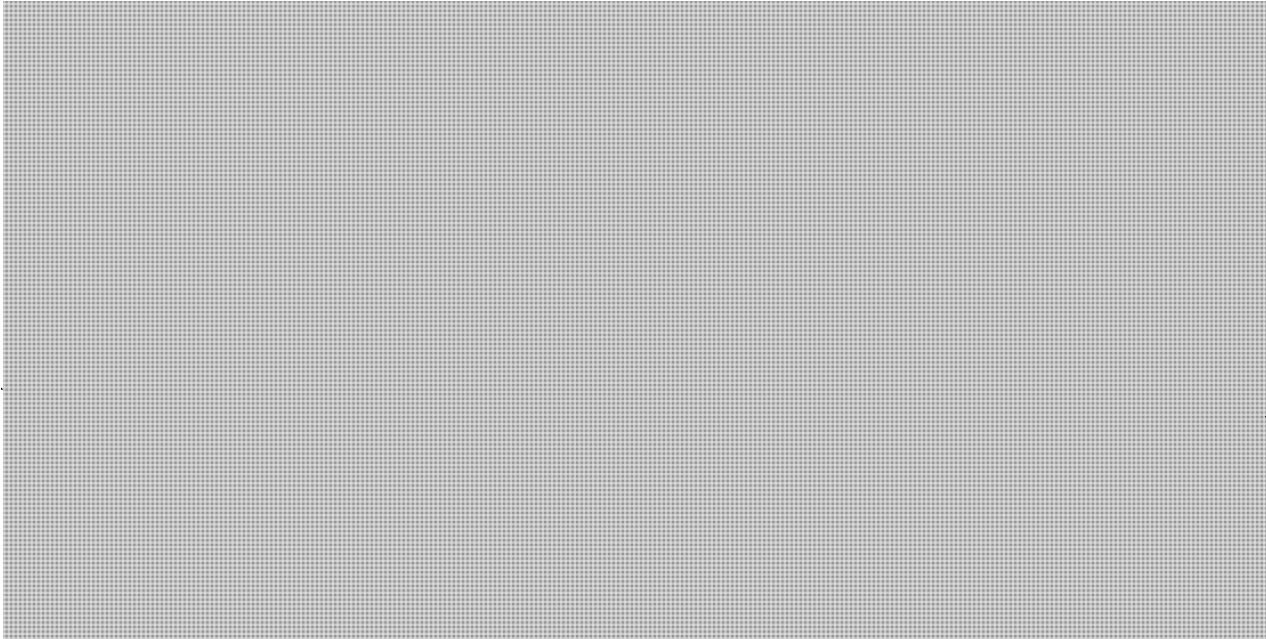
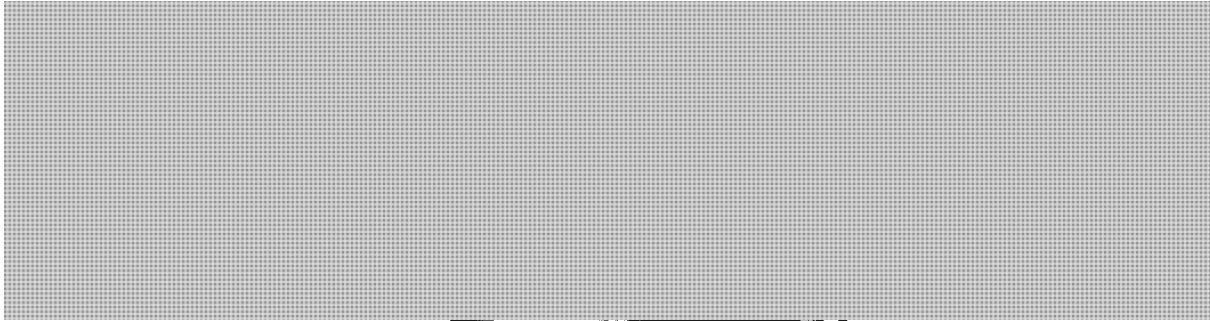


.../2



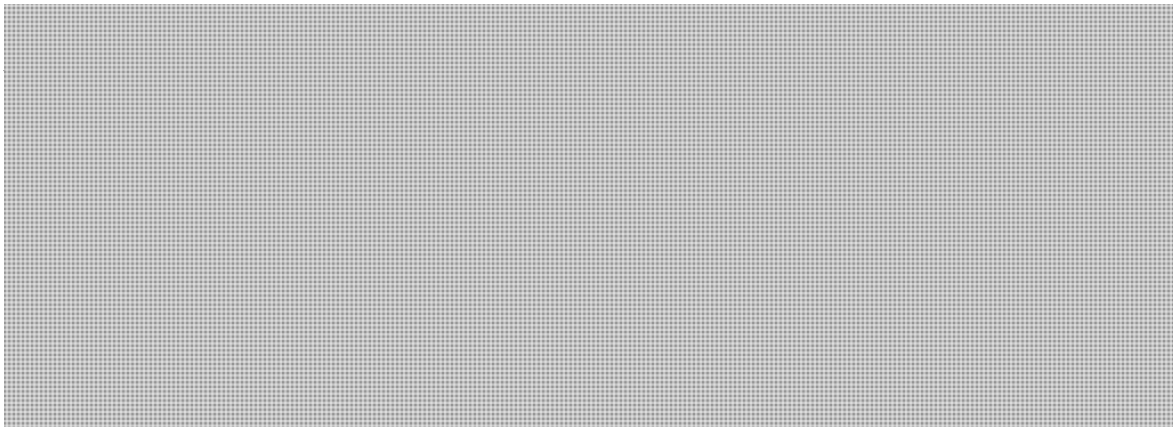
**CONFIDENTIAL**

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



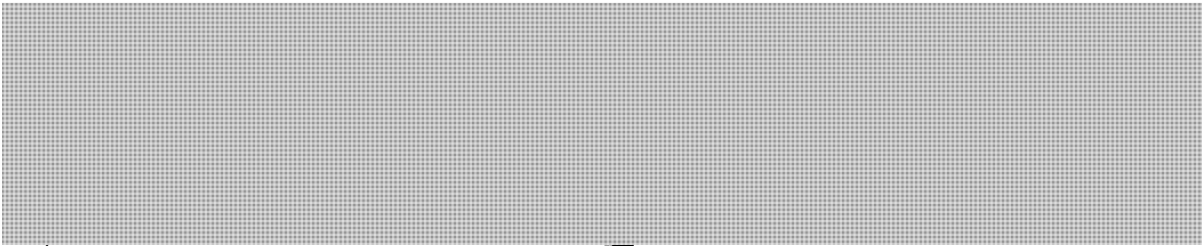
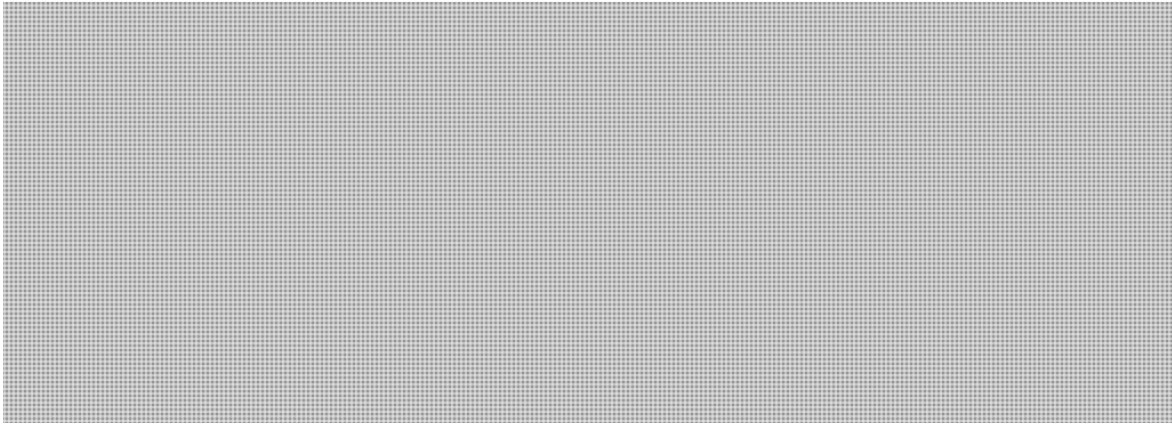
In June 2013, two Canadian TSPs, Rogers (**TAB 4**) and TekSavvy (**TAB 5**) released transparency reports for the first time. The TekSavvy report includes low numbers (52 requests for basic information over two years). Telus has publicly indicated that it intends to release its own transparency report over the coming weeks.

**CONSIDERATIONS**

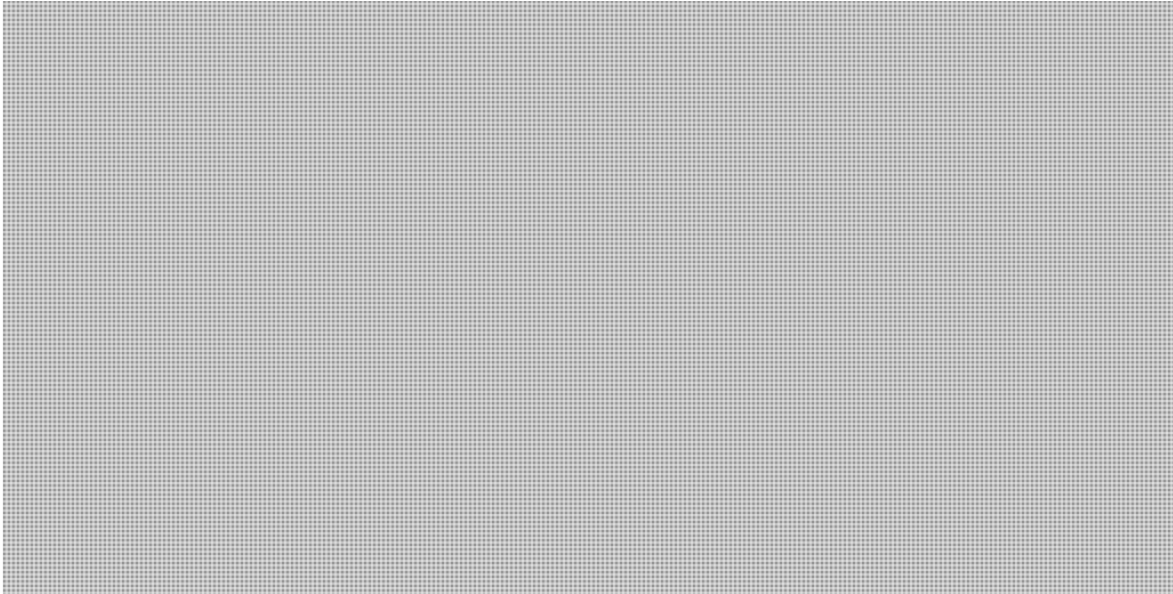


s.21(1)(a)  
s.21(1)(b)  
s.23

**CONFIDENTIAL**



**NEXT STEPS**



**RECOMMENDATION**



Should you require additional information, please do not hesitate to contact me or Mr. Jacques Cloutier, Director General, National Security Operations, at 613-993-4595.

A handwritten signature in black ink, appearing to read "L. Clairmont".

Lynda Clairmont  
Senior Assistant Deputy Minister  
National and Cyber Security

Enclosures: (5)

I approve:

I do not approve:

---

François Guimont

---

François Guimont

Prepared by: Maciek Hawrylak



Public Safety / Sécurité publique  
Canada / Canada

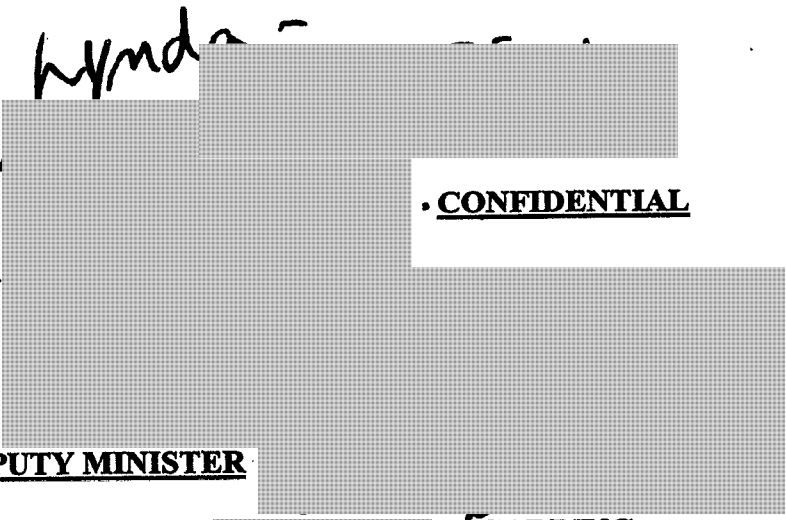
Senior Assistant / Sous-ministre  
Deputy Minister / adjoint(e) principal(e)

Ottawa, Canada  
K1A 0P8

s.15(1) - Subv

s.20(1)(c)

s.21(1)(a)



DATE: *May 26, 2014*

File No.: NS 6950-O1 / 402868  
RDIMS No.: Dragon 22262

**MEMORANDUM FOR THE DEPUTY MINISTER**

**FOLLOW-UP TO YOUR MEETING WITH [REDACTED] RÈGARDING  
TRANSPARENCY REPORTING FOR DIGITAL INFORMATION REQUESTS**

(Information only)

*Nea* **MAY 29 2014**

**ISSUE**

Responding to [REDACTED] request for permission to develop a transparency report for lawful access and other information requests.

