India's Broken Internet Laws Need a Shot of Multi-stakeholderism

Centre for Internet and Society | 2012-04-26

Pranesh Prakash

Cyber-laws in India are severely flawed, with neither lawyers nor technologists being able to understand them, and the Cyber-Law Group in DEIT being incapable of framing fair, just, and informed laws and policies. Pranesh Prakash suggests they learn from the DEIT's Internet Governance Division, and Brazil, and adopt multi-stakeholderism as a core principle of Internet policy-making.

(An edited version of this article was published in the Indian Express as "Practise what you preach" on Thursday, April 26, 2012.)

The laws in India relating to the Internet are greatly flawed, and the only way to fix them would be to fix the way they are made. The Cyber-Laws & E-Security Group in the Department of Electronics and Information Technology (DEIT, who refer to themselves as 'DeitY' on their website!) has proven itself incapable of making fair, balanced, just, and informed laws and policies. The Information Technology (IT) Act is filled with provisions that neither lawyers nor technologists understand (not to mention judges). (The definition of "computer source code" in s.65 of the IT Act is a great example of that.)

The Rules drafted under s.43A of the IT Act (on 'reasonable security practices' to be followed by corporations) were so badly formulated that the government was forced to issue a clarification through a press release, even though the clarification was in reality an amendment and amendments cannot be carried out through press releases. Despite the clarification, it is unclear to IT lawyers whether the Rules are mandatory or not, since s.43A (i.e., the parent provision) seems to suggest that it is sufficient if the parties enter into an agreement specifying reasonable security practices and procedures. Similarly, the "Intermediary Guidelines" Rules (better referred to as the Internet Censorship Rules) drafted under s.79 of the Act have been called "arbitrary and unconstitutional" by many, including MP P. Rajeev, who has introduced a motion in the Rajya Sabha to repeal the Rules ("Caught in a net", Indian Express, April 24, 2012). These Rules give the power of censorship to every citizen and allow them to remove any kind of material off the Internet within 36 hours without anybody finding out. Last year, we at the Centre for Internet and Society used this law to get thousands of innocuous links removed from four major search engines without any public notice. In none of the cases (including one where an online

news website removed more material than the perfectly legal material we had complained about) were the content-owners notified about our complaint, much less given a chance to defend themselves.

Laws framed by the Cyber-Law Group are so poorly drafted that they are misused more often than used. There are too many criminal provisions in the IT Act, and their penalties are greatly more than that of comparable crimes in the IPC. Section 66A of the IT Act, which criminalizes "causing annoyance or inconvenience" electronically, has a penalty of 3 years (greater than that for causing death by negligence), and does not require a warrant for arrest. This section has been used in the Mamata Banerjee cartoon case, for arresting M. Karthik, a Hyderabad-based student who made atheistic statements on Facebook, and against former Karnataka Lokayukta Santosh Hegde. Section 66A, I believe, imperils freedom of speech more than is allowable under Art. 19(2) of the Constitution, and is hence unconstitutional.

While s.5 of the Telegraph Act only allows interception of telephone conversations on the occurrence of a public emergency, or in the interest of the public safety, the IT Act does not have any such threshold conditions, and greatly broadens the State's interception abilities. Section 69 allows the government to force a person to decrypt information, and might clash with Art.20(3) of the Constitution, which provides a right against self-incrimination. One can't find any publicly-available governmental which suggests that the constitutionality of provisions such as s.66A or s.69 was examined.

Omissions by the Cyber-Law Group are also numerous. The Indian Computer Emergency Response Team (CERT-In) has been granted very broad functions under the IT Act, but without any clarity on the extent of its powers. Some have been concerned, for instance, that the broad power granted to CERT-In to "give directions" relating to "emergency measures for handling cyber security incidents" includes the powers of an "Internet kill switch" of the kind that Egypt exercised in January 2011. Yet, they have failed to frame Rules for the functioning of CERT-In. The licences that the Department of Telecom enters into with Internet Service Providers requires them to restrict usage of encryption by individuals, groups or organisations to a key length of only 40 bits in symmetric key algorithms (i.e., weak encryption). The RBI mandates a minimum of 128-bit SSL encryption for all bank transactions. Rules framed by the DEIT under s.84A of the IT Act were to resolve this conflict, but those Rules haven't yet been framed.

All of this paints a very sorry picture. Section 88 of the IT Act requires the government, "soon after the commencement of the Act", to form a "Cyber Regulations Advisory Committee" consisting of "the interests principally affected or having special knowledge of the subject-matter" to advise the government on the framing of Rules, or for any other purpose connected with the IT Act. This body still has not been formed, despite the lag of more than two and a half years since the IT Act came into force. Justice Markandey Katju's recent

letter to Ambika Soni about social media and defamation should ideally have been addressed to this body.

The only way out of this quagmire is to practise at home that which we preach abroad on matters of Internet governance: multi-stakeholderism. Multi-stakeholderism refers to the need to recognize that when it comes to Internet governance there are multiple stakeholders: government, industry, academia, and civil society, and not just the governments of the world. This idea has gained prominence since it was placed at the core of the "Declaration of Principles" from the first World Summit on Information Society in Geneva in 2003, and has also been at the heart of India's pronouncements at forums like the Internet Governance Forum. Brazil has an "Internet Steering Committee" which is an excellent model that practices multi-stakeholderism as a means of framing and working national Internet-related policies. DEIT's Internet Governance Division, which formulates India's international stance on Internet governance, has long recognized that governance of the Internet must be done in an open and collaborative manner. It is time the DEIT's Cyber-Law and E-Security Group, which formulates our national stance on Internet governance, realizes the same.