Comments on '*Multi-stakeholder Process to Develop Consumer Data Privacy Codes of Conduct*'

Submitted to:

The National Telecommunications and Information Administration, Department of Commerce, United States of America

By:

Data Security Council of India

Niryat Bhawan, 3rd Floor,

Rao Tula Ram Marg, New Delhi

April, 2012

DSCI

PROMOTING DATA PROTECTION

A NASSCOM® Initiative

Introduction

Data Security Council of India (DSCI) is pleased to submit its comments on the NTIA's '*Multi-stakeholder Process to Develop Consumer Data Privacy Codes of Conduct*'. DSCI appreciates FTC for recognizing and encouraging industry self-regulation. We are strong advocate of self-regulation, and have been promoting it in the policy discussions in India. With respect to the principles described in *The Consumer Privacy Bill of Rights*, we believe there are practical difficulties when it comes to implementation and enforcement of some of these principles. Our comments in this document are based on this realization.

For further information or queries, please contact:
Dr. Kamlesh Bajaj
Chief Executive Officer
DATA SECURITY COUNCIL OF INDIA (DSCI)
3rd Floor, Niryat Bhawan | Rao Tula Ram Marg | New Delhi - 110057, India
P: +91-11-26155071 | F: +91-11-26155070
E: kamlesh.bajaj@dsci.in

Going forward, we will be pleased to work with NTIA and contribute in the development of the Consumer Data Privacy Codes of Conduct.

Please refer the appendix of this document for details on DSCI and its work on privacy.

DSCI Comments

Consumer Data Privacy Issues to Address through Enforceable Codes of Conduct

1) ***Relevance of Principles such as Consent & Choice in the online world***: The Consumer Privacy Bill of Rights through the '*Individual Control*' principle emphasizes the need for companies to take consent and offer choices to consumers. Though majority of companies do take implicit / explicit consent from the consumers presently, they do not provide any 'real' choice to the consumers. Privacy policy statements such as – '*By visiting this website you agree to be bound by the terms and conditions of this Privacy Policy. If you do not agree please do not use or access our Site*' are prevalent on the internet. Consumers are denied services if they do provide consent. In such a scenario, do principles such as choice and consent have any meaning? Are they negotiable? Can consumers provide limited consent and yet avail full services online? How much possible it is for companies to provide 'real' choice to consumers by tailoring their services based on the personal information provided by the consumers? Also, it is worth considering that online services are not for '*free*' as they appear to be. Online business models thrive on the new currency - personal information.

2) ***Tracing unauthorized information sharing & usage:*** Consumers provide their personal information on multiple websites, through different mechanisms & platforms, which is further shared with various third parties. In cases of unauthorized information sharing & usage, it is

extremely difficult to trace / ascertain the agency to which the information was originally submitted. Solving this issue remains one of the biggest challenges on the Internet. Is there a solution?

3) ***Trust in Mobile Applications***: The development and use of mobile applications across different OS platforms such as android, symbian, etc. is phenomenally increasing. Consumers can access the '*apps markets'* of different OS platforms to download applications ranging from games to m-commerce applications. Many are available for free. However, the challenge is in ascertaining the behavior of these applications from the privacy perspective – who owns the responsibility – the developers of such applications or the company which develops the OS & provides the '*apps markets'* to the consumers of its OS? Can there be an assurance mechanism which is in the benefit of the consumers?

4) ***Retention of information***: Deletion/ purging / de-identification of personal information by companies when no longer needed is one of the globally accepted privacy principles. This is also reflected in the '*Focused Collection'* principle of the Consumer Privacy Bill of Rights. However, implementation of this principle is difficult – since the personal information is shared with multiple third parties (which may share it further) immediately after being submitted to the concerned company, how can it be ensured that the third parties delete/ purge/ de-identify personal information shared with them when no longer required? Does the original company have the required mechanisms to track the information flow & its usage across the entire supply chain?

5) ***Differentiation between Online Privacy (B2C) and Privacy in B2B environments:*** The applicability and enforcement of privacy principles differ for online privacy and privacy in B2B environment, e.g. business process outsourcing engagements, where the data collector transfers the personal information of its consumers (not necessarily collected through the Internet) to data processors for legitimate business purposes. Each has its own issues and privacy protection requirements and need to be addressed accordingly, which may not be possible by using same policy instruments for both online privacy and privacy in B2B environments.

