



Welcome to Data Privacy Day

Naavi
28th January 2011
DSCI Bangalore

1

Cyber Law College



Today is Data Privacy Day

- Declared by US House of Representatives and Senate in 2009
- Celebrated by US, Canada and 27 European Countries
- To promote Privacy Education
 - DSCI joins the celebration with the global community

2

Naavi



The Message from CEO, DSCI

- I wish you a very happy Privacy Day and Encourage you to have discussions and deliberations to make the chapter members aware of
 - the privacy debates going around the world and in India
 - DPF as the Best Practices Approach that can fulfill the requirement of privacy protection and compliance to global regulations

3

Naavi



Issues Raised

- Privacy of individuals engaged in online activities is getting compromised through collection of personal data and
 - sharing of the same by collecting sites with others for commercial reasons and
 - for reasons other than that for which the data is collected

4

Naavi



- Many of the existing privacy principles have been overwhelmed by new technologies and have lost their true meaning
- It is time to rethink privacy principles to enhance trust of individual even as business and innovation are allowed to flourish
- Further attack on privacy appears to come from national security

5

Naavi



- Global data flows between businesses are governed by OECD principles and guiding legislations around the world under the EU Data protection directive
- In B2B data flows governed by contracts these principles may be found inadequate
- Attempting to harmonize laws between countries with different cultures may not be effective

6

Naavi



7

- Solution may be in the development of a globally accepted best practices framework led by Self Regulating organizations
- Such frameworks should form part of the contracts of Service providers

Naavi



Latest Global Discussions

8

Naavi



New EU Initiatives

9

- EU Consultation Paper-9th July 2009- " A Comprehensive Approach to Data Protection in EU"
 - Ensuring Appropriate protection for individuals in all circumstances
 - Increasing legal certainty and providing level playing field for data controllers
 - Reducing the administrative burden
 - Clarifying the rules on applicable law and member state's responsibility
 - Enhancing data controller's responsibility

Naavi



New Initiatives..2

10

- EU Consultation Paper-9th July 2009- Objectives
 - Encouraging Self Regulatory initiatives and exploring EU Certification Schemes
 - Clarifying and simplifying rules for international data transfers
 - Promoting Universal principles
 - Revising data protection rules in the area of Police and Judicial cooperation in criminal matters
 - A Stronger institutional arrangement for better enforcement of data protection rules

Naavi



New Initiatives in US

11

- FTC report , 1st Dec 2010
 - "Protecting Consumer Privacy in an era of rapid change: a proposed framework for Business and Policy makers"
 - Existing models based on "Notice and Choice" and "harm based" approach are insufficient to address evolving privacy issues
 - Consumer consent is missing in the complicated online environment while reputational and psychological harms are also not covered.

Naavi



New Initiatives in US

12

- FTC report , 1st Dec 2010
 - Report suggests a new framework with 3 core principles
 - Privacy by design
 - Simplification of consumer choice
 - Greater transparency
 - Suggests that "do not track" feature to be developed in application to enable consumers to prevent the tracking of their internet initiatives

Naavi



New US Initiatives..3

- Department of Commerce Internet Policy Task Force green paper..16th Dec 2010
 - Focuses on reducing barriers to business development and innovation
 - Recommends minimal regulation using voluntary, enforceable policy codes that would be created by industry.
 - Advocates a privacy framework based on revitalized FIPPs (Freedom of Information and Protection of Privacy) which would provide a baseline of privacy protection.
 - Flexibility in business development and innovation should not endanger consumer trust
 - Importance of global interoperability among diverse international privacy frameworks including "Safe harbors".
 - Ensure nationally consistent breach notification roles

13 Naavi



Indian Initiatives

- India had presented a legislation called "Personal Data Protection Bill-2006" (PDPB) in the Parliament in December 2006 around the same time when Information Technology Amendment Bill 2006 (ITAA 2006) had also been presented.
 - ITAA-2006 finally got passed in end 2008 and became ITA 2008
 - PDPB-2006 however lapsed

