Rules & Regulations Review

The Information Technology Rules, 2011

Key Features of the Rules

- Four sets of Rules have been introduced under the Information Technology Act, 2000, as amended by the Information Technology (Amendment) Act, 2008.
- The Security Practices Rules require entities holding sensitive personal information of users to maintain certain specified security standards.
- The Intermediary Guidelines Rules prohibit content of specific nature on the internet. An intermediary, such as a website host, is required to block such content.
- The Cyber Café Rules require cyber cafés to register with a registration agency and maintain a log of identity of users and their internet usage.
- Under the Electronic Service Delivery Rules the government can specify certain services, such as applications, certificates, licenses etc, to be delivered electronically.

Issues and Analysis

- The Security Practices Rules require sensitive personal information to be disclosed to government agencies. The safeguards against such disclosure differ from those under other laws. Also, these Rules may be superseded by an agreement.
- The Intermediary Guidelines Rules that allow blocking of content on the internet may violate the right to free speech. These Rules differ from the requirements governing content of other media like newspapers and television.
- The Cyber Café Rules may have negative implications for privacy and personal safety of the users.

The Information Technology Act, 2000 was enacted to facilitate electronic commerce by providing legal recognition for electronic transactions.[1] The Act was amended in 2008 to include provisions for (a) protection against liability to intermediaries and (b) protection of data collected, processed or stored electronically. Following the 2008 Amendment, the government notified the following four Rules on April 11, 2011.

1. The IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, prescribe security standards for personal information stored electronically.[2]
2. The IT (Intermediary Guidelines) Rules, 2011, provide due diligence requirements for intermediaries.[3]
3. The IT (Guidelines for Cyber Café) Rules, 2011, require cyber cafés to identify users and maintain records of use.[4]
4. IT (Electronic Service Delivery) Rules, 2011, provide a framework for electronic delivery of services such as licenses, forms and certificates.[5]

Chakshu Roy chakshu@prsindia.org
Harsimran Kalra harsimran@prsindia.org
August 12, 2011

Reasonable Security Practices and Procedures and Sensitive Personal Data and Information Rules

Key Features

G.S.R. 313(E)

The IT Rules dated April 11, 2011

- The Act delegates the power to define the term 'sensitive personal data and information' (SPDI) and prescribe 'reasonable security practices and procedures' (RSPP) in the Rules. These Rules define SPDI and RSPP. As per Section 43A of the Act the Rules related to RSPP apply only in the absence of an agreement between the user and the data holder.
- The Rules define SPDI as personal information which consists of (i) passwords, (ii) financial information such as bank account, credit and debit card details, (iii) physical, physiological and mental health conditions, (iv) sexual orientation, (v) medical records and (vi) biometric information.
- The Rules provide procedures for collecting and storing SPDI. SPDI may be shared only with the prior consent of the individual. However, SPDI may be shared with government agencies on a written request for the purpose of investigation, prevention, prosecution and punishment of offences. The government agency may not share such information further with third parties. SPDI may also be transferred between entities if it is necessary for performance of the entity's contract with the information provider. However, such transfer is only allowed if the entities ensure the same level of protection. The Rules also specify an international standard[6], or any standard issued by an industry association and approved by the government to be RSPP.

Issues and Analysis

Disclosure to government

Rules 6 and 7

Efficacy of delegated powers: Section 43A empowers the government to make rules to (a) define SPDI and (b) specify RSPP. The Rules provide for mandatory disclosure of information to government agencies. As this requirement is not a definition of SPDI, it appears that the provision is included as part of RSPP. However, the RSPP Rules can be overridden by an agreement between the user and the data holder. This implies that the access to government agencies may be denied by private agreement.

Rule 7

Due process: The Supreme Court has determined that the right to privacy is a part of the fundamental right to life guaranteed under Article 21. This right may only be restricted by procedure established by law. The Rules provide for disclosure of information to a government agency on the basis of a written request stating the purpose of such disclosure. This procedure is different from the procedure provided for under other laws. For example, under the Criminal Procedure Code a search may be conducted with a search warrant issued by a magistrate. Interception of telephonic conversation and monitoring of information stored and transmitted over the internet are permissible only upon an order by the Home Secretary to the central or state government.[7]

Following some criticism in the media the government has in its press release stated that "the Rules do not give any undue powers to the government agencies". It also states that the "government agencies are required to follow lawful process and procedures".[8]

Intermediary Guideline Rules, 2011

Key Features

G.S.R. 314(E)

The IT Rules dated April 11, 2011

- The Act defines intermediaries as those who provide internet, telecom, e-mail or blogging services, and includes cyber cafés. An intermediary is not liable for any content hosted or transmitted through it by a user. Intermediaries are required to comply with due diligence standards, and to remove unlawful content upon receiving actual knowledge. Section 79 of the Act empowers the government to prescribe due diligence standards to intermediaries.
- The Rules require each intermediary to publish terms of use. These terms of service are required to prohibit the user from hosting content of certain specified nature, including content that is grossly harmful, harassing, blasphemous, defamatory, obscene, hateful, racially or ethnically objectionable, unlawful in any manner, etc.
- Once the intermediary has the knowledge (either obtained on its own, or when it is informed by any person) that the content being hosted by the intermediary violates the Rules, it is required to initiate action for removal of such content within 36 hours. The intermediary may also terminate the access of the users.

Issues and Analysis

Right to freedom of speech

The Rules provide that the intermediary, in its agreement with users, shall prohibit publication of certain types of content. There are three issues that arise in relation to the specified content.

- Some of the categories of content specified under the Rules are ambiguous and undefined. For instance, 'grossly harmful' and 'blasphemous' content are not defined.

