PRIVACY AND THE INFORMATION TECHNOLOGY ACT,2000

R.R.NANDIGA RUBAVARSHINI
Student, Fifth year, B.AB.L (HONS) ,SAVEETHA UNIVERSITY

Abstract:
The concept of privacy differs from society to society. The concept of privacy in modern times is not restricted to mere physical movement or domiciliary surveillance, but also encompasses protection of a wide range of information, whether it's medical, financial, biometric or personal etc. India does not have specific legislation to deal with issues of privacy, however the Information Technology Act 2000 provides protection in the form of damages in case of failure to protect data and criminal liability in case wrongful disclosure of information in breach of a lawful contract. Protection of data is an important concern as it protects ones right to privacy, further stolen data can be a matter for concern as it can be misused for personal gain and to cause loss to another person. This paper deals with Privacy and the Information Technology Act, 2000 as there is no specified legislation to deal with Privacy.

Keywords:
- Data protection
- Security
- Lawful interception
- Unlawful interception
- Hacking

Introduction:
The Indian Parliament enacted an act called Information Technology Act, 2000. It received the assent of the President on the 9th June, 2000 and its effective from 17th October, 2000, this act is based on the Resolution adopted by the General Assembly of the United Nations on 30th January, 1997 regarding the Model Law on Electronic Commerce earlier adopted by the United Nations lCommission on International Trade Law (UNCITRAL) in its 29th session. It is significant to note that by enactment of the Information Technology Act, 2000, the Indian Parliament provided a new legal idiom to data protection and privacy.

What provision within the IT ACT shield against violation of privacy?
At the offset, it might be pertinent to notice that the IT Act defines a 'computer resource'; ebulliently as as well as a "computer, system, electronic network, data, pc information base or software". As is clear, this definition is wide enough to hide most intrusions that involve any transmission devices or networks – as well as mobile networks. Briefly, the IT Act provides for each civil liability and criminal penalty for variety of specifically verboten activities involving use of a computer– several of that touch privacy directly or indirectly. These are examined well within the following subsections.

Intrusions into pcs associated mobile devices: Section forty three of the IT Act forbids the subsequent actions once performed on or in relevancy a 'computer resource' while not getting the permission of the owner or person to blame of it: (a) accessing (b) downloading/copying/extraction {of information of knowledge of information} or extracts any information (c) introduction of computer contamination or malicious program (d) inflicting injury either to the pc resource or data residing on that (e) disruption (f) denial of access (g) facilitating access by an unauthorized person (h) charging the services availed of by someone to the account of another person, (i) destruction or decreasing valuable of data (j) stealing, concealing, destroying or fixing ASCII text file with associate intention to cause injury.

The Act provides for the civil remedy of "damages by approach of compensation" for damages caused by any of those actions. additionally anyone UN agency "dishonestly" and "fraudulently" will any of those specific acts is at risk of be penalised with imprisonment for a term of up to 3 years or with a fine which can touch 5 100000 rupees, or with each .
BANGALORE tekki condemned FOR HACKING GOVT website

In November 2009, the extra Chief Metropolitan judge, Egmore, Chennai, sentenced N G Arun Kumar, a tekki from urban center to bear a rigorous imprisonment for one year with a fine of Rs five,000 beneath section 420 IPC (cheating) and Section sixty six of IT Act (hacking). Investigations had unconcealed that Kumar was work on to the BSNL broadband net affiliation as if he was the authorised real user and 'made alteration within the database relating broadband net user accounts' of the subscribers. The CBI had registered a cyber crime case against Kumar and disbursed investigations on the idea of a criticism by the Press data Bureau, Chennai, that detected the unauthorised use of broadband net. The criticism additionally expressed that the subscribers had incurred a loss of Rs thirty eight,248 because of Kumar's wrongful act. He wont to 'hack' sites from urban center as additionally from metropolis and different cities, they said.

Childrens privacy online:
As computers and also the net become omnipresent kids have progressively become exposed to crimes like smut and stalking that create use of their non-public data. The fresh inserted section 67B of the IT Act (2008) makes an attempt to safeguard the privacy {of kids|of youngsters|of kids} below eighteen years by making a brand new increased penalty for criminals UN agency target children.

The section first of all penalizes anyone engaged in porn. Thus, anyone UN agency "publishes or transmits" any material that depicts kids engaged in sexually specific conduct, or anyone UN agency creates, seeks, collects, stores, downloads, advertises or exchanges this material is also penalised with imprisonment upto 5 years (seven years for repeat offenders) and with a fine of upto Rs. 10 lakhs. Secondly, this section punishes the web enticement of youngsters into sexually expressly acts, and also the facilitation of kid abuse, that also are punishable as higher than. Viewed along, these provisions request to carve out a restricted domain of privacy for kids from would-be sexual predators.

In addition, the fresh free Draft intercessor Due-Diligence tips, 2011 need 'intermediaries'to give notice users to not store, update, transmit and store any data that's entomb alia, "pedophilic" or "harms minors in any way". associate intercessor UN agency obtains data of such data is needed to "act with efficiency to figure with user or owner of such data to get rid of access to such data that's claimed to be infringing or to be the topic of infringing activity". Further, the intercessor is needed to tell the police regarding such data and preserve the records for ninety days.

