

INTERMEDIARY: LIABILITIES AND DUTIES IN RESPECT OF MONITORING AND INTERCEPTING ENCRYPTED INFORMATION

1) Definition of Intermediary

As per Section 2(w) of the IT Act, 2000 “**Intermediary**” means any person who on behalf of another person receives, stores or transmits any particular electronic record or provides any service with respect to that record and **includes:**

- ★ Telecom service providers,
- ★ Internet service providers,
- ★ Search engines,
- ★ Online payment sites,
- ★ Online auction sites,
- ★ Online market places and
- ★ Cyber cafes

2) Acts and Rules/ Agreements governing monitoring, decrypting and intercepting sensitive encrypted information

The following Acts, rules and agreements govern liabilities and duties of an intermediary in respect of monitoring and decrypting information:

- ★ Indian Telegraph Act, 1885
- ★ Indian Telegraph Rules, 1951
- ★ Information Technology Act, 2000
- ★ Information Technology (Procedure and Safeguards for interception, Monitoring and Decryption of Information) Rules, 2009
- ★ Information Technology (Procedure and safeguards for Monitoring and collecting Traffic Data or Information) Rules, 2009
- ★ Information Technology (Intermediary) Rules, 2021
- ★ Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
- ★ Information Technology (Procedure and safeguards for blocking for access of information by public) Rules, 2009
- ★ Unified Access Service License Agreement/Internet Service Providers Agreement

3) Duties and liabilities of an intermediary in respect of monitoring, interception or decrypting encrypted information.

An intermediary (TSP/ISP) has to discharge bellow mentioned liabilities under various applicable statues, rules or agreements:

3.1 Liabilities under Unified Access Service License Agreement (UASL)

- ★ Under Clause 34.4 of the UASL agreement the licensee (TSP) is required to install the equipment that may be prescribed by the government for monitoring purposes.
- ★ Under Clause 39.1 of the UASL agreement the **Telecom service providers shall not employ bulk encryption equipment in its network**. Any encryption equipment connected to the TSP network for specific requirements has to have prior evaluation and approval of the LICENSOR or officer specially designated for the purpose. The TSP have responsibilities to ensure **protected communication takes place without violation of privacy** and to ensure no unauthorized interception of messages takes place.

For example **SEBI has prescribed a 64/128 bit encryption standard to secure transactions and online trading**

- ★ 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 41.20 (xvi) of the UASL agreement requires the licensee to provide the necessary hardware/software in their equipment to enable the government to enable interception and monitoring from a Centralized location.

3.2 Liabilities under Internet Service Providers License Agreement (ISPL)

- ★ The internet service provider has to ensure that any objectionable material or content which infringes copyright, Intellectual Property Right and international and domestic cyber laws shall not carry in its network
- ★ The ISP is obliged to provide, without delay, all the tracing facilities of the nuisance or malicious messages or communications transported through his equipment and network, to authorized officers of Government of India/State Government, when such information is required for investigations of crimes or in the interest of national security.

3.3 Rights or duties under Indian Telegraph Rules, 1951

- ★ As per **Rule 419 of the Indian Telegraph Rules, 1951** it shall be lawful for the Telegraph Authority to **monitor or intercept a message transmitted through telephone**, for the purpose of verification of any violation of these rules or for the maintenance of the equipment.

- ★ The Telecom service providers shall put in **place adequate and effective internal checks** to ensure that unauthorized interception of message. **(Rule 419A(14))**

3.4 Liabilities under Information Technology Act, 2000

- ★ Intermediaries to **preserve and retain the information. (Section 67C)**
- ★ To **comply with order issued by the competent authority** to grant access to computer resource for the purpose of intercepting, Monitoring or decrypting of information. **(Section 69)**
- ★ To **comply with order issued by the central Government** directing intermediary to block access by public any information contained in any computer resource. **(Section 69A)**
- ★ To protect the data privacy of the third party and not to disclose to any unauthorized person or entity without the third party consent to get wrongful gain or to cause wrongful loss to the third party. **(Section 43A)**
 - The Hon'ble Apex court in its significant decision in **Kharak Singh v. State of Uttar Pradesh and Ors.1962** case held that Article 21 of the Constitution of India does not include any provision for privacy, and hence the right to privacy cannot be considered as a fundamental right.
 - The decision of **Kharak Singh** case was overruled by the apex court in the matter of **Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors.(2017) 10 SCC 1** in which it held that the right to privacy is a part of the right to life and personal liberty enshrined under Article 21. Therefore, any party, complaining of privacy breach has the right to initiate appropriate legal proceedings, under writ jurisdiction, for the enforcement of their rights against the state.
- ★ Not to **disclose personal information of any person** through providing access to the user with the purpose of getting wrongful gain or causing wrongful loss to anyone. **(Section 72A)**

3.5 Liabilities under Information Technology (Procedure and safeguards for blocking for access of information) Rules, 2009

As per Rule 13 an intermediary shall **designate at least one person as (Designated Person)** to receive and handle the directions for blocking of access

by the public any information generated, transmitted, received, stored or hosted in any computer resource.

