TAKSHASHILA
INSTITUTION

DISCUSSION DOCUMENT
July, 2013

India’s Central Monitoring System

Rohan Joshi

EXECUTIVE SUMMARY

As part of the 2011-2012 annual report of the Department of Telecommunications, the Government of India formally announced its decision to implement a Centralised Monitoring System (CMS) for the “lawful interception and monitoring” of electronic communication channels in the country.

The rapid acceptance of mobile telephony and internet in India has had a profound social and economic impact on the country. However, this growth and acceptance of cyberspace in India has coincided with threats to national security and critical national infrastructure being manifested through cyberspace. A framework for legal surveillance, therefore, can be a powerful asset to the government in monitoring and countering such threats.

However, such an inherently pervasive and intrusive program cannot be deployed in a liberal democracy without an adequate level of trust between the government and its citizens and an appropriate framework of checks-and-balances to ensure that entrusted agencies do not overstep their jurisdiction. Thus, it is imperative that the Indian government take its citizens into confidence on the necessity for such a program, evolve an appropriate framework of laws, including those pertaining to privacy and data retention, and establish a system of checks-and-balances to ensure against systemic overreach prior to the implementation of the CMS.

Rohan Joshi is Fellow at The Takshashila Institution, an independent think tank on strategic affairs contributing towards building the intellectual foundations of an India that has global interests.

This document is prepared for the purpose of discussion & debate and does not necessarily constitute Takshashila’s policy recommendations. To contact us email scholars@takshashila.org.in or visit http://www.takshashila.org.in

BACKGROUND

As part of the 2011-2012 annual report of the Department of Telecommunications, the government of India formally announced[1] its decision to implement a Centralised Monitoring System (CMS) for the "lawful interception and monitoring" of electronic communication channels in the country. The ambit of this structure includes the development of capabilities to monitor and intercept mobile and land-based telecommunication and internet-based traffic for purposes of identifying or mitigating threats to the security of the country and its critical IT infrastructure. The CMS is being developed by the Centre for Development of Telematics' (C-DOT's), Telecom Enforcement, Resource and Monitoring (TERM), and once fully implemented, will be operated by the Information Bureau (IB).

Although the Indian government has chosen to remain silent on the scope and nature of the CMS, media reports[2] suggest that government bodies as varied as the Research and Analysis Wing (R&AW), National Investigation Agency (NIA), the Central Board of Direct Taxes (CBDT) and the Enforcement Directorate (ED) will have access to CMS data.

COMMENTS

The rapid acceptance of mobile telephony and internet use in India has had a profound social and economic impact on the country. As of April 2013, there were about 900 million mobile subscribers[3] (second only to China) and about 120 million users[4] of the internet in India. However, the proliferation of mobile and internet-based communication has also presented the government and law enforcement agencies with challenges pertaining to national security.

Terrorist networks are increasingly employing real-time technologies and services to instruct, communicate and disseminate propaganda. For example, terrorists were provided real-time instruction through satellite phones by their handlers in Karachi during the November 2008 terrorist attacks in Mumbai. Terrorist organisations such as al-Qaeda and Jaish-e-Mohammed have used the internet to publish and disseminate propaganda via 'e-magazines'. Thus, governments around the world are enhancing existing legal frameworks and technological capabilities to mitigate and neutralise threats to national security.

In India, the legal basis for interception is provided by the Indian Telegraph Act (1885), the Indian Telegraph Rules (1951) and the Information Technology Act (2000). As threats to the nation and to critical infrastructure manifest themselves through cyberspace, the Indian government must develop preventive, detective and forensic capabilities to address such threats. Doing so while continuing to uphold the rights of its citizens as enshrined in the Constitution of the country is undoubtedly a challenging proposition.

It is not only important, therefore, but imperative, in a liberal democracy such as India for the government to engage its citizens in the development and implementation of programmes that monitor or restrict their rights to free speech and expression. Unfortunately, the Indian government's approach to the CMS has been instructive, rather than one evolved through discourse and consensus. Indeed, a *Reuters* report[5] on the CMS program quoted an unnamed "senior telecommunications ministry official" as having said that India "need(s) surveillance. This is to protect you and your country".