**BACKGROUND**

“Lawful access” refers to the interception of communications and the search and seizure of electronic data, and is a key tool used by law enforcement and intelligence agencies to investigate modern crimes and national security threats. The types of data obtained by government authorities from telecommunications service providers (TSPs) include

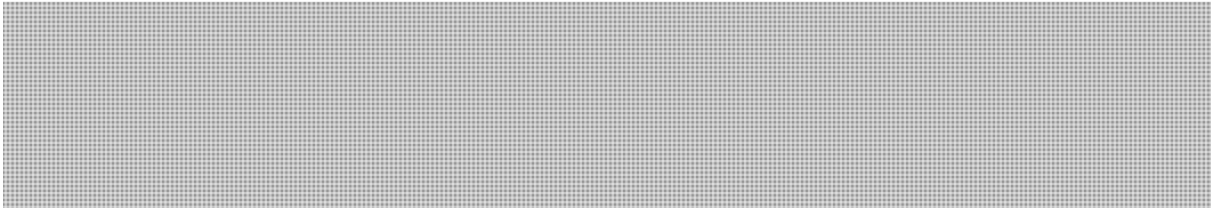
[REDACTED] among others. Except in defined emergency situations, access to these types of information generally requires judicial authorization. Separate from lawful access requests, government agencies may also request more basic types of information, such as basic subscriber information (e.g. name, phone number, and address), usually to start an investigation or explore new leads. TSPs may provide this information without a warrant, but are not required to do so.

Transparency in lawful access and basic information requests has recently been of growing interest in Canada.

The meeting was spurred in part by a January 2014 public campaign by the Citizen Lab (an online human rights group) asking TSPs to publish the number of requests for customer information made by Government agencies in 2013. The Privacy Commissioner also released a special report in January 2014 which called for mandatory transparency reporting by TSPs, among other recommendations. A final factor was the March 2014 disclosure of similar information from Government agencies in response to Parliamentary Written Question Q-233. Finally, the release of transparency reports by several TSPs in

.../2

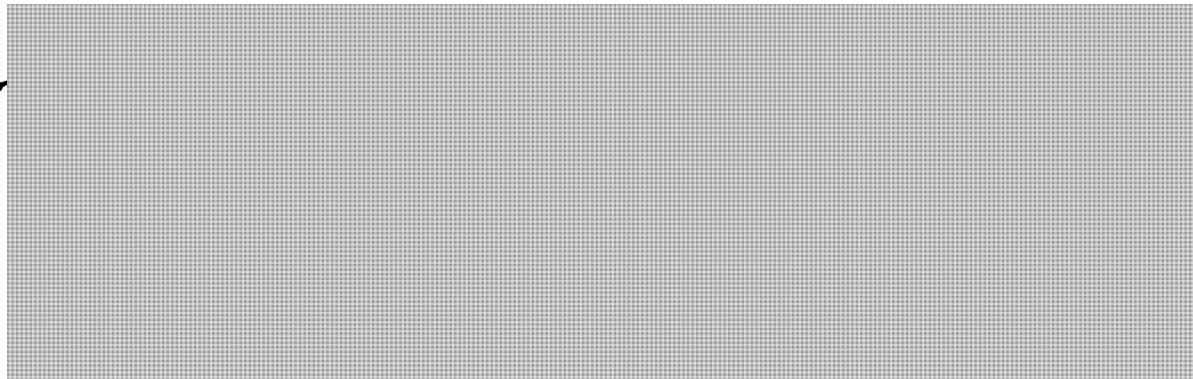
the United States (US), such as Verizon, has increased pressure on Canadian counterparts to do the same.



**CONSIDERATIONS**

The issue of public trust in law enforcement and intelligence agencies and their responsible collection and use of private information is of growing concern in Canada. The distinction between lawful access requests, which almost always require judicial authorization, and basic information requests, which provide much less detailed information and as such generally do not require judicial authorization, is likely not clear to Canadians. However, an Angus Reid poll from October 2013 noted that 78% of Canadians felt that the issue of Government surveillance was either "quite important" or "very important", and that it had in fact risen to a "top 5" issue of concern. A January 2013 poll conducted by the Office of the Privacy Commissioner found that 77% of Canadians are very or somewhat comfortable with law enforcement agencies being able to obtain information from TSPs to investigate serious crime.

This public discourse is evident globally, and TSPs abroad have taken the lead or come under pressure to publish transparency reports in a push to address a perceived imbalance between privacy and security. In the US, TSPs such as Apple, AT&T, Facebook, Google, Microsoft and Verizon have released transparency reports, while in the United Kingdom (UK), Vodafone officially petitioned the UK Government in January 2014 to allow it to publish similar reports. Verizon's report provides aggregate figures on the number of requests for many types of information, including basic subscriber information, geolocation requests, stored content, and wiretaps.



**CONFIDENTIAL**

- 3 -

**NEXT STEPS**

Should you require additional information, please do not hesitate to contact me at 613-990-4976 or Mr. Jacques Cloutier, Director General, National Security Operations, at 613-993-4595.

Lynda Clairmont  
Senior Assistant Deputy Minister  
National and Cyber Security

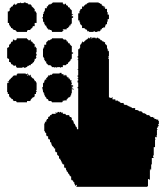
Enclosures: (1)

Prepared by: Maciek Hawrylak

**Pages 31 to / à 34  
are withheld pursuant to section  
sont retenues en vertu de l'article**

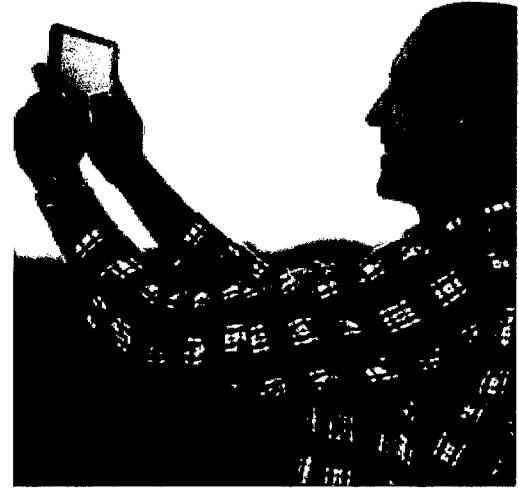
**21(1)(a)**

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



# ROGERS COMMUNICATIONS REQUESTS FOR CUSTOMER INFORMATION |

## 2013 TRANSPARENCY REPORT





## 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.

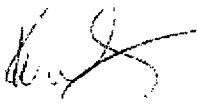
We fully comply with Canadian privacy law and take active steps to safeguard our customers' information. At the same time we are compelled by law to respond to federal, provincial and municipal government and law enforcement agencies when they have a legally valid request – like a search warrant or court 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
<b>Total</b>	<b>174,917</b>

**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\*](#)



**WE'RE DIFFERENT.  
IN A GOOD WAY.**

**TekSavvy Solutions Inc**

800 Richmond Street  
Chatham ON N2M 5J5

**TELEPHONE** 519.360.1575

**TOLL FREE** 877.779.1575

**FAX** 519.360.1716

**teksavvy.com**

Bram Abramson  
Legal & Regulatory

**Direct Line** 647.479.8093

**babramson@teksavvy.ca**

Professor Lisa Austin, Faculty of Law,  
Professor Andrew Clement, Faculty of Information,  
Professor Ron Deibert, Citizen Lab, and  
Dr. Christopher Parsons, Citizen Lab,  
University of Toronto;

Professor Colin Bennett, Department of Political Science  
University of Victoria;

Professor Robert Diab, Faculty of Law  
Robert Thompson University;

Professor Michael Geist, Faculty of Law and  
Professor Valerie Steeves, Department of Criminology,  
University of Ottawa;

Dr. Adam Molnar, Surveillance Studies Centre,  
Queen's University;

Professor Andrea Slane, Faculty of Social Sciences & Humanities,  
University of Ontario Institute of Technology; and

Professor Kevin Walby, Department of Criminal Justice,  
University of Winnipeg.

VIA E-MAIL: <christopher@christopher-parsons.com>.

June 4, 2014

**RE: January 20 Data Request (items 1-10); May 1 Personal Information Template**

Dear Professors and Drs. Austin, Bennett, Clement, Deibert, Diab, Geist, Molnar, Parsons,  
Slane, Steeves, Walby, and Winseck:

As you know, TekSavvy Solutions Inc. ("TekSavvy") is a provider of Internet access, voice  
telephony, and related telecommunication services. On 20 January 2014, you forwarded an  
email setting out ten sets of questions and sub-questions about TekSavvy's information  
disclosure practices.

- 2 -

Part of the mission that TekSavvy has set for itself is to innovate in the protection of consumer rights online. Thus far, our focus has been on ensuring that we do so by providing an open, network-neutral, consumer-oriented service. However, the Edward Snowden leaks based in the U.S. and the multi-national investigative activity following them have helped underline a key commitment that is required to achieve this mission, which is strong data privacy and transparency. In part to better address challenges such as those raised by your letter, by Dr. Parsons' January 22 and March 6 Citizen Lab blog posts relating to it,<sup>1</sup> and a number of public disclosures that have come to light since then, TekSavvy has taken steps to strengthen our internal team dedicated to legal and regulatory matters.

In particular, we in April initiated a review of our privacy policy, consumer terms and conditions, and internal practices with respect to information that we treat as personal. This includes all of the information available to us that is about identifiable individuals, including unique device identifiers and metadata that are able to be correlated with an individual's or household's subscription. Our review involves a full audit of the systems that we have developed as our company has grown from a small access provider to its current size. The purpose of the review is to evaluate how our formal and informal collection, storage, and disclosure practices reflect our commitment and, where appropriate, to formalize our policies and practices in this regard, strengthen them, or both, including the issuance of regular transparency reports. The review is ongoing. Your questions and suggestions have been an important tool in focusing that review.

Because you asked that we respond by 3 March 2014, I would like first to apologise that we have not been able to do so until now. In view of overlap both in content and in audience, our answers are also responsive to a template published and publicized beginning May 1, when Citizen Lab advocated that Canadian telecommunications subscribers forward it to their providers in order to seek the personal information that their providers collect, retain, manage, and disclose about them. As you can imagine, a not-insignificant portion of our legal and regulatory resources have been devoted to process and responding to those template requests. General information about our policies and practices as they relate to that template is set out beginning on page 14 below, after the answers to your January 20 questions and sub-questions.

**Q1. In 2012 and in 2013, how many total requests did your company receive from government agencies to provide information about your customers' usage of communications devices and services:**

A1. In 2012, and 2013, we received 52 requests from government agencies about our customers' usage of communications devices and services. All of these requests were restricted to correlating Internet Protocol ("IP") addresses with subscriber name and information. All of them were received from law enforcement agencies.

**Q1a) Within that total, please list the amount of requests your company received for each type of usage, including but not limited to: 1) Geolocation of device (please distinguish between real-time and historical); 2) Call detail records (as obtained by number recorders or by disclosure of stored data);**

<sup>1</sup> Christopher Parsons, "Towards Transparency in Canadian Telecommunications", 22 January 2014, online: <https://citizenlab.org/2014/01/towards-transparency-canadian-telecommunications/>, and "The Murky State of Canadian Telecommunications Surveillance", March 6, 2014, online: <https://citizenlab.org/2014/03/murky-state-canadian-telecommunications-surveillance/>.

- 3 -

**3) Text message content; 4) Voicemail; 5) Cell tower logs; 6) Real-time interception of communications (i.e. wiretapping); 7) Subscriber information; 8) Transmission data (e.g. duration of interaction, port numbers, communications routing data, etc.); 9) Data requests (e.g. web sites visited, IP address logs); 10) Any other kinds of data requests pertaining to the operation of your network and business.**

A1a) All of those requests were received for 7) subscriber information. None of these requests were received for 1) geolocation, 2) call detail records, 3) text message content, 4) voicemail, 5) cell tower logs, 6) real-time interception, 8) transmission data, including duration of interaction, port numbers, and communications routing data, 9) data requests, including web sites visited, IP address logs, or 10) other kinds of data requests not covered by the categories you have indicated.

**Q1b) For each of the request types, please detail all of the data fields that are disclosed as part of responding to a request.**

A1b) For request type 7 (subscriber information), the data fields we disclosed were: subscriber name, postal address, telephone number, and e-mail address. All of these disclosures were made to government institutions acting with lawful authority in the context of a criminal investigation.

**Q1c) Within the aforementioned total, how many of the requests were made for real-time disclosures, and how many were made retroactively for stored data?**

A1c) Within the aforementioned total, all of the requests were made retroactively for stored data (subscriber name and contact details). None of them were made for real-time disclosures, nor related to information to which real-time disclosures would be relevant.

