Data Security Council of India

Making of Rules under Sections 43A, 67C and 79 of the Information Technology (Amendment) Act, 2008

FOREWORD

The Information Technology (Amendment) Act, 2008 was notified in the Gazette on February 5, 2009 after it received presidential assent. The Department of Information Technology, Ministry of Communications and Information Technology sought views of DSCI and NASSCOM on making of Rules under sections 43A, 67C, and 79 on the following:

- **43A:** '***reasonable security practices and procedures***' – body corporate (IT/ITES SP)
- **43A:** '***sensitive personal data or information***' – body corporate handles it
- **67C:** '***preserve and retain information for such duration and in such manner***…' – intermediary (SP, NSP, ASP, Search engine..)
- **79:** '***due diligence***' by intermediary
- **79:** '***receiving actual knowledge***' by intermediary

DSCI prepared a Consultation Paper highlighting the issues involved on the above themes; circulated it to NASSCOM Members, to the DSCI Steering Committee, DSCI Chapters/E-Security Forums in Bangalore, Delhi, Mumbai, Pune and Kolkata to seek their views. The paper was also put on the DSCI web site (www.dsci.in) for wider dissemination. This was done on March 6, 2009. Prior to that a meeting with the industry was held on February 9, 2009 in Delhi. A number of responses from the industry were received. These have been analyzed, and DSCI, has prepared the following recommendations on behalf of DSCI and NASSCOM for submission to the government.

We propose to keep this on the DSCI web site till the end of April, 2009. Your comments are welcome. The recommendations will be submitted to the government by the first week of May, 2009.

Kamlesh Bajaj

April 13, 2009 **CEO, DSCI**

Making of Rules under Sections 43A, 67C and 79 of the Information Technology (Amendment) Act, 2008

Recommendations of Data Security Council of India and NASSCOM to the Department of Information Technology, Ministry of Communications and Information Technology

DSCI consultation paper on the making of rules under the Information Technology (Amendment) Act, 2008 was widely distributed through e-mail to the DSCI Steering Committee, NASSCOM members, DSCI Chapter members, Industry Associations; it was also put on the DSCI website on the 6th March, 2009, and feedback was requested by March 23rd, 2009. In the absence of adequate responses, this was extended to March 31st, 2009. A total of 12 responses have been received. The respondents include Infosys, TCS, IBM, Accenture, Convergys, Google, AOL India, Airtight Networks, Aujas, Mandamus, R Systems, and a legal consultant. Their comments/suggestions on all the four issues have been examined in detail. A brief summary of the same and recommended rules are presented below:

ISSUE 1

Reasonable Security Practices under Section 43A

"Body corporate has to follow such reasonable security practices that help protect information/data from unauthorized access, damage, use, modification, disclosure or impairment."

Should it be proposed that there should be a set of practices to be followed by all ? If so, should they be based on a combination of ISO 27001 (or ISF), OECD Security Principles for design and operation of ISMS as per the needs of an organization, based on information assets and risk assessment; coupled with security assessments based on CobIT? If so, should an organization be required to declare the standard it is following, apply the same with vigour, and create a mechanism for assessing security controls? It will outline its size, and type of business, and create a written document stating the standard, and the controls selected by it, and how are they deployed. (Should it be a short document in case of small organizations that provides minimum services and collects minimum personal data?). Could this approach be construed to constitute "reasonable security practices"? Will failure to implement the same be construed to be negligence on the part of the organization?

Should the rule categorize body corporates into small, medium, large size, and prescribe standards?

There is general agreement that the companies should follow an existing identified security standard and should declare this as part of their security policy. While there is agreement on the nearly universal acceptance of ISO 27001 standard, there are endorsements for OECD privacy and security principles as also of PCI/DSS standard and CobiT. Since the law is applicable equally to all companies, irrespective of their size, applicability of security standards should be independent of the size, since all body corporates are handling personal information, some of which may be sensitive personal information. Hence, the applicability of standards in the form of reasonable security practices should be universal. On the two extremes of the spectrum, one of the companies is of the view that no standards should be prescribed and the company should be left to identify its own standard. Another view is that Section 43A falls short of the generally accepted privacy principles, and this should be made up by strict adherence to ISO 27001.

A view has also been expressed that since contracting parties could agree on security practices to be followed, it may be mandated under the rules that if such practices are lower than those prescribed under the reasonable security practices, then the latter will prevail.

Proposed Recommendation:

DSCI may propose a combination of ISO 27001 , OECD Security Principles for design and operation of ISMS as per the needs of an organization, based on information assets and risk assessment. An organization will have to declare the standard it is following, apply the same , and create a mechanism for assessing security controls. It will create a written document stating the standard, and the controls selected by it, and how are they deployed. It may not be required to be audited, but in the event of a security breach, it should be able to show to investigators that it was following its practices, and that they were in conformance with its written security policy, and that the controls were commensurate with the assets being protected.. These will constitute "reasonable security practices". Failure to implement it may be construed to be negligence on the part of the organization.

