LatestLaws.com

Critical Analysis of Data Theft in Cyber Space

By: Shivani Johri

The word privacy has been derived from the Latin word "Privatus which mean separate from rest". It can be define as *capability of an individual or group secludes themselves or information about themselves and thereby reveal themselves selectively*. Privacy can be understood as a right of an individual to decide who can access the information, when they can access the information, what information they can access.

Privacy is recognized at international level as Human Rights in different dimension as

- **Privacy of person**
- **Privacy of personal behavior**
- **Privacy of personal communication**
- **Privacy of personal data.**

With advancement of latest technology for which many efforts at technological and legal level are done but still there is threat to information because the scope of privacy has been remain still untouched and to provide complete protection to information it is essential to cover the privacy. Although the digitization of data has created convenience in terms of Availability yet it has created havoc of data overflow that leads to difficulty in management of large data, it also includes personal and sensitive information like credit card information. Improper handling of this data can create damage and loss for individual as well Nation. Globalization and ICT revolution in India has changes the form of information drastically. It made information more accessible portable and handy but it had yet introduce some unforeseen mayhem and expose our private life has introduce some unforeseen mayhem and expose our private life.

Cyber-crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

LatestLaws.com

We can categorize Cyber-crimes in two ways-

The Computer as a Target :-using a computer to attack other computers.

e.g. Hacking, Virus/Worm attacks, DOS attack etc.

The computer as a weapon :-using a computer to commit real world crimes.

e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

Cyber Crime regulated by Cyber Laws or Internet Laws. VI. Proposed Frame work:

Data theft is defined in Section 43 (b) of the Information Technology Act, 2000 (IT Act) as follows: "If any person without permission of the owner or any other person who is in charge of a computer, computer system of computer network, downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network. It is the term used when any information in the form of data is illegally copied or taken from a business or other individual without his knowledge or consent."

"Data", in its intangible form, can at best be put at par with electricity. The question whether electricity could be stolen, arose before the Hon'ble Supreme Court in the case **"Avtar Singh vs. State of Punjab" (AIR 1965 SC 666).** Answering the question, the Supreme Court held that electricity is not a movable property, hence, is not covered under the definition of 'Theft' under Section 378 IPC. However, since Section 39 of the Electricity Act extended Section 378 IPC to apply to electricity, so it so became specifically covered within the meaning of "Theft". It is therefore imperative that a provision like in the Electricity Act be inserted in the IT Act, 2000 to extend the application of section 378 IPC to data theft specifically.

In the era of information technology (IT), data is an important raw material for all businesses, including brick and mortar companies, business process outsourcing units, banking, media and IT companies. Data has become an important tool as well as a weapon for corporates to capture larger market share. Given its importance, data security has become a big concern for all businesses. Data theft and piracy are huge threats that are forcing companies to spend millions of rupees on data analytics. In many cases, the bottom-line of a business depends on the security of its data. A recent episode of the popular television series, **Game of Thrones**, had kindled a huge discussion on data theft. Let us look at some of the issues involved in data security.

Mobility-related Issues: The problem with data theft is that it has no international borders. For example, a computer system may be accessed in the US, its data manipulated in China and

LatestLaws.com

the consequences of that action felt in India. The fact that cyber criminals can operate across different sovereignties, jurisdictions, laws and rules is an issue in itself. Collection of evidence, in such circumstances, is complex. It requires investigations to be conducted in three different countries which may not even be on talking terms with one another; poor technical know-how of our cops only adds to the woes. Lack of coordination between various investigating agencies and navigating the extradition process of various countries is another headache. The absence of specific laws to deal with the crime of data theft is, however, the biggest problem; it allows a culprit to get away by picking and choosing from various legal loopholes, even after being caught.

Our Data Protection Laws:

Data theft has emerged as one of the major cyber-crimes worldwide. India does not have specific laws to deal only with data protection, but we have the IT Act.

Section 43 (b) of the IT Act provides protection against unauthorised downloading, copying, extracting information, data or a database, by imposing heavy civil compensation which could run into crores of rupees. Section 43 (c) provides for compensation in case of unauthorised introduction of computer viruses or other contaminants. Clause (i) provides compensation for destroying, deleting or altering any information residing on a computer or diminishing its value.

Given the emergence of data theft, the law enforcement machinery may sometimes be unsure about the legal nature of the damage caused to the victim. The charges against the thief are framed based on the statement of the victim. It is therefore necessary that the victim is aware of the basic laws relating to information abuse. Some of the charges that can be filed against the perpetrator of data theft are listed below.

