Transparency Reporting Guidelines

Canadians expect that when they share personal information with businesses and private organisations that it will be safe, and will only be shared under specific conditions. This expectation is supported in Canadian privacy law, under which private businesses are required to be open and transparent about their policies and practices with respect to their management of personal information.

While organizations have flexibility in how they meet this obligation, depending on the nature of their business, a number of businesses have proactively elected to voluntarily publish "Transparency Reports" to account for how often, and in what circumstances, they provide information about their customers and clients to government authorities.

Canadian law enforcement, national security agencies, and regulatory authorities rely on the collection of information to enforce the law and protect public safety. Information may be collected in the context of a criminal investigation, a regulatory audit or inspection, to find a lost or injured child, or to protect an individual from an imminent threat to their well-being, among other lawful duties.

In this context, Transparency Reporting Guidelines (the Guidelines) have been prepared to help private organizations be open with their customers, regarding the management and sharing of their personal information with government, while respecting the work of law enforcement, national security agencies, and regulatory authorities.

Specifically, the Guidelines cover categories of disclosures for reporting purposes and limitations to consider when reporting statistics. Multinational companies may be subject to different standards and requirements for reporting in different jurisdictions, which may result in differences in reporting.

A. Categories of Disclosures

Subject to the limitations set out in Part B, organizations may choose to report the number of disclosures made to government authorities by the following categories. For each category, organizations may choose to report any of the following statistics: the number of requests received from government authorities, the number of requests fulfilled, the number of requests rejected or contested; and the number of persons or accounts whose information was disclosed.

1. **Voluntary disclosures at the request of a government organization**: refers to the voluntary disclosure of personal information at the request of law enforcement or other government organizations. These requests deal with circumstances where a warrant or court order is not required to obtain information, including but not limited to criminal investigations, information needed to locate and notify the next-of-kin of an injured, ill or deceased individual, return stolen property, or assist in the search for missing or lost persons.

2. **Voluntary disclosures on the initiative of the organization**: refers to the voluntary disclosure of personal information to government authorities, for the purpose of reporting a crime. In these circumstances, there is no request from government authorities.

3. **Disclosures in emergency or exigent circumstances**: refers to requests made to assist law enforcement agencies in situations involving serious or imminent harm to any person or property without application to a judge. Requests made in emergency or exigent circumstances

include but are not limited to requests for basic identifying information (referring to personal identifiers such as customer name, telephone number, mailing address and the local service provider identifier associated with a telecommunications or other service), intercepted communications, and tracking data (governed by relevant provisions of the *Criminal Code* including ss. 184.1, 184.4 and 487.11, and other relevant statutes and the common law). Requests counted under this category should not be counted again under other data categories.

4. **Disclosures made in compliance with federal or provincial law**: refers to compellable requests made by government agencies under the express authority of federal or provincial legislation, such as the *Customs Act* or *Income Tax Act*, for regulatory enforcement or other government service purpose. These requests are sometimes referred to as "government requirement letters".

5. **Court ordered (warranted) disclosures**: refers to production orders, summons, subpoenas, and search warrants issued by a judge or other judicial officer. There are a number of different types of these orders, including but not limited to:
   a) *Basic identifying information (court ordered*): refers to personal identifiers such as customer name, telephone number, mailing address and the local service provider identifier associated with a telecommunications or other service in circumstances where there is a reasonable expectation of privacy, and disclosed pursuant to a court order.
   b) *Tracking data (obtained via tracking warrant; governed by s.492.1 of the Criminal Code and other relevant statutes)*: refers to data that relates to the location of a transaction, individual or thing.
   c) *Transmission data (obtained via transmission data recorder warrant; governed by s.492.2 of the Criminal Code and other relevant statutes)*: refers to any data obtained by dialling, addressing, routing, or signalling, such as the incoming and outgoing numbers of a phone call, or the time an email was sent and received. Transmission data does not reveal the content of a conversation or message.
   d) *Stored communications content and other stored data (obtained via warrant and production orders; governed by ss, 487, 487.01, and 487.014 – 487.018 of the Criminal Code and other relevant statutes):* may refer to provision of historical data, including the content of stored communications such as text messages or other data such as photos, and provision of other types of stored data.
   e) *Real time interception (obtained via wiretap warrant; governed by Part VI of the Criminal Code and other relevant statutes)*: refers to private communications intercepted by means of any electro-magnetic, acoustic, mechanical or other device.

   To the extent that organizations wish to report separately by the type of court order or warrant received, they should feel free to do so, provided that they respect the limitations set out in Part B of the Guidelines, and are not otherwise prohibited from disclosure.