3.6 Liabilities under Information Technology (Procedure and safeguards for Monitoring and collecting Traffic Data or Information) Rules, 2009

- ★ Duty to **take utmost care** regarding unauthorized monitoring on collection of traffic data or information don't take place as well as to **maintain extreme secrecy** in respect of third party confidential information. **(Rule 5)**
- ★ **Vicarious liability** in respect of non-compliance of **Rule 9(3)** of IT (Procedure and safeguard for Monitoring and collecting Traffic Data or Information), Rules, 2009 by any employee of an intermediary. **(To maintain strict secrecy and confidentiality of information).**

3.7 Liabilities under Information Technology (Intermediary Guidelines) Rules, 2021

- ★ The Rule(3) of the Information Technology (Intermediaries Guidelines) Rules, 2021, (notified on 25.02.2021) which imposes following duties on an intermediary:
 - a) Intermediaries have to **publish rules and regulations (specifying prohibited acts)**, privacy policy as well as user agreement.
 - b) Intermediaries have to **disable such prohibited information within 36 hours** and **storage of same for 90 days** for investigation purposes,
 - c) Intermediaries to **assist authorized government agencies on demand.**
 - d) Intermediaries will **retain user information** collected during registration on computer resource **up-to 180 days** after the date of withdrawal or cancellation of registration.
 - d) Intermediaries to exercise **reasonable measures to secure its computer resource,**
 - e) Intermediaries to **report cyber security incidents to the Indian Computer Emergency Response Team (CERT).**
 - f) Intermediaries have to comply with IT ((Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011;
 - g) Intermediaries will upload on their platform information regarding **Grievance Redressal Mechanism as well as appoint Grievance Officer with contact details**, who will accept complaint about violation of these rules within 24 hours and resolve the same within 15 days from the date of acknowledging the complaint.

4) Exemption from any liability under IT Act, 2000

An intermediary is protected from any sort of liability imposed (under applicable statutes and rules) under following provisions:

4.1 Exemption from any liability under Section 79 of the IT Act,2000

As per this provision, also known as the **Safe Harbour Provision**, an intermediary is not liable for any third party information **if –**

- a) The intermediary has not any **knowledge or control over information** contained or stored in any computer resource for the purpose of granting access to public.
 - b) The intermediary **observes due diligence** to avoid any contravention of applicable acts or statutes while discharging its liabilities or duties.
- **Super Cassettes Industries Ltd. v. Myspace Inc. & Anr. 2011 (48) PTC 49 (Del)** held that intermediaries could be held liable only when-
 - (i) They have actual or specific knowledge and not constructive knowledge of the existence of infringing content on their website.
 - (ii) They do not take any steps to have such content removed
 - The SC in its important judgment in **Shreya Singhal v UOI 2015** held that an intermediary could not benefit from the immunity granted under Section 79 of the IT Act if upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts related to Article 19 are going to be committed, it fails to expeditiously remove or disable access to such material.
 - The court in **Kent RO Systems Ltd. & Anr. Vs. Amit Kotak& Ors. C.S. (COMM) 1655/2016** held that the intermediary is obligated to remove information hosted on its portal only on receipt of an order from the relevant governmental agency or pursuant to a court order.
 - In **Google India Private Ltd Vs. M/S. Visakha Industries,2019** the court observed that the section 79 of the IT Act, 2000 exempts Network Service Provider from liability only on proving that the offense or contravention was committed without its knowledge or that he had exercised all due diligence to prevent the commission of such offense or contravention

4.2 Exemption from any liability under Section 52(1) (c), of the Copy Right Act, 1957

As per section **52 (1) (c) of the Copy Right Act, 1957**the acts of intermediaries are exempted from copyright infringement saving they are conscious or have a reasonable basis for believing that work/content is an infringing copy.

The Hon'ble Delhi High court in **My Space Inc. v. Super Cassettes Industries Ltd. (2017)** categorized copyright matters observed, if intermediaries were handed the responsibility of identifying unlawful content, it could have dangerous effect on free speech. It might lead to private & invisible censorship that would be unconstitutional

Till date there is no such law which could protect citizen data privacy, although the parliament has initiated procedure to come out with such law by drafting **Personal Data Protection Bill, 2019**, which is still pending.

Currently, there is no specific data protection legislation or rules or Guidelines available. Till date there is no such law which could protect citizen data privacy, although the parliament has initiated procedure to come out with such law by drafting **Personal Data Protection Bill, 2019**, which is still pending.