Charge: Criminal Breach of Trust

Section 405 and Section 408 of the IPC

Penalty: Imprisonment of up to 3 years, or fine, or both. If committed by an employee (servant), it attracts imprisonment of up to 7 years, or fine, or both.

What is Criminal Breach of Trust: -: "Whoever, being in any manner entrusted with property, or with any dominion over property, dishonestly misappropriates or converts to his own use that property, or dishonestly uses or disposes of that property in violation of any direction of law prescribing the mode in which such trust is to be discharged, or of any legal

LatestLaws.com

contract, express or implied, which he has made touching the discharge of such trust, or wilfully suffers any other person so to do, commits 'criminal breach of trust' "

Charge: Penalty and compensation for damage to computer, computer system

Section 43 of the IT Act

Penalty: Compensatory penalty of up to Rs. 1 Crore.

Legal Provision: "If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network -

(a) accesses or secures access to such computer, computer system or computer network or computer resource;

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under,

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means; (i) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a

LatestLaws.com

computer resource with an intention to cause damage, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected."

Charge: Computer Related Offences

Section 66 of the IT Act

Penalty: Imprisonment of up to 3 years, or fine of up to Rs. 5 Lakh, or both.

Legal Provision: "If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both."

Charge: Infringement of Copyright

Section 2(o) and Section 63 of the Copyright Act

Penalty: Monetary fine commensurate with the magnitude of the offense. Further, infringement of copyright is a criminal offence.

Legal Provision: "literary work" includes computer programmes, tables and compilations including computer data bases"

In addition to the above, if the stolen data is shared with other parties (such as competitors), the victim can bring an action of criminal conspiracy, collusion, and furtherance of common intention, which makes such other parties an accomplice in the commission of the stealing of data

Data is an intangible asset whose value could run into millions of dollars, but Section 43 does not quantify the compensation to be paid. Hence, a complainant is dependent on the mercy of our courts and the intelligence of his lawyer.

Section 65:

This section provides for computer source code. If anyone knowingly or intentionally conceals, destroys, alters or causes another to do as such shall have to suffer imprisonment of up to 3 years or fine up to 2 lakh rupees. Thus protection has been provided against tampering of computer source documents

LatestLaws.com

Section 70:

This section provides protection to the data stored in the protected system. Protected systems are those computers, computer system or computer network to which the appropriate government, by issuing gazette information in the official gazette, declared it as a protected system. Any access or attempt to secure access of that system in contravention of the provision of this section will make the person accessed liable for punishment of imprisonment which may extend to ten years and shall also be liable to fine.

Section 72:

This section provides protection against breach of confidentiality and privacy of the data. As per this, any person upon whom powers have been conferred under IT Act and allied rules to secure access to any electronic record, book, register, correspondence, information document of other material discloses it to any other person, shall be punished with imprisonment which may extend to two years or with fine which may extend to one lakh rupees or both.

Can Data Theft be covered under IPC?

Section 378 of the Indian Penal Code, 1860 defines 'Theft' as follows

Theft – Whoever, intending to take dishonestly any movable property out of the possession of any person without that person's consent, moves that property in order to such taking, is said to commit theft.

Section 22 of I.P.C., 1860 defines "movable property" as follows:

"The words "movable property" are intended to include corporeal property of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth."

Since Section 378 I.P.C., only refers to "Movable Property" i.e. Corporeal Property, and Data by itself is intangible, it is not covered under the definition of "Theft". However, if Data is stored in a medium (CD, Floppy etc.) and such medium is stolen, it would be covered under the definition of 'Theft', since the medium is a movable property. But, if Data is transmitted electronically, i.e., in intangible form, it would not specifically constitute theft under the IPC Copyright laws: Copyright Act, 1957 Data extraction involves copying, and hence copyright laws are first ones that are analysed. Under Section 2 (o) of the Copyright Act, 1957, defines data compilation (or a data set) as a "literary work". Section 14 of the Copyright Act, 1957

LatestLaws.com

further grants several exclusive rights in favour of the copyright holder (content creator) as the first owner of such copyrighted works (the data compilation / data set) namely: a. Right to reproduce data including storing it by any electronic means; b. Make copies of data; c. Adapt data; d. Communicate data to the public; and e. Translation of data

Section 51 of the Copyright Act further provides that a copyright is "deemed to be infringed" if any of the above enumerated rights under Section 14 are contravened without the permission of the copyright holder in the course of trade.

