The Centre for Internet and Society

GSMA 2014

Indian Law and the Necessary Proportionate Principles

- **No comprehensive provisions for the principles of:**
  - Legitimate Aim,
  - Competent Judicial Authority,
  - Proportionality,
  - Notification,
  - Transparency ,
  - Integrity of Communications and Systems,

- **Partial provisions for the principles of:**
  - Legality,
  - Necessity,
  - Adequacy,
  - Public Oversight,
  - Safeguards for International Cooperation,
  - Safeguards against illegitimate access and right to effective remedy.

Indian Intelligence Agencies

- **Nine agencies authorized to intercept communications**:
  - National Investigation Agency (NIA),
  - National Technical Research Organization (NTRO),
  - Research and Analysis Wing (RAW),
  - Intelligence Bureau (IB),
  - Central Bureau of Investigation (CIB),
  - Directorate of Revenue Intelligence (DRI),
  - Central Board of Direct Taxes (CBDT),
  - Narcotics Control Bureau (NCB)
  - Enforcement Directorate

- **At least eleven additional agencies**:
  - Defence Intelligence Agency
  - Defence Image Processing and Analysis Centre
  - Directorate of Air Intelligence
  - Directorate of Navy Intelligence
  - Military Intelligence Directorate
  - Joint Cipher Bureau
  - Signals Intelligence Directorate
  - Aviation Research Centre
  - Enforcement Directorate
  - Crime Branch of the Criminal Investigation Department
  - Establishment 22, Special Frontier Force

Indian Intelligence Agencies: Oversight and Structure

- Intelligence agencies are established via executive order
- Intelligence agencies are centralized and opaque
- Intelligence agencies are not subject to:
  - parliamentary oversight
  - audit by the CAG
  - The Right to Information Act 2005

- Intelligence agencies report to respective departments.

  For example:
  - RAW and CBI = Prime Ministers Office
  - DRI = Finance Ministry
  - Military intelligence agencies = Defence Ministry

Intelligence Agencies: Sharing of Information

- International
  - MLATS and Letters of Rogatory
  - Central Bureau of Investigation is the nodal agency for sending and receiving MLATS and letters of Rogatory
  - India has MLAT agreements with 36 countries
  - Requests to CBI for initiation of a MLAT or letter of Rogatory can be informal or formal via a court order
- National
  - Sharing of intercepted, monitored, or decrypted information is permitted between agencies
  - Detailed procedures are not publicly available

Regulatory and Important Bodies/Departments National /Cyber Security

- **Ministry of Home Affairs** : Responsible for national security and all matters concerned
- **Ministry of Defence**: Provides the policy framework and wherewithal to Armed Forces
- **National Security Council**: Responsible for the India's political, economic, energy, and strategic strategy concerns.
- **The Department of Telecommunications:** Regulates the Telecom sector including development and issuance of licenses
  - TERM Cells
  - Centre for Development of Telematics: Development of Lawful Intercept and Monitoring solutions, the Central Monitoring System
- **The Department of Electronics and Information Technology**: Develops policy and regulation pertaining to IT and cyber security.
  - CERT-IN
  - Centre for Development of Advanced Computing
- **The Telecom Regulatory Authority of India:** Independent regulator of telecommunication companies in India.

Unlawful interception/leaks

- Nira Radia
  - Leaked tapes of interceptions carried out by the Indian Income Tax Department revealed the 2G scam
- Amit Shah
  - Alleged illegal surveillance of woman architect, commission ordered probe into the circumstances for the surveillance, the instances of unlawful interception of telephone calls in Himachal Pradesh, and the unlawful access to CDRs in Delhi.
- Arun Jaitely
  - Alleged illegal interception of the BJP leader, Arun Jaitley's phone, Union Home Minister clarified that it was not interception but instead access to CDR's, revealed that 100's of MPs have had their CDR's accessed.
- Amar Singh
  - Reliance Infocomm acted upon forged orders and intercepted the phone calls of Amar Singh the former Samajwadi leader. When hearing the case the supreme court questioned the government for not cancelling the licenses of Reliance Infocomm for gross negligence in verifying the interception order.

Examples of arrests based on digital evidence

- Whatsapp

For example: Whatsapp messages were used to arrest Waquar, an MBA student, for mischief, for sending an image of BJP leaders. The arrest was made before Modi was sworn in as PM. The message allegedly incited fear and alarm.

