# Privacy and the Information Technology Act — Do we have the Safeguards for Electronic Privacy?

**How do the provisions of the Information Technology Act measure up to the challenges of privacy infringement? Does it provide an adequate and useful safeguard for our electronic privacy? Prashant Iyengar gives a comprehensive analysis on whether and how the Act fulfils the challenges and needs through a series of FAQs while drawing upon real life examples.**

## What kinds of computer related activities impinge on privacy?

Although Information and Communications Technologies (ICTs) have greatly enhanced our capacities to collect, store, process and communicate information, it is ironically these very capacities of technology which make us vulnerable to intrusions of our privacy on a previously impossible scale. Firstly, data on our own personal computers can compromise us in unpleasant ways — with consequences ranging from personal embarrassment to financial loss. Secondly, transmission of data over the Internet and mobile networks is equally fraught with the risk of interception — both lawful and unlawful — which could compromise our privacy. Thirdly, in this age of cloud computing when much of "our" data — our e-mails, chat logs, personal profiles, bank statements, etc., reside on distant servers of the companies whose services we use, our privacy becomes only as strong as these companies' internal electronic security systems. Fourthly, the privacy of children, women and minorities tend to be especially fragile in this digital age and they have become frequent targets of exploitation. Fifthly, Internet has spawned new kinds of annoyances from electronic voyeurism to spam or offensive e-mail to 'phishing' — impersonating someone else's identity for financial gain — each of which have the effect of impinging on one's privacy.

Although there are a number of technological measures through which these risks can be reduced, it is equally important to have a robust legal regime in place which lays emphasis on the maintenance of privacy. This note looks at whether and how the Information Technology Act that we currently have in India measures up to these challenges of electronic privacy [1].

## What provisions in the IT Act protect against violations of privacy?

At the outset, it would be pertinent to note that the IT Act defines a 'computer resource'; expansively as including a "computer, computer system, computer network, data, computer database or software" [2]. As is evident, this definition is wide enough to cover most intrusions which involve any electronic communication devices or networks — including mobile networks. Briefly, then IT Act provides for both civil liability and criminal penalty for a number of specifically proscribed activities involving use of a computer — many of which impinge on privacy directly or indirectly. These will be examined in detail in the following sub-sections.

Intrusions into computers and mobile devices

- accessing
- downloading/copying/extraction of data or extracts any data

- introduction of computer contaminant[3];or computer virus[4]
- causing damage either to the computer resource or data residing on it
- disruption
- denial of access
- facilitating access by an unauthorized person
- charging the services availed of by a person to the account of another person,
- destruction or diminishing of value of information
- stealing, concealing, destroying or altering source code with an intention

The Act provides for the civil remedy of "damages by way of compensation" for damages caused by any of these actions. In addition anyone who "dishonestly" and "fraudulently" does any of these specified acts is liable to be punished with imprisonment for a term of upto three years or with a fine which may extend to five lakh rupees, or with both [5].

**Bangalore techie convicted for hacking govt site** (2009, Deccan Herald)[6]

In November 2009, The Additional Chief Metropolitan Magistrate, Egmore, Chennai, sentenced N G Arun Kumar, a techie from Bangalore to undergo a rigorous imprisonment for one year with a fine of Rs 5,000 under section 420 IPC (cheating) and Section 66 of IT Act (hacking).
Investigations had revealed that Kumar was logging on to the BSNL broadband Internet connection as if he was the authorised genuine user and 'made alteration in the computer database pertaining to broadband Internet user accounts' of the subscribers.

The CBI had registered a cyber crime case against Kumar and carried out investigations on the basis of a complaint by the Press Information Bureau, Chennai, which detected the unauthorised use of broadband Internet.

The complaint also stated that the subscribers had incurred a loss of Rs 38,248 due to Kumar's wrongful act. He used to 'hack' sites from Bangalore as also from Chennai and other cities, they said.

### Children's privacy online

As computers and the Internet become ubiquitous children have increasingly become exposed to crimes such as pornography and stalking that make use of their private information. The newly inserted section 67B of the IT Act (2008) attempts to safeguard the privacy of children below 18 years by creating a new enhanced penalty for criminals who target children.

The section firstly penalizes anyone engaged in child pornography. Thus, any person who "publishes or transmits" any material which depicts children engaged in sexually explicit conduct, or anyone who creates, seeks, collects, stores, downloads, advertises or exchanges this material may be punished with imprisonment upto five years (seven years for repeat offenders) and with a fine of upto Rs. 10 lakh.

Secondly, this section punishes the online enticement of children into sexually explicitly acts, and the facilitation of child abuse, which are also punishable as above.

Viewed together, these provisions seek to carve out a limited domain of privacy for children from would-be sexual predators.

The section exempts from its ambit, material which is justified on the grounds of public good, including the interests of "science, literature, art, learning or other objects of general concern". Material which is kept or used for bona fide "heritage or religious purpose" is also exempt.

In addition, the newly released Draft Intermediary Due-Diligence Guidelines, 2011 [7] require 'intermediaries'[8]to notify users not to store, update, transmit and store any information that is inter alia, "pedophilic" or "harms minors in any way". An intermediary who obtains knowledge of such information is required to "act expeditiously to work with user or owner of such information to remove access to such information that is claimed to be infringing or to be the subject of infringing activity". Further, the intermediary is required to inform the police about such information and preserve the records for 90 days.

**Electronic Voyeurism**

Although once regarded as only the stuff of spy cinema, the explosion in consumer electronics has lowered the costs and the size of cameras to such an extent that the threat of hidden cameras recording people's intimate moments has become quite real. Responding to the growing trend of such electronic voyeurism, a new section 66E has been inserted into the IT Act which penalizes the capturing, publishing and transmission of images of the "private area" [9]of any person without their consent, "under circumstances violating the privacy" [10] of that person.

