INVESTIGATING AND PREVENTING CRIMINAL ELECTRONIC COMMUNICATIONS ACT: REGULATIONS POLICY

1.0 INTRODUCTION

The following is a brief overview of the policies that could be reflected in the regulations to be drafted under the *Investigating and Preventing Criminal Electronic Communications Act*. Policies summarized in this document reflect proposals which were under consideration at the time of writing and may be subject to further development or modification.

After the regulations are enacted, Administrative Guidelines may also be developed to provide guidance on, and further explanations of, the Act and the Regulations. These Guidelines could include examples where it is considered to be useful.

2.0 DEFINITIONS

The following definitions are used in the Regulations Policy document.

"Act" means the *Investigating and Preventing Criminal Electronic Communications Act*. (*Loi*)

"access device" means a transmission apparatus that enables subscribers' telecommunications to be connected to a telecommunications service provider's telecommunications facilities and that is capable of performing protocol conversion or adaptation. It also aggregates individual subscriber telecommunications for delivery to edge devices. (*dispositif d'accès*)

"authorized", in relation to a person, means having authority, under the *Criminal Code* or the *Canadian Security Intelligence Service Act*, to intercept communications. This is defined in the Act. *(autorisée)*

"agency" means the Canadian Security Intelligence Service (CSIS) or a law enforcement agency whose employees or members could include authorized persons. (*organisme)*

"census agglomeration" means a census agglomeration within the meaning of the Statistics Canada document entitled *Standard Geographical Classification SGC 2006*, as amended from time to time. This currently refers to a small urban core and adjacent integrated urban and rural areas. *(agglomération de recensement)*

"census metropolitan area" means a census metropolitan area within the meaning of the Statistics Canada document entitled Standard Geographical Classification SGC 2006,

as amended from time to time. This currently refers to a large urban core and adjacent integrated urban and rural areas. *(région métropolitaine de recensement)*

"Class 1 apparatus" means a transmission apparatus that is located outside a census agglomeration or a census metropolitan area. (e.g. Rural areas) *(appareil de catégorie 1)*

"Class 2 apparatus" means a transmission apparatus that is located in a census agglomeration (e.g. suburbs or small towns). *(appareil de catégorie 2)*

"Class 3 apparatus" means a transmission apparatus that is located in a census metropolitan area (e.g. Montreal, Toronto). *(appareil de catégorie 3)*

"delivery point" means a demarcation point[1] which provides access to intercepted communications. *(point de livraison)*

"divert" includes any deflection, forwarding, or re-direction of a communication (e.g. call-forwarding on individual lines or 1-800 services, e-mail forwarding, etc.). *(détournement)*

"edge device" means an apparatus that is used to provide a connection into the core of the service provider's telecommunication facilities for one or more access devices and that is capable of performing protocol conversion or adaptation. *(dispositif de périphérie)*

"global limit" is described in the Act and means the maximum number of active simultaneous interceptions that a service provider is legally required to be capable of performing. *(limite globale)*

"interception subject" means a person whose communications are intercepted by an authorized person. *(personne visée)*

"interception subject's service" means a telecommunications service that is associated with an interception subject, whether or not the interception subject is the subscriber to that service. *(service de la personne visée)*

"Minister" means the Minister of Public Safety and Emergency Preparedness *(Ministre)*

"server" means an apparatus that facilitates, manages or operates telecommunications services for a telecommunications facility or acts as a repository and distributor of information, including voicemail, e-mail, video, gateway, softswitch, authentication, authorization and accounting. *(serveur)*

---

[1] Demarcation point means the point of a demarcation and/or interconnection between telephone company communications facilities and terminal equipment, protective apparatus, or wiring at a subscriber's premises" (Newton's Telecom Dictionary, 2009 edition). The "subscriber" in this instance refers to the authorities who receive the intercepted communications.

