Primer on the New IT Act

Centre for Internet and Society | 2009-07-29

Pranesh Prakash

With this draft information bulletin, we briefly discuss some of the problems with the Information Technology Act, and invite your comments.

The latest amendments to the Information Technology Act 2000, passed in December 2008 by the Lok Sabha, and the draft rules framed under it contain several provisions that can be abused and misused to infringe seriously on citizens' fundamental rights and basic civil liberties. We have already written about some of the problems with this Act earlier. With this information bulletin, drafted by Chennai-based advocate Ananth Padmanabhan, we wish to extend that analysis into the form of a citizens' dialogue highlighting ways in which the Act and the rules under it fail. Thus, we invite your comments, suggestions, and queries, as this is very much a work in progress. We will eventually consolidate this dialogue and follow up with the government on the concerns of its citizens.

Intermediaries beware

Internet service providers, webhosting service providers, search engines, online payment sites, online auction sites, online market places, and cyber cafes are all examples of "intermediaries" under this Act. The Government can force any of these intermediaries to cooperate with any interception, monitoring or decryption of data by stating broad and ambiguous reasons such as the "interest of the sovereignty or integrity of India", "defence of India", "security of the State", "friendly relations with foreign States", "public order" or for "preventing incitement to" or "investigating" the commission of offences related to those. This power can be abused to infringe on the privacy of intermediaries as well as to hamper their constitutional right to conduct their business without interference.

If a Google search on "Osama Bin Laden" throws up an article that claims to have discovered his place of hiding, the Government of India can issue a direction authorizing the police to monitor Google's servers to find the source of this information. While Google can, of course, establish that this information cannot be attributed directly to the organization, making the search unwarranted, that would not help it much. While section 69 grants the government these wide-ranging powers, it does not provide for adequate safeguards in the form of having to show due cause or having an in-built right of appeal against a decision by the government. If Google refused to cooperate under such circumstances, its directors would be liable to imprisonment of up to seven years.

Pre-censorship

The State has been given unbridled power to block access to websites as long as such blocking is deemed to be in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States, and other such matters.

Thus, if a web portal or blog carries or expresses views critical of the Indo-US nuclear deal, the government can block access to the website and thus muzzle criticism of its policies. While some may find that suggestion outlandish, it is very much possible under the Act. Since there is no right to be heard before your website is taken down nor is there an in-built mechanism for the website owner to appeal, the decisions made by the government cannot be questioned unless you are prepared to undertake a costly legal battle.

Again, if an intermediary (like Blogspot or an ISP like Airtel) refuses to cooperate, its directors may be personally liable to imprisonment for up to a period of seven years. Thus, being personally liable, the intermediaries are rid of any incentive to stand up for the freedom of speech and expression.

We need to monitor your computer: you have a virus

The government has been vested with the power to authorize the monitoring and collection of traffic data and information generated, transmitted, received or stored in any computer resource. This provision is much too widely-worded.

For instance, if the government feels that there is a virus on your computer that can spread to another computer, it can demand access to monitor your e-mails on the ground that such monitoring enhances “cyber security” and prevents “the spread of computer contaminants”.

Think before you click "Send"

If out of anger you send an e-mail for the purpose of causing “annoyance” or “inconvenience”, you may be liable for imprisonment up to three years along with a fine. While that provision (section 66A(c)) was meant to combat spam and phishing attacks, it criminalizes much more than it should.

A new brand of "cyber terrorists"

The new offence of “cyber terrorism” has been introduced, which is so badly worded that it borders on the ludicrous. If a journalist gains unauthorized access to a computer where information regarding corruption by certain members of the judiciary is stored, she becomes a “cyber terrorist” as the information may be used to cause contempt of court. There is no precedent for any such definition of cyberterrorism. It is unclear what definition of terrorism the government is going by when even unauthorized access to defamatory material is considered cyberterrorism.