



## 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-630	BY / DE Ms. Borg (Terrebonne—Blainville)	DATE June 18, 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 (TSPs) to provide information about customers' usage of communications devices and services: (a) between 2001 and 2013, how many such requests were made; (b) of the total referred to in (a), how many requests were made by the (i) RCMP, (ii) Canadian Security Intelligence Service, (iii) Competition Bureau, (iv) Canada Revenue Agency, (v) Canada Border Services Agency, (vi) Communications Security Establishment Canada; (c) – **See full text of the question attached.**

### REPLY / RÉPONSE

ORIGINAL TEXT  
TEXTE ORIGINAL



TRANSLATION  
TRADUCTION



### Public Safety Canada (PS)

PS and its Portfolio agencies are committed to ensuring the safety and security of all Canadians. PS will continue to work towards an appropriate balance between safeguarding Canadians' privacy rights and providing PS Portfolio agencies with the investigative tools they need to prevent and prosecute serious crimes. In this vein, PS releases figures about the number and type of interceptions conducted by Canada's law enforcement community in its *Annual Report on the Use of Electronic Surveillance* (pursuant to s.195(1) of the *Criminal Code*). This report provides Canadians with a clear understanding of how and why customer communications may be intercepted.

Gaining access to certain information about individuals via telecommunications service providers (TSPs) is integral to investigations in the digital age. In those instances where PS Portfolio agencies (described below) must obtain information about an individual from a TSP, they do so in full compliance with Canadian laws. Current legislation requires prior judicial authorization to obtain most of the types of personal information addressed in this question, save for emergency situations.

Additional safeguards surrounding lawful access include notification to individuals whose private communications were intercepted in the course of law enforcement investigations (as per s. 196(1) of the *Criminal Code*), and disclosure of information gathered by law enforcement agencies in cases that proceed to trial. The Security Intelligence Review Committee is an independent, external review body that reports to the Parliament of Canada on Canadian Security Intelligence Service (CSIS) operations, including its use of

warranted intercepts. In addition, the Commission for Public Complaints Against the Royal Canadian Mounted Police (RCMP) is an independent agency that investigates complaints surrounding the conduct of RCMP members. These entities ensure that CSIS and the RCMP act within the bounds of the law.

### 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. Data provided is from 2012 to 2013. No aggregate statistical data is available from 2001 to 2013.

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

Note that in these cases either communications content ((iii), (iv) and (vi)) or communications data (i.e. the information about a communication but not its content, and referenced in (i), (ii), (v), (vii), (viii), (ix) and (x)) would be disclosed. In each case, prior authorization either from a judge or the Minister of Public Safety and Emergency Preparedness (depending on the circumstance), would be obtained when required.

*Minister could give approval.*

- (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 BSI requests.
  - Geolocation: The location of a cell phone within a cell tower beam area.
  - 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 a cell tower accessed by a customer device.
  - 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
- (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) This question is not applicable to the CBSA.
- (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.
- (o) The CBSA is not able to provide the requested data, as its databases do not permit systematic retrieval of these numbers. Individual requests for subscriber data are retained on each file to which they are pertinent, and cannot be retrieved without a manual review of each file.

Some telecommunications service providers retain records of written requests from law enforcement agencies for this data, however, the CBSA has no centralized mechanism for tracking this data.
- (p) The CBSA is not able to provide the requested data, as its databases do not permit systematic retrieval of these numbers. Individual requests for subscriber data are retained on each file to which they are pertinent, and cannot be retrieved without a manual review of each file.

Some telecommunications service providers retain records of written requests from law enforcement agencies for this data, however, the CBSA has no centralized mechanism for tracking this data.
- (q) No, the CBSA does not maintain internal aggregate statistics on these types of requests.
- (r) Individuals are notified when information from a TSP is used as evidence in support of charges, otherwise it is not a regular practice.

### **Canada Security Intelligence Service**

- (a)-(f) 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 or tradecraft.

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. 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.

- (g) The disclosure of information specific to an investigation would jeopardize CSIS' operations and harm national security; for these reasons, CSIS does not disclose such information.
- (h) 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 or tradecraft.
- (i) Pursuant to section 12 of the *CSIS Act*, CSIS is authorized to collect information respecting activities that may on reasonable grounds be suspected of constituting a threat to the security of Canada. Threats to the security of Canada are defined in section 2 of the *CSIS Act*, and include: terrorism; espionage and sabotage; foreign interference; and subversion.

Pursuant to section 16 of the *CSIS Act*, CSIS may investigate activities at the request of the Ministers of Foreign Affairs and National Defence in relation to the capabilities, intentions, or activities of a foreign state or group of foreign states.

Pursuant to section 21 of the *CSIS Act*, CSIS may make a warrant application to a Federal Court to intercept any communication or obtain any information, record, document or thing, for the purpose of a lawful investigation in relation to threats against the security of Canada.

For public information in relation to the CSIS warrant application regime, including the number of Federal Court warrants approved in a given fiscal year, please refer to the Security Intelligence Review Committee's annual reports found at [www.sirc-csars.gc.ca](http://www.sirc-csars.gc.ca).

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 or tradecraft.