This offence is punishable with imprisonment of upto three years or with a fine of upto Rs. two lakh or both.

**Phishing – or Identity Theft**

The word 'phishing' is commonly used to describe the offence of electronically impersonating someone else for financial gain. This is frequently done either by using someone else's login credentials to gain access to protected systems, or by the unauthorized application of someone else's digital signature in the course of electronic contracts. Increasingly a new type of crime has emerged wherein sim cards of mobile phones have been 'cloned' enabling miscreants to make calls on others' accounts. This is also a form of identity theft.

Two sections of the amended IT Act penalize these crimes:

Section 66C makes it an offence to "fraudulently or dishonestly" make use of the electronic signature, password or other unique identification feature of any person. Similarly, section 66D makes it an offence to "cheat by personation" [11] by means of any 'communication device'[12] or 'computer resource'.

Both offences are punishable with imprisonment of upto three years or with a fine of upto Rs. one lakh.

**Mumbai Police Solves Phishing scam** [13]

In 2005, a financial institute complained that they were receiving misleading e-mails ostensibly emanating from ICICI Bank's e-mail ID.

An investigation was carried out with the e-mails received by the customers of that financial institute and the accused were arrested. The place of offence, Vijaywada was searched for the evidence. One laptop and mobile phone used for committing the crime was seized.

The arrested accused had used open source code e-mail application software for sending spam e-mails. He had downloaded the same software from the Internet and then used it as it is.

He used only VSNL to spam the e-mail to customers of the financial institute because VSNL e-mail service provider does not have spam box to block the unsolicited e-mails.

After spamming e-mails to the institute customers he got the response from around 120 customers of which 80 are genuine and others are not correct because they do not have debit card details as required for e-banking."

The customers who received his e-mail felt that it originated from the bank. When they filled the confidential information and submitted it the said information was directed to the accused. This was possible because the dynamic link was given in the first page (home page) of the fake website. The dynamic link means when people click on the link provided in spam that time only the link will be activated. The dynamic link was coded by handling the Internet Explorer onclick () event and the information of the form will be submitted to the web server (where the fake website is hosted). Then server will send the data to the configured e-mail address and in this case the e-mail configured was to the e-mail of the accused. All the information after phishing (user name, password, transaction password, debit card number and PIN, mother's maiden name) which he had received through the Wi-Fi Internet connectivity of Reliance.com was now available on his Acer laptop.

This crime was registered under section 66 of the IT Act, sections 419, 420, 465, 468 and 471 of the Indian Penal Code and sections 51, 63 and 65 of the Indian Copyright Act, 1957 which attract the punishment of three years imprisonment and fine upto Rs 2 lakh which the accused never thought of.

### Spam and Offensive Messages

Although the advent of e-mail has greatly enhanced our communications capacities, most e-mail networks today remain susceptible to attacks from spammers who bulk-e-mail unsolicited promotional or even offensive messages to the nuisance of users. Among the more notorious of these scams is/was the so-called "section 409 scam" in which victims receive e-mails from alleged millionaires who induce them to disclose their credit information in return for a share in millions.

Section 66A of the IT Act attempts to address this situation by penalizing the sending of:

- any message which is grossly offensive or has a menacing character
- false information for the purpose of causing annoyance, inconvenience, danger, insult, criminal intimidation, enmity, hatred or ill-will

- any electronic e-mail for the purpose of causing annoyance or inconvenience, or to deceive the addressee about the origin of such messages;

This offence is punishable with imprisonment upto three years and with a fine[14]

**Hoax E-mails** [15]

In 2009, a 15-year-old Bangalore teenager was arrested by the cyber crime investigation cell (CCIC) of the city crime branch for allegedly sending a hoax e-mail to a private news channel. In the e-mail, he claimed to have planted five bombs in Mumbai, challenging the police to find them before it was too late.

According to police officials, at around 1p.m. on May 25, the news channel received an e-mail that read: "I have planted five bombs in Mumbai; you have two hours to find it." The police, who were alerted immediately, traced the Internet Protocol (IP) address to Vijay Nagar in Bangalore. The Internet service provider for the account was BSNL, said officials.

**Minor Hoax Spells Major Trouble**

- Sixteen-year-old Rakesh Patel (name changed), a student from Ahmedabad, sent an e-mail to a private news channel on March 18, 2008, warning officials of a bomb on an Andheri-bound train. In the e-mail, he claimed to be a member of the Dawood Ibrahim gang. Three days later, the crime investigation cell (CCIC) of the city police arrested the boy under section 506 (ii) for criminal intimidation. He was charge-sheeted on November 28, 2008.
  Status: Patel was given a warning by a juvenile court.

- A 14-year-old Colaba boy sent a hoax e-mail to a TV channel in Madhya Pradesh, three days after the July 26, 2008, Ahmedabad bomb blasts. He claimed that 29 bombs would go off in Jabalpur. He was picked up by officers of the anti-terrorism squad (ATS) who, with the help of the MP police, were able to trace the e-mail to a cyber café in Colaba.
  Status: No FIR was registered. The Cuffe Parade police registered a non-cognizable (NC) complaint against him, and the boy was allowed to go home after the police gave him a "strict warning".

