Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table

Solicitor Generals Standards

Standard 1: Law enforcement agencies require access to the entire telecommunications transmitted, or caused to be transmitted, to and from the number or other identifier of the target service used by the interception subject. Law enforcement agencies also require access to the call-associated data that is generated to process the call.

Law enforcement must receive ALL telecommunications that is received or transmitted by the target. This is not limited to the audio portion but must also include any data that is transmitted or received. An example of this would be some sort of short message service (SMS) or other data message that would not require an audio channel allocation. The audio channel must also include any analog transmission of fax or data that the target may transmit or receive. Additionally this may include the interception of voice mail services and/or cloning of same.

Standard 2: Law enforcement agencies require access to all mobile interception subjects operating temporarily or permanently within a telecommunications system.

Law enforcement requires the same capability on all users of the system whether they reside in the system permanently or on a temporary basis.

Standard 3: Law enforcement agencies require access in cases where the interception subject may be using features to divert calls to other telecommunications service or terminal equipment, including calls that traverse more than one network or are processed by more than one network operator/service provider before completing.

Law enforcement requires access to advanced calling features such as call forwarding and/or call diverting. It is understood that at least two distinct scenarios may exist here. They are inter-network and intra-network. Inter-network refers to calls originating in one service providers' network and terminating in another service provider's network. Intra-network refers to calls both originating and terminating within the same service providers' network. Capabilities may differ in these scenarios based on the information provided between separate service providers. It is assumed by law enforcement that when the information can be made available and is made available to the customer, it will also be made available to law enforcement. It is important to determine the limitations of this capability in terms of multiple applications of this feature. (i.e. call forwarding a

particular phone number several times. 'A' forwarded to 'B', 'B' forwarded to 'C' etc.)

Standard 4: Law enforcement agencies require that the telecommunications to and from a target service be provided to the exclusion of any telecommunications that do not fall within the scope of the interception authorization.

Simply stated, Law enforcement only has the authority to intercept specific target services to the exclusion of other customers served by the service provider. Law enforcement cannot receive any telecommunications that does not fall within the scope of the authorization and its specific time frame. It is the responsibility of the law enforcement agency to appropriately handle all intercepted material once in the possession of the law enforcement agency, which includes the determination of 'privileged call information' and its appropriate handling. Privileged call information is defined as calls which are intercepted but must be handled by law enforcement in a way which the courts define. (i.e. a solicitor/client conversation)

Standard 5: Law enforcement agencies require access to available call associated data such as:

A) Signaling of access ready status

Law enforcement requires some sort of signal to determine that a target phone has become active. The standard methodology is a continuous DTMF 'C' tone during target inactivity (on-hook) and removal of the tone during target activity (off-hook).

B) Called party number for outgoing connections even if there is no successful connection established

Law enforcement requires that the number dialed by the target be available to law enforcement even if the call is deemed incomplete. Examples of incomplete calls are: call, no answer; call, called part busy; call, called party is out of range (assuming wireless); call, all trunks/network busy; call, call forwarding. Law enforcement is also concerned that due to evidentiary rules, call correlation between call associated data and call content is imperative. Law enforcement requires a 1:1 correlation of call content to call data sessions. These outlined examples may cause problems in this area and affect compliance to standard #10 which requires accurate correlation between call content and call associated data. Preferred correlation methods of call content to call data are outlined in interpretation to standard #10

Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table

C) Calling party number for incoming connections even if there is no successful connection established

Law enforcement requires the calling number information to be forwarded in all examples as outlined above in 5b. It is understood that at least two distinct scenarios may exist here. They are inter-network and intra-network as defined in standard number 3 above. It is assumed by law enforcement as in standard number 3, that when the information can be made available and is made available to the customer, it will also be made available to law enforcement.

D) All digits dialed by the target, including post-connection dialed digits used to activate features such as conference calling and call transfer

*Law enforcement requires that any and all information transmitted by the target must also be relayed to law enforcement. This includes feature activations that do not necessarily constitute a call. It shall also include any digits dialed or feature activations during the progress of a call. This information may be transmitted to law enforcement in different ways however it is assumed that any 'in-band' information will remain in-band as well as be defined in any call associated data session. An example of this is the target dialing a *67 which activates call forwarding. Law enforcement would expect the in-band signaling to remain intact as well as an indication on the data session as to what feature was activated. <u>All transmission of information should occur post call event rather than post call completion.</u>*

E) Beginning, end, and duration of the connection

Law enforcement requires a time stamp on all sessions to establish dates and time of target calls.

F) Actual destination and intermediate directory numbers if call has been diverted.

Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table

Law enforcement requires intermediate destination numbers assuming call forward scenarios. It is understood that at least two distinct scenarios may exist here. They are inter-network and intra-network as defined in standard number 3 above. It is important to determine how many times calls can be diverted and tracked as stated in standard number 3 above

Standard 6: Law enforcement agencies require information on the most accurate geographical location known to the network for mobile subscribers.

There are 5 call scenarios that must be outlined here. They are as follows:
autonomous registration or initial power up of handset
initiation of an outbound call
answer of an incoming call
transfer between cell sites
end of call/hang up of calling party
Additionally, location information needs to be available immediately after the call event rather than after call completion. Further, the resolution of the geographical information sent is important for law enforcement to know. As an example, this information may contain a cell site id, cell sector information, signal strength etc.

Standard 7: Law enforcement agencies require data on the specific service used by the interception subject and the technical parameters for that type of communication.

Law enforcement will require all information with respect to a targets service, which indicate to us the capabilities the target may have. As an example, this information may contain a list of features that the target has like call forwarding, voice mail, call conference, short message service, paging etc. This information must also include any information with respect to roaming agreements on other networks. This particular information would be limited to being notified of the capability. Other information with respect to his services on other networks would be obtained from the other service provider.

Standard 8: Law enforcement agencies require a real- time, full-time monitoring capability for the interception of telecommunications. Call associated data should also be provided in real-time. If call associated data cannot be made available in real time, law enforcement agencies require the data to be

available as soon as possible upon call termination.

Law enforcement assumes that call content information, (audio) will be delivered to the law enforcement agency in real-time. Additionally, call associated data will be made available within milliseconds post call event rather than post call completion. (100ms – 500ms is the desirable target) It is imperative that the call-associated data be made available within this short time frame to allow correlation of call event with audio call details.

Standard 9: Law enforcement agencies require network operators/service providers to provide one or more interfaces from which the intercepted communications can be transmitted to the law enforcement monitoring facility. These interfaces have to be commonly agreed on by the interception authorities and the network operators/service providers. Other issues associated with these interfaces will be handled according to generally accepted practices.

Law enforcement requires that the intercepted material be made available for transmission to law enforcement via industry standard interfaces as well as in a format that conforms to generally accepted practices. Essentially law enforcement would like to see the information available in a non-proprietary format and one that can be easily handled. This formatting of data is wholly dependent on the quantity and type of data made available.

Standard 10: Law enforcement agencies require network operators/service providers to provide call associated data and call content from the target service in a way that allows for the accurate correlation of call associated data with call content.

Law enforcement requires a method of delivery of both the audio content and the data content in a manner that will allow for absolute accuracy of correlation. This is mandatory in terms of evidentiary requirements. Several possibilities are available here. As an example, all audio content and all associated data for each single target are combined in some way and transmitted over the same audio circuit. Another example is all voice content and a pre-determined subset of call associated data for each single target are combined in some way and transmitted over the same audio circuit. In this case, the remaining call associated data must be transmitted via another method to allow correlation of the audio circuit and the data circuit. There are many other options here however the important factor is the absolute accuracy of the audio content and the call-

associated data.

Standard 11: Law enforcement agencies require that the format for transmitting the intercepted communications to the monitoring facility be a generally available format.

Law enforcement requires that the format of the transmissions to law enforcement be standard industry accepted formats. Three different transmission types can be defined here –> in-band data, pure data, and pure audio. Examples of standard formats of each type are as follows but not limited to these examples: In-band data – DTMF, MF, FSK, etc.; Pure data – X.25, serial ASCII, etc.; Pure audio – digital formats, analog formats, etc. Additionally, how many audio paths are required per target to intercept the targets entire service provision. (i.e. Is it possible for the target to be simultaneously utilizing more than one audio path as in a call forward scenario with an inbound call being diverted and allowing outbound calls to be made from target handset.)

Standard 12: If network operators/service providers initiate encoding, compression or encryption of telecommunications traffic, law enforcement agencies require the network operators/service providers to provide intercepted communications en clair.

Law enforcement requires that any type of encryption algorithm that is initiated by the service provider must be provided to the law enforcement agency unencrypted. This would include proprietary compression algorithms that are employed in the network. This does not include end to end encryption that can be employed without the service provider's knowledge.

Standard 13: Law enforcement agencies require network operators/service providers to be able to transmit the intercepted communications to the law enforcement monitoring facility via fixed or switched connections.

Law enforcement requires the ability to connect to the service providers over both switched (dial-up) and fixed (dedicated) lines at the same time. Different agencies may require different connectivity and therefore both these capabilities must be supported simultaneously. It should also be noted that the type of service connection to the agency (i.e.: ISDN, T1 etc.) should be supported independently and also simultaneously. An additional concern to law enforcement is the location point of the intercept. A distributed

intercept capability on a regional basis is more attractive than a centralized one. The reasoning for this is that lawful interception is done on a regional basis. If a centralized interception point was the only method to gain access to the network, the product would have to be transported back to the regional location.