**Q1d) Within the aforementioned total, how many of the requests were made in exigent circumstances, and how many were made in non-exigent circumstances?**

A1d) The aforementioned total is for 2012 and 2013. During that period, we did not store information as to which requests were made in exigent, and which in non-exigent, circumstances. Rather, during that period it was our practice, consistent with sub-paragraph 7(3)(c.1)(ii) of *PIPEDA*,<sup>2</sup> to produce information where (a) pursuant to a lawful authority, (b) in the context of a law enforcement investigation, and (c) restricted to basic subscriber information.

Since that time, we have further restricted our practice as a result of the aforementioned review of all of our privacy policies and practices. It is now our policy to make such disclosures only in response to a warrant, production order,

<sup>2</sup> *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

- 4 -

or instances in which the conditions for such a warrant or order were present but exigent circumstances<sup>3</sup> prevented one from being obtained.

In relation to the above, we understand that draft legislation is currently before the Senate (Bill S-4) which, among other things, would revise subsection 7(3) of *PIPEDA*. These revisions would, irrespective of any findings the Supreme Court of Canada may make in the interim,<sup>4</sup> broaden the circumstances in which organizations may disclose personal information on their own initiative to third parties, and without a judicial order. The revisions would allow organizations to make such disclosures to government institutions or other organizations in relation to a contravention of laws that has been, is being, or about to be committed.<sup>5</sup>

It has been suggested that, had such legislation been introduced earlier, TekSavvy could have responded to the Voltage request<sup>6</sup> differently, such as by choosing to disclose the subscriber information that Voltage requested. To be clear, the policy described above was arrived at despite the draft legislation before the Senate. Should Bill S-4 be passed in its current format, it will not affect TekSavvy's approach to copyright matters.<sup>7</sup>

**Q1e) Within the total, how many of the requests were made subject to a court order?**

A1e) Within the total, one of the requests was made subject to a court order.

**Q1f) Within the total, how many of the requests did your company fulfill and how many did it deny? If your company denied requests, for what reasons did it do so?**

A1f) Within the total, we made 17 disclosures (33 percent) pursuant to lawful authority related to criminal investigations, and denied the remaining 35 (67 percent).

<sup>3</sup> *Criminal Code*, R.S.C. 1985, c. C-4, section 487.11 ("A peace officer, or a public officer who has been appointed or designated to administer or enforce any federal or provincial law and whose duties include the enforcement of this or any other Act of Parliament, may, in the course of his or her duties, exercise any of the powers described in subsection 487(1) or 492.1(1) without a warrant if the conditions for obtaining a warrant exist but by reason of exigent circumstances it would be impracticable to obtain a warrant").

<sup>4</sup> *Spencer v. the Queen*, Case 34644, Supreme Court of Canada, appealing *R. v. Spencer*, 2011 SKCA 144.

<sup>5</sup> *Digital Privacy Act*, Bill S-4 (41<sup>st</sup> Parl., 2<sup>nd</sup> Sess), second reading (8 May 2014), subsections 6(8)-(10).

<sup>6</sup> *Voltage Pictures LLC v. John Doe*, 2014 FC 161.

<sup>7</sup> However, in the event Bill S-4 continues to move forward, TekSavvy intends to review whether Bill S-4's disclosure powers would affect our practice in the following scenario: we are approached directly by a non-Canadian police force in exigent circumstances, such as a U.S. police force acting on a live hostage or bomb threat traced back by an application provider to a TekSavvy IP address. As currently drafted, it is not clear that *PIPEDA* allows a telecommunications service provider to respond to such a situation without informing that individual in writing without delay of the disclosure, notwithstanding such disclosure's possible effect on the ongoing response to the live situation. Refer to *PIPEDA*, paragraph 7(3)(e), since a non-Canadian law enforcement agency is not a "government institution" as contemplated by sub-paragraph 7(3)(c.1)(ii): *Outsourcing of canada.com e-mail services to U.S.-based firm raises questions for subscribers*, *PIPEDA Case Summary 2008-394*.

- 5 -

While we did not, for 2012 and 2013, store information as to the reasons for denial, please refer to A1d above with respect to our general practice. Non-exigent requests by a government institution that were not made (i) pursuant to a lawful authority, (ii) in the context of a law enforcement investigation, and (iii) restricted to basic subscriber information, would generally have been denied without a warrant or production order.

**Q1g) Within the total, please identify how many requests were made by Federal, by provincial, and by municipal government agencies?**

A1g) Within the total, 19 requests were by federal government agencies (37 percent). The remainder were made by provincial agencies, of which five were non-municipal (10 percent) and 28 were municipal (54 percent). These agencies were police forces.

**Q1h) Do you notify your customers when government agencies request their personal information? If so, how many customers per year have you notified?**

A1h) All government agency requests we have received for personal information have related to criminal investigations. Warrants and production orders generally prohibit notification of customers or disclosure of the warrant's or production order's existence to anyone. We have taken the position that the mere aggregation of warrants, production orders, and other requests received in order to enumerate them by relevant category would not in any way inform any third party of the content specific to, or specific existence of, any such judicial order.

We would note that in a non-criminal context, in response to a 2012 request by a third party for disclosure of subscriber information in a civil copyright matter,<sup>8</sup> we notified 2,114 subscribers that the subscriber name and contact details corresponding to their IP address had been requested by a rightsholder that had apparently tied those IP addresses to unauthorized peer-to-peer transfers of a particular film.

To date we have not released any subscriber information to that third party. The judicial order under which we are to do so, which followed lengthy court proceedings and ongoing follow-ups, limited the request to name and address information, and maintained strong court oversight as to how this information could be used and when it was required to be disclosed. We believe that this created an important protective framework for consumers.

**Q2. For each type of usage in 1(a), how long does your company retain those records and the data fields associated with them?**

A2. Q1a) asked about ten types of usage:

**Q201) Geolocation of device (please distinguish between real-time and historical).**

<sup>8</sup> Please refer to note 6 above.



- 6 -

A2.01) We do not undertake geolocation of devices, such as through third-party IP address geolocation. We do undertake the following chain of activity:

- (i) collect modem identifiers (Media Access Control ["MAC"] addresses) in order to authenticate their subscription;
- (ii) associate IP addresses with those MAC addresses, in order to provide Internet access to them; and
- (iii) insert those IP addresses into routing tables organized geographically, in order to route Internet traffic to and from those Internet access points.

Taken together, these data tables would permit geolocation of devices down to the community level. It is our policy, which we are now implementing, to maintain information that is in the correlation table outlined in (ii) for 30 days. This has been reduced from our previous retention policy, which is 90 days, as a result of the aforementioned review, and we are currently in the process of auditing our systems to ensure the universal deployment of this approach.

**Q2.02) Call detail records (as obtained by number recorders or by disclosure of stored data).**

A2.02) Call Detail Records ("CDRs") are call-level metadata records maintained in respect of voice telephony services. We currently provide two voice telephony services, both of them interconnected with the Public Switched Telephone System ("PSTN"): TekTalk, a managed voice-over-Internet service; and Home Phone, a dedicated primary exchange service. We do not have number record records for either service, but do have some stored data, as follows.

TekTalk generates CDRs only for long-distance calls, since local calls are not tolled, and our operational requirement for CDRs is billing-related. At present, those CDRs are archived indefinitely in order to support subsequent billing disputes and analysis and, more broadly, tax and anti-fraud requirements. Our policy review is currently engaged with determining the extent to which we can meet these requirements through aggregation that would allow the deletion of individual CDRs.

TekSavvy Home Phone is based on an Incumbent Local Exchange Carrier ("ILEC") wholesale service. Any CDR connected with a TekSavvy customer's use of TekSavvy Home Phone is generated and retained by the ILEC which, in turn, provides monthly billing records to TekSavvy. Like TekTalk toll CDRs, these billing records have thus far been archived indefinitely, which policy is subject to current review.

**Q2.03) Text message content.**

A2.03) We do not have text message records.

**Q2.04) Voicemail.**

- 7 -

A2.04) Deleted TekTalk voicemail messages can be retrieved by users for up to 14 days. We have not enabled functionality that would allow the onward storage or retrieval of voicemail messages deleted by the user. We do not store TekSavvy Home Phone voicemail messages, in respect of which we direct users to the third-party providers of these services.

**Q2.05) Cell tower logs.**

A2.05) We do not have cell tower logs.

**Q2.06) Real-time interception of communications (i.e. wiretapping).**

A2.06) We do not have real-time interception records.

**Q2.07) Subscriber information.**

A2.07) We retain subscriber information (subscriber name, street address, telephone number, email address where available, social media handles where available) and related billing information even after a subscription ends, in part in order to support the tax, anti-fraud, and related audit functions described earlier. We are currently reviewing our ability to shorten this period to two years after a subscription ends, based on the CASL<sup>9</sup> definition of an "existing business relationship", through techniques such as data de-identification and depersonalization.

We retain correlation tables linking subscriber information to device identifier, as described elsewhere in this response. It is now our policy to overwrite records in these correlation tables after 30 days.

**Q2.08) Transmission data (e.g. duration of interaction, port numbers, communications routing data, etc.).**

A2.08) With respect to Internet access, we avoid logging transmission data that is personal information, such as IP-address-specific transmission data. The transmission data that we do retain in respect of IP addresses is the time and date on which the IP address began to be used (or "leased") and on which the lease expired due to prolonged inactivity. Apart from this information, and except where operational reasons require it such as for troubleshooting, we do not have further relevant transmission data outside the short window during which it is being read and written by our routing and switching equipment. Any such records retained for operational reasons are used only for that purpose and deleted as soon as is practicable.

**Q2.09) Data requests (e.g. web sites visited, IP address logs).**

---

<sup>9</sup> *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, S.C. 2010, c. 23, paragraph 10(10)(a).*

- 8 -

A2.09) We avoid logging user data request records that are personal information, such as IP-address-specific web sites or other activity logs. Except where operational reasons require it, such as for troubleshooting, we therefore do not have relevant data request records outside the short window during which it is being read and written by our routing and switching equipment. Any such records retained for operational reasons are used only for that purpose and deleted as soon as is practicable.

**Q2.10) Any other kinds of data requests pertaining to the operation of your network and business.**

A2.10) The wholesale access services that are an input into our retail Internet access services are billed to us partly on the basis of capacity ("Capacity-Based Billing", or "CBB"). We therefore monitor our users' Internet data usage, which may be reflected on a given monthly bill depending on the package and options they have chosen for that month. This monitoring generates capacity usage records at regular intervals. The capacity usage records do not include port numbers, communications routing data, web sites visited, or other transmission data or metadata. They are aggregated for billing purposes, following which the individual records that have been aggregated are discarded as soon as is practicable.

Our Internet access service is bundled with domain name ("DNS") and email services. DNS requests are anonymized and are not logged. Our email services consist of Internet Message Access Protocol ("IMAP"), inbound Post Office Protocol ("POP3"), and outbound Simple Mail Transfer Protocol ("SMTP") services:

- Deleted IMAP and POP3 email messages that can no longer be retrieved by the account holder are deleted, and no further metadata is stored in their regard—we have not enabled functionality that would allow the onward storage or retrieval of the email messages they have deleted.
- However, use of SMTP to send email generates metadata that is maintained for operational purposes, including spam filtering. At present, those SMTP logs are archived to support subsequent billing disputes and operations analysis, especially trouble-shooting. We are currently reviewing our ability to impose a rolling deletion window for these logs in respect of personal information without hampering operational purposes, such as through aggregation and de-personalization.

We maintain Web pages in order to provide information about our services and, in addition, are active on a range of social media platforms. We are currently reviewing our privacy practices in respect of these activities, particularly with regard to the log files that relate to IP addresses that visit our sites and with regard to our use of third-party marketing-related analysis tools like Google Analytics. Outside our use of third-party analysis tools, our correlation of IP addresses to subscribers is limited by the rolling 30-day window policy described above.

- 9 -

**Q3. What is the average amount of time law enforcement requests for each of the information requests in 1(a) (e.g. 3-5 days of records)? What is the average amount of time that your company is typically provided to fulfill each of the information requests in 1(a)?**

A3. Law enforcement requests that we receive typically relate to subscriber information, for which average time is not a relevant measure. We are typically provided 30 days to respond to a production order. We are asked to respond as soon as possible in exigent circumstances such as a hostage or bomb threat.

**Q4. How many times were you asked to disclose information noted in 1(a) based specifically on:**

**Q4a) child exploitation grounds?**

**Q4b) terrorism grounds?**

**Q4c) national security grounds?**

**Q4d) foreign intelligence grounds?**

A4. For 2012 and 2013, we did not store information as to which requests were made according to the classification set out above. It is our intent to do so going forward.

**Q5. What protocol or policies does your company use to respond to requests for data that are noted in 1(a)?**

To respond to requests for data that are noted in Q1a, we first determine whether the requester is a government institution or not. If they are not a government institution, we generally ask them to address themselves to one. If they are a government institution, we follow the legal standard set out in A5a.

**Q5a) What legal standard do you require government agencies to meet for each type of data request noted in 1(a)?**

A5a) Our general legal standard is to require that government agencies provide a warrant, provide a production order, or demonstrate that obtaining one is justified but unfeasible due to exigent circumstances, such as a live bomb threat.