- Shariq Khan, 18, was arrested in Bhopal on July 26, 2006, for sending out three e-mails claiming to be a member of the terrorist organisation, which the police believed was behind the 7/11 train bombings. He was arrested by the Bhopal police. Later, the ATS brought the boy to Mumbai and also booked him for a five-year-old unsolved case where an unknown accused had sent e-mail warnings to the department of Atomic Energy (DAE) in 2001.
  Status: The police filed a charge-sheet against Shariq who claimed that he had sent the e-mails for fun. Trial is pending in a juvenile court. Shariq is presently out on bail in Bhopal.

- On February 26, 2006, a 17-yearold student from Jamnabai Narsee School called an Alitalia flight bound to Milan at 2 a.m. telling them there was a bomb on board. He wanted to stop his girlfriend from going abroad. She was one of the 12 students on their way to attend a mock United Nations session in Geneva. Status: After being grilled by the police, he was arrested, but let out on bail.

# Lawful Interception and monitoring of electronic communications under the IT Act

In addition to violations of privacy by criminal and the mischievous minded, electronic communications and storage are also a goldmine for governmental supervision and surveillance. This section provides a brief overview of the provisions in the IT Act which circumscribe the powers of the state to intercept electronic communications. The newly amended IT Act completely rewrote its provisions in relation to lawful interception. The new section 69 dealing with "power to issue directions for interception or monitoring or decryption of any information through any computer resource" is much more elaborate than the one it replaced, In October 2009, the Central Government notified rules under section 69 which lay down procedures and safeguards for interception, monitoring and decryption of information (the "Interception Rules 2009"). This further thickens the legal regime in this context.

**Unlawful Intercept**

In August 2007, Lakshmana Kailash K., a techie from Bangalore was arrested on the suspicion of having posted insulting images of Chhatrapati Shivaji, a major historical figure in the state of Maharashtra, on the social-networking site Orkut. The police identified him based on IP address details obtained from Google and Airtel – Lakshmana's ISP. He was brought to Pune and detained for 50 days before it was discovered that the IP address provided by Airtel was erroneous. The mistake was evidently due to the fact that while requesting information from Airtel, the police had not properly specified whether the suspect had posted the content at 1:15 p.m. or a.m.

Taking cognizance of his plight from newspaper accounts, the State Human Rights Commission subsequently ordered the company to pay Rs 2 lakh to Lakshmana as damages [16].

The incident highlights how minor privacy violations by ISPs and intermediaries could have impacts that gravely undermine other basic human rights [17].

In addition to section 69, the Government has been empowered under the newly inserted section 69B to "monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource".

"Traffic data" has been defined in the section to mean "any data identifying or purporting to identify any person, computer system or computer network or any location to or from which communication is or may be transmitted." Rules have been issued by the Central Government under this section (the "Monitoring and Collecting Traffic Data Rules, 2009") which are similar, although with important distinctions, to the rules issued under section 69.

Thus, there are two parallel interception and monitoring regimes in place under the Information Technology Act. In the paragraphs that follow, we provide an overview of the regime of surveillance under section 69 — since they are more targeted towards the individual, and consequently the threats to privacy are more severe — while highlighting important differences in the rules drafted under section 69.

**Who may lawfully intercept?**

Section 69 empowers the "Central Government or a state government or any of its officers specially authorised by the Central Government or the state government, as the case may be" to exercise powers of interception under this section.

Under the Interception Rules 2009, the secretary in the Ministry of Home Affairs has been designated as the "competent authority", with respect to the Central Government, to issue directions pertaining to interception, monitoring and decryption. Similarly, the respective state secretaries in charge of Home Departments of the various states and union territories are designated as "competent authorities" to issue directions with respect to the state government [18].

| | Central Government | State/Union Territory |
|---|---|---|
| Ordinary Circumstances | Secretary in the Ministry of Home Affairs | Secretary in charge of Home Departments of State |
| Emergency | Head or second senior most officer of security and law enforcement | Authorized officer not below the rank of Inspectors General of Police |

However, an exception is made in cases of emergency, either

- in remote areas where obtaining prior directions from the competent authority is not feasible or
- for 'operational reasons' where obtaining prior directions is not feasible.

In such cases it would be permissible to carry out interception after obtaining the orders of the Head or second senior most officer of security and law enforcement at the central level, and an authorized officer not below the rank of Inspector General of Police at the state or union territory level. The order must be communicated to the competent authority within three days of its issue, and approval must be obtained from the authority within seven working days, failing which the order would lapse.

Where a state/union territory wishes to intercept/monitor or decrypt information beyond its territory, the competent authority for that state must make a request to the competent authority of the Central Government to issue appropriate directions.

# Under what circumstances a direction to intercept may be issued?

### Purposes for which interception may be directed

Under section 69, the powers of interception may be exercised by the authorized officers "when they are satisfied that it is necessary or expedient" to do so in the interest of:

- sovereignty or integrity of India,
- defense of India,
- security of the state,
- friendly relations with foreign states or
- public order or
- preventing incitement to the commission of any cognizable offence relating to above or
- for investigation of any offence.

Under section 69B, the competent authority may issue directions for monitoring for a range of "cyber security"[20] purposes including, inter alia, "identifying or tracking of any person who has breached, or is suspected of having breached or being likely to breach cyber security".

### Contents of direction

The reasons for ordering interception must be recorded in writing [21].

In the case of a direction under section 69, in arriving at its decision, the competent authority must consider alternate means of acquiring the information other than issuing a direction for interception [22]. The direction must relate to information sent or likely to be sent from one or more particular computer resources to another (or many) computer resources [23]. The direction must specify the name and designation of the officer to whom information obtained is to be disclosed, and also specify the uses for which the information is to be employed [24].

