Multimedia Training Kit

Group Discussions and Case Studies

Freedom of Privacy

Collection of Cases specific to India

Contents

European Union

DIGITAL EMPOWERMENT foundation
empowering people @ the edge of information

APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

Scenario 1 – India's Central Monitoring System

Lawful interception of telephones is permissible under Section 5(2) of the Indian Telegraph Act 1885 which is governed by Rule 419-A of the Indian Telegraph (Amendment) Rules, 2007.

Section 69 of the Information Technology (Amendment) Act, 2008, which allows for the interception of all information transmitted through a computer resource.

Draft Rule 419B under Section 5(2) of the Indian Telegraph (Amendment) Act, 1885, allows for the disclosure of "message related information" / Call Data Records (CDR) to Indian authorities. According to draft Rule 419B, directions for the disclosure of Call Data Records can only be issued on a national level through orders by the Secretary to the Government of India in the Ministry of Home Affairs, while on the state level; orders can only be issued by the Secretary to the State Government in charge of the Home Department.

In December 2009, the Home Ministry set up and hosted NATGRID. As a part of this, 21 databases are to feed 11 security agencies for national security.

The Central Monitoring System (CMS), which was largely covered by the media in 2013, was actually approved by the Cabinet Committee on Security (CCS) on 16th June 2011. Since then CMS has been operated by India's Telecom Enforcement Resource and Monitoring (TERM) cells, and has been implemented by the Centre for Development of Telematics (C-DOT).

Additional information

- https://indialawyers.wordpress.com/tag/indian-telegraph-act-1885/
- http://www.sacw.net/article4793.html
- http://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about

Questions for Discussion

1. Do you think there is a need for an authority like CMS to prevent cyber-crimes?
2. Does interception of information violates freedom of speech and expression?
3. How can a country prevent cyber-crimes in absence of information?

Scenario 2 – Real Name Registration and Data Retention in Cyber Cafes

In 2011, the Government of India issued the Information Technology (Guidelines for Cyber Café) Rules. These rules govern the establishment and operation of Cyber Cafes in India.

Any user that wishes to avail the services of a cyber café must establish his/her identity by presenting either:

1. Identity card issued by any School or College; or
2. Photo Credit Card or debit card issued by a Bank or Post Office; or
3. Passport; or
4. Voter Identity Card; or
5. Permanent Account Number (PAN) card issued by Income-Tax Authority; or
6. Photo Identity Card issued by the employer or any Government Agency; or
7. Driving License issued by the Appropriate Government; or
8. Unique Identification (UID) Number issued by the Unique Identification Authority of India (UIDAI).

A copy of the ID, photo and various details about the user including; log-in time, log-out time, gender and computer terminal identification must be placed in a log register and submitted to the government.

Browsing history of all the computers in the café and details of any proxy serve must be logged and maintained in a secure location for a period of 1 year and must be turned over to the government in case they ask for them.

The availability of such information, which is personal in nature, with the cyber café could have negative implications on the right to privacy and personal security of the user.

Additional information

- http://deity.gov.in/sites/upload_files/dit/files/GSR315E_10511(1).pdf
- http://trak.in/tags/business/2011/04/26/cyber-cafe-rules-india-guidelines/

Questions for Discussion

1. Are cyber cafés the cheap source of cyber-crimes?
2. Does enforcement of “cyber café laws” prevent cyber-crimes?