Rule 3(2)

- Publication of certain categories of content mentioned in the Rules are not offences under any existing law. For example, blasphemy is not prohibited under Indian laws. The restrictions under the Rules are different from the restrictions under the Norms of Journalistic Conduct issued by the Press Council of India. The Rules prohibit certain content on the internet which are permitted in other mediums such as the newspaper or TV. For example, a newspaper may publish a blasphemous article, but the same article may not be reproduced on the internet.

- Article 19(1) of the Constitution guarantees the right to free speech and expression. As provided under Article 19(2) this right may be restricted in the interest of the State's sovereignty, integrity, security and friendly relations with other States, public order, morality, decency, contempt of court, and for protection against defamation. Some of the categories of objectionable content under the Rules may not meet the requirements of Article 19(2) and may infringe the right to freedom of speech and expression.

The government issued a press release following some media reports about the Rules. It states that the due diligence practices are best practices followed internationally by well-known mega corporations operating on the internet. Further, it states that the Rules are in accordance with the terms used currently by most of the intermediaries, and that any disputes regarding interpretation of the Rules, will be decided by courts.[9]

Effect on free speech

Rule 3(4)

Intermediaries have to remove content prohibited under the Rules. They could be liable for compensation if they fail to do so. As discussed above, several terms are not defined or are ambiguous. Intermediaries would have to determine whether the content violates these terms. In order to minimize the risk of liability, they may block more content than required. This would imply adverse consequences for freedom of expression on the internet.

Cyber Café Rules, 2011

Key Features

G.S.R. 315(E)

- The Act empowers the government to prescribe standards for intermediaries, including cyber cafés. If a cyber café does not comply with the Rules, it would be liable for any misuse by the customer.

IT Rules dated April 11, 2011

- Under the Rules, all cyber cafés have to register with the registration agency notified by the government. The Rules require cyber cafés to maintain records of users' identity, contact details and websites accessed for a minimum period of one year. Cyber cafés are required to disclose the records to inspecting officers on their demand.

- The Rules also provide requirements for seating and lay out. Cyber cafés shall display a board, clearly visible to the users, prohibiting them from viewing pornographic sites and downloading information prohibited under the law.

Issues and Analysis

Personal details available to cyber café owners

Rules 3(1) and 5

Cyber cafés are required to maintain a log containing personal details, such as address and photographs of the users, and their internet usage. This provision is presumably to prevent or investigate crime. However, the availability of such information, which is personal in nature, with the cyber café could have negative implications on the right to privacy and personal security of the user.

Implementation for public access

Rule 7

The Act defines a cyber café as a place where internet access is offered to the public in the ordinary course of business. This implies that businesses such as restaurants, airports and coffee shops that provide access to wi-fi services could be

interpreted as cyber cafés. In that case the Rules related to seating, notice boards, and maintenance of registers may be cumbersome for these entities to comply with.

Electronic Service Delivery Rules, 2011

Key Features

G.S.R. 316(E)

IT Rules dated April 11, 2011

- The Act authorises the government to take steps to provide for electronic delivery of services, such as filing of income tax returns, applications for passports, payment of central excise tax etc.
- The Rules empower the government to notify services to be delivered electronically and the signing authorities for different permits. The government may also notify entities that shall provide access to services.
- The government may authorise the entities to collect such service charges for providing services as the government may prescribe.
- The government may require an audit to be conducted into the affairs of service providers. These audits may look into accounts, performance, security and confidentiality of information and software applications used by the entity.

Issues and Analysis

The purpose of the Rules is to increase efficiency and provide easier access to services. The National e-Governance Plan that targeted 27 projects for electronic delivery of services was approved in 2006-07. Some departments have started electronic delivery of services.[10]

The government has also released a draft bill on Electronic Service Delivery. It would be useful to ensure that the provisions in the Rules are not in conflict with that Bill.

Notes

[1] Statement of Objects and Reasons, Information Technology Act, 2000.

[2] http://www.mit.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf

[3] http://www.mit.gov.in/sites/upload_files/dit/files/GSR314E_10511(1).pdf

[4] http://www.mit.gov.in/sites/upload_files/dit/files/GSR315E_10511(1).pdf

[5] http://www.mit.gov.in/sites/upload_files/dit/files/GSR316E_10511(1).pdf

[6] IS/ISO/IEC 27001 on 'Information Technology – Security Techniques – Information Security Management System – Requirements'.

[7] Section 5, Indian Telegraph Act, 1885 read with Indian Telegraph Rules, 1951, Rule 419A and Section 69, Information Technology Act read with Information Technology (Procedure and safeguards for interception, monitoring and decryption of Information) Rules, 2009.

[8] "Access to sensitive personal information under new IT Rules only with checks and balances: Clarifies DIT", Press Information Bureau, May 10, 2011.

[9] "Exemption from Liability for Hosting Third Party Information: Diligence to be Observed under Intermediary Guidelines Rules", Press Information Bureau, May 11, 2011.

[10] For instance, the number of e-income tax returns filed increased from 3.62 lakhs in 2006 to 52.5 lakhs in 2009-10. Similarly the number of PAN cards allotted through online applications increased from 85 lakhs in 2006-07 to 150 lakhs in 2009-10. (See: Annual Report 2010-11, Ministry of Finance). The government has also launched an e-portal for handling grievances related to pensions. In 2006 the number of grievances registered through the public grievances portal was 13,353, whereas over 87,000 grievances were registered in 2009. In addition, the average time disposal of grievances reduced from 157 days in 2007 to 44 days in 2009. (See: Annual Report 2009-10, Ministry of Personnel, Public Grievance and Pensions).