### Duration of interception and periodic review

Once issued, an interception direction issued under section 69 remains in force for a period of 60 days (unless withdrawn earlier), and may be renewed for a total period not exceeding 180 days [25]. A direction issued under section 69B does not expire automatically through the lapse of time and theoretically would continue until withdrawn.

Within seven days of its issue, a copy of a direction issued under either section 69 or section 69B must be forwarded to the review committee constituted to oversee wiretapping under the Indian Telegraph Act [26]. Every two months, the review committee is required to meet and record its findings as to whether the direction was validly issued in light of section 69(3) [27]. If the review committee is of the opinion that it was not, it can set aside the direction and order destruction of all information collected [28].

**What powers of interception do they have?**

The competent authority may, in his written direction "direct any agency of the appropriate government to intercept monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource"[29].

Accordingly, the subscriber or intermediary or any person in charge of the computer resource is must, if required by the designated government agency, extend all facilities, equipment and technical assistance to:

- provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or
- intercept, monitor, or decrypt[30] the information, as the case may be; or
- provide information stored in computer resource.

The intermediary must maintain records mentioning the intercepted information, the particulars of the person, e-mail account, computer resource, etc., that was intercepted, the particulars of the authority to whom the information was disclosed, number of copies of the information that were made, the date of their destruction, etc. [31]. This list of requisitions received must be forwarded to the government agency once every 15 days to ensure their authenticity [32].

In addition, a responsibility is cast on the intermediary to put in place adequate internal checks to ensure that unauthorized interception does not take place, and extreme secrecy of intercepted information is maintained [33].

## How long can information collected during interception be retained?

Interception rules require all records, including electronic records pertaining to interception to be destroyed by the government agency "in every six months except in cases where such information is required or likely to be required for functional purposes". In the case of the Monitoring and Collecting of Traffic Data Rules 2009, this period is nine months from the date of creation of record.

In addition, all records pertaining to directions for interception and monitoring are to be destroyed by the intermediary within a period of two months following discontinuance of interception or monitoring, unless they are required for any ongoing investigation or legal proceedings. In the case of Monitoring Rules, this period is six months from the date of discontinuance.

## What penalties accrue to intermediaries and subscribers for resisting interception?

Section 69 stipulates a penalty of imprisonment upto a term of seven years and fine for any "subscriber or intermediary or any person who fails to assist the agency" empowered to intercept.

# Data Protection under the IT Act

### Data Retention Requirements of 'Intermediaries'

Section 67C of the amended IT Act mandates 'intermediaries' [34] to maintain and preserve certain information under their control for durations which are to be specified by law.

Any intermediary who fails to retain such electronic records may be punished with imprisonment up to three years and a fine.

### Liability for body-corporates under section 43A

The newly inserted section 43A makes a start at introducing a mandatory data protection regime in Indian law. The section obliges corporate bodies who 'possess, deal or handle' any 'sensitive personal data' to implement and maintain 'reasonable' security practices, failing which they would be liable to compensate those affected by any negligence attributable to this failure.

It is only the narrowly-defined 'body corporates' [35] engaged in 'commercial or professional activities' who are the targets of this section. Thus government agencies and non-profit organisations are entirely excluded from the ambit of this section [36].

"Sensitive personal data or information" is any information that the Central Government may designate as such, when it sees fit to.

The "reasonable security practices" which the section obliges body corporates to observe are restricted to such measures as may be specified either "in an agreement between the parties" or in any law in force or as prescribed by the Central Government.

By defining both "sensitive personal data" and "reasonable security practice" in terms that require executive elaboration, the section in effect pre-empts the courts from evolving an iterative, contextual definition of these terms.

**Mphasis BPO Fraud: 2005** [37]

In December 2004, four call centre employees, working at an outsourcing facility operated by MphasiS in India, obtained PIN codes from four customers of MphasiS' client, Citi Group. These employees were not authorized to obtain the PINs.

In association with others, the call centre employees opened new accounts at Indian banks using false identities. Within two months, they used the PINs and account information gleaned during their employment at MphasiS to transfer money from the bank accounts of CitiGroup customers to the new accounts at Indian banks.

By April 2005, the Indian police had tipped off to the scam by a U.S. bank, and quickly identified the individuals involved in the scam. Arrests were made when those individuals attempted to withdraw cash from the falsified accounts, $426,000 was stolen; the amount recovered was $230,000.

**Draft Reasonable Security Practices Rules 2011 [38]**

In February 2011, the Ministry of Information and Technology, published draft rules under section 43A in order to define "sensitive personal information" and to prescribe "reasonable security practices" that body corporates must observe in relation to the information they hold.

Sensitive Personal Information

Rule 3 of these Draft Rules designates the following types of information as 'sensitive personal information':

- password;
- user details as provided at the time of registration or thereafter;
- information related to financial information such as Bank account / credit card / debit card / other payment instrument details of the users;
- physiological and mental health condition;
- medical records and history;(vi) Biometric information;
- information received by body corporate for processing, stored or processed under lawful contract or otherwise;
- Call data records;

This however, does not apply to "any information that is freely available or accessible in public domain or accessible under the Right to Information Act, 2005".

They and "any person" holding sensitive personal information are forbidden from "keeping that information for longer than is required for the purposes for which the information may lawfully be used"[40]

**Mandatory Privacy Policies for body corporates**

Rule 4 of the draft rules enjoins a body corporate or its representative who "collects, receives, possess, stores, deals or handles" data to provide a privacy policy "for handling of or dealing in user information including sensitive personal information". This policy is to be made available for view by such "providers of information" [41]. The policy must provide details of:

- Type of personal or sensitive information collected under sub-rule (ii) of rule 3;
- Purpose, means and modes of usage of such information;
- Disclosure of information as provided in rule 6 [42].