However, there are two areas that should be ascertained before determining infringement. Ownership, and no fair use exception. It is only the copyright holder / content owner can raise a claim. Hence in the case of a content aggregator – for various users, it is the users who own the copyright and not the content aggregator. This scenario occurs for websites where users generate the content – and the website is merely organizing the display / formatting of the content. **Section 52 of the Copyright Act** lists various exceptions to copyright and care should be taken that the content extracted has not been used under the purposes outlined for fair dealing.

Information Technology Act, 2002, as amended ("IT Act"): Section 10A of the IT Act provides for Validity of contracts formed through electronic means – Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

Accordingly, clickwrap, browse-wrap and other means of contract formation on the internet are covered under this clause. And most websites provide services to consumers under either of these means for contract formation. For example, if a person has to accept the terms of service, by clicking "I Agree" or typing in "I Agree" – it is commonly known as a clickwrap agreement. Under a browse-wrap agreement, a user may continue to use / browse a content owners website and consent of the user to the terms of the website are implied because the user continues to browse the website. In India, there are no judicial precedents involving a browsewrap or clickwrap agreement / contract.

LatestLaws.com

Does India have sufficient Laws?

The problem of data theft which has emerged as one of the major cyber-crimes worldwide has attracted little attention of law makers in India. Unlike U.K which has The Data Protection Act, 1984 there is no specific legislation in India to tackle this problem, though India boasts of its Information Technology Act, 2000 to address the ever-growing menace of cyber-crimes, including data theft. The truth is that our IT Act, 2000 is not well equipped to tackle such crime

How to file a complaint on data theft-

To file a complaint if data theft takes place, here are the following measures:

First of all, for the cyber complaint, write an application to the head of the cyber cell.

Provide the following things in the application:

Name

Address

Email address

Phone number

In case of hacking or say Data theft, the following details are required for cyber cell complaint:

Logs of the server

A hard copy and soft copy of the defected page

If the data of the defected site is compromised you will need a soft copy of the original data as well as the compromised data.

Control mechanisms details of access in which you have to tell who has accessed your computer.

If you have any doubt or you are feeling suspicious about anyone, then you have to provide the list of those suspicions.

You can file a complaint from any of the cyber cells of the city or you can directly mail at their respective websites. Here is the complete information of the prominent cyber cells of the country. You can refer this link for the same.

LatestLaws.com

How can companies prevent its employees or former employees to prevent them from committing data theft?

If the employees or the former employees of the company steals the data, the company has authority to punish them under **section 66A of the Information Technology Act, 2005** which penalises or imprisons on those who commit computer related offences like damage to computer system or network or steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage.

Non-Disclosure Agreement

Moreover, the provision of Non-Disclosure-Agreement is also one of the ways in which the company can stop its employees or former employees from stealing the data. By signing an NDA, the employees are legally by means of a contract bound not to disclose data and other relevant information of the companies to third parties outside the course of business.

To observe privacy In Indian work culture we have to adopt above framework which clearly define general guidelines of information addressing in different phases. In this we cover all the necessarily measures while considering the threat to privacy and try to remove vulnerability present in the system. This model mitigates the risk to privacy to the appetite level. So that further threaten to privacy will reduce its impact. We divide the privacy protection in four phases Data Collection, Data Security, Data Process, and Data Access which describe are as follows.

(a)Data Collection:-

First step of privacy protection is start with data collection itself, there must be strict data collection policy impose by the top authority which clearly mention the following points-

- **Information is collected by authorize appointed agency only.**
- **Information is collected for lawful purpose only.**
- **Personal data shall be adequate, relevant and not excessive.**
- **Purpose of information collection must be mention.**

If we capture the information properly then it is easy to maintain the information security in next steps. Government shall authorize the agencies for data collection government must also

LatestLaws.com

insure that they follow the regulation by doing periodic audit. Whenever information needs for collection it must be collected for lawful purpose only its commercial use is strictly avoided

(b)Data Security and Storage

After data capture, personal data shall be kept accurately and kept up-to-date. Appropriate technical and organizational measure shall be applied. Technical measures include all information security controls which are necessary to keep information security over internet. If data is store on the server then that server must be fully controlled by government of India. Server must be taken all security safeguard against unauthorized access, use and other modification. Organization measure includes classification of information according to its nature. 'Segregation of Duties' and 'Need to know' arranges the information according to its need no single person have full control over information user subject is fully mapped with its all information components.

