

Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications (Rev. Nov. 95)

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.
2. Law enforcement agencies require access to all mobile interception subjects operating temporarily or permanently within a telecommunications system.
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.
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.
5. Law enforcement agencies require access to available call associated data such as:
 - Signaling of access ready status
 - Called party number for outgoing connections even if there is no successful connection established
 - Calling party number for incoming connections even if there is no successful connection establish
 - All digits dialed by the target, including post-connection dialed digits used to activate features such as conference calling and call transfer

- Beginning, end, and duration of the connection
 - Actual destination and intermediate directory numbers if call has been diverted
6. Law enforcement agencies require information on the most accurate geographical location known to the network for mobile subscribers.
 7. Law enforcement agencies require data on the specific service used by the interception subject and the technical parameters for that type of communication.
 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.
 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.
 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.
 11. Law enforcement agencies require that the format for transmitting the intercepted communications to the monitoring facility be a generally available format.

12. If network operators/service providers initiate encoding, compression or encryption of communications traffic, law enforcement agencies require the network operators/service providers to provide intercepted communications en clair.
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.
14. Law enforcement agencies require that the transmission of the intercepted communications to the monitoring facility meet applicable Government of Canada security requirements.
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 fulfil the interception order. In particular, the operation of the target service must appear unchanged to the interception subject.
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.
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.
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.

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.
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.
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.
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.

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.

G L O S S A R Y

Access

The technical capability to interface with a communications facility, such as a communications line or switch, so that a law enforcement agency can acquire and monitor communications and call associated data carried on the facility.

Call

Any connection (fixed or temporary) capable of transferring information between two or more users of a telecommunications system.

Call Associated Data

Signaling information passing between a target service and the network or another user. Includes signaling information used to establish the call and to control its progress (e.g. call hold, cell handover). Call associated data also includes information about the call that is available to the network operator/service provider (e.g., duration of connection).

Interception

As used here, the statutory-based action of providing access and delivery of a subject's telecommunications and call associated data to law enforcement.

Interception Interface

The physical location within the service provider's telecommunications facilities where access to the intercepted communications or call associated data is provided. The interception interface is not necessarily a single, fixed point.

Interception Order

An order placed on a network operator/service provider for assisting a law enforcement agency with a lawfully authorized telecommunications interception.

Interception Subject

Person or persons identified in the lawful authorization and whose incoming and outgoing

communications are to be intercepted and monitored.

Law Enforcement Agency

A service, including national security agencies, authorized by law to carry out telecommunications interceptions.

Law Enforcement Monitoring Facility

A law enforcement facility designated as the transmission destination for the intercepted communications and call associated data of a particular interception subject. The site where monitoring/recording equipment is located.

Lawful Authorization

A authorization granted to a law enforcement agency under certain conditions to intercept specified telecommunications. Typically this refers to an order or warrant issued by a judge.

Network Operator/service Provider

"network operator" = the operator of a public telecommunications infrastructure which permits the conveyance of signals between defined network termination points by wire, by microwave, by optical means or by other electromagnetic means";

"service provider" = the natural or legal person providing a public telecommunications service(s) whose provision consists wholly or partly in the transmission and routing of signals on a telecommunications network.

Quality of Service

The quality specification of a communications channel, system, virtual channel, computer communications session, etc. Quality of service may be measured, for example, in terms of signal-to-noise ratio, bit error rate, message throughput rate, or call blocking probability.

Reliability

The probability that a system or service will perform in a satisfactory manner for a given period of time

w h e n u s e d u n d e r s p e c i f i e d o p e r a t i n g c o n d i t i o n s .

Roaming

T h e a b i l i t y o f s u b s c r i b e r s o f m o b i l e
t e l e c o m m u n i c a t i o n s s e r v i c e s t o p l a c e , m a i n t a i n , a n d
r e c e i v e c a l l s w h e n t h e y a r e l o c a t e d o u t s i d e o f t h e i r
d e s i g n a t e d h o m e s e r v i n g a r e a .

Target Service

A s e r v i c e a s s o c i a t e d w i t h a n i n t e r c e p t i o n s u b j e c t a n d
u s u a l l y s p e c i f i e d i n a l a w f u l a u t h o r i z a t i o n f o r
i n t e r c e p t i o n .

Telecommunications

A n y t r a n s f e r o f s i g n s , s i g n a l s , w r i t i n g , i m a g e s ,
s o u n d s , d a t a , o r i n t e l l i g e n c e o f a n y n a t u r e t r a n s m i t t e d
i n w h o l e o r i n p a r t b y a w i r e , r a d i o , e l e c t r o m a g n e t i c ,
p h o t o e l e c t r o n i c , o r p h o t o o p t i c a l s y s t e m .

(Rev.Nov.95)