Content Regulation on Mobile Phones:
The current legal position of Indian service providers
Mohd. Salman Waris
mohdsalmanwaris@gmail.com

Evolving technological innovation will continue to drive opportunities for their misuse as instruments in crime. In an over legislated country with a dubious enforcement record, it would be prudent not to rush in by adopting 3G mobile technology without having a proper legislative framework in place to regulate its misuse. This has become all the more important in view of the recent MMS sex clip expose.¹

The seriousness of the situation is evident from the fact that not a single conviction so far has taken place under the Information Technology Act 2000. The filing of a recent PIL in the Supreme Court of India against unsolicited voice calls to consumers by telemarketers, the DPS MMS scandal, are only some of the repercussions of a slack regulatory environment and can be seen as just the beginning of woes for the Indian service providers.

Under the provisions of section 79 of the present Indian Information Technology Act 2000 an NSP can escape liability for any third party information or data made available by him if he proved that the offence was committed without his knowledge or that he had exercised all due diligence to the commissioning of the such offence. The Act describes a “network service provider” as an intermediary and “third party information” as any information dealt with him as an intermediary. The IT Act itself has obsolescence built into it, as the terms “due diligence” is not defined. While Supreme Court of India on the other hand has only used the “test of a reasonable man” to determine this. Now under the present legal situation with reference to the Information Technology Law, this can only be interpreted to mean compliance in terms of production, retention, transmission and storage of all information. Internationally the access providers in general claim that they merely acting as messengers and their role should be compared to that of a publisher. Yet, technically speaking it resembles that played by telephone companies, which connect callers or interconnect fax and data transmissions.

In the Church of Scientology case the court in Netherlands decided that the information providers do nothing more than offer an opportunity to publish, and that in principle they are unable to exercise influence on, or even be aware of what people say or are able to say on the internet. It follows that there is in principle no reason to hold the service provider liable for unlawful acts committed by the users. However, liability could be assumed in situations in which it is unmistakably clear that a

publication of a user is unlawful and in which it may be assumed in all reasonableness that this is also known to the service provider, for example the service provider has been informed about this. Applying this analogy to the MMS scandal we arrive at a conclusion that Bazee.com was not liable in the case as the offending CD was on the site for just over 40 hours and Bazee.com blocked transactions as soon as it was informed that the CD actually depicts the infamous Delhi Public School sex clip. Besides the website already had a sophisticated software installed on its server that sieved through the content being uploaded for auction for terms like sex, pornography, guns etc. Thus, in this case Bazee.com should not have been held liable, but the police took a very restrictive interpretation of the relevant section and hurriedly moved in taking advantage of another infamous section of the I.T Act, section 80 that gives them sweeping powers.

It is not that Indian service providers do not at present comply with any laws and standards. Many do conform to international standards but in a situation where there is no specific law dealing with and regulating the functioning for the Indian Service providers, be it the internet service providers or for that matter the mobile service providers, it is in the Indian industry’s interest to collectively evolve a stringent information security and privacy policy that would have to be compulsorily complied with. This has become all the more important with the proposed launch of 3G technology in India in the coming months.

With the launch of 3G technology the stakes would become three times higher for what crime was committed over a period of several weeks in the DPS MMS case, i.e. publishing of information obscene in nature when the MMS clip of “Delhi girls having fun” was converted into a CD and put up for sale on Bazee.com, with 3G technology can be committed with in a matter of few minutes. This new technology involves the first truly portable internet devices characterized by internet access at GPRS speeds, with video streaming and capture and broadband applications and download speeds increasing up to 384 Kb/s, and also provide rich media streaming, video, audio and graphics and allow access to colour WAP and MMS as well as SMS chat and mobile services personalization in the form of icons and logos, content and premium SMS as a method of payment for content and mobile internet search engines such as mopilot, enhanced features like internet browsers, embedded software like multimedia players for viewing and recording audio and video clips, larger color screens and java applications that enable individuals to the access a growing variety of content through the hand held mobile devices.

Hence, there have arisen serious judicial concerns of techno-legal dimension, with the advent of these new forms of communications, the legal fraternity is now faced with several major challenges such as identity and fixity of liability for misuse of these high tech. services and the extent of responsibility of the operators and service providers. It would be essential to explore the questions and the complications that revolve around the facilities provided by the service providers an put in place a proper regime to regulate content on 3G mobile phones.

Though the government has proposed certain changes in the present Information Technology Act 2000, however a cursory glance of the proposed amendments would convince the reader that while on one hand it tries to remove the ambiguities in some provisions of the old act on the other hand it also introduces several provisions that would as such make the practical implementation of the act and prosecutions of the cyber criminals a nightmare. The existing Sections (viz. 43, 65, 66 and 72) have been
revisited and some amendments/more stringent provisions have been provided for, to do away with concerns about the operating provisions in IT Act related to “Data Protection and Privacy” in addition to contractual agreements between the parties. There is a proposal to add Sec. 43(2) related to handling of sensitive personal data or information with reasonable security practices and procedures thereto. According to provisions of section 43 (2), “If any body corporate, that owns or handles sensitive personal data or information in a computer resource that it owns or operates, is found to have been negligent in implementing and maintaining reasonable security practices and procedures, it shall be liable to pay damages by way of compensation not exceeding Rs. 1 crore Approx. $220,000, to the person so affected.