"telecommunications service provider" is defined in the Act and means a person that, independently or as part of a group or association, provides telecommunications services. (*télécommunicateur*)

"telecommunications facility" is defined in the Act and means any facility, apparatus or other thing that is used for telecommunications or for any operation directly connected with telecommunications. (*installation de télécommunication)*

"transmission apparatus" is defined in the Act and refers to any apparatus of a prescribed class whose principal functions include switching, routing communications, input, capture, storage, retrieval, output or other processing of communications. A transmission apparatus may also control the speed, content, protocol, format or similar aspects of communications. (*appareil de transmission*)

3.0 REGULATION POLICIES RELATED TO INTERCEPTION

3.1 TELECOMMUNICATIONS SERVICE PROVIDERS' OBLIGATIONS - GENERAL REQUIREMENTS

3.1.1 Intercepted Communications. The Act requires that service providers should have the capability to intercept any communications effected by means of telecommunications. Regulations may further elaborate the definition of "communication" that is in the Act. This includes communication that is attempted, abandoned or otherwise interrupted, not completed or diverted, as well as mobile, stored or multi-communications. In addition, regulations may also stipulate that related telecommunications data should be made available to authorities. Regulations may also specify exceptions where they may apply.

3.1.2 Response Time by Service Providers For Interception Requests. Regulations may elaborate a service provider's obligations to enable the interception of communications as soon as feasible, within a maximum of two business days, in normal circumstances.

Regulations may also elaborate a service provider's obligations to accelerate the activation of interceptions of communications in exceptional circumstances. For an interception set up remotely through the use of electronic devices, without the physical displacement of equipment or personnel, service providers could have up to 30 minutes to enable the interception after receiving a written or oral request to do so from an authorized person. For other types of interceptions in exceptional circumstances, service providers could be obliged to enable that interception within eight hours after receiving a written or oral request from an authorized person.

Exceptional circumstances could be where the authorized person believes immediate interception is necessary to investigate a threat to national security, or to prevent an unlawful act that could reasonably be expected to cause serious harm to any person or property.

3.1.3 Security and Confidentiality of Interceptions and Intercepted Communications. Regulations may elaborate a service provider's obligations to take measures to protect the confidentiality of intercepted communications.

Regulations may elaborate a service provider's obligations to protect documents and information related to authorized interceptions or related to subscriber information requests, taking into account disclosures required by law.

Regulations may elaborate a service provider's obligations to maintain an accurate, secure record of each activated interception.

Regulations may elaborate a service provider's obligations to limit access to certain equipment or software used for interceptions.

Regulations may elaborate a service provider's obligations to take certain measures in response to a breach of confidentiality or security measures.

3.1.4 Transmission Obligations. Regulations may elaborate a service provider's obligations to have the capability to transmit the intercepted communications to authorities while they are occurring (in real-time). However, if a service provider's telecommunications facilities cannot send the transmission data for the intercepted communications in real-time for any reason, regulations may specify that a service provider is to have the capability to send the transmission data no later than one second after the content portion of the intercepted communication is intercepted.

Regulations may elaborate a service provider's obligations to provide information that will allow the establishment of correlation between the content of any intercepted communication and the transmission data for that intercepted communication.

3.1.5 Delivery Of Intercepted Communications. Regulations may elaborate a service provider's obligations with respect to providing the intercepted communications to the authorized persons by specifying the form, manner, location and timing of delivery.

3.1.6 Delivery Form and Manner For Intercepted Communications. Regulations may stipulate that a service provider could be required to provide intercepted communications to an authorized person in a format that conforms to a national or international telecommunications standard that is recognized in Canada by the telecommunications industry.

Regulations may also elaborate that, before using a different type of connection protocol or delivery format, a service provider will have to provide a minimum of 90 days notice to all agencies from which it will have received requests for interception in the preceding 12 months.

Regulations may elaborate that all communications of an interception subject will be delivered to an authorized person in such a way that permits each communication to be identified separately. This includes situations where an interception subject uses a telecommunications service without terminating their previous communication on that service (e.g. call-waiting). Service providers may also be asked to ensure that the intercepted communications are not lost.

3.1.7 Delivery Points. Regulations may elaborate requirements with respect to delivery points. These requirements may take into consideration advances in technology, both known and anticipated, as well as the current operational and technical environment for both the authorities and service providers.