You have asked how the legal standard that we require applies to each type of data request noted in Q1a, which asked about ten types of usage:

**Q5a.01) Geolocation of device (please distinguish between real-time and historical).**

A5a.01) We do not undertake geolocation of devices, such as through third-party IP address geolocation. We would apply the above-noted general legal standard in response to data requests for disclosure of the information set out in A2.01.

**Q5a.02) Call detail records (as obtained by number recorders or by disclosure of stored data).**

- 10 -

A5a.02) We would apply the above-noted general legal standard to disclosure of stored CDRs that are in our possession. We do not have number recorder records.

**Q5a.03) Text message content.**

A5a.03) We do not have text message records.

**Q5a.04) Voicemail.**

A5a.04) We would apply the above-noted general legal standard to disclosure of stored voicemails that are in our possession.

**Q5a.05) Cell tower logs.**

A5a.05) We do not have cell tower logs.

**Q5a.06) Real-time interception of communications (i.e. wiretapping).**

A5a.06) We do not have real-time interception records.

**Q5a.07) Subscriber information.**

A5a.07) We would apply the above-noted general legal standard to subscriber information and IP-to-subscriber correlation disclosure.

**Q5a.08) Transmission data (e.g. duration of interaction, port numbers, communications routing data, etc.).**

A5a.08) We do not generally have such transmission data. In the unlikely event that we do have it, as a result of trouble-shooting or other operational needs, we would apply our general legal standard to its disclosure.

**Q5a.09) Data requests (e.g. web sites visited, IP address logs).**

A5a.09) We do not generally have such data request records. In the unlikely event that we did have it, we would apply the above-noted general legal standard to its disclosure.

**Q5a.10) Any other kinds of data requests pertaining to the operation of your network and business.**

A5a.10) We would apply the above-noted general legal standard to data requests pertaining to the operation of our network and business.

**Q5b) What are the average number of subscribers who typically have their information disclosed in government agencies requests, for each type of request noted in 1(a)?**

- 11 -

A5b) The answers to Q1a noted that all of the requests we received in 2012 and 2013 from government agencies, to provide information about our customers' usage of communications devices and services, pertained to 7) subscriber information. None of these requests were received for 1) geolocation, 2) call detail records, 3) text message content, 4) voicemail, 5) cell tower logs, 6) real-time interception, 8) transmission data, including duration of interaction, port numbers, and communications routing data, 9) data requests, including web sites visited, IP address logs, or 10) other kinds of data requests not covered by the categories indicated.

Such requests from law enforcement agencies typically covered single subscribers. In response to your question as to the average number of subscribers who typically have their information disclosed in law enforcement agencies requests, the number therefore varies between zero and one. While Q1a and Q5b do not relate to government agencies requests for 2014, we have received one such request in 2014 that relates to more than one subscriber. It is the Federal Court order in respect of a copyright claim noted in A1d and A1h (Voltage), in respect of which no subscribers have had their information disclosed to date.

**Q5c) Does your company have distinct policies to respond to exigent and non-exigent requests? If yes, what are these policies or how do they differ?**

A5c) Yes. In non-exigent circumstances, it is our policy to require a warrant or production order. In exigent circumstances, it is our policy to (i) require that the government institution, generally a law enforcement agency, demonstrate that obtaining one is justified but unfeasible due to the circumstances; and to (ii) confirm the veracity of such demonstrations.

**Q5d) Is your company required to design your networks and services so government agencies can more readily access customer data in a real time or in a retroactive manner? If yes, please detail those requirements.**

A5d) TekSavvy does not provide mobile PSTN services subject to the *Solicitor-General's Enforcement Standards for Lawful Interception of Telecommunications*.

We are aware of *Criminal Code* provisions under which law enforcement requests could result in an order to provide for real-time interception or install tracking devices or number recorders,<sup>10</sup> *CSIS Act* provisions under which CSIS requests could result in a real-time interception order,<sup>11</sup> *National Defence Act* provisions under which CSEC requests could result in a real-time foreign-communications interception order,<sup>12</sup> and *Child Pornography Reporting Act* provisions under which we could be required to preserve data at a secure offline

<sup>10</sup> *Criminal Code*, sections 184.1, 194.2, 194.3, 185, 186 (telewarrant), 492.1 and 492.2.

<sup>11</sup> *CSIS Act*, R.S.C., 1985, c. C-23, section 21.

<sup>12</sup> *National Defence Act*, R.S.C. 1985, c. N-5, section 273.65.

- 12 -

location.<sup>13</sup> In the event we become subject to such orders, we may not have an avenue to be compensated for the costs of compliance unless "the financial consequences [are] so burdensome that it would be unreasonable in the circumstances to expect compliance."<sup>14</sup> We also anticipate the coming into force of, *Copyright Act* paragraph 41.26(1)(b) requiring us to retain records for six months—and, if a claimant commences proceedings during that period, one year after proceedings have been commenced—in respect of which regulatory provisions may provide a way to recover our compliance costs.

All of these provisions could create an incentive for TekSavvy to design its networks and services so that the cost of any mandatory orders can reasonably be absorbed. However, to date we have not acted on that incentive with respect to our network and services design.

**Q5e) Does your company have a dedicated group for responding to data requests from government agents? Are members of this group required to have special clearances in order to process such requests? What is the highest level company official that has direct and detailed knowledge of the activities of this group?**

A5e) Our company does not have a dedicated group for responding to data requests from government agents. We do not require employees to have special clearances in order to be available for processing such requests. Company officials at our company's highest levels have direct and detailed knowledge of our responses to data requests from government agents.

**Q6. What is the maximum number of subscribers that the government requires you to be able to monitor for government agencies' purposes, for each of the information types identified in 1(a)? Have you ever received an official order (e.g. ministerial authorization court order, etc.) to expand one of those maximum numbers?**

A6. Government agencies have not sought to require TekSavvy to undertake real-time monitoring of subscribers. Please see also A5b (above).

**Q7. Has your company received inappropriate requests for information identified in 1(a)? If yes, why were such requests identified as inappropriate and who makes a decision that a request is inappropriate? And if yes, how did your company respond?**

A7. TekSavvy denied 67 percent of requests received in 2012 and 2013 for the reasons set out in A1d and A1f (above). Although we did not, for 2012 and 2013, store information as to the reasons for denial, we did not generally receive requests from government institutions that had the appearance of being frivolous, for an improper purpose, or anything other than professional.

<sup>13</sup> *Child Pornography Reporting Act*, S.C. 2011, c. 4, section 4.

<sup>14</sup> *Tele-Mobile Co. v. Ontario*, [2008] 1 S.C.R. 305, paragraph 67.

- 13 -

**Q8. Does your company have any knowledge of government agencies using their own:**

**Q8a) tracking products (e.g. 'IMSI Catchers')?**

**Q8b) infiltration software (e.g. zero day exploits, malware, such as FinFisher, etc.)?**

**Q8c) interception hardware (i.e. placed within or integrated with your company's network)?**

**Q8d) If yes to 8(a), (b), or (c), please explain.**

A8. We do not have any experience of government agency tracking products, infiltration software, or interception hardware on our network.

**Q9. Does your company cooperate with government agencies that use their own tracking equipment or provide information on how to interoperate with your company's network and associated information and subscriber information? If yes, how does it cooperate, how many requests does it receive for such cooperation, and how many of your subscribers have been affected by such equipment or interoperation?**

A9. No, we do not cooperate or provide the kind of information referred to.

**Q10. In 2012 and 2013, did your company receive money or other forms of compensation in exchange for providing information to government agencies? If yes, how much money did your company receive? And if yes, how much does your company typically charge for specific services (please refer to the list in 1(a) above)?**

A10. No, we did not receive compensation in 2012 and 2013 for providing information to government agencies.

**Q10a) Does your company charge different amounts depending on whether the request is exigent or non-exigent? Does your company charge fees for exigent cell phone tracking requests from law enforcement authorities?**

A10a) Please refer to A10.

**Q10b) Please include any written schedule of fees that your company charges law enforcement for these services?**

A10b) We are aware of ILEC Law Enforcement Agency Services ("LEA Service") tariffs establishing charges for Customer Name and Address and for Service Provider Identification Service requests relating to telephone numbers.<sup>15</sup> TekSavvy, whose services are not tarified, has not created any similar schedule of fees. In any case, our current policy of requiring a warrant, production order, or exigent

<sup>15</sup> *Provision of subscribers' telecommunications service provider identification information to law enforcement agencies*, Order CRTC 2001-279, 30 March 2001; *Provision of subscribers' telecommunications service provider identification to law enforcement agencies*, Telecom Decision CRTC 2002-21, 12 April 2002.



- 14 -

circumstances, which is described in A1d and A5c above, limits the circumstances in which imposition of a fee schedule is likely possible.

**Q10c) Does your company operate purely on a cost recovery basis for providing information to government agencies?**

A10c) Please refer to A10. In the past the combined volume of private information requests, from government agencies seeking third-party information and from individuals requesting records containing their own information, has not required in-depth review of costs incurred. We are now reviewing these costs in the context of the aforementioned policy review.

The above-noted questions were posed, and our answers to them provided, in part in order to tell you about our data retention and sharing policies. On 1 May 2014 Citizen Lab published a blog posting entitled "Responding to the Crisis in Canadian Telecommunications". The blog posting argued that Canadians ought to fill in a provided template and issue it to the telecommunications companies providing them with service. The blog posting suggested that doing so would help Canadians improve their ability to understand how companies manage the personal information entrusted to them and then make informed decisions about whether they want to maintain that commercial relationship.<sup>16</sup>

As a telecommunications company providing Canadians with service, we have received many such template requests, whose content relates to the above-noted questions and answers. In view of the overlap between your 20 January 2014 letter and Citizen Lab's 1 May 2014 blog posting, we are therefore providing further information that is responsive to the Citizen Lab template, relating the information it seeks to the answers set out above. It is our intent that the review we have initiated of our privacy policy, consumer terms and conditions, and internal practices result in the making available of this information to our users in a readily-accessible format. It is our hope that, in the interim, including it in this published letter will be of assistance.

**T1. All logs of IP addresses associated with me, my devices, and/or my account (e.g. IP addresses assigned to my devices/router, IP addresses or domain names of sites I visit and the times, dates, and port numbers).**

T1(R). We log the IP addresses associated with the MAC addresses that correspond to particular devices, and log which of those devices are associated with particular customers, in the manner described in A2.01.

It is our policy to retain the IP-to-MAC-address correlation information for 30 days. As described in A2.08 and A2.09, we do not store information as to the IP addresses or domain names of sites that subscribers visit or their times, dates, or port numbers.

**T2. Listing of 'subscriber information' that you store about me, my devices, and/or my account.**

<sup>16</sup> Christopher Parsons, "Responding to the Crisis in Canadian Telecommunications", 22 January 2014, online: <https://citizenlab.org/2014/05/responding-crisis-canadian-telecommunications/>.

- 15 -

T2(R). Our subscribers can access much of the information that we store about them online through TekSavvy's My Account portal, including name, address, service address, phone number, email address, usage information, and past bills. The subscriber information that we store that cannot yet be accessed through the My Account portal consists generally of:

- modem type, firmware, and MAC address;
- current-billing-cycle usage information;
- communications opt-ins; and
- internal notes on file, including call logs.

Please also refer to the answers provided above, particularly A2.07, A2.10, and A5a.07.

**T3. Any geolocational information that you may have collected about me, my devices, and/or associated with my account (e.g. GPS information, cell tower information).**

T3(R). As we do not provide mobile services, we do not have GPS or cell tower information, nor undertake targeted geolocation of devices. However, please refer to A2.01 above with respect to routing table information that could geolocate a subscriber's device down to the neighbourhood.

**T4. Text messages or multi-media messages (sent and received, including date, time, and recipient information).**

T4(R). As we do not provide mobile services, we do not have text ("SMS") or multimedia ("MMS") messages. We do provide voicemail and email services, which are addressed above at A2.02 and A5a.04 (voicemail) and A2.10 (email), respectively

**T5. Call logs (e.g. numbers dialed, times and dates of calls, call durations, routing information, and any geolocation or cellular tower information associated with the calls).**

T5(R). We maintain logs for operational purposes whose information is deleted after one week. We also maintain last-ten call information (last ten calls missed, answered, and dialed, respectively) that is available, if applicable, in the My Account portal. However, most call logs and the related data fields described in parentheses are stored either in Call Detail Records that we retain, and in billing records. Our treatment of CDRs is set out above in A2.02. Our treatment of bills is set out above in T2(R).

**T6. Information collected about me, or persons/devices associated with my account, using one of your company's mobile device applications.**

T6(R). Our company does not have mobile device applications.

**T7. Any additional kinds of information that you have collected, retained, or derived from the telecommunications services or devices that I, or someone associated with my account, have transmitted or received using your company's services.**

- 16 -

T7(R). All of the kinds of information that we routinely collect, retain, or derive are described in the answers included in this letter. Please refer, in particular, to A2.01 through A2.10, which address related issues.

**T8. Any information about disclosures of my personal information, or information about my account or devices, to other parties, including law enforcement and other state agencies.**

T8(R). Our approach to such disclosures is addressed above at A1h.