- Facebook

For example: In 2012 two women were arrested for posts placed on Facebook commenting on the city wide Bundh that was taking place in reaction to the Shiv Sena's party leader, Bal Thackery's, death

- Phone Tapping

For example: S.K. Jain, a bank manager was arrested based on intercepted material and nternal intelligence of 5-6 months that was used in investigation and lead to his arrest. He allegedly accepted large bribes to extend a line of credit

- Anvar v. Basheer and the declaration of a new law with respect to

Schemes

- CMS
  - Since 2009 the Government of India has been developing the Central Monitoring System – a system that seeks to automate and centralize the interception process. In doing so it will allow security agencies to bypass the service provider. Along with a Centralized Monitoring System(CMS), Regional Monitoring Systems (RMS) for the lawful interception of telecommunications will be established. CMS is under the Centre for Development of Telematics (C-DoT), a registered society under Department of Telecommunications and Ministry of Information Technology
- NETRA
  - The Centre for Artificial Intelligence and Robotics – a branch of DRDO has developed the Network Traffic Analysis software. The software has the capabilities to intercept and analyse internet traffic via specified filters. The software is currently being used by RAW, IB, state level law enforcement agencies. The project is being piloted by the Ministry of Home Affairs
- Mega Policing Cities
  - In 2013 the Ministry of Home Affairs, PM Division published guidelines for the development of mega policing projects. It is envisioned that Delhi, Kolkata, Mumbai, Chennia, Hyderabad, Bangalore, and Ahemadabad would implement the Mega City Policing projects. The project envisions the establishment of CCTVs in all public areas and a centralized data centre that provides access to multiple databases such as vehicle registration, pan card, residential address etc.

Telecommunication Companies in India

- **State owned:**

  BSNL (Government on Board of Directors), MTNL (Government on Board of Directors)

- **Private and National:**

  Bharti Airtel (ex Government on Board of Directors) , Aircel LTD, Reliance Communications, Tata Teleservices, Vodafone, Idea Cellular, Reliance Jio Infocomm

- **Private and International:**

  Vodafone, Telenore (Uninor), SingTel (Bharti Airtel), Axiata (Ideacellular), Sistema (MTS), Bell Canada (tata teleservices)

Telecom Licenses: Security Requirements

Service Providers must provide…

- Tracing facilities for malicious or obnoxious calls
- Monitoring equipment for at least 210 simultaneous calls for seven security agencies
- Hardware and software for lawful interception and monitoring
- Traceable identity of subscribers including geographical location
- Database of subscribers on password protected website
- Retention of commercial records for a period of one year
- Collection of meta data including CDRs and location data
- Verification of identity for all new subscribers/verification of users of public wifi
- Nodal officers that are citizens of India for the handling of interceptions.
- Facilities for monitoring all intrusions and attacks

Telecom Licenses: Security Requirements

Service Providers must obtain…

- Security clearance for imported equipment including the details of the equipment as well as details of equipments supplier and manufacturers including Original Equipment Manufacturers
- Security clearance for executive positions held by foreign nationals
- Annual audits of their networks from a security point of view

Service Providers must have in place…

- Organizational policy on security and security management of their networks as per ISO 15408 and ISO 27001
- Records of all command logs for a period of 12 months, software changes and updations, supply chain of products,

Service Providers are subject to…

- A penalty of Rs. 50 Crore for a security breach resulting from inadvertent inadequacies

Government Developed Security and Surveillance Solutions

- **CDOT**: Autonomous Centre under the Department of Telecommunications responsible for the development of intelligent software and designing and developing digital exchanges
  - **Example Solutions/projects**
    - Central Monitoring System
    - LIM"s
    - Intelligent Network Solutions
    - Network Management Solutions
    - Terrestrial & Satellite
  - **Example clients**: C-DOT provides its solutions to government, law enforcement, and telecoms. C-DOT exchanges technology solutions with a number of countries including Costa Rica, Namibia, Nigeria, Uganda, Ghana, Yemen, Ethiopia, Tanzania, Nepal, Bhutan. Bangladesh, Vietnam.
- **CDAC**: Within the Centre for Development of Advanced Computing the Resource Centre for Cyber Forensics is a research and development centre working in the areas of Disk Forensics, Network Forensics, Device Forensics, and Live Forensics.
  - **Solutions:**
    - TrueBack: Digital evidence seizure and acquisition tool
    - CyberCheck: Forensic tool to extract thumbnails images.
    - Win LiFT: Live forensics tool for acquisition and analysis of volatile data present in live windows system.
    - MobileCheck: Digital forensics solution for acquisition and analysis of mobile phones, smart phones, and personal digital assistants.
    - Network Session Analyzer: Captures and analyzes network traffic. Features include the ability to capture, filter, recreate, and export data.
    - TrueImager: Hardware based disk imaging tool which can perform seize, seize and acquire, and cloning operations.
    - True Traveller : Portable forensic tool kits capable of performing digital forensics seizure, acquisition, and anaylsis.
    - SIMXtractor: Forensic solution for imaging and analysing SIM cards.
    - Advik: CDR analyzer which can import and analyze CDR/Tower and CDR logs of any service provider in India.
  - **Clients:** CERT-In, Kerala Police, Army Cyber Security Establishment, Intelligence Bureau, State Level Subsidiary Intelligence Bureau, Delhi Police, CBI Academy, Central Forensics Science Laboratory, Cyber Cells Bangalore, National Academy of Taxes, Economic Offence Wing, Cabinet Secretariat, Office of the Director General of Income Tax, Office of the Director General of Revenue Intelligence, Data Security Council of India, Indo-Syrian Centre of Excellence in IT