3.2 TELECOMMUNICATIONS SERVICE PROVIDERS' OBLIGATIONS - TECHNICAL REQUIREMENTS

3.2.1 Transmission Apparatus. Transmission Apparatus is defined in the Act by the principal functions that the apparatus performs, and the different classes of such apparatuses may be elaborated in the regulations. For further clarity, the regulations may elaborate that such classes could include access devices, edge devices and servers.

For instance, a current example of an access device is a Cable Modem Termination System (CMTS) and a current example of an edge device is a broadband remote access server (BRAS). An email server, for example, could be categorized simply as a server for the purposes of the regulations under this Act if it cannot be defined as any other class of device (such as an access or edge device).

3.2.2 Simultaneous Interceptions Capacity. Service providers may be asked to perform multiple simultaneous interceptions. These simultaneous interceptions can be categorized in at least three ways:

- Simultaneous targets – this implies a number of different interception subjects whose communications can be intercepted (on the same transmission apparatus) at the same time.
- Simultaneous multi-agency – this implies delivery of intercepted communications to multiple agencies at one time with the possibility of multiple targets operating independently.
- Single target/multi-agency – this implies the support of simultaneous agencies operating on the same target independently.

Regulations may elaborate that a service provider will be required to have the capacity to enable the interception of all communications of a single interception subject, by up to five different agencies at the same time.

Regulations may elaborate the minimum and maximum capacity a service provider will be required to have for simultaneous interceptions for an apparatus. The service provider's equipment or software needs to be capable of meeting the minimum capacity and reaching the maximum capacity, when required, with some advance notice.

3.2.3 Advance Notice to Increase Capacity for Simultaneous Interceptions from the Minimum up to the Maximum on an Apparatus. Regulations may elaborate the timeframe under which a service provider would be required to comply with a request made under the Act to increase capacity for multiple interceptions on a device, beyond the minimum specified capacity.

Regulations may elaborate that service providers would have five business days after the request for increased capacity is received to meet the request. If the request resulted in

more than 100% increase over the required minimum capacity on a device, then the service provider would have 10 business days after the request is received.
Example: Authorized persons from different agencies require 14 simultaneous interceptions from a Class 2 access device, whose minimum is two and maximum is 16. The service provider would have 10 business days to increase the capacity of that device to 14.

3.2.4 Required Simultaneous Interception Capacity Calculations. Regulations may elaborate that a service provider should calculate its capacity for simultaneous interceptions based on its access devices, or its edge devices, or a combination of both. Where applicable, capacity calculations could be based on a server[2].

Where an interception subject has more than one telecommunications service being generated by or transmitted through the same access device, edge device, or server, the interception of these services would count as a single interception for maximum capacity calculation and global limit calculation purposes.

3.2.5 Calculations for Capacity Based On Access Devices. Regulations may elaborate the method that a service provider would be required to use to calculate capacity for simultaneous interceptions.

Regulations may elaborate that if a service provider calculates its capacity for intercept capabilities based on access devices, the minimum amount of intercept capabilities required for each device would be two.

Regulations may elaborate that the maximum number of simultaneous interceptions that a service provider could be requested to enable on a device would be:

(a) 4 per Class 1 apparatus;

(b) 16 per Class 2 apparatus; and,

(c) 64 per Class 3 apparatus.

3.2.6 Calculations for Capacity Based on Edge Devices. Regulations may elaborate that if a service provider calculates its capacity for intercept capabilities based on edge devices, the minimum number of simultaneous interception capacity for each edge device would be the aggregate of the minimum number of simultaneous interception capabilities for each access device (two per access device) connected to it.

i.e. Minimum number for each edge device = Σ minimum number of interceptions for the access device connected to that edge device.