This effectively means that the Indian government is urging its citizens to put their faith behind an intrusive surveillance program despite the fact that the government has neither engaged the civil society nor Parliament in discussions on its necessity, not clarified its jurisdiction, nor the checks and balances in its scope of operations. That the CMS operates, in part, under the Information Technology Act (2000), which was passed in Parliament with little debate, and makes punishable a broad range of 'offences' (Section 66A) including publishing content that is "grossly offencive or has menacing character..." or for the purpose of "causing annoyance or inconvenience," should be a matter of concern.

A legal surveillance program of this magnitude will undoubtedly collect and store vast amounts of information concerning the activities of ordinary citizens and corporations in the country. However, the absence of privacy and data retention laws in India means that there is no clarity over the information that is collected, how, where and under what conditions it is stored, who it is shared with (including local and potentially, international law enforcement agencies and governments) and how long such data is retained.

Worse, the lack of parliamentary oversight over such a program and no requirement for law enforcement agencies to report to an oversight committee on ongoing surveillance targeting Indian citizens means that operators of the CMS will enjoy sweeping powers over the collection, sharing and use of information of ordinary citizens with effectively no checks-and-balances of power. Such a program that provides the government and law enforcement agencies unbridled power over the collection, use and control of information contravenes the spirit of the Constitution over freedoms of speech and expression. Historical trends of the government of India's attempts to control the dissemination of information on the internet should be a cause for concern.

Indeed, Google's Transparency Report data between 2010-2013 indicates that requests from the government of India to Google to block content were primarily motivated not by national security concerns, but by websites it deemed to be religiously offensive (55 percent), violated individuals' privacy and security (17 percent) or criticised the government (6 percent). Only 1 percent of all requests to filter content made by the government of India to Google pertained to national security. From a technological standpoint, the implementation of the CMS will allow the Indian government to monitor land and cellular-based telephony. The CMS will provide the Indian government the ability to monitor fixed and cellular traffic on a real-time basis, as well as datamine call data records (CDRs) and session initiation protocol records (SDRs) for investigation and forensics.

It is unclear, however, as to how effective the CMS will be in providing coverage over internet-based traffic. An effective monitoring system will require the possession of the requisite technological capabilities as well as the ability to exercise control over services and service providers. As a considerable volume of internet services consumed in India today originates from providers in other countries (e.g., webmail services like Gmail or Outlook.com, or social media platforms like Facebook or Twitter), the ability of the Indian government to exercise full control over data communicated through these services or gain access to user data is questionable.

Moreover, terrorist networks are now employing popular and secure Voice over Internet Protocol (VoIP) services to communicate, which will render the CMS ineffective unless Indian agencies are able to intercept and decrypt VoIP traffic, or have active assistance from foreign governments. It is unclear as to whether these capabilities have been developed by agencies in India. The CMS will, of course, allow law enforcement agencies to monitor, filter and gain access to a large volume of unencrypted content and user data on the internet.

There are other technological challenges as well. The government of India will need to be able to provide high speed, high availability network, processing and storage infrastructure to support the massive amounts of data being captured from multiple sources and accessed by agencies across the country on a real-time basis. Further, as large amounts of data is collected over time, law enforcement agencies will need to be able to organise data in a meaningful manner so that it can be queried against and accessed for precise reporting.

Indeed, although no confirmation from the government of India exists, a report in the *Wall Street Journal*[6] indicates that parts of the CMS program have stalled as a result of the system not having the capability to accurately query data. Without the ability to query the data in the CMS, it is unlikely that law enforcement agencies will find the system to be particularly useful.

In summary, the implementation of legal interception will provide the Indian government certain capabilities to monitor or control telephonic and internet communication. However, these capabilities will also inherently provide law enforcement agencies the ability to transgress on civil liberties of Indian citizens without a system of adequate checks-and-balances. It is necessary for the Indian government to evolve appropriate laws on privacy and data protection, and implement effective parliamentary oversight over agencies with access to CMS data before the system is fully operational.

REFERENCES

[1] Annual Report, 2011- 2012, Department of Telecommunications, Ministry of Communications and Information Technology, Government of India

[2] How the world's largest democracy is preparing to snoop on its citizens, July 03, 2013, *Mint*

[3] Press Release, Telecom Regulatory Authority of India, 3rd July 2013

[4] Internet users in India, www.jana.com

[5] India sets up elaborate system to tap phone calls, email, *Reuters*, June 20, 2013

[6] India's surveillance program stalled, *India Real Time, The Wall Street Journal*, July 6, 2013