



India ▼

UPDATED: March 2017 | SOURCE: Telenor Group with support from Hogan Lovells

Provision of Real-time Lawful Interception Assistance

Disclosure of Communications Data

National Security and Emergency Powers

Oversight of the Use of Powers

Provision of Real-time Lawful Interception Assistance

LEGISLATIVE BACKGROUND

Indian Telegraph Act 1885 (“ITA Act”)

This is the parent legislation governing telecommunications in India and the government grants the following licenses to service providers in accordance with the provisions of this Act:

Unified Access Service License (“UASL”)

This is the license governing the provision of access services in India by entities granted licenses prior to 2013.

Internet Service Provider License (“ISP License”)

This is the license governing the provision of internet services in India by entities granted licenses prior to 2013.

Unified Licenses (“UL”)

The Department of Telecommunications (“DoT”) since 2013 issues the Unified License, which is an umbrella license covering all services such as access, internet, national long distance and international long distance. This implies that a service provider can provide all or any licensed telecommunications services under a single license by obtaining the relevant service authorisations under the Unified License. Current UASL and ISP licensees will have to migrate to the Unified Licence Regime on expiry of their existing licenses. For the purposes of this report, we have referred to all three major types of telecommunications licenses in existence today: the UL, the UASL and the ISP License, highlighting differences between them if relevant.

INFORMATION TECHNOLOGY LAWS

The laws generally governing communications over the Internet are as follows:

Information Technology Act (“IT Act”)

This is the parent legislation governing information technology in India. It empowers the government to undertake various forms of electronic surveillance and censorship in accordance with procedures prescribed in the following rules:

IT (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (“Interception Rules”)

These Rules specify the procedure the government must follow to intercept, monitor and decrypt electronic information stored, generated, transmitted or received in any computer resource.

IT (Procedures and Safeguards for Monitoring and Collecting Traffic Data Collecting or Information) Rules, 2009 (“Traffic Data Rules”)

These Rules specify the procedure the government must follow to monitor and collect traffic data or information for the purposes of cybersecurity.

IT (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (“Blocking Rules”)

These Rules specify the procedure the government must follow to order the blocking of IP addresses.

IT Rules, 2011 (“Intermediaries Guidelines”)

These Rules specify the obligations of intermediaries to take down content under specified circumstances.

Code of Criminal Procedure, 1973

This is the principal law governing criminal procedure in India, and which authorises courts and law enforcement agencies to demand the production of documents or other information in the course of an investigation

LEGISLATION

Under Section 5(2) of the ITA Act read with Rule 419-A (I) of the Indian Telegraph Rules, 1951 (ITR), either the Secretary to the Ministry of Home Affairs (in the case of the central government) or the Secretary to the Home Department (in case of the state government or union territory) or a person above the rank of Joint Secretary (in unavoidable circumstances) authorised by

the respective government, during a public emergency or in the interests of public safety, may issue a written order directing an interception, if the official in question believes that it is necessary to do so in the: (a) interest of sovereignty and integrity of India; (b) the security of the State; (c) friendly relations with foreign states; (d) public order; or (e) the prevention of incitement of offences.

In case of an emergency, the prior approval of the aforementioned government officials may be dispensed with. In such a case, the interception or monitoring will have to be carried out by an officer not below the level of the Inspector General of Police.

Section 69 of the IT Act permits authorised government officials to intercept or monitor information transmitted, generated, received or stored in any computer. Accordingly, the service provider is required to extend all technical facilities, equipment and technical assistance to the authorised government officials to intercept the information and to provide information stored in the computer. The Interception Rules lay down the procedure to be followed by the government to authorise such interception or monitoring.

Under Section 69 of the IT Act read with Rule 3 of the Interception Rules, either the Secretary to the Ministry of Home Affairs (in the case of the central government) or the Secretary to the Home Department (in the case of the state government) or a person above the rank of Joint Secretary authorised by the relevant government department (in unavoidable circumstances), may issue an order for the interception of any electronic information transmitted, stored or generated over any computer, if the official in question believes that it is necessary to do so in: (a) the interest of sovereignty and integrity of India; (b) the security of the State; (c) friendly relations with foreign states; (d) public order; or (e) the prevention of incitement of offences.

The UASL, UL and the ISP License require the licensee to implement the necessary facilities and equipment for interception purposes in terms of the following provisions:

1) Clause 39.23 (xvi) of Part-I of the UL, Clause 41.20 (xvi) of the UASL and Clause 34.28 (xvi) of the ISP License require the licensee to ensure that the necessary hardware/software in their equipment is available for the carrying out of the lawful interception and monitoring from a centralised location.