[2] For more details on capacity for servers, see section 3.2.7 of this document

Regulations may elaborate that the maximum number of simultaneous interceptions per edge device that a service provider could be requested to enable would be the lesser of:

> the aggregate of the upper limit of the number of multiple simultaneous interceptions required for access devices connected to the edge device, or 400.

i.e. Maximum number for each edge device = Minimum ((400, (Σ maximum number of interceptions for the access device connected to that edge device))

For example:

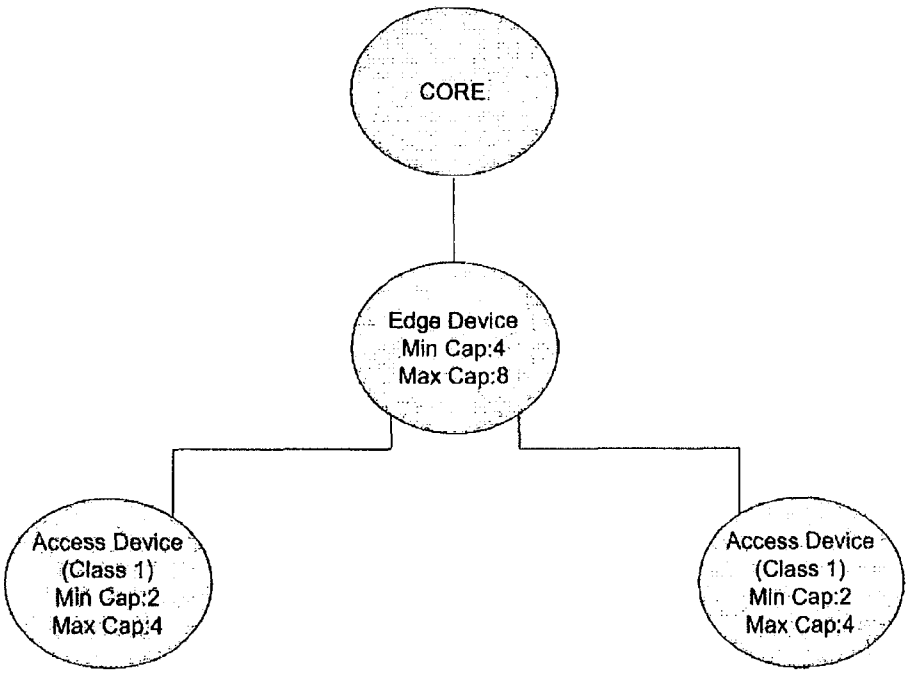

Figure 1. Example for Edge Device Calculations

3.2.7 Calculations for Capacity of Servers. Regulations may elaborate that capacity calculations are required for servers in situations where targeted communications cannot be fully intercepted solely through the use of access or edge devices, and where some of the communications goes through a server. Calculations for minimum and maximum numbers of simultaneous interceptions for servers, when applicable, may be done using the same method employed for calculating the capacity requirements for edge devices connected to the server. Examples include e-mail and Voice Over Internet Protocol (VOIP).

For example:

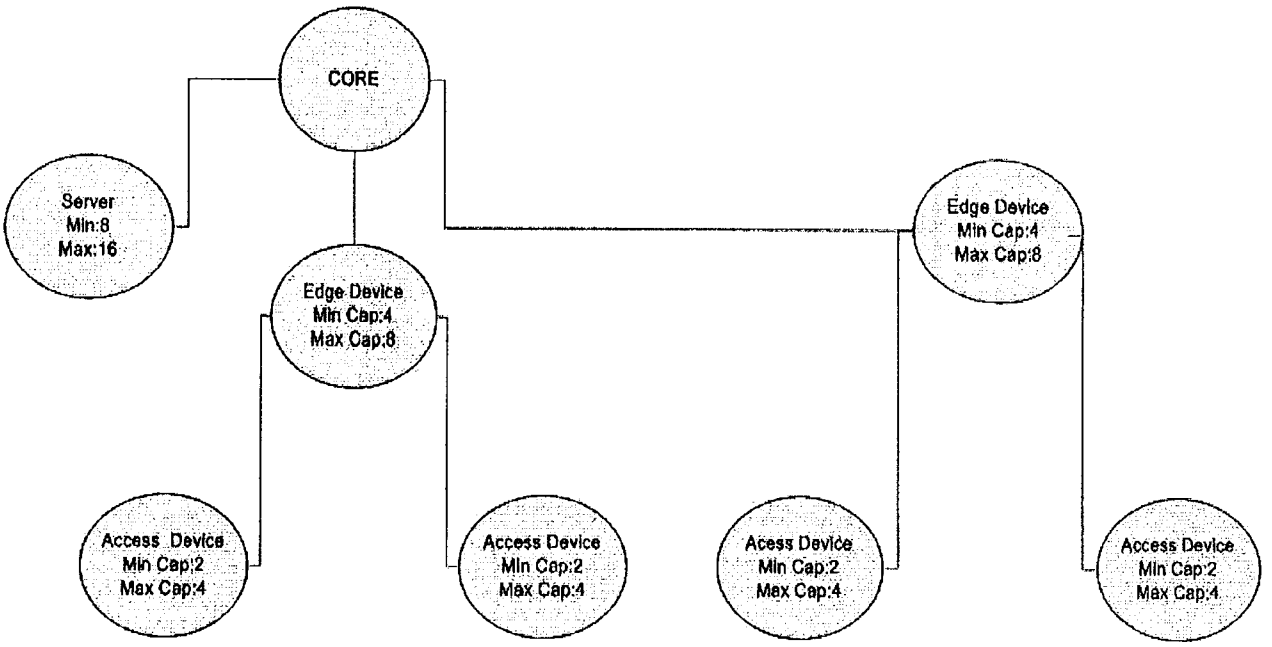

Figure 2. Example for Server Based Calculations – the Class 1 Access Devices

3.2.8 Capacity Calculations for Telecommunications Facilities that Contain Grandfathered and New Equipment. Operational requirements only apply[3] when a service provider begins to operate a transmission apparatus (described in s.10 of the Act) or installs new software for any transmission apparatus that the service provider operates (s.11 of Act). As such, transmission apparatus or software that is already in operation at the time s.10 and/or s.11 of the Act comes into force, is not subject to those sections and can be deemed "grandfathered", that is, exempt from those provisions until the apparatus or software is upgraded or updated in some fashion.

A service provider may have a mix of devices where the operational requirements of the Act (s.7) apply to some ("new") but not to others ("grandfathered") within the same telecommunications facility.

Regulations may elaborate that where an edge device or server is "new", the minimum and maximum capacity requirements would be determined based on the total number of

[3] Although the requirements of the Act apply once it receives Royal Assent, the obligations that would normally begin because a service provider has begun to operate new transmission apparatus (section 10) or software (section 11) will be postponed until the end of an 18-month initial transition period that follows the legislation coming into force. After this 18-month period, the requirements will take full effect, and will apply to transmission apparatus and software deployed or installed during this transmission period and beyond.

all access devices connected to the edge device. This includes "grand-fathered" access devices. That is to say, if an edge device is "new", for capacity calculation purposes, it wouldn't matter whether the access devices connected to it are "new" or "grand-fathered". However, when the edge device is "grandfathered", the calculation would only reflect the numbers associated with the new access devices.

Example 1:

Edge Device 1 (grandfathered) has three access devices (Class 1, min: 2, max: 4). Two of these access devices are grandfathered and one is new. While there would be no operational requirements under the law for this edge device, if a service provider calculates maximum capacity for its facilities based on edge devices, only the new access device would be used for purposes of capacity calculations. Maximum capacity for this edge device for calculation purposes would be 4 x 1 = 4.

Example 2:

Edge Device 2 (grandfathered) has two access devices (Class 1). Both access devices are new. The maximum capacity number would be 4 x 2 = 8.

Example 3:

Edge Device 3 (new) has three access devices. All the access devices are grandfathered. Maximum capacity for this edge device would be 4 x 3=12.

3.2.9 Global Limit – Maximum Number of Enabled (Active) Simultaneous Interceptions Required on the Entire Telecommunications Facilities

Regulations may specify that regardless of the calculation methods outlined in the sections above and the total sum of the maximum capacity numbers calculated for each device in a telecommunications facility, a service provider would not be required to increase its capability for simultaneous active interceptions for its network beyond the total of the number of its subscribers divided by 5,000.

However, if a service provider has 10,000 or fewer subscribers, then the global limit would be two.

The global limit is only applicable with respect to the number of active simultaneous interceptions in the service provider's telecommunications facilities that are possible and does not apply to capacity numbers on a transmission apparatus. Only a Ministerial Order under the Act would require a service provider to go beyond the global limit. Such a request would be subject to reasonable compensation.