Electronic voyeurism:
Although once thought to be solely the things of spy cinema, the explosion in client physical science has down the prices and also the size of cameras to such associate extent that the threat of hidden cameras recording people's intimate moments has become quite real. Responding to the growing trend of such electronic paraphilia, a brand new section 66E has been inserted into the IT Act that penalizes the capturing, publication and transmission of pictures of the "private area"of anyone while not their consent, "under circumstances violating the privacy" of that person.

This offence is punishable with imprisonment of upto 3 years or with a fine of upto Rs. 2 100000 or each.

Phishing or identity theft:

The word 'phishing' is usually wont to describe the offence of electronically impersonating somebody else for gain. this can be oft done either by mistreatment somebody else's login credentials to realize access to protected systems, or by the unauthorized application of somebody else's digital signature within the course of electronic contracts. progressively a brand new style of crime has emerged whereby sim cards of mobile phones are 'cloned' sanctionative miscreants to form calls on others' accounts. this can beadditionally a kind of fraud.

Who may lawfully intercept:

Section sixty nine empowers the "Central Government or a authorities or any of its officers specially authorised by the Central Government or the authorities, because the case could be" to exercise powers of interception below this section.

Under the Interception Rules 2009, the secretary within the Ministry of Home Affairs has been selected because the "competent authority", with reference to the Central Government, to issue directions concerning interception, observance and decoding. Similarly, the several state secretaries accountable of Home Departments of the varied states and union territories square measure selected as "competent authorities" to issue directions with reference to the authorities. just in case of emergency, t would be permissible to hold out interception once getting the orders of the pinnacle or second senior most officer of security and enforcement at the central level, and a licensed officer not below the rank of military officer of Police at the state or union territory level. The order should be communicated to the competent authority at intervals 3 days of its issue, and approval should be obtained from the authority at intervals seven operating days, failing that the order would lapse.

Where a state/union territory desires to intercept/monitor or rewrite info on the far side its territory, the competent authority for that state should create an invitation to the competent authority of the Central Government to issue applicable directions.

Purposes that interception is also directed:

Under section sixty nine, the powers of interception is also exercised by the approved officers "when they're happy that it's necessary or expedient" to try to to therefore within the interest of:

- sovereignty or integrity of Asian nation
- defense of Asian nation,
- security of the state,
- friendly relations with foreign states or
- public order or
- preventing incitement to the commission of any knowable offence with reference to higher than or
- for investigation of any offence

  Under section 69B, the competent authority could issue directions for observance for a variety of "cyber security" functions as well as, inter alia, "identifying or following of a person UN agency has broken, or is suspected of getting broken or being probably to breach cyber security".

Duration of interception and periodic review:

Once issued, AN interception direction issued below section sixty nine remains effective for

a amount of sixty days (unless withdrawn earlier), and will be revived for a complete amount not surpassing one hundred eighty days . A direction issued below section 69B doesn't expire mechanically through the lapse of your time and on paper would continue till withdrawn.

Within seven days of its issue, a replica of a direction issued below either section sixty nine or section 69B should be forwarded to committee ingrained to administrate wiretapping below the Indian Telegraph Act each 2 months, the review committee is needed to fulfill and record its findings on whether or not the direction was with validity issued in lightweight of section 69(3). If the review committee is of the opinion that it absolutely was not, it will put aside the direction and order destruction of all info collected.

Section sixty nine stipulates a penalty of imprisonment upto a term of seven years and fine for any "subscriber or go-between or a person UN agency fails to help the agency" sceptered to intercept.

Unlawful intercept:

In August 2007, Lakshmana Kailash K., a technician from Bangalore was inactive on the suspicion of getting announce insulting pictures of Chhatrapati Shivaji, a serious historical figure within the state of Maharashtra, on the social-networking website Orkut. The police known him supported IP address details obtained from Google and Airtel – Lakshmana's ISP. He was dropped at Pune and detained for fifty days before it absolutely was discovered that the IP address provided by Airtel was incorrect. the error was manifestly as a result of the very fact that whereas requesting info from Airtel, the police had not properly specified whether or not the suspect had announce the content at 1:15 p.m. or a.m.

Taking cognizance of his plight from newspaper accounts, the State Human Rights Commission after ordered the corporate to pay Rs a pair of hundred thousand to Lakshmana as damages .

Conclusion:

Thus from the above it could be concluded that even though there are various provisions in the Information Technology Act, 2000 to protect privacy but in reality it is not efficient enough to protect privacy of the people from the intruders. Thus it should be effectively implemented with growing needs of the society as it there is no specified legislation to protect privacy.

Books referred:

- **Information technology act,2000 bare act.**
- Information technology ,author vakul Sharma,third edition.

Websites referred:

- **www.google.com**
- **www.yahoo.com**
- **www.legalservices.com**