Prior Consent and Use Limitation during Data Collection

In addition to the restrictions on collecting sensitive personal information, body corporate must obtain prior consent from the "provider of information" regarding "purpose, means and modes of use of the information". The body corporate is required to "take such steps as are, in the circumstances, reasonable"[43] to ensure that the individual from whom data is collected is aware of :

- the fact that the information is being collected; and
- the purpose for which the information is being collected; and

- the intended recipients of the information; and
- the name and address of :
- the agency that is collecting the information; and
- the agency that will hold the information.

During data collection, body corporates are required to give individuals the option to opt-in or opt-out from data collection [44]. They must also permit individuals to review and modify the information they provide "wherever necessary" [45]. Information collected is to be kept securely [46], used only for the stated purpose [47] and any grievances must be addressed by the body corporate "in a time bound manner" [48].

Unlike "sensitive personal information" there is no obligation to retain information only for as long as is it is required for the purpose collected.

**Limitations on Disclosure of Information**

The draft rules require a body corporate to obtain prior permission from the provider of such information obtained either "under lawful contract or otherwise" before information is disclosed [49]. The body corporate or any person on its behalf shall not publish the sensitive personal information [50]. Any third party receiving this information is prohibited from disclosing it further [51]. However, a proviso to this sub-rule mandates information to be provided to 'government agencies' for the purposes of "verification of identity, or for prevention, detection, investigation, prosecution, and punishment of offences". In such cases, the government agency is required to send a written request to the body corporate possessing the sensitive information, stating clearly the purpose of seeking such information. The government agency is also required to "state that the information thus obtained will not be published or shared with any other person" [52].

Sub-rule (2) of rule 6 requires "any information" to be "disclosed to any third party by an order under the law for the time being in force." This is to be done "without prejudice" to the obligations of the body corporate to obtain prior permission from the providers of information [53].

**Reasonable Security Practices**

Rule 7 of the draft rules stipulates that a body corporate shall be deemed to have complied with reasonable security practices if it has implemented security practices and standards which require:

- a comprehensive documented information security program; and
- information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected.

In case of an information security breach, such body corporate will be "required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security program and information security policies".

The rule stipulates that by adopting the International Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements", a body corporate will be deemed to have complied with reasonable security practices and procedures.

The rule also permits "industry associations or industry clusters" who are following standards other than IS/ISO/IEC 27001 but which nevertheless correspond to the requirements of sub-rule 7(1), to obtain approval for these codes from the government. Once this approval has been sought and obtained, the observance of these standards by a body corporate would deem them to have complied with the reasonable security practice requirements of section 43A.

# Penalties and Remedies for breach of Data Protection

### Civil Liability for Corporates

As mentioned above, any body corporates who fail to observe data protection norms may be liable to pay compensation if:

- it is negligent in implementing and maintaining reasonable security practices, and thereby
- causes wrongful loss or wrongful gain to any person;[54]

Claims for compensation are to be made to the adjudicating officer appointed under section 46 of the IT Act. Further, details of the powers and functions of this officer are given in succeeding sections of this note.

### Criminal liability for disclosure of information obtained in the course of exercising powers under the IT Act

Section 72 of the Information Technology Act imposes a penalty on "any person" who, having secured access to any electronic record, correspondence, information, document or other material using powers conferred by the Act or rules, discloses such information without the consent of the person concerned. Such unauthorized disclosure is punishable "with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both."

### Criminal Liability for unauthorized disclosure of information by any person of information obtained under contract

Section 72A of the IT Act imposes a penalty on any person [55] (including an intermediary) who

- has obtained personal information while providing services under a lawful contract and
- discloses the personal information without consent of the person,
- with the intent to cause, or knowing it is likely to cause wrongful gain or wrongful loss [56]

Such unauthorised disclosure to a third person is punishable with imprisonment upto three years or with fine upto Rs five lakh, or both.

# Whom to call? Adjudicatory Mechanism and Remedies under the IT Act

This section provides a brief outline of the mechanism installed by the IT Act to activate the various remedies and penalties prescribed in various sections of the Act. As a victim of online intrusion, how does one use the IT Act to seek redressal?

As mentioned above, the IT Act provides for both the civil remedy of damages in compensation (Chapter IX) as well as criminal penalties for offences such as imprisonment and fine (Chapter XI). In general, claiming a civil remedy does not bar one from seeking criminal prosecution and ideally both should be pursued together. For clarity, in the sections that follow, we will be discussing the two procedures separately.

# Civil Damages and Compensation

**Whom to approach?**

Section 46 of the IT Act empowers the Central Government to appoint "adjudication officers" to adjudicate whether any person has committed any of the contraventions described in Chapter IX of the Act (See section 2.1 and 4.2 above) and to determine the quantum of compensation payable. Accordingly, the Central Government has designated the secretaries of the Department of Information Technology of each of the states or union territories as the "adjudicating officer" with respect to each of their territories [57].

However, a pecuniary limit has been placed on the powers of adjudicating officers, and they may only adjudicate cases where the quantum of compensation claimed does not exceed Rs. five crores. In cases where the compensation claimed exceeds this amount, jurisdiction would vest in the "competent court", under the Code of Civil Procedure [58].

Section 61 of the Act bars ordinary civil courts from jurisdiction over matters which the adjudicating officers have been empowered to decide under this Act.

# When must a complaint be filed?

The Limitation Act provides that a suit must be filed within three years from when the right to sue accrues [59].

# What is the procedure?

Section 46 and the rules framed under that section provide elaborate guidelines on the procedure that is to be followed by the adjudicating officer. Thus, the adjudicating officer is required to give the accused person "a reasonable opportunity for making representation in the matter". Thereafter, if , on an inquiry, "he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section."