Example 1:

A service provider has 400 Class 1 access devices and one million subscribers, and its capacity is calculated based on access devices. According to the access device capacity calculations, the service provider would be required to have a minimum capacity of two interceptions per device, i.e. 800 simultaneous interceptions in the network (400 x 2 per device). The maximum required capacity across all its telecommunication facilities (network) would be 1600 (400 x 4). However, the global limit is 200 active interceptions (1 million ÷ 5,000). This means that the service provider would only be expected to be able to accommodate a maximum of 200 simultaneous interceptions in its telecommunications facilities.

If the interception solution were based on an intercept licence regime, the provider would be required to have a licence to support 200 active simultaneous intercepts, which could be deployed anywhere within the network, within the prescribed times.

Example 2:

A service provider has 30 Class 2 access devices and one million subscribers. The service provider could have a maximum required capability of 480 interceptions on its access devices (aggregate).

However, if the service provider is basing its calculations on edge devices and has one edge device, then the maximum required capability on that device would be 400 (the defined maximum). If it has two edge devices, and each device has an equal number of access devices (ex: 15 Class 2 access devices each), then the maximum required capability on those devices would be 240 (15 x 16) per edge device. The total maximum interception capacity required from the service provider would be 480 (240 x 2). Regardless, the service provider would only be expected to be able to accommodate a maximum of 200 simultaneous interceptions in its telecommunications facilities.

4.0 REGULATION POLICIES RELATED TO SUBSCRIBER INFORMATION

4.1 REQUESTS TO SERVICE PROVIDERS FOR SUBSCRIBER INFORMATION

The Act requires telecommunications service providers to provide subscriber information to designated police, CSIS and Competition Bureau personnel upon request. The provisions in the Act related to subscriber information, as well as the regulations associated with these provisions, would establish a new and comprehensive legal scheme to govern these types of requests.

The Act specifies, and thereby limits, the information which may be requested and the purposes for making such requests. It also establishes restrictions on the persons who may make such requests, as well as the manner and situations in which they may do so.

It also implements an accountability regime for these requests. Regulations may establish further controls pertaining to the process of making these requests.

4.2 AGENCIES' REQUEST-MAKING OBLIGATIONS

The Act specifies that, under normal circumstances, only a person who has been officially designated to make these requests by the head of a police agency, CSIS or the Competition Bureau (i.e., a "designated person") may do so. It further specifies that in serious emergency situations, referred as "exceptional circumstances" in the Act, any police officer (not necessarily one who has been officially designated) may request subscriber information.

While the Act specifies the subscriber information that may be requested, regulations would specify the form of that information, the manner, time and the circumstances under which particular information is to be provided. These regulations would ensure requests for subscriber information are focused and not unnecessarily broad in scope. Regulations may elaborate that a designated person from the police, Competition Bureau and CSIS, or a police officer in exceptional circumstances, would have to present the service provider with a subscriber identifier[4] to gain one or more subscriber identifiers in return. For instance, under the regulations, a designated person may be required to first give a service provider a subscriber's IP address, along with the corresponding date and time it was used, or could be required to first provide an email address, in order to receive the corresponding customer name and address, or the customer telephone number.

4.3 DELEGATION OF POWER TO DESIGNATE PERSONS MAKING REQUESTS

The Act provides the Commissioner of the RCMP, the Director of CSIS, the Commissioner of Competition and the Chief or Head of a Police Service with the power to designate persons who can make requests for subscriber information. The Act further provides that the Commissioner of the RCMP and the Director of CSIS may delegate this responsibility to senior officers within their organizations. Regulations may elaborate on and limit the delegated senior staff to whom the designation power could be assigned.

For example, the regulations could specify that the powers to designate a person may be delegated as follows:

(a) For the Commissioner of the RCMP, the power could be delegated to: (1) the Deputy Commissioners for the regions and commanding officers for the divisions (except Depot Division) of the RCMP; and (2) the Deputy Commissioners at headquarters responsible for operational programs and services and for operational support services.

---

[4] Subscriber identifiers specified in the Act are: name; address; telephone number; e-mail address; Internet Protocol (IP) address; mobile identification number; electronic serial number; local service provider identifier; international mobile equipment identity number, international mobile subscriber identity number; and subscriber identity module card number associated with the subscriber's service and equipment.