Examples of Private Security Companies

- **Innefu Labs Pvt Ltd: Is** Is a ICT and Security Solutions company that is ISO 9001:2008 certified. Its board of advisors consists of former army officers and academics, and has clients in both the private and public sector. Its clients include government, law enforcement, BPO's, and telecoms
  - **Example of Solutions**
    - Internet Interception & Monitoring System which includes customized packet interception software, deep packet inspection technology, and applied filters.
    - Tactile Internet Monitoring System is a portable Internet Monitoring System which can be deployed at multiple servers including GPRS/3G and Internet Broadband servers.
    - Link Analysis includes features such as CDR Mining, operational intellienece unit, interrogation reports, and data integration and heuristics analysis.
    - Cyber Café Surveillance includes features such as authenticating every user of the Cyber Café, intercepting all mails and other communications from the Cyber Café, providing link anaylsis, and pre-empting a cime by prediticing future criminal actions.

- **Third Entity Security Solutions:** Is a ICT and Security Solutions company that is ISO 9001:2008 certified, it is NSIC registered, and has been empanelled by DRDO. Its board of advisors consists of former army officers and academics, and has clients in both the private and public sector. Third Entity Security Solutions partners with multiple international companies such as Magnet Forensics.
  - **Example of Solutions**
    - Innsight offers access to a comprehensive database of social conversations, real-time coverage and historical archive. Aggregates data to identify emerging trends.
    - AuthShield provides two factor authentication solutions and is supported by multiple platforms.
    - InteleLinx-Pro is a CDR Analysis Software that includes a number of features including uploading data from any service provider in India, carrying out Time-Spatial analysis, map the route of a number over a period of time, identify the 'night resting place' of suspects.

Security Expos

- Convergence : Exhibitors from India, China, Germany, Korea, Singapore, UK, and USA
  - Example companies: Comint Systems and Solutions, COAI India, Net Optics, and Nokia,
  - Supported by: Department of Telecommunications, Department of Electronics and Information Technoligy, Ministroy of Communications and Information Technology, Ministry of Information & Broadcasting, NSIC
- Secutech : Features IP solutions, equipment, and software suppliers.
  - Example technologies include: CCTV, digital surveillance, access control, management platform, smard card, biometrics, identification and authentication, firewall, public key infrastructure, malicious code protection, vulnerability scanners, forensics, and media sanitizing
  - Supported by: NSIC, Gujurat Safety Council, fpai, SMB Chamber, Asian Professional Security Association
- International Police Expo
  - Example companies: Matrix: Telecom Security, Swissloxx, motorola solutions, panasonic, cellebrite, dupont
- Secure Cities
  - Example companies: Dell Software, Verint, Esri India, Palo Alto Networks, Motorola Solutions, Steria, Teleste, Panasonic, Eye Watch, Indian Eye Security
  - Supported by: UK Trade Investment, Defense & Security Organization, NCIIPC, DEITY, NEGP
- India International Security Expo :
  - Supported by: Ministry of Home Affairs, Central Industrial Security Force, SPGI , Indo Tibetan Border Police Force, Delhi Police, Border Security Force, Bureau of Police Research & Development, Central Reserve Police, Delhi Fire Services, National Security Guard, National Disaster Management Authority

FinFisher in India

- In 2013 it was found that the command and control servers for FinSpy backdoors, a component of FinFisher ‘remote monitoring solutions’, was found in India.
- FinFisher remote monitoring solutions include: FinSpy, FinSpy Mobile, FinFly USB, FinFly LAN, FinFly Web, FinFly ISP
- The active use of FinFisher spy ware was confirmed
- According to the Citizen Lab, FinSpy servers in India have been detected through the HostGator operator and the first digits of the IP address are: 119.18.xxx.xxx.

Export, Import, and Selling of Security and Surveillance Equipment

- Export: no standards, except defense equipment
- Import: Security clearance by DoT for Telecom equipment

The Way Forward

- Policy
  - Stronger safeguards for surveillance
  - Breach of Confidence
  - Harmonized Surveillance Standards
  - Export standards
  - Certification standards

- Regional Workshop
  - Partnering with ORF
  - Security, Governments, and Technology: Exploring policy and practice.
    - Challenges and present scenario associated with cyber security and surveillance in India for law enforcement and state security
    - Law & Policy: data acquisition and use
    - Privatized intelligence acquisition
    - Import and export licensing regimes for security and surveillance technologies
    - The security market in India – international and local players
    - Challenges, International scenario , and best practice

- Security Companies and Government Procurement
  - RTI's and finding conclusive evidence of government department procuring technology and from which vendors.
  - Using publicly available information to research security companies in India, what solutions are offered, and who are their clients
  - Engagement with relevant actors