(j)-(n) N/A

- (o)-(q) 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 or tradecraft.
- (r) The disclosure of information specific to an investigation would jeopardize CSIS' operations and harm national security; for these reasons, CSIS does not disclose such information.

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

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


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

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

**Royal Canadian Mounted Police**

With regard to requests by government agencies to TSPs to provide information about customers' usage of communications devices and services:

- (a) 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 BSI and reports this data, when requested to do so, through Access to Information requests, as well as inquiries from the Office of Privacy Commissioner and other federal and provincial authorities such as Attorneys General.
- (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), (vii)-(x) The RCMP does not maintain a central data repository to provide the requested information.  
(vi) The RCMP reports on the use of electronic surveillance through the Minister of Public Safety and Emergency Preparedness pursuant to section 195 of the *Criminal Code*. Judicial authorizations may be obtained to intercept private communications pursuant to section 185 of the *Criminal Code* and for video surveillance pursuant to section 487.01 of the *Criminal Code*. In addition, the RCMP may intercept private communications in emergency circumstances pursuant to section 188 of the *Criminal Code*. Statistical information from 2001 and 2002 is no longer available for real-time interception of communications (i.e., wiretapping). The following table provides a statistical breakdown of the three categories per year (a judicial authorization may include more than one individual):



Year	Judicial authorizations to intercept private communications	Emergency interception of private communications	Judicial authorizations for video surveillance
2003	76		5
2004	89		27
2005	63	1	17
2006	45		14
2007	51		31
2008	51	2	7
2009	60		28
2010	48		28
2011	64		36
2012	61		31
2013	56	4	30
<b>Total</b>	<b>664</b>	<b>4</b>	<b>254</b>

- (d) 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 and/or the information held by the provider.
- (e) (i) The RCMP does not maintain a central repository for the requests 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. Between 2003 and 2013 the RCMP was judicially authorized 668 times to intercept private communications.
- (ii) The RCMP does not maintain a central repository for the requests made to TSPs for stored data, retroactively.
- (iii) The RCMP does not maintain a central repository for the requests made to TSPs for requests made in exigent circumstances with the exception of judicial authorizations to intercept private communications in emergency circumstances pursuant to section 188 of the *Criminal Code*. Between 2003 and 2013, the RCMP was judicially authorized four times to intercept private communications under emergency circumstances.
- (iv) The RCMP does not maintain a central repository for the requests made to TSPs in non-exigent circumstances. However, it does maintain data regarding the number of requests it makes for real-time interception of communications (wiretapping). Between 2003 and 2013 the RCMP was judicially authorized 664 times to intercept private communications.
- (v) The RCMP does not maintain a central repository for the requests made to TSPs subject to court orders. However, it does maintain data regarding to the number of requests it makes for real-time interception of communications (wiretapping), including those made under emergency circumstances. Between 2003 and 2013 the RCMP was judicially authorized 668 times to intercept private communications.
- (f) The RCMP does not maintain a central repository of the number of requests TSPs fulfill or deny.
- (g) The RCMP does notify persons affected when prescribed by law or through the conditions of judicial authorizations. The RCMP does not notify persons impacted by BSI requests; however, persons affected 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.
- (h) (i) The length of time the RCMP retains information obtained from TSPs 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 periods of time valid for audio interception (s. 185 of the *Criminal Code*) and for video warrants (s. 487.01 of the *Criminal Code*) are enumerated in the table below:

Year	Audio Interceptions	Video Interceptions
2003	61.3 days	66.0 days
2004	66.8 days	73.4 days
2005	65.2 days	66.5 days
2006	65.2 days	61.4 days
2007	65.6 days	72.7 days
2008	61.0 days	71.4 days
2009	56.2 days	53.9 days
2010	81.0 days	88.0 days
2011	67.0 days	87.6 days
2012	77.9 days	95.5 days
2013	59.6 days	68.1 days

(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 TSPs about customers' usage of communications devices and services are those set out in Parts VI and XV of the *Criminal Code*.
- (j) (i), (ii) and (iv) The RCMP does not maintain a central data repository to provide the requested information.
  - (iii) Foreign Intelligence: this does not apply to the RCMP.
- (k) There is no 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 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 they are not willing to comply with the authorization, the RCMP works with the provider to determine the cause and attempt to achieve resolution. If no resolution is reached, the matter may ultimately be brought before the courts for 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 their network infrastructure. There is no central repository which captures all payments related to service providers in relation to judicial authorizations. The RCMP may provide compensation to service providers in relation to BSI which ranges from \$1.00 - \$3.00 per request. The RCMP may, however, be required to compensate service providers for the development, deployment and utilization of technical solutions in relation to judicial authorizations.
- (o) The RCMP does not maintain a central data repository regarding how many users, accounts, IP addresses and individuals were subject to disclosures related to requests made to TSPs for customers' usage of communications devices and services.
- (p) The RCMP does not maintain a central data repository regarding how many requests to TSPs for customers' usage of communications devices and services were made without a warrant.
- (q) The RCMP does not maintain a central data repository of the types and kind of information requested from TSPs.
- (r) The RCMP does notify persons affected when prescribed by law or through the conditions of judicial authorizations. The RCMP does not notify persons impacted by BSI requests; however, persons affected may be notified through the Crown's obligation to disclose when the investigation results in prosecution.