(b) For the Director of CSIS, the power could be delegated to Directors General of operational branches at Headquarters and to the Director General of each region.

4.4 AGENCIES' OTHER OBLIGATIONS RELATED TO SUBSCRIBER INFORMATION REQUESTS

4.4.1 Form and Manner of Requests to Service Providers. The Act requires that designated persons make subscriber information requests to service providers in writing under normal circumstances. Regulations may outline how this subscriber information could be requested from a service provider, including the form and manner in which particular information could be provided.

Regulations may set out specific subscriber information request forms that the designated person could use to request subscriber information from service providers. Regulations may also establish rules to protect the confidentiality of requests, as appropriate, and may impose security measures on agencies to protect the records and the subscriber information related to these requests, as appropriate.

4.4.2 Record Keeping. In addition, regulations may elaborate the information that a designated person would have to keep in internal records, when making a subscriber information request to a service provider. Such records could facilitate audits of the agencies' practices and their compliance with the provisions of the Act and regulations governing subscriber information requests. These records could include the following information:

(a) the name of the designated person and at least one other piece of identifying information, such as that person's employee identity number, police officer badge number or date of birth;

(b) if the request is made in relation to the investigation of an offence or the enforcement of a federal or provincial law or an instrument made under such a law, then a reference to the applicable provision may be required;

(c) a file number or other record identifier relating the request to an investigation or other duty or function referred to in subsection 16 (2) of the Act; and

(d) a record identifier relating the request made to the service provider to the subscriber information, that the service provider produces in response to the request[5].

Regulations may elaborate that when the information outlined above in (a) through (d) is identical for multiple subscriber information requests, a single record may be created. This may happen when an investigation leads to multiple subscriber information requests.

[5] This allows the correlation between the subscriber information request and the subscriber information that was obtained in response to that request.

The regulations prescribing the information about subscriber information requests that is to be kept in the agencies' internal records may also apply to requests made in exceptional circumstances.

4.4.3 Service Providers' Obligations Related to Subscriber Information. Regulations may elaborate service providers' obligations with respect to providing requested subscriber information to designated persons or a police officer in the exceptional circumstances specified in the Act.

Regulations may elaborate service providers' obligations to provide, in written form, the name, address and other identifiers associated with the subscriber to a designated person as soon as feasible, but within two business days after having received the request for the information. In exceptional circumstances, this information should be provided to the requesting police officer as soon as feasible but no longer than within 30 minutes.

Regulations may also establish confidentiality and security measures for service providers receiving subscriber information requests, including those made orally in exceptional circumstances.

5.0 OTHER OBLIGATIONS RELATED POLICIES

5.1 ORDER SUSPENDING OBLIGATIONS

The Act stipulates that the Minister may suspend operational requirements of a service provider if the service provider has applied for such suspension. The application should set out the reason for the request and a plan to show how the service provider proposes to meet the operational requirements by the end of the suspension period, including milestones to measure progress.

Regulations may elaborate the content, form and manner in which an application may be made to the Minister in order to have interception capability obligations suspended. These obligations may be suspended in whole or in part, under certain conditions, for a period up to three years, at the Minister's discretion.

5.2 OBLIGATION TO PROVIDE INFORMATION

5.2.1 Facilities and Services Information. Regulations may elaborate the information that a service provider will be required to provide to the police or CSIS relating to its telecommunications facilities and services, upon request, in the course of police or CSIS duties.

5.2.2 Location Information. Regulations may elaborate a service provider's obligations to provide to persons lawfully authorised to request it, certain information that is in its possession or control respecting the location of equipment used by an interception subject (individual). This information could include the street address, or longitudinal and latitudinal coordinates, or the cell site, sector, or beam area (where applicable).

Regulations may also elaborate when this location information needs to be provided to authorities.

5.2.3 Mandatory Reporting. The Act specifies mandatory reporting obligations for service providers on their transmission apparatus, with respect to interception, within six months of the Act coming into force. There are also reporting obligations for a service provider that starts to operate transmission apparatus acquired from another service provider.

