

Recommendations to Proposed Amendments to Information Technology Act 2000

By
OneWorld South Asia

September 27, 2005

1. Background

On August 29, 2005, the Government of India released the Final Report of the Expert Committee on Amendments to IT Act 2000 (referred hereafter ‘the Amendment’), formed in January 2005. The Department of Information Technology, Ministry of Communications and Information Technology (Government of India) thereafter requested feedbacks from the members of the public on the said Amendment. Accordingly, OneWorld South Asia, a network of partners in development, organized a consultation on 23 September 2005 with experts to draw opinions from the development sectors on the implications of the Amendment to the wider socio-economic development. To elicit views from its partner organizations, OneWorld South Asia hosted a Consultation, engaging its partners and experts in this field. Delegates reached to certain viewpoints that Government of India shall consider to effectively implement the Amendment for the purpose of socio-economic development.

2. Specific recommendations

2. 1. E-governance

a. **Recognising** that e-governance mechanism facilitates Right to Information Act, 2005 (referred hereafter RTI Act, 2005), the Amendment shall provide provisions to enactment of the provisions laid down in the Right to Information Act, 2005, which, “means the right to information accessible under this Act which is held by or under the control of any public authority and includes the right to—(i) inspection of work, documents, records; (ii) taking notes, extracts or certified copies of documents or records; (iii) taking certified samples of material; (iv) obtaining information in the form of diskettes, floppies, tapes, video cassettes or in any other electronic mode or through printouts where such information is stored in a computer or in any other device”;

Recognising that the Amendment specifies, in Chapter III, Section 2, that, “(2) The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe- (a) the manner and format in which such electronic records shall be filed, created or issued; (b) the manner or method of payment of any fee or charges for filing, creation or issue, or delivery of service either directly or through its authorized service provider, of any electronic record under clause (a)”;

Recommendations to Amendments to IT Act 2000

We call for a definition of e-governance that encapsulates the essence of RTI Act, 2005; understanding that the term ‘e-governance’ extends to the provisioning of people’s participation in governance through ICT means, hence the need for a clear definition in the Act.

We call for appropriate provisions for creating the governmental e-governance machinery accountable to the members of the public, as espoused in the RTI Act, 2005 – particularly in reference to Chapter II of the Act (Right to information and obligations of public authorities).

2. 2. Controller

b. **Recognising** that the Amendment in its Section 17 (1), Chapter VI, has authorised the Central Government to appoint a ‘Controller’ with several functions, including, “ 18 (f) specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of an Electronic Signature Certificate and the public key”; “(g) specifying the form and content of an Electronic Signature Certificate and the key”, among others;

Realising that the Controller of Certifying Authorities is a public regulatory body;

We call for a re-examination of the composition of existing Controller of Certifying Authorities, whereby making a provision for civil society organisations (CSOs) to participate as the Member of the Board of Controller.

2. 3. Computer related offences

c. **Recognising** that information revolution demands that every citizen shall have access to computing resources and that access to computing resources can be shared using ‘cyber café’ or ‘public access centres’;

We call for lawful exemption to the users of the public access centres from penalties (or ‘Common Service Centre’ as defined by Department of Information Technology in “Establishment of 100,000 Common Service Centres”; or Village Knowledge Centre, referred to the budget speech of Union Budget 2005-06 by Shri P. Chidambaram, Union Finance Minister) as prescribed in Section 43, Chapter IX (Compensation for damage to computer, computer system, etc.; Penalties and Adjudication) of the Amendment.

We call for a demarcation between cyber cafes, which provide electronic services on a commercial basis, for generating profits; and cyber cafes (referred as “Common Service Centre” or “Village Knowledge Centre”) which provide electronic services for

community development – to exempt the latter (CSC) from the purview of intermediary liability as provided in Section 79, Chapter XII.

2. 4. Publishing obscene information

d. **Recalling** that India is a signatory to the “Convention on the Rights of the Child”, Adopted and opened for signature, ratification and accession by UN General Assembly resolution 44/25 of 20 November 1989, which calls for states to guarantee the protection of children from pornography, stating that,

Article 16

1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.
2. The child has the right to the protection of the law against such interference or attacks.

Article 17

States Parties recognize the important function performed by the mass media and shall ensure that the child has access to information and material from a diversity of national and international sources, especially those aimed at the promotion of his or her social, spiritual and moral well-being and physical and mental health. To this end, States Parties shall:

- (e) Encourage the development of appropriate guidelines for the protection of the child from information and material injurious to his or her well-being, bearing in mind the provisions of articles 13 and 18.

Realising that combating pornography in electronic format requires extensive capacity building among the law enforcement agencies; central, provincial and local governmental authorities; sensitising and awareness-raising among parents, children and the general public; technological and human capacity building among intermediaries (e.g. Internet Service Providers or ISPs); among others;

We call for the establishment of an independent federal body composed of representatives of government, private sector and the civil society, to undertake, supervise, encourage such measures that help curbing the child pornography (paedophile);

We recognise that such a public body is also be made responsible for acting against online sexual harassments, spam, adware, spyware, and other forms of cyber crimes.

2. 5. Provisions for Adhering to Disable-friendly Technology

e. **Recognising** that the shared ‘public access centres’ or ‘cyber cafes’ shall be equipped with facilities appropriate to the physically challenged persons, that computers in these centres need to be equipped with screen reader software and screen magnifier software in local language;

We call for the Amendment to propose a set of standards for manufacturing and service provisioning of electronic equipment adhering to the disabled-friendly technology standards.

2. 6. Penalty for Cyber Crime

f. **Recognising** that electronic crime pervades all media;

We call for retention of imprisonment terms as laid down in Chapter XI of the original Act.

3. Major International and National ICT Instruments

This recommendation draws significantly from international and national ICT policies that include:

3.1 World Summit on the Information Society. Declaration of Principles and Plan of Action.

3.2 The United Nations Convention on the Rights of the Child

3.3 Declaration and Action Plan. Sexual Abuse of Children, Child Pornography and Paedophilia on the Internet: An international challenge - Expert Meeting, UNESCO, Paris, 18-19 January

3.4 Government of India. Right to Information Act, 2005

3.5 Government of India. National E-governance Action Plan.

3.6 Mission 2007. Recommendations by Taskforces of Connectivity, Content, Care & Management, Capacity Building and Coordination. Second National Consultation of Mission 2007, July 2005, New Delhi.

4. About OneWorld South Asia

OneWorld South Asia, based in New Delhi, India, is a part of the OneWorld Network, which was formed in the U.K. in 1995. It is an international non-profit network engaged in using ICTs like the Internet, mobile telephones and community radio for poverty alleviation. With more than 500 organisations including NGOs, donors, multilateral organisations, private sector, media, academicians and governments as its partners, OneWorld South Asia (OWSA) is dedicated to “voicing the voiceless” and positioning of ICTs towards realisation of Millennium Development Goals (MDGs).OWSA focuses on developing appropriate programmes and projects, which would enhance communication opportunities, build capacities and explore alternative tools and techniques for empowering the grassroots. Besides, OWSA undertakes several initiatives to build and strengthen Communities of Practice (CoPs) around the MDGs to facilitate knowledge and information sharing in the region through a bouquet of on-line and off-line methods.OWSA’s key programmes include Grassroots Communication, Knowledge for Development, Research and Analysis, and Policy Advocacy supported by Capacity Building & Technical Services and Partnerships & Networking.

Ends