2) Under Clause 23.2 of Part-I of the UL, Clause 41.7 of the UASL, and Clause 34.4 of the ISP License the licensee is required to install the equipment that may be prescribed by the government for monitoring purposes.

3) As per Clause 39.23 (xiv) of Part-I of the UL, Clause 34.28(xiv) of the ISP License and Clause 41.20 (xiv) of the UASL, in case of remote access of information, the licensee is required to install suitable technical devices enabling the creation of a mirror image of the remote access information for monitoring purposes.

4) Clause 8.2 of Part-II, Chapter VIII of the UL, and Clause 41.10 of the UASL License requires the licensee to install the necessary hardware/software to enable the government to monitor simultaneous calls.

Under Rules 12 and 13 read with Rule 19 of the Interception Rules, once the interception order has been issued as per Rule 3 of the Interception Rules, an officer not below the rank of the Additional Superintendent of Police shall make a written request to the intermediary to provide all facilities and the necessary equipment for the interception of the information.

Section 2(w) of the IT Act defines intermediary to include ‘telecom service providers, network service providers and internet service providers’.

LICENSES

Until 2013, the UASL was entered into between a telecom service provider and the DoT for the provision of access services. Similarly, until 2013, the ISP License was entered into between an internet service provider and the DoT for the provision of internet services. Both these licenses were granted typically for a period of 20 years. Under the UL, the UASL and the ISP License, licensees are bound to take all steps and provide all facilities to enable the government to carry out interception of communications. Clause 40.2 of Part-I of the UL, Clause 42.2 of the UASL and Clause 35.5 of the ISP License provide that the licensee must provide the necessary interception facilities as required under Section 5 of the IT ACT.

Clause 8.2 of Part-II of the UL, Clause 41.10 of the UASL and Clause 34.6 of the ISP License provide that designated government officials shall have the right to monitor the telecommunication traffic at any technically feasible point. The licensee is required to make arrangements for simultaneous monitoring by the government.

Clause 7.2 and 7.3 of Part-II, Chapter IX of the UL, Clause 34.8 of the ISP License, requires each ISP to maintain a log of all connected users and the service that they are using. The ISP is also required to maintain every outward login. The logs and the copies of all the packets originating from the Customer Premises Equipment (“CPE”) of the ISP must be available in real time to the government.

CENTRAL MONITORING SYSTEM

The Central Monitoring System (“CMS”) is an interception and monitoring project of the Government of India which was approved in 2011. There is no legislation authorising the setting up of the CMS. Minimal information is available through newspaper reports and Parliamentary Questions. The Minister of Communications and Information Technology of the Government of India confirmed in 2016 that the CMS was already operational in Delhi and Mumbai, and is being set up in phases.

CMS is intended to automate the process of the interception and monitoring in order to ensure that the Law Enforcement Agencies and the telecommunications and internet companies are not involved in the process of interception. Under the UASL with respect to the CMS, the licensee is required to provide the connectivity through dark fibre up to the nearest multi-protocol label switching network at its own cost. The UL also has provisions for the licensees to assist the government in centralised monitoring.

Disclosure of Communications Data

LEGISLATION

The Code of Criminal Procedure (“CrPC”) empowers a court or police officer in charge of a police station to seek the production of any ‘any document or other thing’ if the officer believes that said document is necessary for the purposes of any investigation.

Section 69 of the IT Act permits authorised government officials to intercept or monitor information transmitted, generated, received or stored in any computer. Accordingly, the service provider is required to extend all technical facilities, equipment and technical assistance to the authorised government

officials to intercept the information and to provide information stored in the computer.

LICENSES

Under the UL, the UASL and the ISP License Agreement, the licensee is required to provide access to all call data records as well any other electronic communication. Under Clause 8.3 of Part-II, Chapter VIII of the UL, and Clause 41.10 of the UASL, the licensee is required to provide the call data records of all the calls handled by the licensee as and when required by the government.

Clause 38.2 of Part-I of the UL, and Clause 33.4 of the ISP License requires the licensee to provide the government with the required tracing facilities to trace messages or communications, when such information is required for investigation of a crime or for national security purposes.

Section 91 of the CrPC permit a court or officer in charge of a police station to issue a summons or written order respectively, requiring the production of “any document or other thing... necessary or desirable for the purposes of any investigation, inquiry, trial or proceeding”.

Section 69 of the IT Act permits authorised government officials to “intercept or monitor information transmitted, generated, received or stored in any computer”. Accordingly, the service provider is required to extend all technical facilities, equipment and technical assistance to the authorised government officials to intercept the information and to provide information stored in the computer.

Interception has been defined under Rule 2(l) of the Interception Rules to include the acquisition of “the contents of any information” through any means in so far as it enables the content of the information to be made available to a person other than the intended recipient.