6. **Other**: In some cases, organizations may also wish to report on the following categories of requests, should they feel it is relevant and appropriate to do so, given their particular circumstances.
   a) *Foreign agency requests (court ordered):* Refers to requests received from government agencies outside of Canada regarding criminal matters. The Government of Canada may facilitate such requests pursuant to the *Mutual Legal Assistance in Criminal Matters Act*.
   b) *Preservation demands and orders (governed by s.487.012 and s.487.013 of the Criminal Code):* Refers to demands (by peace or public officers) or orders (by a justice or judge) requiring a person to preserve computer data for either 21 or 90 days, depending on the circumstances. Preservation demands and orders simply compel a person to not delete data in their possession or control. This allows government agencies time to submit an appropriate request to obtain the preserved information, such as obtaining a court authorized production order to obtain historical text messages. These requests should be counted separately and not contribute to the total number of requests, since no information is actually obtained by government agencies making preservation requests. Where these agencies submit general warrants, production orders, or other applications to obtain information subsequent to preservation requests, the request will be

counted under the relevant former category.

B. Limitations

When reporting statistics by each of the categories listed in Part A, organizations should respect the following limitations, in order to protect the work of law enforcement, national security, and regulatory agencies.

1. As presented in the sample chart below, figures between 0 and 100 should be represented in a band of '0-100' when any figure in column A (Number of Requests) or Column B (Number of Disclosures) is less than 100. In such cases the banding of figures should apply to all columns for that data type whose figure is between 0-100. Any figure over 100 may be represented by its actual number. This is to protect the operational activities and capabilities of Canadian government and law enforcement agencies.

2. Figures should be aggregated to reflect Canada-wide statistics, and should not differentiate between law enforcement, national security, and regulatory agencies (i.e. there should be no breakdown by geography or specific agency). Moreover, these figures should also be aggregated such that service type and its associated network technology are not distinguishable (i.e. cellular voice services should not be subdivided and reported according to 2G, 3G or 4G/LTE network type, etc.). This is to protect the operational activities and capabilities of Canadian government and law enforcement agencies.

3. There should be a six month delay in reporting timeframe. For example, if a report covers the period January 1 to December 31, 2014, it should not be released before July 1, 2015. This is to ensure that most active investigations have no possibility of being compromised.

The limitation provisions will ensure that transparency reporting does not impair or compromise national security or criminal investigations, and the safety and security of Canada and its citizens.

These provisions are dynamic and may be subject to change based on sensitive Canadian government operations that necessitate additional or other safeguards, or to keep pace with suspected criminal and unlawful activities that use telecommunications services and related technologies.

This template has been provided as an example:

*Figures between 0 and 100 should be represented in a band of '0-100' when any figure in column A (Number of Requests) **or** Column B (Number of Disclosures) is less than 100.*

Law Enforcement, National Security, and Regulatory Agency Requests for Customer Data (2014)

	A	B	C	D
Data type	Number of requests (0-100 or exact # if over 100)	Number of disclosures (full or partial information disclosed) (0-100 or exact # if over 100)	Number of requests rejected or contested (see limitation on banding 0-100)	Number of persons or accounts with data was disclosed (see limitation on banding 0-100)
Voluntary disclosure at the request of a government agency	e.g. 127,754	114,773	9,981	98,824
Voluntary disclosure on the initiative of the organization	e.g. N/A	114,733	N/A	98,824
Disclosures in emergency or exigent circumstances	e.g. 35,365	35,365	0	Not tracked
Disclosures made in compliance with federal or provincial law	e.g. 1,735	e.g. 1,733	2	5,384
Court ordered (warranted) disclosures*	e.g. 68,653	67,967	686	56,647
a) Basic identifying information (court ordered)	e.g. 47,491	47,106	475	38,629
b) Tracking data	e.g. 8,881	8,792	89	6,985
c) Transmission data	e.g. 7,539	7,464	75	7,043
d) Stored communications content and other stored data	e.g. 4,742	4,695	47	3,990
e) Real time interceptions	e.g. 0-100	0-100	0-100	0-100
Other Requests:				
a) Foreign Agency Requests (court ordered)	e.g. 0-100	0-100	0-100	Not tracked
b) Preservation demands and orders	e.g. 52,791	52,791	0	61,839
Total Requests**	e.g. 354,951	455,379	11,355	378,165

***** Organizations are encouraged, where and when possible, to provide additional aggregate details on court ordered (warranted) requests, as described above.
** "Total" does not include any figure in which the 0-100 band is applied.