6) ***Enforcement of Privacy Principles***: Given the large and ever growing number of websites, which could be hosted anywhere in the world, enforcement of privacy principles could be big issue. Can a single regulator (FTC) monitor such large number of websites? Is self-regulation / co-regulation the answer? Will it be effective?

Process to prioritize Issues

To prioritize the privacy issues, we suggest that following factors may be taken into consideration:

- ***Harm*** – extent of harm / damage a privacy issue, if left unaddressed, may cause to the consumers;
- ***Urgency*** – given the pace of proliferation of activities on the Internet, (e.g. development of mobile applications) issues which if left unaddressed now, can invite lot of re-engineering / re-

designing later, leading to avoidable increase in cost and efforts. For example, it is better to make applications that take privacy into consideration from the design phase rather than making the required changes later when these applications have already been developed.

- ***Impact on innovation***- innovation is the lifeline of the Internet and it must go on. Any privacy related issues which can adversely impact innovation on the Internet must be addressed.

Appendix

DSCI and its Privacy Initiatives

Since its inception in 2008, DSCI has emerged as a think tank in cyber security, data security and data privacy in India. It works with the governments, industry and global think tanks for enhancing data protection and cyber security. Following activities summarize DSCI initiatives in data privacy.

DSCI Privacy Initiatives

- **Public Advocacy**

- DSCI worked closely with the Government of India and made significant contributions in the framing of the **Information Technology (Amendment) Act, 2008**. Section 43A of this Act, established the legal framework for data privacy in India.

  http://www.dsci.in/sites/default/files/DSCI%20Comments%20on%20draft%20Rules%2043A-79_v1%200.pdf

  http://www.dsci.in/sites/default/files/rules_for_it_act_dsci_consultation_paper.pdf

  http://www.dsci.in/sites/default/files/DSCI%20response%20to%20members'%20queries%20on%20Section%2043A.pdf

- DSCI is being consulted by Government of India (Planning Commission and Department of Personnel & Training) for **drafting of the Privacy Bill** for India. It has representations on committees setup by the Government for this purpose.

  http://www.dsci.in/sites/default/files/Legal%20Framework%20for%20Data%20Protection%20and%20Security%20and%20Privacy%20norms_0.pdf

- DSCI is working with the Government of India for getting **India the EU status of 'adequate' country for data protection**, under the India-EU Free Trade Agreement.

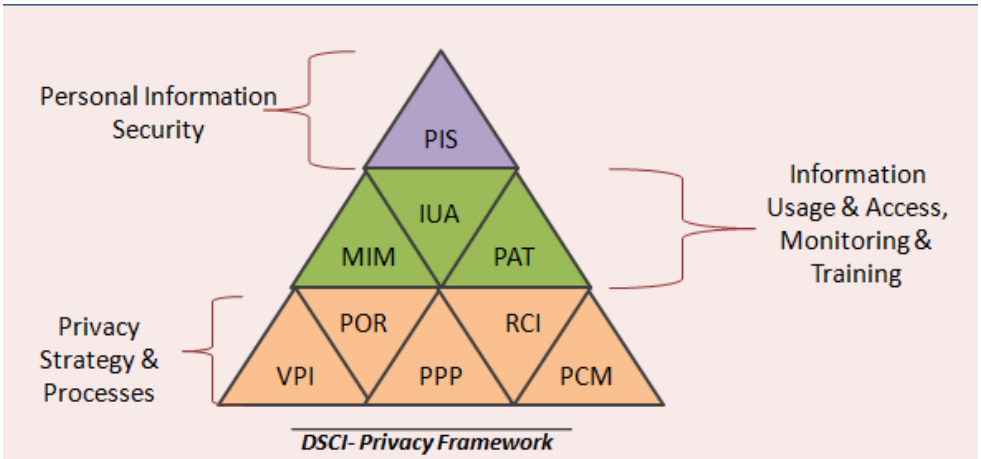
- DSCI has been engaged with the European Union and submitted its **comments on different consultation papers** released by the EU and is closely monitoring the revision of the EU data protection directive.

  http://www.dsci.in/sites/default/files/DSCI%20Response%20to%20Comprehensive%20Approach%20on%20Personal%20Data%20Protection%20in%20EU_Final.pdf

  http://www.dsci.in/sites/default/files/DSCI%20Response%20to%20Future%20of%20Data%20Protection_EU.pdf

- **Thought Leadership**

- DSCI has developed ***DSCI Privacy Framework (DPF)*** which comprises of 9 practice areas across 3 layers. It enables organization to design and implement a privacy program which is in compliance with globally acceptable privacy principles. DPF is being implemented by organizations in India. As a next step, DSCI is developing DSCI Assessment Framework for assessing organization's practice against DPF.