ISSUE 2

Defining Personal Information and Sensitive Personal Information under Section 43A

Should personal information be defined as information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Should Sensitive personal information be defined to include data such as that pertaining to racial or ethnic origins, political or religious beliefs, or health or sex life?

The responses are in favour of defining personal information and sensitive personal information in line with the EU Directive since the service providers are focused on trans-border data flows from the US and Europe to India for processing. However, since the definition under the rules applies to every person whose information is being processed by body corporates, Indian conditions have to be kept in view. Particular concern has been raised in the context of racial information, political and religious beliefs. Given the political situation and the way the religious, ethnic, and racial groups behave, much of this information about individuals may be publically known and defining such information to be part of sensitive personal information may pose a challenge. In fact, such a rule may lead to non-compliance on the part of the body corporate processing on the personal information. While the definition alignment with the EU Directive is essential to enhance trust in outsourcing to India, the same may have an undesirable effect in the context of personal information of Indian citizens held by such entities as banks, telecom companies, e-commerce websites, government data bases.

Proposed Recommendation:

Personal information may be defined as information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Sensitive personal information may be defined to include data such as that pertaining to (racial or ethnic origins, political or religious beliefs, or – this part from EU definition may be excluded) health or sex life.

ISSUE 3

Preservation and Retention of Information by Intermediaries under Section 67C

Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

Should an intermediary be required to store traffic data that identifies a subscriber or a user relating to a transaction or communication conducted by him, for a period of 6 months following the time of transaction, in a secure way, and make it available to authorized persons, within reasonable time? (What should constitute reasonable time - within 24 hours?). Should the content be required to be stored? If so, then the question of format and duration need to be addressed?

All the responses are in agreement that an intermediary should preserve and retain traffic data which is adequate to identify a subscriber or a user relating to a transaction and communication conducted by him. The storage period for such retention has been recommended for a period of 6 months to 3 years. There is also agreement on retaining only the traffic data and not storage of content of transaction, since such storage will pose immense challenge for the intermediary not only from the view of storage, but also from risks associated with maintaining privacy of subjects. A view has also been expressed that beyond a certain period of retention, say 6 months, government may bear the cost of storage.

Proposed Recommendation:

An intermediary may store traffic data that identifies a subscriber or a user relating to a transaction or communication conducted by him, for a period of 6 months following the time of transaction, in a secure way, and make it available to authorized persons, within reasonable time (or without delay or within 24 hours)". Retention requirement beyond this period may be at cost to the government.

The content need not be stored.

ISSUE 4

Due Diligence by Intermediary under Section 79(2)

Should the guidelines u/s 79(2) (c) prescribe that an intermediary be required to declare its privacy policy, security policy and the operations policy and process with respect to handling of third party content, and expect its subscribers to read and agree with the same? Should the intermediary be required to give an undertaking to cooperate with, and work under the direction of officers designated by the government under various sections of the IT (Amendment) Act, 2008? Should it undertake to act within 24- 72 hours of receiving any orders for removing any offensive content? Should it be obliged to take any action on any offensive content hosted by it on its infrastructure from any person other than the designated government officers?

The responses are in agreement with the proposal that an intermediary should declare its privacy policy, security policy and the operations policy and process with respect to handling of third party content.

There is a view that the intermediary should be identified for each activity such as hosting of website or applications, acting as a conduit, providing search capabilities. A need has also been expressed for defining the rule so as to clearly lay down limitation of liability since section 84C on punishment for attempt to commit offences could be as interpreted overriding section 79- intermediary may be held liable for causing an offence to be committed.

Further, a concern has been raised that immunity under Section 79(3) seems to be taken away
by Section 67 which prescribes punishment if the intermediary "causes to be published or transmitted". Under the rules, intermediaries who are merely acting as neutral platforms or as conduits for third party content, should be excluded.

There is also a view that if an intermediary observes 79(2) he should be deemed to have observed due diligence.

Rules should also clarify that Section 84C that provides for punishment for attempt to commit offence will not apply to intermediaries who are conduits or provide neutral platform for third party content.

Proposed Recommendation:

An intermediary will declare his privacy policy, security policy and the operations policy and process with respect to handling of third party content, and expect its subscribers to read and agree with the same; it will work under the direction of officers designated by the government under various sections of the IT (Amendment) Act, 2008, and will act within 3 -5 working days of receiving any orders for removing any offensive content – such an order. If it receives information about any offensive content hosted by it on its infrastructure from any person other than the designated government officers, it will not be obliged to take any action on the same.

Intermediaries who are merely acting as conduits may not attract the provisions of sections 67 and/or 84C if they are found to observe due diligence.