In order to carry out their duties adjudicating officer have been invested with the powers of a civil court which are conferred on the cyber appellate tribunal [60]. Additionally, they have the power to punish for their contempt under the Code of Criminal Procedure.

Rules framed under the section provide further details on the procedure that must be followed and provide for the issuance of a "show cause notice", manner of holding enquiry, compounding of offences, etc. [61].

Section 47 provides that in adjudging the quantum of compensation, the adjudicating officer shall have due regard to the following factors, namely:—

- the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;
- the amount of loss caused to any person as a result of the default;
- the repetitive nature of the default.

## Where must a complaint be filed and in what format?

The complaint must be made to the adjudicating officer of the state or union territory on the basis of location of computer system, computer network. The complaint must be made on a plain paper in the format provided in the Performa attached to the rules [62].

In case the offender or computer resource is located abroad, it would be deemed, for the purpose of prosecution to be located in India [63].

## How long does the process take?

The Rules direct that the whole matter should be heard and decided "as far as possible" within a period of six months [64].

## How much does it cost?

The Rules stipulates a variable fee payable by a bank draft calculated on the basis of damages claimed by way of compensation.

| | |
|---|---|
| a) Upto Rs. 10,000 | 10% ad valorem rounded off to nearest next hundred |
| b) From 10001 to Rs.50000 | Rs. 1000 plus 5% of the amount exceeding Rs.10,000 rounded off to nearest next hundred |
| c) From Rs.50001 to Rs.100000 | Rs. 3000/- plus 4% of the amount exceeding Rs. 50,000 rounded off to nearest next hundred |
| d) More than Rs. 100000 | Rs.5000/- plus 2% of the amount exceeding Rs. 100,000 rounded off to nearest next hundred |

### Appeals to the Cyber Appellate Tribunal and the High Court

The Act provides for the constitution of a cyber appellate tribunal to hear appeals from cases decided by the adjudicating officer.

Within 25 days of the copy of the decision being made available by the adjudicating officer, the aggrieved party may file an appeal before the cyber appellate tribunal.

Section 57 provides that the appeal filed before the cyber appellate tribunal shall be dealt with by it as expeditiously as possible and endeavor shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal. Section 62 gives the right of appeal to a high court to any person aggrieved by any decision or order of the cyber appellate tribunal on any question of fact or law arising out of such order. Such an appeal must be filed within 60 days from the date of communication of the decision or order of the cyber appellate tribunal.

**Can contraventions be compounded (compromised) with the offender?**

Except in the case of repeat offenders, contraventions may be compromised by the adjudicating officer or between the parties either before or after institution of the suit. Where any contravention has been compounded the IT Act provides that "no proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded"[65].

**Criminal Penalties**

The process described above applies to "contraventions" under Chapter IX of the Act. In addition to being liable to pay compensation, in the cases falling under section 43, such offenders may also be liable for criminal penalties such as imprisonment and fines [66]. This sub-section of this paper deals with the procedure to be followed with respect to the criminal offences set out under Chapter XI of the Act (for example, see sections 2.2 to 2.5 above).

# Whom to approach? Who can take cognizance of offences and investigate them?

Section 78 of the IT Act empowers police officers of the rank of Inspectors and above to investigate offences under the IT Act.

Many states have set up dedicated cyber crime police stations to investigate offences under this Act [67]. Thus, for example, the State of Karnataka has set up a special cyber crime police station responsible for investigating all offences under the IT Act with respect to the entire territory of Karnataka [68].

# When must a complaint be lodged?

Although there is no time limit prescribed by the IT Act or the Code of Criminal Procedure with respect to when an FIR must be filed, in general, courts tend to take an adverse view when a significant delay has occurred between the time of occurrence of an offence and it's reporting to the nearest police station.

The Code of Criminal Procedure forbids courts from taking cognizance of cases after three years "if the offence is punishable with imprisonment for a term exceeding one year but not exceeding three years". Where either the commission of the offence was not known to the person aggrieved, or where it is not known by whom the offence

committed, this period is computed from the date on which respectively the offence or the identity of the offender comes to the knowledge of the person aggrieved [69].

## What is the procedure?

No special procedure is prescribed for the trial of cyber offences and hence the general provisions of criminal procedure would apply with respect to investigation, charge sheet, trial, decision, sentencing and appeal.

## Can offences be compounded?

Offences punishable with imprisonment of upto three years are compoundable by a competent court. However, repeat offenders cannot have their subsequent offences compounded. Additionally, offences which "affect the socio-economic conditions of the country" or those committed against a child under 18 years of age or against women cannot be compounded [70].

**Bibliography**

[1].The IT Act is only one of the various laws which safeguard citizens from violations of online privacy. In addition, in the domain of finance, for instance, various RBI regulations mandate strong security protocols with respect to data held by financial institutions. Since this is the subject of a different dispatch on banking and privacy which we have brought out, these regulations are omitted from this discussion.

[2].Section 2(k) of the IT Act defines 'computer' as any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network.

[3].Section 43 defines "computer contaminant" as any set of computer instructions that are designed— (a) to modify, destroy, record, transmit data or program residing within a computer, computer system or computer network; or (b) by any means to usurp the normal operation of the computer, computer system, or computer network;

[4].Similarly, "computer virus" has been defined in section 43 as "any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer resource;

[6].Section 66 of the IT Act. Anon, 2009. Bangalore techie convicted for hacking govt site. Deccan Herald. Available at: http://goo.gl/jCvAh. [Accessed March 29, 2011];

[7].The Information Technology (Due Diligence observed by Intermediaries Guidelines) Rules, 2011;

[8].'Intermediary' has been defined very expansively under section 2(w) of the Act to mean, with respect to any electronic record, "any person who on behalf of another person receives, stores or transmits that record, or

provides any service with respect to that record and includes telecom service providers, network service providers, Internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes

[9].'Private area' has been defined in section 66E as "the naked or undergarment clad genitals, pubic area, buttocks or female breast".