National Security and Emergency Powers

LEGISLATION

Under Section 5(1) of the ITA Act, if there is a public emergency or in the interest of public safety, the government believes it is necessary, the government has the power to temporarily take possession of the ‘telegraph’

established and maintained or worked on by any person authorised under the IT Act.

LICENSES

The government has the following special powers under the UASL and the ISP License:

- 1) Under Clause 39.16 of Part-I of the UL, Clause 41.13 of the UASL and Clause 10.5 of the ISP License; the government may “take over the service, equipment and networks of the licensee” in the event that such directions are issued in the public interest by the Government of India in the event of a national emergency, war, low-intensity conflict, or any other eventuality.
- 2) As per Clause 39.1 of Part-I of the UL, Clause 41.1 of the UASL and Clause 34.1 of the ISP License, the licensee must “provide necessary facilities depending upon the specific situation at the relevant time to the Government to counteract espionage, subversive act, sabotage or any other unlawful activity”.
- 3) Under Clause 39.24 of Part-I of the UL, Clause 41.5 of the UASL and Clause 5.1 of the ISP License, the government may revise the license Clauses at any time if “considered necessary in the interest of national security and public interest”.
- 4) In terms of Clause 39.15 of Part-I of the UL, Clause 41.11 of the UASL and Clause 34.9 of the ISP License, the government may, through appropriate notification, block the usage of mobile terminals in certain areas of the country. In such cases, the licensee must deny service in the specified areas within six hours of receiving the request.
- 5) Under Clause 39.23 (xviii) of Part-I of the UL, 41.20(xviii) of the UASL and Clause 34.28(xviii) of the ISP License, the government may restrict the licensee from operating in any sensitive area on national security grounds. In addition, Clause 33.7 of the ISP License and Clause 39.14 of the UL provide that the “use of the network for anti-national activities” (such as breaking into an Indian network) may be deemed sufficient reason to revoke the license, and will be considered an offence punishable under criminal law. The IT Act, the UASL and the ISP License do not prescribe the method and the instrument that the government may use in this regard.

Oversight of the Use of Powers

There is no judicial oversight over the interception process.

With respect to the review of the interception of telephonic communication under the IT Act and the ITR, a Review Committee has been established under Rule 419-A(16) of the ITR at both the central and the state level. As per the ITR, every order issued by the relevant government officials has to be sent to the Review Committee.

The Review Committee is required to meet once every two months and if the Review Committee is of the opinion that an interception order was not in accordance with the provisions of the IT Act and the ITR, it may set aside the interception order and also order the destruction of the information obtained through interception.

Rule 419-A (17) provides that in cases where the interception has been carried out in an emergency, the relevant government official has to be informed of such interception within three working days and the interception has to be confirmed within 7 working days, otherwise the interception will have to cease and the same message cannot be intercepted without the prior approval of Union or state Home Secretary.

A similar Review Committee has also been established under the Interception Rules. Rule 22 of the Interception Rules provides for the establishment of a Review Committee to examine the interception or monitoring directions. If the Review Committee is of the opinion that the interception or monitoring directions are not in accordance with Section 69 of the IT Act, then it may set aside the direction and also order the destruction of the information obtained through interception.

With respect to CMS there is no judicial oversight over the project. The Review process is the same as provided for under Rule 419-A of the ITR as described above.

upon, resulting work must be distributed under the same, similar, or compatible license. The license allows commercial use. • From time to time, the Global Network Initiative (“GNI”) provides information on this website. In providing any such information, GNI undertakes no obligation to update or otherwise modify that information to ensure that it is complete, up-to-date, or otherwise accurate. No statements, information, or communications on this website are intended to provide, nor should they be construed as GNI providing, any legal advice or legal opinions. GNI specifically notes that the information on this website may not necessarily reflect the current state of the law, or a complete statement of the law, in any particular jurisdiction. Furthermore, the factual information on this website may not be accurate, up-to-date, or complete. You should independently verify relevant facts and legal standards (including by seeking the advice of counsel) before taking any action or refraining to taking any action. GNI will not be responsible for any damage or loss arising from the use in any way of any information on this website, even if such information is deemed to be inaccurate, incomplete, untimely, or otherwise. You agree that your use of this site and any information contained herein is at your own risk. • Your use of this website and/or of the information provided on the website does not create any legal relationship between you and GNI, including but not limited to any attorney-client relationship. • The materials provided on this website are provided “as is” and “as available,” without warranty of any kind, express or implied. To the fullest extent permissible by law, GNI disclaims all express and implied warranties with regard to the use of this web site or the use of any information contained herein, including without limitation implied warranties of merchantability, fitness for a particular purpose, and non-infringement.



© Global Network Initiative 2019