Short note on IT Amendment Act, 2008

Centre for Internet and Society | 2010-02-01

Pranesh Prakash

Pranesh Prakash of the Centre for Internet and Society wrote a short note in February 2009 on the Information Technology (Amendment) Act, 2008. This is being posted as a precursor to a more exhaustive analysis of the Act and the rules sought to be promulgated under the Act.

The new amendments to the Information Technology Act, 2000 that got passed by the Lok Sabha last December deserve a careful reading. There are a number of positive developments, as well as many which dismay. Positively, they signal an attempt by the government to create a dynamic policy that is technology neutral. This is exemplified by its embracing the idea of electronic signatures as opposed to digital signatures. But more could have been done on this front (for instance, section 76 of the Act still talks of floppy disks). There have also been attempts to deal proactively with the many new challenges that the Internet poses.

Freedom of Expression

The first amongst these challenges is that of child pornography. It is heartening to see that the section on child pornography (s.67B) has been drafted with some degree of care. It talks only of sexualized representations of actual children, and does not include fantasy play-acting by adults, etc. From a plain reading of the section, it is unclear whether drawings depicting children will also be deemed an offence under the section. Unfortunately, the section covers everyone who performs the conducts outlined in the section, including minors. A slight awkwardness is created by the age of "children" being defined in the explanation to section 67B as older than the age of sexual consent. So a person who is capable of having sex legally may not record such activity (even for private purposes) until he or she turns eighteen.

Another problem is that the word "transmit" has only been defined for section 66E. The phrase "causes to be transmitted" is used in section 67, 67A, and 67B. That phrase, on the face of it, would include the recipient who initiates a transmission along with the person from whose server the data is sent. While in India, traditionally the person charged with obscenity is the person who produces and distributes the obscene material, and not the consumer of such material. This new amendment might prove to be a change in that position.

Section 66A which punishes persons for sending offensive messages is overly broad, and is patently in violation of Art. 19(1)(a) of our Constitution. The

fact that some information is "grossly offensive" (s.66A(a)) or that it causes "annoyance" or "inconvenience" while being known to be false (s.66A(c)) cannot be a reasons for curbing the freedom of speech unless it is directly related to decency or morality, public order, or defamation (or any of the four other grounds listed in Art. 19(2)). It must be stated here that many argue that John Stuart Mill's harm principle provides a better framework for freedom of expression than Joel Feinberg's offence principle. The latter part of s.66A(c), which talks of deception, is sufficient to combat spam and phishing, and hence the first half, talking of annoyance or inconvenience is not required. Additionally, it would be beneficial if an explanation could be added to s.66A(c) to make clear what "origin" means in that section. Because depending on the construction of that word s.66A(c) can, for instance, unintentionally prevent organisations from using proxy servers, and may prevent a person from using a sender envelope different form the "from" address in an e-mail (a feature that many e-mail providers like Gmail implement to allow people to send mails from their work account while being logged in to their personal account). Furthermore, it may also prevent remailers, tunnelling, and other forms of ensuring anonymity online. This doesn't seem to be what is intended by the legislature, but the section might end up having that effect. This should hence be clarified.

Section 69A grants powers to the Central Government to "issue directions for blocking of public access to any information through any computer resource". In English, that would mean that it allows the government to block any website. While necessity or expediency in terms of certain restricted interests are specified, no guidelines have been specified. Those guidelines, per s.69A(2), "shall be such as may be prescribed". It has to be ensured that they are prescribed first, before any powers of censorship are granted to any body. In India, it is clear that any law that gives unguided discretion on an administrative authority to exercise censorship is unreasonable (*In re Venugopa*l, AIR 1954 Mad 901).

Intermediary Liability

The amendment to the provision on intermediary liability (s.79) while a change in the positive direction, as is seeks to make only the actual violators of the law liable for the offences committed, still isn't wide enough. This exemption is required to be widely worded to encourage innovation and to allow for corporate and public initiatives for sharing of content, including via peer-to-peer technologies.

Firstly, the requirement of taking down content upon receiving "actual knowledge" is much too heavy a burden for intermediaries. Such a requirement forces the intermediary to make decisions rather than the appropriate authority (which often is the judiciary). The intermediary is no position to decide whether a Gauguin painting of Tahitian women is obscene or not, since that requires judicial application of mind. Secondly, that requirement is vitiates the principles of natural justice and freedom of expression because it allows a communication

and news medium to be gagged without giving it, or the party communicating through it, any due hearing. It has been held by our courts that a restriction that does not provide the affected persons a right to be heard is procedurally unreasonable (*Virendra v. State of Punjab*, AIR 1957 SC 896).

