Liability of Network Service Providers

This document is an extract from the book *Cyber Crime & Digital Evidence – Indian Perspective* authored by Rohas Nagpal. This book is available as courseware for the **Diploma in Cyber Law** and **PG Program in Cyber Law** conducted by Asian School of Cyber Laws

Asian School of Cyber Laws

www.asianlaws.org

21. Liability of Network Service Providers

According to section 79 of the IT Act

For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

Explanation.—For the purposes of this section,—

(a) "network service provider" means an intermediary;

(b) "third party information" means any information dealt with by a network service provider in his capacity as an intermediary;

This section seeks to restrict the liabilities of a network service provider in certain cases. Let us first understand the term “network service provider” (NSP). Section 79 says that an NSP is an intermediary. The IT Act has defined the term “intermediary”.

According to section 2(1)(w) of the IT Act

"intermediary" with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message;

An NSP, in respect of a particular electronic message, therefore has the following characteristics:

3. It **receives** the message on behalf of another person, or
4. It **stores** the message on behalf of another person, or
5. It **transmits** the message on behalf of another person, or
6. It **provides any service** with respect to that message.

The term “electronic message” has not been defined in the IT Act. The UNCITRAL Model Law on Ecommerce defines a **data message** as “information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy”.

Note: The IT Act has been based largely on the UNCITRAL Model Law on Ecommerce.

The IT Act has inserted section 88A into the Indian Evidence Act. This section relates to an electronic message forwarded through an electronic mail server.

After considering the definition of data message under the UNCITRAL Model Law and the context of electronic message under section 88A of the Indian Evidence Act, it may be concluded that the term NSP is a narrow term that relates to electronic message service providers only (such as email service providers).

It does not apply to other service providers such as search engines, auction websites etc. Even for Internet Service Providers (ISP), the benefits of this section would extend only to the email, voicemail, telephony etc services provided by them and not to the Internet connection services offered by them.

However, this section must be read in conjunction with section 85 of the IT Act that relates to liabilities of companies. This is discussed in the next chapter of this book.

Now let us examine the restrictions on the liabilities of NSPs. An NSP is not liable for any third party information or data made available by him if:

1. the NSP proves that the offence or contravention was committed without his knowledge, or

2. the NSP proves that he had exercised all due diligence to prevent the commission of such offence or contravention.

The important terms used in this section are:

Knowledge implies “clear perception of a fact” or “specific information”.

Illustration 1
Noodle Ltd is an email service provider. The Noodle management has read several articles in the newspapers that many people use email accounts to store and distribute pornography.

Sameer has signed up for an email account provided by Noodle Ltd. He is arrested by the police for suspected publication of cyber pornography.

In this case Noodle Ltd will not be liable for the offence. The Noodle management did not have specific knowledge about Sameer's misuse of the email account. They only had a vague and general knowledge about email accounts being misused by some unidentified people.

Illustration 2
Noodle Ltd is an email service provider. Sameer has signed up for an email account provided by Noodle Ltd. Another Noodle subscriber sends an email to the Noodle Customer Service department stating that Sameer is misusing his email account for spreading cyber pornography.

Noodle does not take any action. Many days later Sameer is arrested by the police for suspected publication of cyber pornography.

In this case, Noodle Ltd will be liable for the offence. Noodle Ltd had specific knowledge about Sameer's misuse of the email account.

All due diligence implies "such caution and foresight as the circumstances of the particular case demand".

Illustration
Noodle Ltd is an email service provider. Sameer has signed up for an email account provided by Noodle Ltd. Another Noodle subscriber sends an email to the Noodle Customer Service department stating that Sameer is misusing his email account for spreading cyber pornography.

Noodle Ltd immediately verifies the genuineness of the complaints and deactivates Sameer's account. It also keeps a check on new email accounts being created from the IP addresses previously used by Sameer to create and access his account.

Many days later Sameer is arrested by the police for suspected publication of cyber pornography. He was using a Noodle account that he had created from a cyber café using a fictitious name.

In this case Noodle Ltd will not be liable for the offence. Noodle Ltd had taken all due diligence.

Liability of ISPs in India

In respect to ISPs in India, their liabilities are also determined by the **License for Internet Services** based on guidelines dated 24th August, 2007.

The license as applicable on 30th October 2007 is provided in the CD ROM accompanying the ASCL publication titled "**Fundamentals of Cyber Law**".