(c) Data Process

Personal data shall be process fairly and lawfully here processing means not only computer processing. We have to process data only when the consent of user is involved, if the user is in contract and one of the party of the contract, process if it's required for judicial proceeding, process if its legitimate use for national interest, process if it's vital interest of data subject. Data should be process for only given purpose. After processing, the data must be properly disposed. Retention policy must be specified as including purpose and duration of retention.

(d) Data Access

The data access must follow Need to Know Basis. There must be control that information not goes beyond the Indian Territory. If data is going beyond territory then appropriate control must be taken to ensure that information is protected outside the India, there must be legal obligation between two countries about data handling. Within the country any Indian or non-government industry process the data they must have to follows all above the norms followed by the Indian government'(a) e-Governance

There is unique privacy challenges associated with e-governance due to large storage of personal and sensitive data. Obviously e-governance has given new dimension to development and globalization but there should be systematic improvements in governmental privacy leadership; and other technology-specific policy rules limiting, how the government collects and uses personally identifiable information. Government also has unparalleled opportunity to

LatestLaws.com

lead by example, by establishing strong, consistent rules that protect citizens without harming the government's ability of functioning. To achieve the specified goal we have to follow certain guidelines like:

 Creating a Union Chief Privacy Officer

 Installing chief privacy officers (CPOs) at all major departments

Shrikant Ardhapurkar et. al. / International Journal of Engineering Science and Technology

 Ensuring that Data Mining techniques are addressed by the Privacy Act

 Strengthening and standardizing privacy notices including "privacy impact assessments"

 Privacy Protection on agency website

 Complaint processing in case of breach of privacy

(b) e-Jurisdiction

Finally India got its first awaited model e-Court at the Ahmedabad City Evidently the implementation of e-court in India is in its commencing state The issues like privacy are still untouched. Without substantiation of the standard of technological framework and processes used by e-courts, the system of certainty upon which the courts and law are based has the potential to become inherently uncertain. It will be better to embed the privacy frame work to e court instead of including it later .The e-court must provide security and privacy of electronic filings. Court shall make any document that is filed electronically publicly available online."

 There must be unified and coherent policy for the privacy protection and access rights.

 Except where otherwise noted, the policies apply to both paper and electronic files.

 The availability of case files at the courthouse will not be affected or limited by these policies.

(c) e-Media

e-Media include television channels, radio, internet podcast, and all electronic journalism which are used by today's media. Main purpose of media is to bridge the gap between government policy and public grievances. As there is no information classification in India every information is floated over the media its adverse impact is seen at 26/11 incident all government moves are shown on TV channel which is used by terrorist as a feedback they

LatestLaws.com

make their attack strong. Privacy is most concern about celebrities but media is big threat to their privacy every gossip of celebrity is become a Breaking new in most of the new channel. Casting couch is very popular tool used by media now a day which directly hammer the individual privacy. There is no guideline to handle this issue privacy frame will provide solution to solve this problem.

(d) BPO

BPO is Business process outsourcing in IT/ITES industries. BPO play major role for revenue generation in India, complement to BPO there are other types of industries also well establish like KPO (Knowledge process outsourcing), LPO (Legal process outsourcing) and others this is majorly based on information processing. India's BPO industry grew 60 percent to US $6.6 billion in the fiscal year ending 31 March 2008, according to the National Association of Software and Service Companies (NASSCOM), in New Delhi. India's business process outsourcing, or BPO, industry says its security standards match the best in the world. There has never been a major instance of data theft in India. Nonetheless, companies in the United States do fear such an event, says Richard M. Rossow director of operations at the U.S.-India Business Council in Washington, D.C. The fear is "*not because they are at a higher risk of such a thing taking place in India, but rather because public perception of sending work to India is so bad that it will take only one major event for the affected company to 'pull the plug' on their India data service venture."*

If we do not ensure companies about strong privacy protection framework, we will lose outsourcing sector. We still rely on some international standard but unless if we not have legal framework, it will difficult to safeguard stake holder interest. Privacy at work place is also ignored field, thousands of workers are work in the premises as ‘people are the weakest link in information security’ there must be guideline at work place like cell phone are strictly avoided, prior screening of employee, all work under electronic surveillance, technology used to access employees computer.