[10].Defined as "circumstances in which a person can have a reasonable expectation that (i) he or she could disrobe in privacy, without being concerned that an image of his or her private area was being captured or (ii) any part of his or her private area would not be visible to the public regardless of whether that person is in a public or private place". See explanation to Section 66E

[11]."Cheating by personation" is a crime defined under section 416 the Indian Penal Code. According to that section, "a person is said to "cheat by personation" if he cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is." The explanation to the section adds that "the offence is committed whether the individual personated is a real or imaginary person". Two illustrations to the section further elaborate its meaning: (a) A cheats by pretending to be a certain rich banker of the same name. A cheats by personation (b) A cheats by pretending to be B, a person who is deceased. A cheats by personation.

[12].Communication device" has been defined to mean "cell phones, personal digital assistance (sic) or combination of both or any other device used to communicate send or transmit any text, video, audio or image".

[13].2005. Cyber Crime Cell, Mumbai: Case of Phishing. Mumbai Police. Available at: http://www.cybercellmumbai.com/case-studies/case-of-fishing [Accessed March 23, 2011].

[14]. Although no maximum limit is prescribed for the fine under this section, Section 63 of the Indian Penal Code declares that "Where no sum is expressed to which a fine may extend, the amount of fine to which the offender is liable is unlimited, but shall not be excessive".

[15].Hafeez, M., 2009. Crime Line: Curiosity was his main motive, say city police. Crime Line. Available at: http://mateenhafeez.blogspot.com/2009/05/curiosity-was-his-main-motive-say-city.html [Accessed March 23, 2011].

[16]. Holla, A., 2009. Wronged, techie gets justice 2 yrs after being jailed. Mumbai Mirror. Available at: http://www.mumbaimirror.com/index.aspx?
page=article&sectid=2&contentid=2009062520090625031445786810374 83 [Accessed March 23, 2011].

[17].See also Nanjappa, V., 2008. 'I have lost everything'. Rediff.com News. Available at: http://www.rediff.com/news/2008/jan/21inter.htm [Accessed March 23, 2011].

[18]. By contrast, rules framed under Section 69B designates only the Secretary to the Government of India in the Department of Information Technology under the Ministry of Communications and IT as the "competent authority" to issue orders of interception.

[19].It is unclear what these "operational reasons" could mean. The text of the rules provide no useful guidance.

[20].“Cyber security breach” is defined as meaning “any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly acceptable security policy resulting in unauthorized access, denial of service, disruption, unauthorized use of a computer resource for processing or storage of information or changes to date, information without authorization”. Rule 2(f) of the Monitoring and Collecting of Traffic Data Rules 2009.

[21].Rule 7 of the Interception Rules 2009; Rule 3(3) of the Monitoring and Collecting of Traffic Data Rules 2009

[22].Rule 8 of the Interception Rules 2009

[23]. Rule 9 of the Interception Rules 2009

[24].Rule 10 of the Interception Rules 2009;

[25].Rule 11 of the Interception Rules 2009

[26].Rule 7 of the Interception Rules 2009

[27].Rule 22 of the Interception Rules 2009

[28]. Ibid

[29].Section 69 of the IT Act.

[30].The intermediary is required to assist in the decryption only to the extent that the intermediary has control over the decryption key. See Sub-Rule 13(3) of the Interception Rules 2009. Rule 17 enjoins the holder of a decryption key to provide decryption assistance when directed to by the competent authority.

[31].Rule 16 of the Interception Rules 2009

[32].Rule 18 of the Interception Rules 2009

[33]. Rule 20 of the Interception Rules 2009; Rules 10 & 11 of the Monitoring and Collecting of Traffic Data Rules 2009. Failure to maintain secrecy of data may attract punishment under Section 72 of the Information Technology Act.

[34].Supra n. 6 for definition

[35].Section 43A defines '"body corporate" as any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

[36].This does not necessarily mean that these entitles are exempt from taking reasonable care to safeguard information that they collect, maintain or control – only that remedies against the government must be sought under general common law, rather than under the IT Act.

[37].Anon, 2005. The MphasiS Scandal – And How it Concerns U.S. Companies Considering Offshore BPO. Carretek. Available at: http://www.carretek.com/main/news/articles/MphasiS_scandal.htm [Accessed March 29, 2011]. See also Anon, 2005. MphasiS case: BPOs feel need to tighten security. Indian Express. Available at: http://www.expressindia.com/news/fullstory.php?newsid=44856 [Accessed March 29, 2011].

[38]. The Information Technology (Reasonable security practices and procedures and sensitive personal information) Rules, 2011. Available at

http://www.mit.gov.in/sites/upload_files/dit/files/senstivepersonainfo07_02_11.pdf, last accessed February 15th, 2011.

[39].Rule 5 of the Draft Rules.

[40]. This is perhaps a bit vague, since the potential 'lawful uses' are numerous and could be inexhaustible. It is unclear whether "lawful usage" is coterminous with "the uses which are disclosed to the individual at the time of collection". In addition, this rule is framed rather weakly since it does not impose a positive obligation (although this is implied) to destroy information that is no longer required or in use.