We trust that the information we have provided in this letter responds to your questions. As noted, this information is part of an ongoing process at TekSavvy. We work to ensure that all of our practices comply with our *PIPEDA*<sup>17</sup> and *CRTC*<sup>18</sup> obligations. However, we have come to believe that it is also TekSavvy's responsibility, as part of its understanding with its subscribers and as part of the value it delivers to Canadian telecommunications markets, to lead with respect to going beyond those obligations.

While that process is ongoing, we are glad to have embarked upon it, and would be pleased to continue this dialogue with you as we further refine our policies and practices in this area.

Yours sincerely,

*[transmitted electronically]*

Bram Abramson  
Chief Legal and Regulatory Officer

---

<sup>17</sup> Cited above, at note 2.

<sup>18</sup> We note, in particular, the confidentiality provisions requiring that, unless a customer provides express consent or disclosure pursuant to a legal power, information other than the customer's name, address, and listed telephone number is not to be disclosed to anyone but: (a) the customer or (b) their agent; another (c) telephone company or (d) service provider, for operational purposes and provided it is on a confidential basis; or (e) a collections agent, again on a limited basis. *Confidentiality provisions of Canadian carriers*, Telecom Decision CRTC 2003-33, 30 May 2003, paragraph 49, as extended by *Follow-up to Telecom Decision CRTC 2003-33 – Confidentiality provisions of Canadian carriers*, Telecom Decision CRTC 2004-27, 22 April 2004, paragraph 22.



**Office of the Deputy Attorney General**  
Washington, D.C. 20530

January 27, 2014

Sent via Email

Colin Stretch, Esquire  
Vice President and General Counsel  
Facebook Corporate Office  
1601 Willow Road  
Menlo Park, CA 94025

Kent Walker, Esquire  
Senior Vice President and General Counsel  
Google Corporate Office Headquarters  
1600 Amphitheater Parkway  
Mountain View, CA 94043

Erika Rottenberg, Esquire  
Vice President, General Counsel/Secretary  
LinkedIn Corporation  
2029 Stierlin Court  
Mountain View, CA 94043

Brad Smith, Esquire  
Executive Vice President and General Counsel  
Microsoft Corporate Office Headquarters  
One Microsoft Way  
Redmond, WA 98052-7329

Ronald Bell, Esquire  
General Counsel  
Yahoo Inc. Corporate Office and Headquarters  
701 First Avenue  
Sunnyvale, CA 94089

Dear General Counsels:

Pursuant to my discussions with you over the last month, this letter memorializes the new and additional ways in which the government will permit your company to report data concerning requests for customer information. We are sending this in connection with the Notice we filed with the Foreign Intelligence Surveillance Court today.

In the summer of 2013, the government agreed that providers could report in aggregate the total number of all requests received for customer data, including all criminal process, NSLs,

Letter to Colin Stretch, Kent Walker, Erika Rottenberg, Brad Smith and Ronald Bell  
Page 2

and FISA orders, and the total number of accounts targeted by those requests, in bands of 1000. In the alternative, the provider could separately report precise numbers of criminal process received and number of accounts affected thereby, as well as the number of NSLs received and the number of accounts affected thereby in bands of 1000. Under this latter option, however, a provider could not include in its reporting any data about FISA process received.

The government is now providing two alternative ways in which companies may inform their customers about requests for data. Consistent with the President's direction in his speech on January 17, 2014, these new reporting methods enable communications providers to make public more information than ever before about the orders that they have received to provide data to the government.

Option One.

A provider may report aggregate data in the following separate categories:

1. Criminal process, subject to no restrictions.
2. The number of NSLs received, reported in bands of 1000 starting with 0-999.
3. The number of customer accounts affected by NSLs, reported in bands of 1000 starting with 0-999.
4. The number of FISA orders for content, reported in bands of 1000 starting with 0-999.
5. The number of customer selectors targeted under FISA content orders, in bands of 1000 starting with 0-999.
6. The number of FISA orders for non-content, reported in bands of 1000 starting with 0-999.<sup>1</sup>
7. The number of customer selectors targeted under FISA non-content orders, in bands of 1000 starting with 0-999.

A provider may publish the FISA and NSL numbers every six months. For FISA information, there will be a six-month delay between the publication date and the period covered

---

<sup>1</sup> As the Director of National Intelligence stated on November 18, 2013, the Government several years ago discontinued a program under which it collected bulk internet metadata, and no longer issues FISA orders for such information in bulk. See <http://icontherecord.tumblr.com/post/67419963949/dni-clapper-declassifies-additional-intelligence>. With regard to the bulk collection of telephone metadata, the President has ordered a transition that will end the Section 215 bulk metadata program as it currently exists and has requested recommendations about how the program should be restructured. The result of that transition will determine the manner in which data about any continued collection of that kind is most appropriately reported.

Letter to Colin Stretch, Kent Walker, Erika Rottenberg, Brad Smith and Ronald Bell  
Page 3

by the report. For example, a report published on July 1, 2015, will reflect the FISA data for the period ending December 31, 2014.

In addition, there will be a delay of two years for data relating to the first order that is served on a company for a platform, product, or service (whether developed or acquired) for which the company has not previously received such an order, and that is designated by the government as a "New Capability Order" because disclosing it would reveal that the platform, product, or service is subject to previously undisclosed collection through FISA orders. For example, a report published on July 1, 2015, will not reflect data relating to any New Capability Order received during the period ending December 31, 2014. Such data will be reflected in a report published on January 1, 2017. After data about a New Capability Order has been published, that type of order will no longer be considered a New Capability Order, and the ordinary six-month delay will apply.

The two-year delay described above does not apply to a FISA order directed at an enhancement to or iteration of an existing, already publicly available platform, product, or service when the company has received previously disclosed FISA orders of the same type for that platform, product, or service.

A provider may include in its transparency report general qualifying language regarding the existence of this additional delay mechanism to ensure the accuracy of its reported data, to the effect that the transparency report may or may not include orders subject to such additional delay (but without specifically confirming or denying that it has received such new capability orders).

#### Option Two.

In the alternative, a provider may report aggregate data in the following separate categories:

1. Criminal process, subject to no restrictions.
2. The total number of all national security process received, including all NSLs and FISA orders, reported as a single number in the following bands: 0-249 and thereafter in bands of 250.
3. The total number of customer selectors targeted under all national security process, including all NSLs and FISA orders, reported as a single number in the following bands, 0-249, and thereafter in bands of 250.

\* \* \*

I have appreciated the opportunity to discuss these issues with you, and I am grateful for the time, effort, and input of your companies in reaching a result that we believe strikes an appropriate balance between the competing interests of protecting national security and furthering transparency. We look forward to continuing to discuss with you ways in which the

**Letter to Colin Stretch, Kent Walker, Erika Rottenberg, Brad Smith and Ronald Bell**  
**Page 4**

**government and industry can similarly find common ground on other issues raised by the  
surveillance debates of recent months.**

Sincerely,

A handwritten signature in black ink, appearing to read 'James M. Cole', written in a cursive style.

**James M. Cole**  
**Deputy Attorney General**



Public Safety / Sécurité publique  
Canada / Canada

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

Ottawa, Canada  
K1A 0P8

s.19(1)

**For your meeting with: Telus Corp.**  
**DATE: April 17, 2014**  
**TIME: 1:00 to 2:00 p.m.**  
**LOCATION: Executive Boardroom**

**REÇU AU BUREAU  
DU SM**  
  
AVR 16 2014  
**RECEIVED IN  
DM'S OFFICE**

**CONFIDENTIAL**

DATE: 16 AVR. 2014

File No.: NS 6950-O1 / 402684  
RDIMS No.: Dragon 22163

**MEMORANDUM FOR THE DEPUTY MINISTER**

**MEETING WITH TELUS CORPORATION TO DISCUSS  
TRANSPARENCY REPORTING FOR ELECTRONIC SURVEILLANCE**

(Information only)

**ISSUE**

You will be meeting with representatives from Telus Corp. on April 17, 2014, to discuss transparency of reporting for electronic surveillance activities, specifically what statistical information they are permitted to disclose (agenda attached at **TAB 1**).

The Telus representatives will be [REDACTED]

You will be accompanied by Peter Hammerschmidt and Paul Shuttle.

**BACKGROUND**

Transparency in electronic surveillance (i.e. the interception of communications and the search and seizure of electronic data) has been an item of growing interest in the global public environment and particularly over the last four months in Canada. In January 2014, the federal Privacy Commissioner issued a special report on surveillance, which called for increased transparency related to electronic surveillance practices, as well as new studies and guidelines. The same month, the Citizen Lab, a digital human rights group at the University of Toronto, asked Canada's top 16 telecommunications service providers (TSPs) to disclose the number of surveillance requests they had received from government agencies; and the NDP digital issues critic, Charmaine Borg, submitted Written Question Q-233 in Parliament, asking the Government to disclose surveillance figures.

.../2



- 2 -

In March 2014, 10 TSPs responded to the Citizen Lab request, but largely declined to provide statistics about the number of government requests, claiming that they were prohibited by law from doing so. However, Telus, in its response (**TAB 2**), committed to asking the Government what the rules governing disclosure were. On March 24, 2014, government agencies released their responses to Q-233 (the Public Safety Canada (PS) portfolio response is at **TAB 3**), which generated mixed responses in the media.

The principal electronic surveillance reporting mechanism in Canada is the *Annual Report on the Use of Electronic Surveillance*, which the Minister is required under section 195 of the *Criminal Code* to table in Parliament every year. The report provides a range of information on intercepted communications, including the number of authorizations granted, the number of people intercepted, and the types of offences for which authorizations were granted. It does not, however, include information on requests for other types of information, such as basic subscriber information (e.g. name, phone number, address) or metadata. At this time, Canadian TSPs do not issue their own reports.

The increased interest in transparency is not limited to Canada. The United States (US) has been seized with privacy and security matters recently, especially as a result of the unauthorized disclosures relating to the bulk collection of metadata by former National Security Agency (NSA) contractor Edward Snowden. In August 2013, in the wake of those disclosures, President Obama commissioned two independent expert groups to report on electronic surveillance issues, and at the same time eased rules and policies governing disclosures of aggregate statistical information by US TSPs. TSPs, including Google and Microsoft had been suing the US Government for this authority. Companies such as AT&T, Google, Microsoft and Verizon now release Transparency Reports detailing how many and what types of requests for information were made by government agencies (Verizon's most recent report is at **TAB 4**). Acting on the recommendations of the two independent expert groups, the President announced on March 27, 2014, that he would work with Congress to introduce legislation to end the bulk metadata collection program and strengthen judicial oversight over some types of electronic surveillance. He also solicited public views on the privacy-security balance via an online survey and announced a study on metadata.

### CONSIDERATIONS

With respect to constraints in the area of law enforcement,

[REDACTED]

from TSPs.

inquiries for data

.../3

**SECRET//CEO**

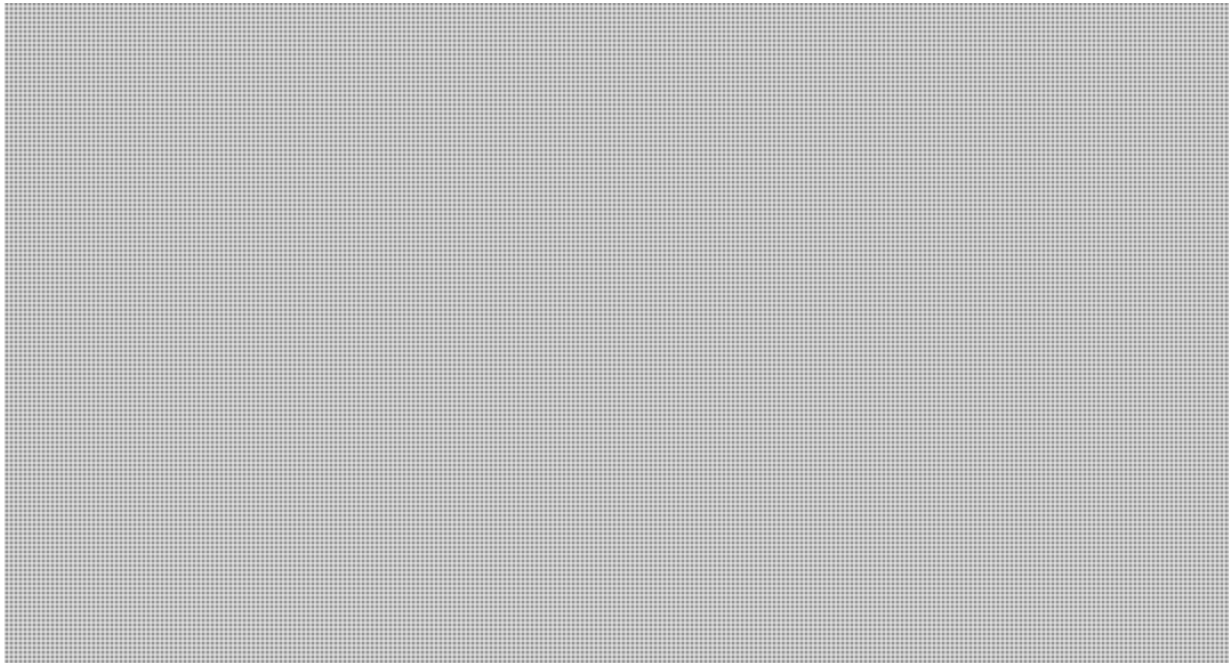
s.15(1)(d)(ii)

s.21(1)(a)

s.21(1)(b)

s.23

- 3 -



Enhanced transparency is key to demonstrating to the public that electronic surveillance is conducted responsibly, but there is a need to evaluate whether sensitive details about operations could be revealed through mass aggregate reporting of data. In the US, for example, the Federal Bureau of Investigation consulted with a wide range of law enforcement agencies over many months before clarifying what US TSPs could disclose. In the Canadian case, considerable consultation would be required with key stakeholders



**Key messages**

- The support that the law enforcement and intelligence community receives from Telus and other TSPs is essential to being able to investigate and prosecute crimes.
- PS is committed to protecting the safety and security of Canadians while respecting their privacy. 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.
- Any change in current practices would require extensive consultations with all relevant stakeholders.

