

Encryption Policy Of India Needed



Encryption Technology has many beneficial and legitimate uses these days. Without Encryption the sensitive and strategic information and details can be compromised and leaked. In the era of [M-Health](#), [Cloud Computing](#), [Internet Banking](#), [Mobile Banking](#), [E-Commerce](#), etc the absence of Encryption Policy of India is really surprising. With the matter of formulation of an [E-Mail Policy of India](#), the encryption related issues may also get some attention.

A Techno Legal Encryption Legal Framework of India is also required to prevent Unauthorised and Illegal E-Surveillance Activities that are presently rampant World over. For instance, India has launched Projects like [Aadhar](#), [National Intelligence Grid \(NATGRID\)](#), [Crime and Criminal Tracking Network and Systems \(CCTNS\)](#), [National Counter Terrorism Centre \(NCTC\)](#), [Central Monitoring System \(CMS\)](#), [Centre for Communication Security Research and Monitoring \(CCSRM\)](#), [Internet Spy System Network And Traffic Analysis System \(NETRA\) of India](#), etc. None of them are governed by any Legal Framework and none of them are under [Parliamentary Scrutiny](#). The role of Encryption becomes more crucial in these circumstances.

Use of Encryption in India has never been smooth. Intelligence Agencies in general and Central Home Ministry of India in particular are very much concerned about use of Encryption beyond 40 bits. However, what Home Ministry is not realising is that anything below 128 bits of encryption is definitely “Unsafe” and anything below 256 is “Potentially Unsafe”.

The Stakeholders that need “Higher Encryption Level Protection” includes Banks, Stock Exchanges, E-Mail Service Providers, Corporate Communications, Sensitive Government Communications, etc. It is “Not Feasible” to ask for Encryption Level below 256 bits.

Obviously, Indian Government has to take care of National Security and Law Enforcement needs as well. This does not mean we should have a “Weak Cyber Security Infrastructure” in India. On the contrary, we must ensure a Strong, Robust and Resilient [Cyber Security Infrastructure for India](#).

Perry4Law

An Exclusive Techno-Legal Corporate, IP & ICT Law Firm

New Delhi, India

At [Perry4Law Organisation](#) and [Perry4Law's Techno Legal Base \(PTLB\)](#) we believe that India should invest in establishing good Techno Legal [Offensive and Defensive Cyber Security Capabilities](#) on the one hand and Cyber Skills and [Intelligence Gathering Skills Development in India](#) on the other hand. We believe that E-Surveillance can never be an "Alternative" for good and effective Cyber Security and Intelligence Gathering Capabilities. E-Surveillance must "Supplement" Intelligence Gathering Skills and "Not Supplant" the same. This entire problem is happening because we have no Encryption Policy in India that clearly demarcates what level of Encryption can be used and what level cannot be. Further, we have no Legal Framework regarding Encryption usage in India.

We also have no Encryption Laws in India or Encryption Framework and Norms in India that have been "Prescribed" by the Parliament of India. All we have are "Encryption Guidelines" that are incorporated in various "Civil Contracts" with Telecom Companies and other such Companies. At most they are "Departmental Guidelines" but they do not have the "Force of Law".

They are indirectly made applicable as "Forced Conditions" by the Telecom Companies and other Stakeholders. The "Legality" of this is very much doubtful as "End Users" have no "Autonomy" and "Free Choice" in such cases.

The Cyber Law of India, as applicable through Information Technology Act 2000 (IT Act 2000) has a single provisions in this regard. Section 84A of IT Act 2000 says that the Central Government may prescribe the modes or methods of Encryption. Till now the Central Government has not prescribed any "modes or methods" of Encryption usage in India. In fact, the IT Act 2000 is so "Badly Drafted" that many of its provisions are "Unconstitutional" and there is an urgent need to "Repeal" the [Cyber Law of India](#) and [Indian Telegraph Act, 1885](#).

It is high time for us to formulate a Techno Legal Encryption Policy for India as soon as possible. The Encryption Policy of India must keep in mind the Commercial, Cyber Security, Cyber Law, National Security, Intelligence Agencies and Law Enforcement requirements.

Further, the Indian Encryption Policy must also keep in mind the [Civil Liberties in Cyberspace](#). Recently, the United Nations has declared that "Access to Internet" is a Human Right. Indian Government must "[Balance](#)" the National Security Requirements with Civil Liberties Protection in Cyberspace as giving "Primacy" to one over another is not feasible. The United Nations (UN) Third Committee has also approved the text titled [Right to Privacy in the Digital Age](#).

Perry4Law and PTLB hope that Indian Government would take immediate steps to accommodate these "Suggestions" of ours.

5, Jagriti Apartments, Sainik Vihar, New Delhi – 110034

Website - <http://perry4law.com/>, <http://www.ptlb.in/>, <http://perry4law.org/>