(e)Telecommunication:

Service providers (SPs) including Internet service providers, number-database operators, telecommunications contractors, emergency call persons; public number directory publishers, authorized researchers and their respective employees must protect the confidentiality of information. The use or disclosure of any information or document which comes into their possession in the course of business must be restricted .This could apply,

LatestLaws.com

For example, to law enforcement officers who receive billing information, who may receive information in connection with their functions, publishers who receive information in connection with the publication and maintenance of a public number directory, or other service providers who may have received information for billing or network maintenance purposes.

(f) Health

Health sector is the important concern in privacy. Your health information includes any information collected about your health or disability, and any information collected in relation to a health service you have received.

Many people consider their health information to be highly sensitive. Before proceeding it is very important to consider what all the issues that come under Health Information are:

- **notes of your symptoms or diagnosis and the treatment given to you**
- **your specialist reports and test results**
- **your appointment and billing details**
- **your prescriptions and other pharmaceutical purchases**
- **your dental records**
- **your genetic information**
- **Any other information about your race, sexuality or religion, when collected by a health service provider.**

There is certain legislative framework also prepared in other countries for the privacy issue like HIPPA and PSQIA- Patient Safety Rule made by US government.

Keeping all this in mind it is mandatory to have a proposed system of health domain that mainly focused on privacy from Indian perspective. We must have administrative safeguard, technical safeguard, physical safeguard that will clearly define policy and procedure to provide safety of patient information. It covers issues like- there must be supported proceedings in case if someone disclose health information without consent of patient, there must be a written set of policy procedure and designate a officer responsible for implementing the procedure, Policy must clearly define class of employees that are allowed to access Electronic Patient Health Information, access of equipment that contains sensitive information must be properly

LatestLaws.com

monitored and controlled, protect your system from direct view of public, before transmitting any information must ensure the authenticity of the other party.

(g) E-Business

Indian economy majorly based on e-business outsourcing

We need a privacy framework purely focused on e-business and cover privacy issues and provide legal assistance in case of any fraud, crime .Issues that are need to cover under privacy framework like proper storage of sensitive credentials like credit card, safe credit of money during online transaction, Confidentiality, Integrity availability, authentication of party must be ensured before beginning of transaction, Encrypt the data before transmission of sensitive information, Restrict access based on need to know basis, assign unique identification to the parties that are involved in the business for authentication purpose. Also maintain the policy that addresses e-business privacy.

(h) Tourism

India is the vast combination of heritage and culture. Due to this reason it generates most of the revenue 6.23% to the national GDP and 8.78% of the total employment in India from the tourism industry. When tourist visits in India they perform several transaction, but there is no guarantee that this provided information is not further misused Each tourist must have right that their information is protected, corrected, erased as per their wish. Employing the most appropriate physical and technical measures, staff training and awareness, to ensure that unauthorized access to, alteration or destruction of personal data does not take place. Similarly, for the Medical Tourism the personal information of the patient must be protected. After the completion of the transaction the credit card information must be destroyed If such issues are covered in the privacy framework of the tourism then it must add on in Indian revenue, tourist feel safe while visiting the country, it also reduce the crime rate.

(i)National Security Surveillance

The collection of personal information by means of a surveillance system is lawful and justifiable as a policy choice, and if so, it must be ensured how privacy protective measures can be built into the system. " Reasonable expectation of privacy" is one of the keys to surveillance being legal. Using surveillance systems to address concrete, confirmed problems and/or incidents is acceptable only if the practice meets all statutory requirements. The activities like Access, Use, Disclosure, Retention, Security and

LatestLaws.com

Disposal of Surveillance Records must be regulated -

- **Prior to adopting a proposed surveillance program/practice an assessment of the impact on privacy is necessary**
- **Public bodies should consider public consultations prior to introducing surveillance and inform those impacted once adopted**
- **The design and operation of surveillance program/practice should minimize privacy intrusion to what is absolutely necessary to achieve its goals like designing and installing Surveillance Equipment**
- **System operators require privacy-sensitivity training**

It's a matter of preserving national security, heritage, culture and life of each citizen. When we talk about national security with privacy concern then it is more focused on the safeguard of country sensitive information, agreement and security policies. Privacy of national security can be breached when espionage like activity can be performed by an individual to harm the reputation of the country.