.../4

**SECRET//CEO**

- 4 -

Should you require additional information, please do not hesitate to contact me at  
613-990-4976 or Ms. Lara Dyer, Acting Director General, National Security Operations,  
at 613-993-4595.



Lynda Clairmont  
Senior Assistant Deputy Minister  
National and Cyber Security

Enclosures: (4)

Prepared by: Maciek Hawrylak

s.21(1)(a)

s.21(1)(b)

**UNCLASSIFIED**

**Meeting to discuss transparency reporting consideration for telcos/TELUS**

April 17, 2014 – 1:00-2:00 p.m.  
19<sup>th</sup> floor, Executive Boardroom, 269 Laurier Avenue West

**AGENDA**

---

**1. Background information**


Current situation in Canada  
No transparency reporting at current time  
Note: aggregate disclosure to OPC in 2011  
Increasing pressure to disclose  
Standard 17 restrictions – scope

Transparency reporting in the U.S.  
Shareholder/public pressure re Verizon and AT&T  
NSA issues – Snowden disclosures

---

**2. Issue – whether/what to disclose**

Considerations for telcos

A large rectangular area of the document is redacted with a grey grid pattern, covering several lines of text under the second agenda item.

**3. Next steps**

---



**TELUS Compliance and Privacy Office**  
10020 – 100 Street, Floor 10  
Edmonton, Alberta  
Canada T5J 0N5  
www.telus.com

**Heather Hawley**  
Chief Compliance and Privacy Officer  
Member of the TELUS team

March 5, 2014

Christopher Parsons  
University of Toronto  
Citizen Lab, Munk School of Global Studies  
315 Bloor Street West  
Toronto, ON, M5S 1A3

Re: Data Retention and Sharing Policies of TELUS

Dear Mr. Parsons,

Thank you for your letter dated January 20, 2014, inquiring about the data retention and sharing policies of TELUS Communications Company ("TELUS"). Certainly, your objective to make informed public policy decisions about how to best protect the security and privacy of Canadians is laudable and one that TELUS shares.

The privacy and security of our customers and employees is of paramount importance to TELUS and, as such, we only disclose confidential customer information to third parties, including government agencies, in accordance with the company's service terms, its privacy policies, valid court orders or other applicable law. In fact, such is the passion that TELUS has for keeping the information of our customers confidential, that the Privacy Commissioner of Ontario has recognized our President and CEO, Darren Entwistle, as a Privacy Ambassador.

You may be aware that TELUS recently challenged a general warrant obtained by a law enforcement agency regarding the provision of text message data that TELUS felt was overreaching, and successfully pursued the matter all the way to the Supreme Court of Canada. The resulting decision of the Supreme Court has served to enhance the protection of privacy rights of Canadians. We are not aware of any other instance where a telecommunications company in Canada has taken similar action to protect the privacy of its customers. Indeed, it is notable that as we pursued this Supreme Court of Canada challenge we did it with little public support. In future, we would welcome your collaboration as we pursue privacy positions that are in the best interests of our customers, Canadians, and the moral fabric of our country.

Your letter has requested a great amount of detail regarding how, when, and why TELUS discloses information to government agencies. Respectfully, TELUS does not publicly disclose the information that has been requested in your letter. In fact, as you are probably aware, Standard 17 in the *Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications* prohibits network operators from disclosing certain information about interceptions. Therefore, it is more appropriate to request the desired information directly from the governmental agencies themselves, as the parties that initiate the disclosure requests, rather than from the telecommunications service providers who are, in contrast, simply adhering to the laws that apply to them. Government agencies are better positioned to balance transparency considerations with other important considerations such as the need for confidentiality in relation to investigative techniques, and other law

enforcement or national security concerns. In this regard, we will request the Government to clarify and limit the scope of current confidentiality requirements and to consider measures to facilitate greater transparency.

An area of concern, and one that as privacy advocates we would recommend that you consider, is the extensive scope of court orders obtained by law enforcement agencies. Notably, when TELUS receives court orders from law enforcement agencies, they can often be far reaching. Given your area of expertise, you might consider ways to encourage more restraint in the scope of such orders. This might be accomplished by advocating for the adoption of a model similar to that which exists in the United States where law enforcement agencies pay the costs associated with the production of the records which they obtain. The imposition of a moderate cost in this regard acts as a check and balance to ensure that court orders are focused and thus limited to those records which are considered by law enforcement agencies to be absolutely necessary. This would help to deter orders that are too broad in scope and that may unnecessarily impact the privacy of citizens.

We note that the Privacy Commissioner of Canada has recommended that existing federal privacy legislation be amended to provide for greater transparency with respect to disclosure of personal information by organizations to government agencies. If Parliament sees fit to amend the legislation as recommended, TELUS will, of course, fully comply.

Once again, we commend you for your efforts to enhance the security and privacy of Canadians and wish you well in this pursuit through the proper and appropriate government channels.

Yours truly,



Heather Hawley  
Chief Compliance and Privacy Officer



# INQUIRY OF MINISTRY DEMANDE DE RENSEIGNEMENT AU GOUVERNEMENT

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

QUESTION NO./N° DE LA QUESTION Q-233	BY / DE Ms. Borg (Terrebonne—Blainville)	DATE January 27, 2014
---	---	--------------------------

REPLY BY THE MINISTER OF PUBLIC SAFETY AND  
EMERGENCY PREPAREDNESS  
RÉPONSE DU MINISTRE DE LA SÉCURITÉ PUBLIQUE ET DE LA  
PROTECTION CIVILE

The Honourable Steven Blaney, P.C., M.P.

PRINT NAME OF SIGNATORY  
INSCRIRE LE NOM DU SIGNATAIRE

SIGNATURE  
MINISTER OR PARLIAMENTARY SECRETARY  
MINISTRE OU SECRÉTAIRE PARLEMENTAIRE

### QUESTION

With regard to requests by government agencies to telecommunications service providers (TSP) to provide information about customers' usage of communications devices and services: (a) in 2012 and 2013, how many such requests were made; (b) of the total referred to in (a), how many requests were made by (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 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 fulfil 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; and (n) in 2012 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?

REPLY / RÉPONSE

ORIGINAL TEXT  
TEXTE ORIGINAL

TRANSLATION  
TRADUCTION

### Public Safety Canada (PS)

PS is committed to protecting the safety and security of Canada while respecting Canadians' privacy. PS will continue to ensure an appropriate balance between Canadians' privacy rights, and giving public safety agencies the investigative tools they need to prevent and prosecute serious crimes, including terrorism. Transparency is key to giving Parliament and Canadians confidence in our ability to meet both of these objectives.

- 2 -

Agencies have made every reasonable effort to provide as open and transparent a response as possible, while also respecting the need to keep sensitive details confidential to avoid helping criminals and terrorists in their activities. In addition to the following information, PS releases figures about the number and type of interceptions conducted by the Royal Canadian Mounted Police (RCMP) in its *Annual Report on the Use of Electronic Surveillance*. The Department believes this is a valuable tool in being open with Canadians about how often and for what purposes their communications may be intercepted.

Access to certain limited information about individuals from telecommunications service providers (TSPs) is key to modern investigations and is a proportionate response to the need for public safety agencies to investigate criminal activities and threats to the security of Canada in the digital age. In just the last year, media reported on at least three alleged terrorist plots,<sup>1</sup> all of which were prevented in part because the RCMP was able to obtain information from TSPs ranging from basic subscriber information to intercepted communications.

Where Public Safety Portfolio agencies (described below) must obtain information about an individual from a TSP, they do so in full respect of Canadian laws, which are some of the strongest in the world at protecting privacy. These laws require prior judicial authorization to obtain most of the types of information noted in this question, given the relatively high expectation of privacy associated with the information involved. The only exception is basic subscriber information (such as a customer's name and address), which carries a lower expectation of privacy, and as such may be requested on the basis of an organization's authority (i.e. without a warrant) according to Canadian law.

Additional safeguards include notification to those whose private communications were intercepted in the course of law enforcement investigations, and full disclosure of all information gathered by law enforcement for those cases that proceed to trial. Moreover, both the Canadian Security Intelligence Service (CSIS) and the RCMP have independent oversight bodies that review their activities to ensure they act within the law.

In response to question (a), the total number of requests by Public Safety Portfolio agencies to TSPs to provide information about customers' usage of communications devices and services, from approximately April 1, 2012, to March 31, 2013, was a minimum of 18,926. These are broken down by agency below.

#### **Canada Border Services Agency (CBSA)**

The CBSA requests information from TSPs about their customers when it believes that the information is required in support of an investigation into contraventions of legislation the Agency is responsible to enforce.

(b) (v) 18,849 total requests by the CBSA.

---

<sup>1</sup> Chiheb Esseghaier and Raed Jaser were arrested in April 2013 for plotting against passenger rail lines near Toronto. Amanda Korody and John Nuttall were arrested in July 2013 for plotting to detonate explosive devices at a Victoria Canada Day celebration. Dr. Khurram Sher is accused of planning attacks in Ottawa and elsewhere, and his trial began in February 2014.



- 3 -

- (c) (i) 63 geolocation requests  
(ii) 118 call detail records requests  
(iii) 77 text message content requests  
(iv) 10 voicemail requests  
(v) 128 cell tower log requests  
(vi) 0 real-time intercepts  
(vii) 18,729 requests for basic subscriber information (BSI)  
(viii) 113 requests for transmission data  
(ix) 78 requests for web sites visited, IP addresses  
(x) 15 requests for other data pertaining to the operation of TSPs' networks and businesses
- (d) Data fields disclosed per type of request:  
N.B. - all requests for the information found below, including content or non-content data, would require prior judicial approval, with the exception of basic subscriber information requests.
- Geolocation: The cell phone tower location
  - Call Detail Records or Transmission Data: Subscriber information for the owner of the phone number, and any associated subscribers within these records that belong to the issuing TSP; date/time of call; calling number; called number; redirecting number; duration. Wireless call detail records or transmission data may also include switch, first cell tower, and last cell tower.
  - Text message content: The telephone number or other identifier associated with the sender and the recipient of a text message, the time and date of its transmission, as well as the content of the message itself.
  - Voicemail: The telephone number or other identifier associated with the sender and the recipient of a message, the time and date of its transmission, as well as the content of the voicemail itself.
  - Cell tower logs: The physical location of the cell tower
  - Subscriber information: The identity and address details provided to the TSP when the cellular account was created, e.g. service status (e.g. active, suspended, cancelled); activation date; end date; subscriber name and address; service type (e.g. prepaid or postpaid); account number.
  - Web sites visited: The Internet Protocol addresses of the requesting site and the requested site, date and time, and port numbers, as/if applicable
  - Other Data: Information regarding the subscriber's contract; date of birth
- (e) (i) 0 real-time disclosures  
(ii) 18,849 requests for stored data  
(iii) 0 requests in exigent circumstances  
(iv) 18,849 in non-exigent circumstances  
(v) 52 requests subject to a court order
- (f) (i) 18,824 requests fulfilled by TSPs  
(ii) 25 requests denied, due to:
- Phone number no longer active or ported to different TSP;
  - TSP only forwarded phone number; and
  - Other reasons.