The intermediary loses protection of the act if (a) it initiates the transmission; (b) selects the receiver of the transmission; and (c) selects or modifies the information. While the first two are required to be classified as true "intermediaries", the third requirement is a bit too widely worded. For instance, an intermediary might automatically inject advertisements in all transmissions, but that modification does not go to the heart of the transmission, or make it responsible for the transmission in any way. Similarly, the intermediary may have a code of conduct, and may regulate transmissions with regard to explicit language (which is easy to judge), but would not have the capability to make judgments regarding fair use of copyrighted materials. So that kind of "selection" should not render the intermediary liable, since misuse of copyright might well be against the intermediary's terms and conditions of use.

Privacy and Surveillance

While the threat of cyber-terrorism might be very real, blanket monitoring of traffic is not the way forward to get results, and is sure to prove counter-productive. It is much easy to find a needle in a small bale of hay rather than in a haystack. Thus, it must be ensured that until the procedures and safeguards mentioned in sub-sections 69(2) and 69B(2) are drafted before the powers granted by those sections are exercised. Small-scale and targetted monitoring of metadata (called "traffic data" in the Bill) is a much more suitable solution, that will actually lead to results, instead of getting information overload through unchannelled monitoring of large quantities of data. If such safeguards aren't in place, then the powers might be of suspect constitutionality because of lack of guided exercise of those powers.

Very importantly, the government must also follow up on these powers by being transparent about the kinds of monitoring that it does to ensure that the civil and human rights guaranteed by our Constitution are upheld at all times.

Encryption

The amending bill does not really bring about much of a change with respect to encryption, except for expanding the scope of the government's power to order decryption. While earlier, under section 69, the Controller had powers to order decryption for certain purposes and order 'subscribers' to aid in doing so (with a sentence of up to seven years upon non-compliance), now the government may even call upon intermediaries to help it with decryption (s.69(3)). Additionally, s.118 of the Indian Penal Code has been amended to recognize the use of encryption as a possible means of concealment of a 'design to commit [an] offence punishable with death or imprisonment for life'.

The government already controls the strength of permissible encryption by way of the Internet Service Provider licences, and now has explicitly been granted the power to do so by s.84A of the Act. However, the government may only prescribe the modes or methods of encryption "for secure use of the electronic medium and for promotion of e-governance and e-commerce". Thus, it is possible to read that as effectively rendering nugatory the government's efforts to restrict the strength of encryption to 40-bit keys (for symmetric encryption).

Other Penal Provisions

Section 66F(1)(B), defining "cyberterrorism" is much too wide, and includes unauthorised access to information on a computer with a belief that that information may be used to cause injury to decency or morality or defamation, even. While there is no one globally accepted definition of cyberterrorism, it is tough to conceive of slander as a terrorist activity.

Another overly broad provision is s.43, which talks of "diminish[ing] its value or utility" while referring information residing on a computer, is overly broad and is not guided by the statute. Diminishing of the value of information residing on a computer could be done by a number of different acts, even copying of unpublished data by a conscientious whistleblower might, for instance, fall under this clause. While the statutory interpretation principle of *noscitur a socii* (that the word must be understood by the company it keeps) might be sought to be applied, in this case that doesn't give much direction either.

While all offences carrying penalties above three years imprisonment have been made cognizable, they have also been made bailable and lesser offences have been made compoundable. This is a desirable amendment, especially given the very realistic possibility of incorrect imprisonments (Airtel case, for instance), and frivolous cases that are being registered (Orkut obscenity cases).

Cheating by personation is not defined, and it is not clear whether it refers to cheating as referred to under the Indian Penal Code as conducted by communication devices, or whether it is creating a new category of offence. In the latter case, it is not at all clear whether a restricted meaning will be given to those words by the court such that only cases of phishing are penalised, or whether other forms of anonymous communications or other kinds of disputes in virtual worlds (like Second Life) will be brought under the meaning of "personation" and "cheating".

While it must be remembered that more law is not always an answer to dealing with problems, whether online or otherwise, it is good to note that the government has sought to address the newer problems that have arisen due to newer technologies. But equally important is the requirement to train both the judiciary and the law enforcement personnel to minimize the possibility of innocent citizens being harassed.