Regulations may elaborate the form and manner in which a service provider will be required to submit a report to the Minister. This report may include contact information, information respecting a service provider's telecommunications services and identification of the transmission apparatus and its capability to meet operational requirements.

If the service provider does meet all the requirements under the legislation at the time the Act comes into force, regulations may require only an attestation to that effect. However, if the service provider is not capable of meeting all the requirements under the legislation at the time the Act comes into force, regulations may require the service provider to identify the non-compliant transmission apparatus, as well as the requirements that are not being met.

5.3 OBLIGATION TO ASSIST – ASSESSMENT AND TESTING OF TELECOMMUNICATIONS FACILITIES

Regulations may elaborate the assistance to be provided by a service provider to a police officer or employee of the RCMP or CSIS, in the assessment and testing of the service provider's facilities that may be/are used to intercept telecommunications. This assistance may be necessary to confirm the following:

- the service provider's telecommunications facilities can perform/are performing the interception;
- the intercepted communications are from the interception subject's service(s); and
- the service provider's telecommunications facilities can provide/are providing the intercepted communications to the delivery point.

5.4 SMALL SERVICE PROVIDERS

Under the Act, small service providers[6] can provide a physical connection point to meet their intercept capability obligations for the first three years the Act is in force. Regulations may elaborate the meaning of "affiliated or associated telecommunications

[6] Under the Act, service providers that have less than 100,000 subscribers are deemed small service providers.

service providers". This would help service providers determine whether they are considered to be a small service provider.

Regulations may also elaborate the provision of the physical connection point (i.e. how small service providers provide access to their telecommunications facilities physically).

6.0 REGULATION POLICIES RELATED TO ADMINISTRATIVE MONETARY PENALTIES

Regulations may designate particular sections of the Act with which a contravention would be considered a violation. Regulations may also specify the maximum administrative monetary penalty that could be imposed as a result of a particular violation.

Regulations may elaborate the criteria to be taken into account in assessing the amount of a penalty, and could include:

(a) whether an interception was compromised, delayed or prevented by temporary technical impediments beyond the control of the service provider;

(b) the complexity of an interception or of a request made by a designated person for subscriber information;

(c) the volume of requests for subscriber information received simultaneously by the service provider;

(d) the volume of interceptions simultaneously provided by the service provider;

(e) whether the violation compromised physical, personnel and/or electronic security; and

(f) if interception was compromised, the length of time during which this was the case.

7.0 REGULATION POLICIES RELATED TO PAYMENT TO SERVICE PROVIDERS

Regulations may elaborate on the three following circumstances for which a service provider is entitled to receive payment under the Act.

7.1 MINISTERIAL ORDERS

Regulations may elaborate the type of costs that the Minister shall consider in determining a reasonable amount to pay service providers for complying with a Ministerial Order under the Act. These costs could be:

(*a*) the cost of assessing and developing a method for the service provider's existing telecommunications facilities to comply, including an engineering assessment;

(*b*) the actual cost of equipment;

(*c*) the actual cost of software;

(*d*) the actual cost of software licences;

(*e*) the actual cost of installation and testing of equipment and software; and,

(*g*) the actual cost of physical modifications to telecommunications facilities to meet confidentiality and security.

Regulations may elaborate that in determining a reasonable payment, the Minister could consider such things as:

- whether the service provider would make a profit from the payment; and
- the manner in which compliance with the order would be achieved, including whether it is achieved in a cost-effective or appropriate manner.

7.2 SPECIALIZED TELECOMMUNICATIONS SUPPORT

Service providers are entitled to payment when they provide specialized telecommunications support related to interception. Regulations may elaborate the conditions under which service providers are entitled to payment when they provide specialized telecommunications support related to an interception. Regulations may specify how the amount of payment could be determined for providing this specialized support.

7.3 PROVISION OF SUBSCRIBER INFORMATION

Telecommunications service providers are entitled to payment when they provide subscriber information to police, CSIS and the Competition Bureau, in accordance with S.16 and S.17 of the Act. The regulations may specify the fees associated with the provision of this information. Other obligations specified in the Act are not subject to compensation.

Date modified: 26 October 2010