Privacy on the Internet in India

Case Studies

RIM and GOI

- GOI cannot listen to RIM traffic
- Anxiety about foreign countries ability to intercept what should ideally be domestic traffic
- Since 2008 GOI has threatened ban on RIM services in India.
- Solutions offered by GOI: establish domestic server, create mirror image of all emails and data and save for six months, Government to Government solution
- Solutions offered by RIM: open access to consumer emails, voice, SMS, IP address of BES and the PIN and IMEI numbers of BlackBerry mobiles, data on request to request basis
- RIM set up a noc in Mumbai and DoT has required service providers to install necessary software to provide access to RIM communications.

Local servers

- GOI has contemplated local servers for Gmail, Yahoo, Nokia Intellisinc Email, and a India centric Skype
- Indian ISPs have asked GOI to require Google, Facebook and other US companies to set up local servers.

DoT asks Telcos for location accuracy

- 2013 the DoT requires telecom operators to install Location Based Servers to track calls up to 50 meters in real time.
- Location details in the form of longitude and latitude will be apart of CDRs
- Cost to Operators - $5Billion

The Central Monitoring System

- Envisioned in 2009 Carried out by C-DOT
- Will allow central monitoring of phone and internet communications including emails, chats, IM's, video & audio files etc.
- Will bypass service providers and allow for direct access by the government.
- Exact specifications and functions still unclear
-

Internet Monitoring System: Assam Tender

- IMS will contain probe servers to be installed at the ISP and at various points within the network.
- Collection server installed at ISP and used to filter, analyze, aggregate
- Intercept, collect, and analyze internet traffic according to different protocols, keywords, filters, and watch lists.

India and EU Data Secure Status

- GOI has threatened to stall the proposed Free Trade Agreement with Europe unless EU data secure status is granted to India.
- India has argued that US has safe harbour with EU and the US and India have data adequacy agreement, thus EU should give data secure status.
- EU has established a Joint Working Group to look at technical aspects and work with India to help ensure that India will be able to gain data secure status.

Report of the Group of Experts on Privacy

- Recommendations for a Privacy Legislation
- Nine Privacy Principles
- The Privacy Commissioner
- Co-regulation

Policy

ITA

Reasonable Security Practices and Procedures and Sensitive Data or Information Rules

- Quasi data protection provisions
- Protects sensitive personal information
- Applicable to all body corporates (but not the government)
- Currently being debated as to whether comprehensive enough for EU “Data Secure” status

Salient Features

Reasonable Security Practices and Procedures and Sensitive Data or Information Rules

- **Personal Data:** Information that relates to a natural person, which, either directly or indirectly, in combination with other information available is capable of identifying such person
- **Sensitive personal data:** password, financial information such as a Bank account or credit card or debit card or other payment instrument detail, physical, physiological, and mental condition, sexual orientation, medical records and history, biometric information

Salient Features

Reasonable Security Practices and Procedures and Sensitive Data or Information Rules

- Privacy Policy: Body corporates must have in place a privacy policy for handling or dealing with personal or sensitive personal information. Must specify type of information collected, purpose of collection, disclosure of information, and security practices in place.
- Collection of Information: Allowed only after consent is given and the collection is necessary and proportionate. Notice must be given during collection and collected information can only be used for stated purposes and retained for as long as lawfully necessary.
- Disclosure of Information: Disclosure of information is allowed only with consent except with Government agencies as mandated under law or for the purpose of verification of identity, prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. To access information

Salient Features

Reasonable Security Practices and Procedures and Sensitive Data or Information Rules

- Access and Correction: Individuals have the right to amend inaccurate information.
- Right to opt in or out: Individuals have the right not to provide personal information.
- Right to withdraw consent: Individuals have the right to withdraw consent at any point of time.
- Grievance officer: Every corporate body must have a grievance officer to handle complaints.

ITA

Cyber Cafe Rules

- **Requirement for proof of identification:** Eight accepted forms of identification – stored for one year.
- **Log register**: name, address, gender, contact number, type and detail of identification document, date, computer terminal identification, log in time, log out time – submitted on a monthly basis to the prescribed agency.
- **Log Records:** History of websites access for each access, logs of proxy's installed – stored for one year.
- **Physical layout:** Cubicles not to exceed four ½ feet in height from floor level. All computer screens must face outwards.
- **Inspection:** An officer authorised by the registration agency is authorised to inspect the cyber cafe at any time and the owner must provide every related document, registers, and necessary information.

ElectraCard Heist

- ElectraCard processes prepaid travel cards
- Two coordinated hits withdrawing $45 million
- Hacked into Indian and US credit card processing company

ITA: section 66

- Fraudulent or dishonest use of the internet -
- Sending of offensive messages, electronic mail messages for the purpose of causing annoyance
- Fraudulently or dishonestly retains any stolen computer resource or communication device
- Fraudulently or dishonestly makes use of the electronic signature, password, unique identification features of another persons
- Cheating by personation
- Intentionally capturing, publishing, or transmitting the image of a private area without consent
- Introducing computer contaminants/attempting to penetrate a computer system

ITA

Section 67

- Publishing or transmitting obscene material in electronic form
- Publishing or transmitting material containing a sexually explicit act.
- Publishing or transmitting material depicting children in a sexually explicit act.

ITA

The Controller

- Power to undertake investigation of any contravention of the ITA
- Will be given access to any computer system, apparatus, data or any other material connected with such system.

ITA

Procedures and Safeguards for Interception, Monitoring, and Decryption of Information Rules

- Authorizing authority and review committee
- Information generated transmitted, received, or stored in any computer resource
- Seven grounds for access
- Service provider co-operation
- Decryption of information and storage of decryption key
- Penalty for non compliance or unauthorised interception by service provider

ITA

Procedure and safeguard for Monitoring and Collecting Traffic Data or Information Rules

- Authorising Authority: Secretary to the GOI in Department of information Technology
- View, inspect, record, collect by means of a monitoring device
- Nine grounds
- Review Committee
- Service provider co-operation: extend all facilities, assistance in installation, removal and testing of equipment, enabling online access
- Penalty for monitoring or collection without authorization

Encryption

- ITA allows the Government to establish the nationally permitted standard for encryption.
- Currently limited to 40 bit with a prohibition on bulk encryption for ISPs and service providers under ISP and UAS license.
- Not recommended by business in India i.e RBI banking standards recommend 128 bit encryption to protect online transactions.

ISP License and UASL

- Applies to service providers
- Monitoring, intercepting, and tracing capabilities
- Provision of subscriber information
- Provision of CDR's, IP address, called numbers, duration, time etc., traceable identities
- Physical facilities: 10x10 and air conditioning
- Restriction on encryption
- User logs retained for one year
- Anonymous access prohibited