14 Naavi



The Background

- ITA 2008 did address some issues of Privacy from the Data Protection perspective
 - Introduced Sec 43A and 72A in particular providing for civil and criminal penalties for Privacy breach
 - Provided statutory backing to business contracts

15 Naavi



Sec 43A: Compensation for failure to protect data

- Where a body corporate,
 - possessing, dealing or handling any sensitive personal data or information in a computer resource
 - which it owns, controls or operates,
 - is negligent in implementing and maintaining reasonable security practices and procedures and
 - thereby causes wrongful loss or wrongful gain to any person,
 - such body corporate shall be liable to pay damages by way of compensation, to the person so affected.



Innovative Sec 43A drafting

- "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment,
 - as may be specified in an agreement between the parties or
 - as may be specified in any law for the time being in force and
 - in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

17 Naavi



72 A Punishment for Disclosure of information in breach of lawful contract (Inserted vide ITAA-2008)

- Save as otherwise provided in this Act or any other law for the time being in force,
 - any person including an intermediary who,
 - while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person,
 - with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses,
 - without the consent of the person concerned, or
 - in breach of a lawful contract, such material to any other person
 - shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.



Conflicts

- ITA 2008 also has provision for Data Retention
- ITA 2008 also protects national security interests by providing for enormous powers of interception, blocking, monitoring, decryption and data demand
- Makes unauthorized privacy invasion punishable with imprisonment
- Encryption guidelines under Section 84A awaited

19 Naavi



New Challenges

- UID Project has enhanced the stakes
 - If not handled properly, the interests of a large part of population may be put to stake.
- Nira Radia tapes issue has brought the Privacy issue to the doors of Supreme Court
- Wikileaks affecting Indians has also opened a debate on public interest vs Privacy rights
- Cyber Crime investigators have often found hurdles to investigation because of privacy excuses by intermediaries

20 Naavi



New Challenges

A new draft of Privacy Protection Act is under preparation

21 Naavi



The Issues that Privacy Legislation has to address..

- Privacy as a right Vs Public Interest
 - How to balance them
- Privacy as a protection to the individual Vs Protecting the Data with the business
- Information in Digital vs Non digital form
- Right of a Government to access information of a Citizen Vs its ability to safeguard misuse
- ..etc

22 Naavi



DSCI's Role

- As a body with a specific mandate for Data Protection, DSCI is obligated to work towards bringing about a reconciliation of the differing views
- DSCI has been working with Government agencies to provide expert views on legislation
- DSCI is also sending responses to global bodies since global laws will affect Indian BPO industry

23 Naavi



DSCI Recommendations

- India is a vast country where outreach can be through industry associations and other NGOs and not through a single bureaucratic DPA
- Have light weight regulations based on global privacy principles that value economic benefits of data usage and flow while guaranteeing privacy to citizens

24 Naavi



DSCI Recommendations..2

- Avoid bureaucratic structure that could hinder business interests and lose the spirit of the intent in the operational implementation
- Rely on self-regulation of businesses that promote practices, making the privacy program relevant to technology advancements

25 Naavi



DSCI Recommendations..3

- Provide legal recognition to the role of self-regulatory bodies, promoted by industry associations in enforcing codes for the privacy in the interest of citizen's rights
- Notify and implement through self-regulatory organisations like industry associations

26 Naavi



DSCI Recommendations...4

- Allow businesses self declare the codes of practices that they have implemented to protect the privacy rights of the customers
- Establish a mechanism in the form of public private partnership to resolve the disputes and grievances of citizens.
- DSCI has drafted a suggested Data Protection Framework

27 Naavi



Industry Action Plan

- Study the Global developments
- Study the DPF suggested by DSCI
- Interact with academia to develop appropriate DPF for different types of industries and different scales of operation
- Develop alternative plans of action
- Help evolve an Industry's Best Practices Guideline

28 Naavi



Thank you

Naavi
www.naavi.org
naavi@vsnl.com

29 Naavi