According to **clause 33** of this license:

1. ISPs must prevent unlawful content, messages or communications from being carried on their network. This includes objectionable, obscene, unauthorized and other content.

2. Once specific instances of such content are reported to the ISP by the enforcement agencies, they must immediately prevent the carriage of such material on their network.

3. ISPs must ensure that content carried by them does not infringe "international and domestic cyber laws".

4. The use of ISP networks for anti-national activities would be construed as an offence punishable under the Indian Penal Code or other laws.

5. ISPs are required to comply with the IT Act provisions. They are responsible for any damages arising out of default in this compliance.

6. ISPs must ensure that their networks cannot be used to endanger or make vulnerable a networked infrastructure.

7. ISPs must ensure that their services are not used to break-in or attempt to break-in to Indian networks.

8. ISPs must provide, without any delay, all the tracing facilities to trace nuisance, obnoxious or malicious calls, messages or communications transported through their equipment and

network. These tracing facilities are to be provided to authorized officers of Government of India including Police, Customs, Excise, Intelligence Department officers etc.

9. ISPs must provide necessary facilities to the Government to counteract espionage, subversive acts, sabotage or any other unlawful activity.

According to **clause 34** of this license:

1. Government can monitor telecommunication traffic in the ISP network. The ISP has to pay for the necessary hardware and software for this monitoring.

2. ISPs must maintain a log of all users connected and the service they are using (mail, telnet, http etc.).

The term **telnet** can be explained through a simple illustration. Sameer runs a telnet program on his computer. Using the program he connects to Pooja's computer using a valid username and password. He then enters commands through the telnet program and these commands are executed directly on Pooja's computer.

http (hypertext transfer protocol) is the standard method for transferring websites on the Internet.

3. ISPs must also log every outward login or telnet through their computers. These logs, as well as copies of all the packets originating from the Customer Premises Equipment of the ISP, must be available in real time to the Telecom Authority.

Logs are computer based records of activities e.g. a log of a web server may contain details of the users who visited the website, their IP addresses, the Internet browsers used by them etc.

Data travels on the Internet in the form of **packets**. Each packet carries information that will help it get to its destination. This information includes:

a. the sender's IP address,
b. the intended receiver's IP address,
c. how many packets this e-mail message has been broken into
d. identification number of the particular packet.

Customer Premises Equipment (CPE) is the equipment and inside wiring located at a subscriber's premises and connected with the ISPs channels. E.g. Pooja has signed up for Noodle's Internet services. Noodle has placed a telephone, a modem and some wiring at Pooja's house. This equipment is for use with Noodle's services and is CPE.

Real time means instantaneous. In the current context it means that the packets and logs must be made available at the very instant that they are generated or transmitted.

4. ISPs must ensure privacy of communication on their network.

5. ISPs must ensure that unauthorized interception of messages does not take place on their networks.

6. The Government can takeover the service, equipment and networks of ISPs in case of emergency, war etc.

7. The complete and updated list of the ISP's subscribers must be available in a password protected portion of the ISP's website. This is for the use of authorized Intelligence Agencies.

8. In case of dedicated line customers, the ISP must maintain logs in the following format:

Customer name	IP Address allotted	Bandwidth provided	Address of Installation	Date of Installation / Commissioning	Contact person with Phone / email

9. The Chief Officer-In-Charge of technical network operations and the Chief Security Officer of the ISP should be a resident Indian citizen.

10. ISP must ensure that the information transacted by the subscribers is secure and protected.

11. The ISP officials dealing with the lawful interception of messages must be resident Indian citizens.

12. The majority Directors on the Board of the ISP must be Indian citizens.

13. Ministry of Home Affairs will regularly do security vetting in case foreigners are holding the positions of the Chairman, Managing Director, Chief Executive Officer (CEO) and/or Chief Financial Officer (CFO) of the ISP.

14. ISPs are required to physically monitor, on a monthly basis, those customers who have a high UDP traffic value.

UDP (user datagram protocol) is generally used for transmitting voice, streaming video, IP TV, voice over IP and online games.

Asian School of Cyber Laws

www.asianlaws.org

Head Office

6th Floor, Pride Senate,
Behind Indiabulls Mega Store,
Senapati Bapat Road,
Pune - 411016.
India

Contact Numbers

+91-20-25667148
+91-20-40033365
+91-20-64000000
+91-20-64006464

Email: info@asianlaws.org
URL: www.asianlaws.org