[41]."Provider of data" is not the same as individuals to whom the data pertains, and could possibly include intermediaries who have custody over the data. We feel this privacy policy should be made available for view generally – and not only to providers of information. In addition, it might be advisable to mandate registration of privacy policies with designated data controllers.

[42]. This is well framed since it does not permit body corporates to frame privacy policies that detract from Rule 6.

[43].One wonders about the convoluted language used here when a simpler phrase like "take reasonable steps" alone might have sufficed - reasonableness has generally been interpreted by courts contextually. As the Supreme Court has remarked, "`Reasonable' means prima facie in law reasonable in regard to those circumstances of which the actor, called upon to act reasonably, knows or ought to know. See Gujarat Water Supply and Sewage Board v. Unique Erectors (Guj) AIR 1989 SC 973.

[44].Sub-Rule 5(7).

[45].Sub-Rule 5(6). It is unclear what would count as a 'necessary' circumstance and who would be the authority to determine such necessity.

[46].Sub-Rule 5(8).

[47].Sub-Rule 5(5).

[48].Sub-Rule 5(9).

[49]. Sub-Rule 6(1) There are two problems with this rule. First, it requires prior permission only from the provider of information, and not the individual to whom the data pertains. In effect this whittles down the agency of the individual in being able to control the manner in which information pertaining to her is used. Second, it is not clear whether this information includes "sensitive personal information". The proviso to this rule includes the phrase "sensitive information", which would suggest that such information would be included. This makes it even more important that the rule require that prior permission be obtained from the individual to whom the data pertains and not merely from the provider of information.

[50].Sub-Rule 6(3).

[51].Sub-Rule 6(4).

[52].This is a curious insertion since it begs the question as to the utility of such a statement issued by the requesting agency. What are the sanctions under the IT Act that may be attached to a government agencies that betrays this statement? Why not instead, insert a peremptory prohibition on government agencies from disclosing such information (with the exception, perhaps, of securing conviction of offenders)?

[53].This sub-rule does not distinguish between orders issued by a court and those issued by an administrative/quasi-judicial body.

[54]. "Wrongful loss" and "wrongful gain" have been defined by Section 23 of the Indian Penal Code. Accordingly, "Wrongful gain" is gain by unlawful means of property which the person gaining is not legally entitled. "Wrongful loss"- "Wrongful loss" is the loss by unlawful means of property to which the person losing it is legally entitled." The section also includes this interesting explanation "Gaining wrongfully, losing wrongfully- A person is said to gain wrongfully when such person retains wrongfully, as well as when such person acquires wrongfully. A person is said to lose wrongfully when such person is wrongfully kept out of any property as well as when such person is wrongfully deprived of property". Following this, it could be possible to argue that the retention of data beyond the period of its use would amount to a "wrongful gain".

[55]. Section 3(39) of the General Clauses Act defines a person to include "any company or association or body of individuals whether incorporated or not". An interesting question here would be whether the State can be considered "a person" so that it can be held liable for unauthorized disclosure of personal information. In an early case of Shiv Prasad v. Punjab State AIR 1957 Punj 150, the Punjab High Court had excluded this possibility. However, the case law on this point has not been consistent. In Ramanlal Maheshwari v.Municipal Committee, the MP High Court held that the Municipal Council could be treated as a 'person' for the purpose of levying a fine attached to a criminal offence. Statutory corporate bodies (such as the proposed UID Authority of India) have been held to be 'persons' for purposes of law . See Commissioners, Port of Calcutta v. General Trading Corporation, AIR 1964 Cal 290. Here under the Calcutta Port Act, Port Commissioners were declared to be a "body corporate", and hence were held to be a 'person'.

[56].See supra n. 44.

[57]. See G.S.R.240(E) New Delhi, the 25th March, 2003 available at < http://www.mit.gov.in/content/it-act-notification-no-240> .

[58].See Section 46(1A).

[59].Schedule I, Part X of the Limitation Act "Suits for which there is no prescribed period."

[60].The powers of the Cyber Appellate Tribunal under Section 58 include the powers of (a) summoning and enforcing the attendance of any person and examining him on oath; (b) requiring the discovery and production of documents or other electronic records; (c) receiving evidence on affidavits; (d) issuing commissions for the examination of witnesses or documents; (e) reviewing its decisions; (f) dismissing an application for default or deciding it ex parte.

[61].Information Technology (Qualification and Experience of Adjudicating Officers and Manner of holding Enquiry) Rules, 2003 [GSR 220(E)] Available at <http://cca.gov.in/rw/resource/notification-gsr220e.pdf?download=true>.

[62]. Ibid Rule 4(b).

[63]. Section 75.

[64]. Ibid, Rule 4(k).

[65]. Section 63 of the Act.

[66].Prior to amendment in 2008, contraventions listed in Section 43 were only liable to be compensated by damages through civil proceedings. Thus in 2007, the Madras High Court annulled an FIR lodged in a police station which listed an activity mentioned in 43(g). See S. Sekar vs The Principal General Manager < http://indiankanoon.org/doc/182565/> This position has however been changed with the new Section 66 which makes all actions listed in Section 43 an offence when committed with dishonest or fraudulent intent. Thus an FIR can be lodged with respect to these activities as well.

[67].An incomplete list of cyber crime cells of police in different states can be viewed at <http://infosecawareness.in/cyber-crime-cells-in-india>.

[68]. Home and Transport3 Secretariat, Notification no. HD 173 POP 99 Bangalore, Dated 13th September 2001 Available at < http://cyberpolicebangalore.nic.in/pdf/notification_1.pdf>.

[69]. Sections 468 and 469 of the Code of Criminal Procedure, 1973.

[70]. Section 77A of the Information Technology Act.