Standard 14: Law enforcement agencies require that the transmission of the intercepted communications to the monitoring facility meet applicable Government of Canada security requirements.

Government security policies dictate how this must be achieved. The level of security for the RCMP and other Canadian law enforcement agencies will be met if the service providers can achieve the required level of security for CSIS. Copies of the relevant chapters of the Government Security Policy are available upon request.

Standard 15: Law enforcement agencies require interceptions to be implemented so that neither the interception target nor any other unauthorized person is aware of any changes made to fulfill the interception order. In particular, the operation of the target service must appear unchanged to the interception subject.

Law enforcement requires that the interception be conducted so as not to affect the target service in any way. Additionally, no unauthorized personnel are to be made aware of the interception.

Standard 16: Law enforcement agencies require the interception to be designed and implemented to preclude unauthorized or improper use and to safeguard the information related to the interception.

Law enforcement requires the service provider to detail the procedures and safeguards that are implemented to prevent improper use of information related to the interception. All internal security measures should be detailed to comply. This necessitates select individuals to be security cleared to the Top Secret level. Information regarding the security clearance process will be provided.

Standard 17: Law enforcement agencies require network operators/service providers to protect information on which and how many interceptions are being or have been performed, and not disclose information on how interceptions are carried out.

Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table

Law enforcement requires the service provider to detail the procedures and safeguards that are implemented to prevent improper use of information related to the interception. All internal security measures should be detailed to comply.

Standard 18: Law enforcement agencies require network operators/service providers to ensure that intercepted communications are only transmitted to the monitoring agency specified in the interception authorization.

Law enforcement requires only those targets whom have been named by the specific agency and/or department be transmitted to that agency and/or department. By law, it is imperative that other agencies targets are not to be transmitted to any other agency unless specifically named by that agency. Note that different departments within the same agency should be considered as different agencies.

Standard 19: Based on a lawful inquiry and before implementation of the interception, law enforcement agencies require **(1)** the interception subject's identity service number or other distinctive identifier**, (2)** information on the services and features of the telecommunications system used by the interception subject and delivered by network operators/service providers, and **(3)** information on the technical parameters of the transmission to the law enforcement monitoring facility.

Law enforcement requires all pertinent information about the target in question in order to prepare and present the legal authorization document before the courts. This information would also include any services provided to the target such as voice mail, advanced calling features, roaming capability etc.

Standard 20: During the interception law enforcement agencies may require information and/or assistance from the network operators/service providers to ensure that the communications acquired at the interception interface are those communications associated with the target service.

Law enforcement will require the assistance of the service provider when beginning a lawful interception. This may entail the initial setup and testing of the targets intercepted communications to the law enforcement agency. It may also require the presence of the individual whom assisted law enforcement in a court appearance.

Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table

Standard 21: Law enforcement agencies require network operators/service providers to make provisions for implementing a number of simultaneous intercepts. Multiple interceptions may be required for a single target service to allow monitoring by more than one law enforcement agency. In this case, network operators/service providers should take precautions to safeguard the identities of the monitoring agencies and ensure the confidentiality of the investigations.

Law enforcement requires multiple intercepts to be simultaneously operating on an ongoing basis, which can be categorized in at least 3 ways:

- ***Simultaneous targets** – implies a number of simultaneous targets that can be intercepted on a per switch basis. This maximum number is important to law enforcement.*
- ***Simultaneous multi-agency** – this implies the support of multiple agencies at one time with the possibility of multiple targets operating independently. The total number of agencies that can be supported is important to law enforcement.*
- ***Single target/multi-agency** – this implies the support of simultaneous agencies operating on the same target independently.*

In all cases outlined, law enforcement requires service providers to safeguard the identities of the monitoring agencies to all other agencies involved as well as ensure confidentiality of the separate investigations underway.

Standard 22: Law enforcement agencies require network operators/service providers to implement interceptions as quickly as possible (in urgent cases within a few hours or minutes). The response requirements of law enforcement agencies will vary by the type of target service to be intercepted.

Law enforcement requires various priorities of interception implementations to be carried out by the service providers most of which will have prior notification of 3 to 5 days. There are however emergency and priority situations which may require immediate response from the service provider. An example of this would be a hostage situation where time is of the essence.

Standard 23: For the duration of the interception, law enforcement agencies require that the reliability of the services supporting the interception at least equals the reliability of the target services provided to the interception subject. Law enforcement agencies require the quality of service of the intercepted transmissions forwarded to the monitoring facility to comply with the performance standards of the network operators/service providers.

Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications - Compliance Table

Law enforcement would expect nothing more/less than the quality of service afforded to any other customer.