Also, a gradation has been made of severity of computer related offences committed dishonestly or fraudulently and punishment thereof under Section 66. Besides, the language of Section 66 penalising computer related offences has been revised to be in lines with Section 43 related to penalty for damage to computer resource. Further, with the intent to protect the privacy of the individual subscribers, there is also a proposal for inserting an additional Section 72 (2) that deals with breach of confidentiality with intent to cause injury to a subscriber. According to this section, “if any intermediary who by virtue of any subscriber availing his services has secured access to any material or other information relating to such subscriber, discloses such information or material to any other person, without the consent of such subscriber and with intent to cause injury to him, such intermediary shall be liable to pay damages by way of compensation not exceeding Rs. 25 lakhs to the subscriber so affected.”

The amendments to the IT Act, which have been submitted to the law ministry for approval, address issues never explored before in Indian legal history. The issues of privacy, including the definition of what constitutes a private moment and which are the private parts of a human body, have all been dealt with in the new version of the Act submitted to the law ministry.

There is strict legislation governing privacy in all developed countries, but this is the first time these issues have been addressed in India. The law on privacy in India, as it stands today, is limited to the right enshrined under Article 21 of the Constitution and case law on the subject. However, like other fundamental rights, it is not absolute, and is subject to reasonable restrictions imposed by the state. The proposed amendments add a paragraph to the IT Act which states, “Whoever intentionally captures or broadcasts an image of an individual without consent, and knowingly does so under circumstances violating the privacy of that individual, shall be held liable.” This is the first time that a right to privacy has so expressly found its way into the statute books in India.

The Act also recommends a compensation of Rs 25 lakh to the person whose privacy has been infringed. The offender can also be jailed for one year with a fine of Rs 2 lakh. This means that even television channels which carry images of MMS clips can be held liable even though they may not have originally captured it.

‘Private area’ has also been defined in the Act in detail to prevent any misinterpretation. While, defining this in detail narrows its misuse, the impact of the legislation is reduced. Infringement of privacy may not just involve images of a person disrobed or their private parts. Even the law on obscenity does not define privacy, but leaves it to interpretation to capture it in entirety as it may vary from person to person and may even be affected by religious leanings.
Violation of privacy has been much more widely defined as “circumstances in which a reasonable person would believe he or she could disrobe in privacy without being concerned that an image or a private area of the individual is being captured.” Thus the Act has limited the definition of privacy by curtailing it to just disrobing. The definition also covers public places. It says, “Circumstances in which a reasonable person would believe that a private area of the individual would not be visible to the public, regardless of whether that person is in a public or a private place.” On the issue of child pornography, which has again not been expressly covered under the Indian statute, the Act takes a fairly conservative view. For the purpose of child pornography, the Act defines it as material that features a child engaged in sexually explicit conduct. According to lawyers, famous cases in the West like those involving Michael Jackson’s have shown that it need not be “sexually explicit conduct”.

The Information Technology Act of 2000 at present covers only unauthorized access and data theft from computers and networks, with a maximum penalty of about $220,000, and does not have specific provisions relating to privacy of data. The new clauses are likely to enable the act to conform to the so-called adequacy norms of the European Union’s (EU) Data Protection Directive and the Safe Harbor privacy principles of the U.S.

A Practical Solution A practical solution to the present paradox is to have an industry self-regulatory body (like IBF) that plays the role of policy maker & day-to-day watchdog. Along with a “higher authority” (Government body), this will periodically audit the watchdog and ensure that it stays in line. Such a step would not be out of sync with the current trend both at the national as well as the international level. Some time back, the Indian Broadcasting Federation (IBF) the Indian television industry official body, has announced their proposed code for regulation of content for satellite TV channels. Billed as the mother of all codes, this set of rules is part of an ongoing attempt at self-regulation. Considering that IBF guidelines are more stringent than the Indian Government’s programming code. Besides, the fact that IBF had earlier published norms for surrogate advertising, speaks volumes of the industry serious intention about self-regulation. On another front, the Indian Editors Guild has announced a draft code for Print & TV journalists. Earlier, a former Press Council Chairman had also suggested setting up of a Media Council to keep watch on the electronic & print media. Towards this end, the Govt’s proposed Media Council Act will lay down guidelines to regulate content for the media & media persons, as Cable Television Network Act has nowhere specified provisions for the regulation of content.

While the conflicting sets of judicial anxieties that revolve around Information technology, data protection and privacy issues, have necessitated the fine-tuning and radical overhauling of omnipotent and omniscience technological jurisprudence and the regulatory mechanism governing mobile content and data in India. The present mess surrounding the Indian mobile service providers and other technology crime issues that Indian mobile industry stands in today is a product of India’s’ eagerness to project itself as the new IT destination during the DotCom boom by framing a legislation where issues related to privacy, content regulation and data protection where overlooked. Hence, its high time that Indian government learnt from its mistakes of the past and came up with a comprehensive law that provides for a secure data future. There is an urgent need to dove tail the regulatory concerns and technological imperatives of Information Technology and outsourcing communications. There is also a necessity to address the issues that arise due to the trans-border nature of the data
transfers, the rights and liabilities of the various parties involved in the process and the steps which can be taken to curb future misuse of sensitive personal data of offshore clients, to arrive at a sui generis law in the conspectus of global and comparative jurisprudence.