- 4 -

- (g) No, subscribers are not normally notified as this is not required by law, except for wiretapping. However, an individual may become aware of this disclosure if enforcement action is taken against that person and data provided by the TSP is used as evidence in support of charges. In those instances, the information would be disclosed to the accused in a court of law.
- (i) 13 subscribers notified
  - (ii) CBSA
- (h) (i) The CBSA retains customs information for seven years. All other information is kept in accordance with the *Privacy Act* which states that personal information is kept for a maximum of two years after the information was used for an administrative purpose. Where criminal charges have been laid, all files are kept for a period of seven years before being destroyed.
- (ii) Requests for judicially-authorized access to stored information such as call detail records would normally be for between 30-120 days, depending on the case.
  - (iii) On average, TSPs are given 30 business days to reply to a request if a judicial order is involved. BSI requests have no timeframe, but are usually completed within 2-3 business days.
  - (iv) An average is not possible as only one fiscal year of information is provided.
- (i) All requests for information other than BSI requests are done via a judicially-authorized production order (section 487.012 of the *Criminal Code*). Production orders require Border Service Officers to demonstrate to the court that there are reasonable grounds to believe that an offence has been or will be committed, and that the data sought will provide evidence of the offence. BSI requests are made under section 43 of the *Customs Act*. These requests seek only identifying information about an individual, and their disclosure is usually permitted by the terms and conditions of the contract agreed to between the subscriber and the TSP upon registration.
- (j) Note that this item is not regularly tracked by the majority of CBSA regions, and as such the figures below are illustrative only. Many requests are related to drug trafficking.
- (i) 0 terrorism requests
  - (ii) 2 national security requests
  - (iii) 0 foreign intelligence requests
  - (iv) 0 child exploitation requests
- (k)(l) This question is not applicable to the CBSA.
- (m) Yes, TSPs may refuse to comply with some requests.
- (i) TSPs may refuse to comply with requests for subscriber information in the case of non-published telephone numbers.
  - (ii) CBSA may seek a warrant if possible.
- (n) Yes, compensation was provided to TSPs in some cases.
- (i) A minimum of \$24,211.00 over the one year period to pay for BSI requests, with most requests costing between \$1.00 and \$3.00. These fees partially offset the administrative cost to TSPs of responding to requests. Compensation is not provided for judicially-authorized requests for information, such as production orders.

- (ii) There are different levels of compensation for BSI requests depending on whether circumstances are exigent or non-exigent; exigent requests generally cost around \$1.00-\$10.00 per request. However, CBSA did not submit any exigent BSI requests.

### **Canadian Security Intelligence Service (CSIS)**

CSIS is mandated to investigate and advise the Government about suspected threats to the security of Canada. In the course of those duties, CSIS may request TSPs to provide subscriber information and access to the content of communications in support of specific investigations. For each investigation, Federal Court warrants are required to intercept or otherwise collect the content of communications.

All of CSIS' activities are conducted in accordance with the law and are subject to full and independent review by the Security Intelligence Review Committee, and like other government departments and agencies, CSIS is also subject to the scrutiny of the Privacy Commissioner and other officers of Parliament, such as the Auditor General.

For reasons of national security and to protect CSIS' ability to collect intelligence and provide advice to Government, CSIS does not disclose details of its operations and tradecraft. In fact, unlike its law enforcement partners, the Service cannot disclose information obtained in the performance of its duties and function, except under the conditions outlined in section 19 of the *CSIS Act*.

Due to rapid changes in technology, the technical capability to carry out a 'wiretap' is complex. Being unable to fulfill a warrant to collect voice and/or data communications for technical reasons negatively affects the quality, availability and timeliness of information available to CSIS investigators. To help mitigate this growing challenge, when resources permit, CSIS will contribute to developing technical solutions.

### **Correctional Service Canada (CSC)**

CSC does not contact, by way of mandate, telecommunications service providers for information about customers' usage of communications devices and services.

### **Parole Board of Canada (PBC)**

The PBC does not contact, by way of mandate, telecommunications service providers for information about customers' usage of communications devices and services.

### **Royal Canadian Mounted Police (RCMP)**

The RCMP only obtains the enumerated usage information through judicial authorization, with the exception of real-time interception of communications under exigent circumstances (as defined in section 184.4 of the *Criminal Code*, immediate interception/imminent harm) and basic subscriber information. Any other interception of communications is obtained with judicial authorization. The RCMP does not maintain a centralized data repository that would allow it to determine the total number of requests to telecommunications service providers for customers' usage of communications devices and services. However, the RCMP does collect some types of data regarding customers' usage of communications and devices and reports this data when requested to do so, through Access to Information requests, the Office

- 6 -

of the Privacy Commissioner, the federal Minister of Public Safety, and provincial authorities such as attorneys-general. The RCMP also reports on the use of electronic surveillance through the Minister of Public Safety as per section 195 of the *Criminal Code*.

- (b) (i) The RCMP does not maintain a central data repository regarding all requests it makes for customers' usage of communications devices and services.
- (c) (i)-(v)(viii)-(x)  
The RCMP does not maintain a central data repository to provide the requested information.
  - (vi) Real-Time Interception of Communications (i.e. wiretapping): In 2012, the RCMP was granted 52 judicial authorizations to intercept private communications pursuant to section 185 of the *Criminal Code* and 25 judicial authorizations for video surveillance pursuant to section 487.01. The RCMP has not yet collected statistics for 2013.
  - (vii) Subscriber Information: Basic subscriber information may be obtained voluntarily from service providers without judicial authorization. However, the RCMP does not maintain a central data repository that contains the requested information.
- (d) Data fields disclosed per type of request:  
Subscriber information: The service provider may make available customer name and address for a specific date and time for which an offence is suspected to have been committed.  
  
All other data fields: The data fields which could be disclosed by telecommunications or internet service providers varies from request to request based on several factors, such as the specific information requested via judicial authorization, or the information held by the provider.
- (e) (i) The RCMP does not maintain a central data repository to provide the number of requests it has made to TSPs for real-time disclosures. However, it does maintain data regarding the number of requests it makes for real-time interception of communications (wiretapping), including those made under exigent circumstances: in 2012 the RCMP was judicially authorized 52 times to make real-time interceptions of communications. The RCMP has not yet collected statistics for 2013.
  - (ii)-(iv) The RCMP does not maintain a central data repository to provide the requested information.
  - (v) The RCMP does not maintain a central data repository to provide the number of requests it has made to TSPs that were subject to court orders. Every request for information, except for basic subscriber information or for those in exigent circumstances as defined by section 184.4 of the *Criminal Code*, requires judicial authorization, which is obtained through a court order. There were 52 judicial authorizations for real-time interception of communications in 2012. No data is yet available for 2013.
- (f) (i) The RCMP does not maintain a central data repository that provides the level of detail requested in this question.
- (g) The RCMP does notify persons affected when prescribed by law or through the conditions of judicial authorization. The RCMP does not notify persons impacted by basic subscriber information; however, persons may be notified through the Crown's obligation to disclose when the investigation results in prosecution. The RCMP does not maintain a central data repository to provide the requested information.

- 7 -

- (h) (i) The length of time the RCMP retains information obtained from telecommunications service providers corresponds to the nature of the offence being investigated and varies based on the current policies and statutes regarding the retention and archiving of investigational files.
  - (ii) The period of time the requested information covers varies based on a number of factors, such as the type of request, nature of the offence and the particulars of each specific investigation. The RCMP does not maintain a statistical repository for these types of activities and as such it cannot provide the average time period as requested, with the exception of real-time interception of communications (i.e. wiretapping). The average period of time valid for audio interception (s. 185 of the *Criminal Code*) was 80.2 days and 102.2 days for video warrants (s. 487.01 of the *Criminal Code*).
  - (iii) In cases where a judicial authorization is obtained, the service provider is given a reasonable amount of time to collect and submit the requested information. This period of time varies based on a number of factors, such as the complexity of the request.
  - (iv) The RCMP does not maintain statistics related to the average number of subscribers who have their information disclosed.
- (i) The legal standards used by the RCMP to request, through judicial authorization, information from telecommunications service providers about customers' usage of communications devices and services are those set out in Parts VI and XV of the *Criminal Code*.
- (j) (i)(ii)(iv) The RCMP does not maintain a central data repository to provide the requested information.
  - (iii) Foreign Intelligence: This ground does not apply to the RCMP.
- (k) There is no set maximum number of subscribers that service providers are required to monitor.
- (l) Since there are no established maximums, the RCMP has not had to request an increase in the maximum number of subscribers monitored.
- (m) Service providers may challenge judicial authorization and refuse to comply with it. This has occurred.
    - (i) Requests may be refused for a number of reasons. The RCMP does not maintain a central data repository of situations where the judicial authorization was challenged by the service provider and reasons for the challenge were given.
    - (ii) When the RCMP is advised by a service provider that the service provider is not willing to comply with the authorization, the RCMP works with the service provider to determine the cause and to attempt to achieve a resolution. If no resolution is reached, the matter may ultimately be brought before the courts for a ruling.
- (n) There currently is no standard payment schedule and compensation may vary from provider to provider based on a number of factors such as the complexity of the request and the service providers' network infrastructure. The RCMP may be required to compensate service providers for the development, deployment and utilization of technical solutions in relation to judicial authorizations. However, there is no RCMP central repository which captures all payments related to service providers in relation to judicial authorizations. For basic subscriber information, the RCMP may also provide compensation to service providers in relation to basic subscriber information, which ranges from \$1.00 - \$3.00 compensation per request.

# Verizon Transparency Report

## U.S. Data

In 2013, Verizon received approximately 320,000 requests for customer information from federal, state or local law enforcement in the United States. We do not release customer information unless authorized by law, such as a valid law enforcement demand or an appropriate request in an emergency involving the danger of death or serious physical injury.

The table below sets out the number of subpoenas, orders, and warrants we received from law enforcement in the United States last year. We also received emergency requests and National Security Letters. The vast majority of these various types of demands relate to our consumer customers; we receive relatively few demands regarding our enterprise customers.

Overall, we saw an increase in the number of demands we received in 2013, as compared to 2012.

### Law Enforcement Demands for Customer Data — United States (2013)

<b>Subpoenas</b>	164,184
<b>Orders</b>	70,665
	62,857 General Orders
	6,312 Pen Registers/ Trap & Trace Orders
	1,496 Wiretap Orders
<b>Warrants</b>	36,696
<b>Emergency Requests From Law Enforcement</b>	50,000 (approximately)
<b>Total</b>	<b>321,545</b>
<b>National Security Letters</b>	<b>1000-1999</b>

### Which Verizon services does this Transparency Report cover?

The figures in this Report include demands for customer data regarding our Verizon wireline services, such as phone, Internet or television, and our Verizon Wireless services.

### Does this Transparency Report include information on the number of national security orders you receive?

1/22/2014

Verizon Transparency Report

Like all other companies to issue transparency reports, we are not permitted at this time to report information on national security orders (like FISA orders). We do report, within a range, the number of National Security Letters that we received from the FBI in 2013; we report only a range because, like the other companies that have published transparency reports, we have not been granted permission to indicate the exact number of National Security Letters we received. Last week, President Obama announced that telecommunications providers will be permitted to make public more information in the future; we encourage greater transparency and, if permitted, will make those additional disclosures.

**Does Verizon reject law enforcement demands?**

Yes. If a demand is facially invalid, or if a demand seeks certain information that can only be obtained with a different form of process (for example, a subpoena, rather than a warrant, improperly is used to seek stored customer content), we reject the demand. If a demand is overly broad or vague we will not produce any information, or will seek to narrow the scope of the demand and produce a subset of the information sought. In many cases we do not produce any information at all, including because the demand seeks information we do not have.

**Is Verizon reporting on the percentage of demands for which it did not produce any data?**

We did not track the percentage of demands to which we produced some or no data in 2013, but will be doing so going forward. As just noted, we carefully review each demand and reject in whole or part those that are deficient.

**Does Verizon charge law enforcement for providing data?**

In some instances, Federal and most state laws authorize providers to charge a reimbursement fee for responding to law enforcement demands for records or to recoup reasonable expenses in complying with a wiretap order or pen register or trap and trace order. In the majority of instances, however, we do not seek reimbursement for responding to law enforcement requests. We do not charge for responding to emergency requests and do not charge for responding to most subpoenas. When we do charge a reimbursement fee, our fees are permitted by law or court order and seek to recoup only some of our costs.

**Does Verizon also receive requests for data in civil cases?**

Yes, we do. Requests in civil cases comprise a small percentage of the total requests we receive. This report focuses on requests from law enforcement.

**Will Verizon issue future transparency reports?**

Yes, on a semi-annual basis.

**What obligations to report on demands already apply to the United States government?**

Federal law already places substantial reporting requirements on federal and state governments.

Each year the United States Attorney General and the principal prosecuting attorney for each state have to report the number of applications for wiretap orders, the number of orders granted, the types of communications intercepted, the number of persons whose communications were intercepted and the numbers of arrests and convictions resulting from such interceptions. That information is summarized for Congress. See 18 U.S.C. § 2519(2),(3). Similarly, the Attorney General must make detailed annual reports to Congress on the number of pen registers and trap and trace orders. See 18 U.S.C. § 3126.

The Attorney General also has to report to Congress each year regarding information obtained in emergencies, in some contexts. See 18 U.S.C. § 2702(d). And the Director of the FBI has to report twice each year to Congress regarding the number of National Security Letters issued. See 18 U.S.C. § 2709(e).

## Subpoenas

We received approximately 164,000 subpoenas from law enforcement in the United States last year. We are required by law to provide the information requested in a valid subpoena. The subpoenas we receive are generally used by law enforcement to obtain subscriber information or the type of information that appears on a customer's phone bill. More than half of the subpoenas we receive seek only subscriber information: that is, those subpoenas typically require us to provide the name and address of a customer assigned a given phone number or IP address. Other subpoenas also ask for certain transactional information, such as phone numbers that a customer called. The types of information we can provide in response to a subpoena are limited by law. We do not release contents of communications (such as text messages or emails) or cell site location information in response to subpoenas.

