

# Policing the Net

## The Dangers of India's New IT Act

SIDDHARTH VARADARAJAN

Passed in the Lok Sabha on 16 May 2000 with unseemly haste, the Information Technology Act attempts to achieve two contradictory objectives. The law is premised on the assumption that the new information technologies are a liberating tool for the economy and for governance; but some of its provisions are imbued with a police mentality that seeks to control and restrain the manner in which citizens use computers. While India is one of the few countries to put in place legislation to facilitate e-commerce and protect computer networks from cyber crime, the careless manner in which some of the prescribed offences have been defined - and the sweeping powers granted to the police - make it almost certain that the law will be misused.

### Defining Obscenity

As it is, the Indian Penal Code's definition of the crime of obscenity (Section 292) is archaic and in urgent need of revision. Though the Supreme Court has narrowed the focus of obscenity through liberal interpretation of existing statutes, law enforcement officials and lower courts frequently entertain the flimsiest of 'obscenity' petitions. When the same IPC definition of obscenity is made applicable to the 'publishing' or 'transmitting' of material in electronic form, chances are that a wide range of Internet related material could come within the ambit of the law.

The IT Act defines as obscene "any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons...who are likely to read, see or hear the matter contained or embodied in it". The penalty for a first offence is 5 years imprisonment; subsequent convictions will result in 10 years imprisonment. Leaving aside for the moment the subjective and arbitrary nature of the definition, neither the bureaucrats and 'experts' who drafted the IT law, nor the parliamentary standing committee which vetted its provisions, have applied their mind to the problem of defining what exactly 'publishing' and 'transmitting' entail in the context of the Internet.

Let us imagine that an 'obscene' website existing out in cyberspace is accessed by a customer of a cyber cafe. He may have explicitly sought the site or clicked on it in error out of a long list of sites thrown up by a search engine. If you don't believe that can happen, try searching for 'White House' on any engine and see what you get.

Once the 'lascivious' site appears, could the cyber cafe owner be hauled up for allowing it to come up on one of his computers? Could the customer be accused of attempting

to 'deprave and corrupt' a police officer who happens to glance at the screen? And what happens if the URL of the site is stored in the browsing software's history or in the computer's cache? Would that amount to publishing and transmitting? Finally, what about sites that provide a search engine or chat rooms? Could they too be targeted?

What makes the IPC Act especially dangerous is that the nebulousness of the prescribed offence is matched by the sweeping nature of the powers granted to the police. Police officers, and even ordinary government officials, are allowed to search public places like cyber cafes and arrest persons suspected of committing a crime under the new law. Clause 79 of the IT Act reads: "Notwithstanding anything contained in the Code of Criminal Procedure (CrPC), any police officer, not below the rank of a Deputy Superintendent of Police, or any other officer of the Central government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act".

### **Police Abuse**

Curiously, IT minister Pramod Mahajan told Parliament that this clause was actually a 'safeguard' since the CrPC grants similar search and arrest powers to any policeman and not just to a senior officer. But this explanation is faulty on three accounts.

> First, it ignores the fact that the relevant provisions of the CrPC - Sections 151 and 157 in particular - are routinely abused by the police. Section 151, in fact, says any person so arrested can only be held in prison for 24 hours. Though this is rarely followed, persons arrested without a warrant under the IT Act have not even been given the benefit of such a safeguard.

> Second, the CrPC does not grant the police such powers for non-cognisable offences. Certain offences under the IPC such as Sections 172, 173, 175 (omission to produce document to public servant by persons legally bound to produce it) and 204 (destruction of document to prevent its production as evidence) are non-cognisable and hence the police cannot simply arrest a person without a warrant. Under the IT Act, the electronic versions of these crimes have, by default, become cognisable since the police have been granted the power to act on their own without a magistrate's authorisation.

> The IT Act empowers not just police officers but any class of government official as decided by the government.

The IT Act seems to be especially targeted at 'public places' (i.e. cyber cafes), where more than 75 per cent of Indian net users access the web.

### **New Law, Old Notion**

According to new media theorist Ravi Sundaram, the IT Act is built on the premise of 19th century definitions of territoriality. "Crime needs a physical location and this territory must be policed. The new law is shot through with this notion".

During the Standing Committee's review of the draft, in fact, MPs were quickly convinced by the arguments of Delhi's police commissioner of the need to watch cyber cafes. They inserted an amendment making it mandatory, on pain of imprisonment, for cyber cafe

owners to maintain a record of the identity of their customers and a list of web sites visited by them. Fortunately, better sense prevailed and at the last moment the Vajpayee government agreed to drop this amendment.

However, the clauses on obscenity and police powers were not dropped or modified. When these begin to be invoked by petty officials or those with a political or 'culturalist' agenda, one can only hope that the courts will step in to protect the citizen's right to information and unfettered communication. In the mean time, the government should give serious thought to amending the Act to eliminate the scope for abuse.

To,  
The Editor  
The Hindu

Re: Covert Censorship

Sir,

I am a subscriber to VSNL's Internet service with the following email address skaziknde.vsnl.net.in. Since September end, 2000, I noticed that all emails to and from me to Middle East Socialist Network (MESN) could neither go through nor reach me. MESN is an e-group with 123 members across the world who receive messages regarding news and political developments in that region. Its members are largely researchers or people interested in political events and struggles in that region. Anyone can access the MESN website and messages at [www.egroups.com/group/mesn](http://www.egroups.com/group/mesn).

After futile attempts to set things right myself, I came to know from the MESN moderator that my account had, for some unknown reason, been 'blocked' by my server. On October 31, upon visiting the VSNL office at Bangla Sahib Road, it was confirmed by VSNL that my account had indeed been blocked. Upon inquiring as to why this had been done without my knowledge or consent, one of VSNL's managers - Mr. Goel from the Customer Services Section - informed me that since "Muslims have links with Pakistan and because of reasons of security", they had taken this step. Upon protesting this covert, undeclared censorship, Mr. Goel, with a grandiose gesture, declared "We can do anything". He alleged that "some people" had complained against me - an allegation which he has failed to prove or substantiate. MESN only emails its subscribers, and also has an anti-spamming policy, so the question of anyone receiving any unsolicited mail from MESN does not arise.

My mail was 'unblocked' after filing a written complaint and meeting a couple of other managers! Needless to say VSNL is still to account for its outrageous unwarranted policing and censorship of my mail. I would like to ask Mr. Goel and VSNL: is this how you treat your Muslim customers? Are we, once again, to be collectively branded and placed in the 'suspect' category due to the prejudice and communal bias of VSNL officers?

Seema Kazi, New Delhi