DSCI- Privacy Framework

VPI – Visibility Over Personal Information	**POR** – Privacy Organization & Relations	**PPP** – Privacy Policy & Processes
RCI – Regulatory Compliance Intelligence	**PCM** – Privacy Contract Management	**MIM** – Privacy Monitoring & Incident Management
IUA – Information Usage & Access	**PAT** – Privacy Awareness & Training	**PIS** – Personal Information Security

http://www.dsci.in/taxonomypage/116

- DSCI is member of the **Cloud Services Measurement Initiative Consortium** (CSMIC) led by **Carnegie Mellon University**, US and is providing inputs for privacy and security.
- DSCI has conducts **surveys on privacy and security** for different industry verticals in India, in collaboration with leading consulting firms.

  http://www.dsci.in/sites/default/files/DSCI%20-%20KPMG%20Banking%20Survey%20Report%20-%20Final.pdf

  http://www.dsci.in/sites/default/files/DSCI-KPMG%20Survey%202010%20-%20State%20of%20Data%20Security%20and%20Privacy%20in%20Indian%20BPO%20Industry.PDF

  http://www.dsci.in/sites/default/files/Data%20Protection%20Challenges%20in%20Cloud%20Computing.pdf

  http://www.dsci.in/sites/default/files/data_security_survey_2009_report_final_30th_dec_2009.pdf

  http://www.dsci.in/sites/default/files/kpmg_survey_on_data_protection_practices.pdf
- DSCI has **authored various thought papers**, position papers, articles etc. on privacy.

  http://www.dsci.in/node/301; http://www.dsci.in/node/51; http://www.dsci.in/node/314; http://www.dsci.in/node/302; http://www.dsci.in/node/1033; http://www.dsci.in/node/778

About DSCI

DSCI is a focal body on data protection in India, setup as an independent Self-Regulatory Organization (SRO) by NASSCOM®, to promote data protection, develop security and privacy best practices & standards and encourage the Indian industries to implement the same.

DSCI is engaged with the Indian IT/BPO industry, their clients worldwide, Banking and Telecom sectors, industry associations, data protection authorities and other government agencies in different countries. It conducts industry wide surveys and publishes reports, organizes data protection awareness seminars, workshops, projects, interactions and other necessary initiatives for outreach and public advocacy. DSCI is focused on capacity building of Law Enforcement Agencies for combating cyber crimes in the country and towards this; it operates several Cyber labs across India to train police officers, prosecutors and judicial officers in cyber forensics.

Public Advocacy, Thought Leadership, Awareness and Outreach and Capacity Building are the key words to with which DSCI continues to promote and enhance trust in India as a secure global sourcing hub, and promotes data protection in the country.

About NASSCOM

NASSCOM® is the premier body and the chamber of commerce of the IT-BPO industries in India. NASSCOM is a global trade body with more than 1200 members which include both Indian and multinational companies that have a presence in India. NASSCOM's member and associate member companies are broadly in the business of software development, software services, software products, consulting services, BPO services, e-commerce & web services, engineering services offshoring and animation and gaming and constitute over 95 % of the industry revenues in India and employs over 2.24 million professionals.

NASSCOM's Vision is to maintain India's leadership position in the global sourcing IT industry, to grow the market by enabling industry to tap into emerging opportunity areas and to strengthen the domestic market in India. NASSCOM aims to drive the overall growth of the global offshoring market and maintain India's leadership position, by taking up the role of a strategic advisor to the industry.

DATA SECURITY COUNCIL OF INDIA

A NASSCOM® Initiative

L: Niryat Bhawan, 3rd Floor, Rao Tula Ram Marg, New Delhi - 110057, India
P: +91-11-26155071 | F: +91-11-26155070 | E: info@dsci.in | W: www.dsci.in