LEGAL ISSUES PERTAINING TO CYBER SECURITY AND SURVEILLANCE IN INDIA

Barnik Ghosh

Introduction

- Overview of Right to Privacy
- Legislations dealing with interception
- Provisions related to surveillance in License Agreements for ISPs, TSPs as well as the UAS License
- Relevant Rules regarding Cyber Security under the Information Technology Act 2000
- Major Regulatory Authorities dealing with Surveillance and Cyber Security
- Digital Evidence, Evidentiary Value and how to present the same in Court of Law

Right to Privacy

- India a signatory to the Universal Declaration of Human Rights and International Convention on Civil and Political Rights
- Kharak Singh v Union of India AIR 1963 SC 1295
- Govind v State of MP AIR 1975 SC 1378
- Rajagopalan Tests

Legislations regarding surveillance

- The Indian Telegraph Act 1885
- Information Technology Act 2000
  - Section 69 of the IT Act 2000
  - Section 69 of the IT Act expands the grounds upon which interception can take place as compared to the Telegraph Act.
  - As such, the interception of communications under Section 69 is carried out in the interest of:
    - The sovereignty or integrity of India;
    - Defense of India;
    - Security of the State;
    - Friendly relations with foreign States;
    - Public order;
    - Preventing incitement to the commission of any cognizable offense relating to the above; and
    - For the investigation of any offense.

Legislations Governing Surveillance

- Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009
  - Just like with Rule 419A of the Indian Telegraph Rules, the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (“IT Interception Rules”) framed under Section 69 and 69B stipulate as to who may issue directions of interception and monitoring, how such directions are to be executed, the duration they remain in operation, to whom data may be disclosed, confidentiality obligations of intermediaries, periodic oversight of interception directions by a Review Committee under the Telegraph Act, the retention of records of interception by intermediaries and to the mandatory destruction of information in appropriate cases.
  - Relevant propositions to be discussed in details

Legislations Governing Surveillance

- Indian Post Office Act 1898
- Code of Criminal Procedure 1973
- Indian Wireless Telegraphy Act 1933
- Central Motor Vehicle Act 1898 and 2012 Rules

License Agreements for Internet Service Providers (ISPs) and Telecom Service Providers (TSPs)

- ISP License Agreement
  - Internet Service Providers (ISPs) in India are required to comply with the License Agreement for Provision of Internet Services in order to operate, which is issued by the Department of Telecommunications of the Ministry of Communications and Information Technology. This License Agreement is governed by the Indian Telegraph Act, 1885, the Indian Wireless Telegraphy Act, 1933, and by the Telecom Regulatory Authority of India Act, 1997, as modified throughout time.
  - Relevant Clauses to be discussed

- TSP License Agreements
  - Telecom Service Providers (TSPs) in India have to comply with two license agreements in order to operate: the Cellular Mobile Telephone Service (CMTS) License Agreement and the License Agreement for the Provision of Basic Telephone Services (BTS). The first license agreement applies to cellular mobile communications, whereas the second applies to landlines.
  - Relevant Clauses of both Agreements to be added

Unified License (Access Services) Agreement

- The Unified License (Access Services) Agreement of 2013 also applies to both ISPs and TSPs in India. Part VI (“Security Conditions”) mandates that the interception of communications is carried out by ISPs and TSPs which comply with this License Agreement.
- Relevant Clauses to be discussed

Legal Landscape for Cyber Security

- Section 69B of the IT Act empowers the Central Government to authorise the monitoring and collection of information and traffic data generated, transmitted, received or stored through any computer resource for the purpose of cyber security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country.
- According to this section, any intermediary who intentionally or knowingly fails to provide technical assistance to the authorised agency which is required to monitor and collection information and traffic data shall be punished with an imprisonment which may extend to three years and will also be liable to a fine.
- The term “cyber security” has been defined in section 2(nb) the IT Act as “protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction”. Further clarity on the meaning and import of the term can be gleaned from the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 which are discussed below.

The Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009

- The Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 issued under section 69B of the Information Technology Act stipulate that directions for the monitoring and collection of traffic data or information can be issued by an order made by the competent authority for any or all of the following purposes related to cyber security:
  - forecasting of imminent cyber incidents;
  - monitoring network application with traffic data or information on computer resource;
  - identification and determination of viruses or computer contaminant;
  - tracking cyber security breaches or cyber security incidents;
  - tracking computer resource breaching cyber security or spreading virus or computer contaminants;
  - identifying or tracking any person who has breached, or is suspected of having breached or likely to breach cyber security;
  - undertaking forensic of the concerned computer resource as a part of investigation or internal audit of information security practices in the computer resources;
  - accessing stored information for enforcement of any provisions of the laws relating to cyber security for the time being in force;
  - Any other matter relating to cyber security

Cyber Crimes and Terrorism

- Hacking
- Cyber Terrorism
- Voyeurism (Section 66 of the IT Act 2000)
- Breach of Confidentiality and Privacy
- Identity Theft
- Cheating by Impersonation
- Offences relating to Interception
- Data Protection (Section 43A of IT Act 2000)

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

- Rule 3: Designates what types of information can be treated as sensitive personal information
- Rule 4: Duty of body corporates
- Rule 6: Conditions for disclosure of Personal Information and Sensitive Personal Data
- Rule 7: Transfer of Sensitive Personal Data
- Rule 8
- Relevant Rules to be discussed in details

Regulatory Landscape for Surveilance and Cyber Security

- Department of Electronics and Information Technology
  - ✓ Controller of Certifying Authorities
  - ✓ Cyber Appellate Tribunal
  - ✓ The Standardisation Testing and Quality Certification Directorate
  - ✓ Indian Computer Emergency Response Team
- Department of Telecommunications
  - ✓ Telecom Enforcement Resource Management Cells (TERM Cells)
  - ✓ Centre for Development of Telematics
  - ✓ Telecommunication Engineering Centre
  - ✓ National Telecommunications Institute for Policy Research
  - ✓ Telecom Regulatory Authority of India

Security and Law Enforcement Landscape

- National Investigation Agency
- National Technical Research Organisation
- Research and Analysis Wing
- Intelligence Bureau
- Central Bureau of Investigation
- Directorate of Revenue Intelligence
- Defence Intelligence Agency
- Military Intelligence Directorate
- Directorate of Air Intelligence
- Directorate of Navy Intelligence
- Joint Cipher Bureau
- Aviation Research Centre
- Enforcement Directorate
- Crime Branch

Ministry of Home Affairs

- Border Management Division
- Internal Security Division – I
- Internal Security Division – II
- Left Wing Extremism Division
- North East Division
- Police Division - II

Digital Evidence Landscape

- Concept of a Digital Signature
- Section 47A of IT Act 2000
- Sections 65A and 65B of IT Act 2000
- Section 67A of IT Act 2000
- Section 73A of IT Act 2000
- Section 81A of IT Act 2000
- Section 85A, 85B and 85C of IT Act 2000
- Section 88A of IT Act 2000
- Section 90A of of IT Act 2000
- Section 131 of IT Act 2000

Cyber Security Policy 2013

- 1. Set up a 24×7 National Critical Information Infrastructure Protection Centre (NCIIPC) for protecting critical infrastructure of the country.
- 2. Create a taskforce of 5,00,000 cyber security professionals in next five years.
- 3. Provide fiscal schemes and benefits to businesses for adoption of standard security practices.
- 4. Designate CERT-In as the national nodal agency to co-ordinate cyber security related matters and have the local (state) CERT bodies to co-ordinate at the respective levels.
- 5. All organizations to designate a CISO and allot a security budget.
- 6.Use of Open Standards for Cyber Security.
- 7. Develop a dynamic legal framework to address cyber security challenges (Note: The National Cyber Security Policy 2013 does not have any mention of the IT Act 2000)
- 8. Encourage wider use of Public Key Infrastructure (PKI) for government services.
- 9. Engage infosec professionals / organizations to assist e-Governance initiatives, establish Centers of Excellence, cyber security concept labs for awareness and skill development through PPP - a common theme across all initiatives mentioned in this policy.
- 10. Apart from the common theme of PPP across the cyber security initiatives, the policy frequently mentions of developing an infrastructure for evaluating and certifying trustworthy ICT security products.

THANK YOU