### **Does a law enforcement officer need to go before a judge to issue a subpoena?**

Under federal law and the law in many states the government does not need judicial approval to issue a subpoena. A prosecutor or law enforcement official may issue a subpoena to seek evidence relevant to the investigation of a possible crime.

### **Are there limits on the types of data law enforcement can obtain through a subpoena?**

Yes, in response to a subpoena, we only release the six types of information specifically identified in section 2703(c)(2)(A)-(F) of Title 18 of the United States Code: customer name, address, telephone or other subscriber number, length of service, calling records and payment records. Some states have stricter rules. We do not release any content of a communication in response to a subpoena.

### **Are there different types of subpoenas?**



Yes, we may receive three different types of subpoenas from law enforcement: a grand jury subpoena (the subpoena is issued in the name of a grand jury investigating a potential crime); an administrative subpoena (generally, a federal or state law authorizes a law enforcement agency to issue a subpoena); or a trial subpoena (the subpoena is issued in the name of the court in anticipation of a trial or hearing).

## Orders

We received about 70,000 court orders last year. These court orders must be signed by a judge, indicating that the law enforcement officer has made the requisite showing required under the law to the judge. The orders compel us to provide some type of information to the government.

*General Orders.* Most of the orders we received last year – almost 63,000 – were “general orders.” We use the term “general order” to refer to an order other than a wiretap order, warrant, or pen register or trap and trace order. Almost half of the general orders required us to release the same types of basic information that could also be released pursuant to a subpoena. We do not provide law enforcement any stored content (such as text messages or email) in response to a general order.

*“Pen/Trap” Orders and Wiretap Orders.* A small subset of the orders we received last year – about 7,800 – required us to provide access to data in real-time. A pen register order requires us to provide law enforcement with real-time access to phone numbers as they are dialed, while a trap and trace order compels us to provide law enforcement with real-time access to the phone numbers from incoming calls. We do not provide any content in response to pen register or trap and trace orders. We received about 6,300 court orders to assist with pen registers or trap and traces last year, although generally a single order is for both a pen register and trap and trace. Far less frequently, we are required to assist with wiretaps, where law enforcement accesses the content of a communication as it is taking place. We received about 1,500 wiretap orders last year.

### **What is a pen register or trap and trace order?**

Pen register or trap and trace orders require a wire or electronic communications provider (like Verizon) to afford access to “dialing, routing, addressing or signaling information.” With a pen register order we must afford real-time access to the numbers that a customer dials (or IP addresses that a customer visits); with a trap and trace order we must afford real-time access to the numbers that call a customer. Such orders do not authorize law enforcement to obtain the contents of any communication.

### **What is a wiretap order?**

A wiretap order is an order that requires a wire or electronic communications provider to provide access to the content of communications in real-time to law enforcement. The order can relate to the content of telephone or Internet communications.

### **What are the different showings that law enforcement has to make for the different orders?**

A wiretap order is the most difficult for law enforcement to obtain. Under the law, law enforcement may not obtain a wiretap order unless a judge finds that there is probable cause to believe that an individual is committing one of certain specified offenses and that particular communications concerning that offense will be obtained through the wiretap. A wiretap order is only issued for a specified time.

A general order requires law enforcement to offer specific and articulable facts showing that there are reasonable grounds to believe that the records sought are relevant and material to an ongoing criminal investigation. In federal court, such orders are authorized under 18 U.S.C. § 2703(d).

A pen register order or trap and trace order requires law enforcement to make a lesser showing -- that the information likely to be obtained is relevant to an ongoing criminal investigation.

## Warrants

We received about 36,000 warrants last year. To obtain a warrant a law enforcement officer must show a judge that there is "probable cause" to believe that the evidence sought is related to a crime. This is a higher standard than the standard for a general order. While many warrants seek the same types of information that can also be obtained through a general order or subpoena, most warrants we received in 2013 sought stored content or location information.

### What showing must law enforcement make to obtain a warrant?

To obtain a warrant a law enforcement officer has to show a judge that there is probable cause to believe that the evidence it seeks is related to a crime and in the specific place to be searched.

### What is the difference between stored content and non-content?

"Stored content" refers to communications or other data that our users create and store through our services, such as text messages, email or photographs. We require a warrant before disclosing stored content to law enforcement, absent an emergency involving the danger of death or serious physical injury. Non-content refers to records we create such as subscriber information that a customer provides at the time she signs-up for our services, and transactional information regarding the customer's use of our services, such as phone numbers that a customer called.

## Content and Location Information

*Content.* We are compelled to provide contents of communications to law enforcement relatively infrequently. Under the law, law enforcement may seek communications or other content that a customer may store through our services, such as text messages or email. Verizon only releases such stored content to law enforcement with a warrant; we do not produce stored content in response to a general order or subpoena. Last year, we received approximately 14,500 warrants for stored content.

As explained above, law enforcement may also present a wiretap order to obtain access to the content of a communication as it is taking place, which they did about 1,500 times last year. Taken together, the number of orders for stored content and to wiretap content in real-time accounted for only about five percent of the total number of demands we received in 2013.

*Location Information.* Verizon only produces location information in response to a warrant or order; we do not produce location information in response to a subpoena. Last year, we received about 35,000 demands for location data: about 24,000 of those were through orders and about 11,000 through warrants. In addition, we received about 3,200 warrants or court orders for "cell tower dumps" last year. In such instances, the warrant or court order compelled us to identify the phone numbers of all phones that connected to a specific cell tower during a given period of time. The number of warrants and orders for location information are increasing each year.

## Emergency Requests

Law enforcement requests information from Verizon that is needed to help resolve serious emergencies. We are authorized by federal law to provide the requested information in such emergencies and we have an established process to respond to emergency requests, in accordance with the law. To request data during these emergencies, a law enforcement officer must certify in writing that there was an emergency involving the danger of death or serious physical injury to a person that required disclosure without delay. These emergency requests are made in response to active violent crimes, bomb threats, hostage situations, kidnappings and fugitive scenarios, often presenting life-threatening situations. In addition, many emergency requests are in search and rescue settings or when law enforcement is trying to locate a missing child or elderly person.

We also receive emergency requests for information from Public Safety Answering Points regarding particular 9-1-1 calls from the public. Calls for emergency services, such as police, fire or ambulance, are answered in call centers throughout the country, known as PSAPs. PSAPs receive tens of millions of calls from 9-1-1 callers each year, and certain information about the calls (name and address for wireline callers; phone numbers and available location information for wireless callers) is typically made available to the PSAP when a 9-1-1 call is made. Yet a small percentage of the time PSAP officials need to contact the telecom provider to get information that was not automatically communicated by virtue of the 9-1-1 call or by the 9-1-1 caller.

In 2013, we received 85,116 emergency requests for information from law enforcement in emergency matters involving the danger of death or serious physical injury or from PSAPs relating to particular 9-1-1 calls from the public for emergency services. While in 2013 we did not track whether an emergency request was made by law enforcement or PSAPs, we are doing so now. We estimate that at least half of these requests – approximately 50,000 – were from law enforcement pursuant to the emergency procedures discussed above and the remainder were from PSAPs after receiving 9-1-1 calls from the public.

## National Security Letters

We also received between 1,000 and 2,000 National Security Letters in 2013. We are not permitted to disclose the exact number of National Security Letters that were issued to us, but the government will allow us to provide a broad range.

### What is an NSL?

1/22/2014

Verizon Transparency Report

A National Security Letter, or NSL, is a request for information in national security matters; it cannot be used in ordinary criminal, civil or administrative matters. When the Director of the Federal Bureau of Investigation issues a National Security Letter to a wire or electronic communications provider (like Verizon) such a provider must comply. The law that authorizes the FBI to issue NSLs also requires the Director of the FBI to report to Congress regarding NSL requests.

**Under what circumstances can the FBI issue an NSL?**

The FBI does not need to go to court to issue an NSL. Rather, the Director of the FBI or a senior designee must certify in writing that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States.

**What types of data can the FBI obtain through an NSL?**

The FBI may seek only limited categories of information through an NSL: name, address, length of service and toll billing records. The FBI cannot obtain other information from Verizon, such as content or location information, through an NSL.

**Does this Transparency Report include information on the number of national security orders you receive?**

We report only information about National Security Letters. Like all other companies to issue transparency reports, we are not permitted at this time to report information on national security orders (like FISA orders).

© 2014 Verizon

# Verizon Transparency Report

## National Security

The table below sets forth the number of national security demands we received in 2013. We note that while we now are able to provide more information about national security orders that directly relate to our customers, reporting on other matters, such as any orders we may have received related to the bulk collection of non-content information, remains prohibited.

### National Security Demands

	Jan. 1, 2013 – June 30, 2013	July 1, 2013 – Dec. 31, 2013
<b>National Security Letters</b>	0-999	0-999
Number of customer selectors	2000-2999	2000-2999
<b>FISA Orders (Content)</b>	0-999	*
Number of customer selectors	4000-4999	*
<b>FISA Orders (Non-Content)</b>	0-999	*
Number of customer selectors	0-999	*

\* The government has imposed a six month delay for reporting this data

### National Security Letters

We explained in our Transparency Report that we had received between 1000 and 1999 National Security Letters in 2013. We separately provide details for the first half and second half of 2013 now; in the future, we will make semi-annual reports regarding only the immediately preceding six month period. In the first half of 2013, we received between 0 and 999 NSLs from the FBI. Similarly, we received between 0 and 999 NSLs in the second part of 2013. In the first six months of the year, those NSLs sought information regarding between 2000 and 2999 "selectors" used to identify a Verizon customer. The same is true for the second half of 2013. (The government uses the term "customer selector" to refer to an identifier, most often a phone number, which specifies a customer. The number of selectors is generally greater than the number of "customer accounts." An NSL might ask for the names associated with two different telephone numbers; even if both phone numbers were assigned to the same customer account, we would count them as two selectors.)

As we explained in our Transparency Report, the FBI may seek only limited categories of information through an NSL: name, address, length of service and toll billing records. Verizon does not release any other information in response to an NSL, such as content or location information.

3/3/2014

Verizon Transparency Report

## FISA orders

The government requires that we delay the report of any orders issued under the Foreign Intelligence Surveillance Act for six months. Thus, at this time, we may report FISA information only for the first half of 2013. In July, or soon thereafter, we will report FISA information regarding the second half of 2013.

### Content

From January 1, 2013 through June 30, 2013, we received between 0 and 999 FISA orders for content. Those orders targeted between 4000 and 4999 "customer selectors" used to identify a Verizon customer.

### Non-Content

From January 1, 2013 through June 30, 2013, we received between 0 and 999 reportable FISA orders for non-content. Some FISA orders that seek content also seek non-content; we counted those as FISA orders for content and to avoid double counting have not also counted them as FISA orders for non-content. Those orders targeted between 0 and 999 "customer selectors."

We will update our Transparency Report again in the middle of the year.



Download a PDF of this page

(/themes/site\_themes/transparency/Verizon-Transparency-Report-National-Security.pdf)

© 2014 Verizon

# Verizon Transparency Report

## International Data

This table shows the total number of demands for customer information made by law enforcement to Verizon in 2013 in every country in which we do business, and had any such demands, other than the United States. While we offer services to business, government and consumer customers in the United States, our focus outside the United States is on business and enterprise customers. Only countries from which we received demands in 2013 are included in this chart. As explained below, there are some limits to what we can disclose regarding law enforcement demands.

These figures reflect requests made by law enforcement within a country for data stored within that same country. It is very rare that we receive a request from a government for data stored in another country. When this occurs, it generally is a request for United States consumer data from a government entity outside the United States; when we receive these infrequent requests, we do not comply and instead direct the requesting government agency to make its request through any applicable diplomatic channels (like the Mutual Legal Assistance Treaty process) in its country. In 2013, we did not receive any demands from the United States government for data stored in other countries. We received a small number of requests last year from non-U.S. governments for data stored in the United States, all of which were referred to the MLAT process.

On occasion, we are required by government orders, regulations or other legal requirements to block access to specified websites outside the United States. While we have not received such blocking demands in the United States, we did receive such demands in five countries in 2013. In Colombia, we were required to block access to approximately 1,200 websites that the Colombian government believed contained child pornography. In Greece, we were required to block 424 sites related to online gambling. We were also required to block websites in Belgium (37) and Portugal (2) related to online gambling or copyright issues. Finally, we were required to block access to websites in India but are precluded by law from identifying the specific number of websites. (These figures relate to the number of websites we were required to block access to in 2013. We may be required to block access to such websites for an ongoing period of time, but we count such demands only for the year in which they were initially made.)

### Law Enforcement Demands for Data (Outside of the United States - 2013)

Australia	29
Austria	8
Belgium	473
France	1,347
Germany	2,996
Italy	13
Japan	14
Netherlands	65

1/22/2014

Verizon Transparency Report

Sw itzerland	60
Taiw an	1
UK	386

**Is this International Report impacted by countries that do not allow Verizon to report certain data?**

Yes, the laws in some countries, such as Australia and India, limit what we can disclose. In Australia we are precluded by law from reporting the number of warrants we received from law enforcement for interceptions or stored communications. And, in India we are precluded by law from discussing any information about the requests we might receive from the Government of India or identifying the specific number of websites that we were asked to block by the Government of India.

© 2014 Verizon