With respect to national security there is exemption of privacy from it. Must have separate framework with proper defined national security privacy guidelines. It must include that the government has authority to investigate about any citizen, can seize any personal information regarding an individual when it mounts to National Security, because it is primary and foremost concern. Authority can access information anytime whether it belongs to private and public interest if they found susceptible or threat to national security. It has overall authority as it is deal with the preservation of millions of life.

Net neutrality case study-

Net neutrality is the principle that Internet service providers treat all data on the Internet equally, and not discriminate or charge differently by user, content, website, platform, application, type of attached equipment, or method of communication. For instance, under these principles, internet service providers are unable to intentionally block, slow down or charge money for specific websites and online content. This is sometimes enforced through government mandate. These regulations can be referred to as "common carrier" regulations. This does not block all abilities that Internet service providers have to impact their customer's services. Opt-in/opt-out services exist on the end user side, and filtering can be done on a local

LatestLaws.com

basis, as in the filtration of sensitive material for minors. Net neutrality regulations exist only to protect against misuse. As of August 2015, there were no laws governing net neutrality in India, which would require that all Internet users be treated equally, without discriminating or charging differentially by user, content, site, platform, application, type of attached equipment, or mode of communication. There have already been a few violations of net neutrality principles by some Indian service providers. The government has once again called in for comments and suggestions regarding net neutrality as of 14 August, and has given the people one day to post their views on the mygov forum. After this, the final decision regarding the debate will be made. On 28 November 2017 the TRAI released its recommendations on Net Neutrality. With that, India is one step closer to ensuring that net neutrality is enforced nationwide.

The debate on network neutrality in India gathered public attention after Airtel, a mobile telephony service provider in India, announced in December 2014 additional charges for making voice calls (VoIP) from its network using apps like WhatsApp, Skype, etc.

In March 2015, Telecom Regulatory Authority of India (TRAI) released a formal consultation paper on Regulatory Framework for Over-the-top (OTT) services, seeking comments from the public. The consultation paper was criticised for being one sided and having confusing statements. It received condemnation from various politicians and Indian Internet users. The last date for submission of comment was 24 April 2015 and TRAI received over a million emails.

On 8 February 2016, TRAI took a revolutionary decision, prohibiting telecom service providers from levying discriminatory rates for data, thus ruling in favor of Net Neutrality in India. This move was welcomed by millions of Indians and also by people from other countries who are fighting or fought for net neutrality , and the inventor of the World Wide Web, Tim Berners Lee.

2017

On 28 November 2017 the TRAI released its recommendations on Net Neutrality. With that, India is one step closer to ensuring that net neutrality is enforced nationwide. Telecom minister Manoj Sinha said on 12 December that the TRAI's recommendations were similar to the views expressed by a DoT committee in 2015 that had also acknowledged the need for net neutrality and suggested allowing for legitimate traffic management. It had, however, disallowed

LatestLaws.com

exploitative or anti-competitive traffic management, app-based specific control within the Internet traffic and traffic prioritization on paid basis.

2018

On 14 June 2018, BEREC and TRAI have published a Joint Statement for an Open Internet.

On 11 July 2018, the Department of Telecommunications has approved TRAI recommandations on Net neutrality

There are no laws enforcing net neutrality in India. Although TRAI guidelines for the Unified Access Service license promotes net neutrality, it does not enforce it. The Information Technology Act, 2000 also does not prohibit companies from throttling their service in accordance with their business interests. In India, telecom operators and ISPs offering VoIP services have to pay a part of their revenues to the government.

Violations of net neutrality have been common in India. Examples beyond Facebook's Internet.org include Aircel's Wikipedia Zero along with Aircel's free access to Facebook and WhatsApp, Airtel's free access to Google, and RCom's free access to Twitter

Conclusion-

At 462.12 million, India has the second highest number of internet users in the world after China but lacks the legal framework to ensure data protection and privacy with current laws inadequate for the rapidly-evolving sector, say cyber security experts.

These are the laws which are applicable in today's era for the prevention of data theft. Though these laws have been made by the legislature there is no proper implementation of these laws. Neither the executory body nor the caretakers have taken these laws seriously. On the other hand, when we talk about the citizens, they are even hardly aware of these laws.

This has led to a lot of increasing cyber-crimes including data theft in the I.T. sector. So it is the sheer need to make these people aware of these laws and direct the concerned authority for proper implementation and lodging proper complaints and providing justice to the victims. It is a common responsibility of the government and judiciary to seriously look into the laws and take strict actions if these laws are being violated in any form, be it by any person like the police officer, and common man, just anyone.