Legal Framework for Data Protection and Security and Privacy norms

Consultation Paper

Submitted to DoPT

5th July 2010

Data Security Council of India

3rd Floor, Niryat Bhawan, Rao Tula Marg,

New Delhi 110057

DSCI

PROMOTING DATA PROTECTION

Preamble

NASSCOM studied many of the worldwide privacy initiatives over several years before establishing Data Security Council of India (DSCI) to focus on data protection. It was recognized that every society has its own privacy culture, though commercial transactions require that the information privacy and security obligations be determined by point of origination of data. Irrespective of where the data is processed in a globally networked environment, the business that originally collects the data, is required to meet the originating privacy obligations, regardless of where the data flows. Particular expectations for privacy are thus truly local, while data flows are global. However, it is difficult to govern cross-border data flows under any one country's laws or legal frameworks. The challenge, therefore, is for IT and BPO companies to meet privacy and information security obligations when national laws differ. DSCI recognizes that cultural notions and laws on privacy are diverse, but that there is widespread agreement around international data protection and information security principles; prominent among these are the OECD Privacy Principles, the EU Data Protection Directive, the US Safe Harbor Program, and the APEC Privacy Principles. These principles anticipate cross-border data flows on the premise that data processing must be global to reap benefits of a digital economy. A corporation's enterprise-wide data handling rules, grounded upon the APEC and OECD principles as a foundation, can achieve basic compliance with substantive requirements that might be found in any country. Likewise, an IT or BPO service provider can design its operations in the same way. It can assess its adherence to common data management principles, as also against the specifics such as requirements for health, financial sector, or other personally identifiable information. A self-regulatory organization (SRO) can verify a service provider's voluntary compliance with the accepted Privacy Principles and the customer company's own promises and obligations.

It is against this background that DSCI's mission as an SRO was prepared - specifically focused on self-regulatory role in promoting privacy accountability in outsourcing. DSCI is a not-for-profit, independent entity – a Section 25 Company, that is governed by corporate laws, with an independent Board of Directors. Its Charter & Mission are as follows:

- **Public Advocacy on data protection and cyber security, both in India and abroad:** Engage with governments, law enforcement agencies and judiciary for a strong and credible data protection regime through appropriate policy instruments.
- **Capacity Building** through security and privacy awareness seminars, workshops, trainings, and conferences
- **Thought Leadership:** Develop, Promote and Implement **Best Practices** and Standards for Data Security and Data Privacy
- **Independent Oversight** as a credible and committed body that would oversee data security and privacy implementations and evolve a mechanism to provide independent assurance over service provider's preparedness.
- **Establish a Dispute Resolution** Mechanism based on Alternative Dispute Resolution Procedures acceptable to clients and service providers

- **Cyber Crimes Speedier Trials** through training of law enforcement agencies and judiciary in cyber forensics

DSCI has followed the 4E Initiative of NASSCOM for ensuring that India remains a trusted destination for outsourcing: These are as follows:

- Engagement
- Education
- Enactment
- Enforcement

DSCI creates awareness through Education and outreach programs; Enacts best practices and standards based on international best practices, works with governments on policies, laws and regulations; Engages with all concerned to promote best practices on security and privacy; and will Enforce the best practices and standards among IT/BPO companies to promote India as a secure global sourcing partner. Membership of DSCI will provide an assurance that the company to which work is being outsourced is following the requirements of data security and privacy and could be trusted.

We believe that self-regulation by industry associations should be encouraged by any proposed privacy legislation, to ensure that technological advancements are taken advantage of, while bureaucratic structures do not hinder the growth of technology and its adoption in integrating the country in global digital economy. Experience of many countries, as explained below, shows that self-regulation in the form of co-regulation is important even with enactment of privacy laws.

Dr. Kamlesh Bajaj
Chief Executive Officer,
Data Security Council of India

Contents

1. Privacy Concepts

In the 1890 seminal article, Samuel Warren and Louis Brandeis (later Supreme Court judge), coined the phrase, the 'right to be let alone' as defining privacy. This was in response to the technology of times – the newspapers – violating privacy of influential people by printing stories about them. However, it was only in the 1940s that 'Privacy' was internationally regarded as a fundamental civil liberty. This was followed by a paragraph on privacy in The Universal Declaration of Human Rights (1948). The 1950 European Convention on the Protection of Human Rights and Fundamental Freedoms included a similar clause.

A more modern definition of the term 'privacy' is "the claim of individuals, groups, or institutions to determine when, how, and to what extent information about them is communicated to others" (Privacy and Freedom, by Dr. Alan F. Westin 1967).

Personal Information (PI) is generally defined as any information relating to an identified or identifiable natural person. It may be referred to as personal data, personal information, non-public personal information, etc. Examples include: Name, Address, Date of Birth, Telephone Number, Fax Number, Email Address, Government Identifier (e.g. PAN Number, PF account number, etc.), Account Number (Bank Account, Credit Card, etc.), Driving License Number, IP Address, Biometric Identifier, Photograph or Video Identifiable to an Individual and any other unique identifying number, characteristic or code.

With the growth of digital age, more and more personal information of consumers, citizens finds its way into massive databases held by the private sector, and the governments. Access to personally identifiable information (PII) in such databases raises three social concerns that drive the issue of privacy. These include individuals' fears about:

- how personal information is used or shared;
- how it is protected; and
- who is accountable for its misuse.

In response to these concerns, many laws, regulations and guidelines exist across the globe. Some of these include the Organization for Economic Cooperation and Development (OECD) privacy guidelines, the European Union (EU) Data Protection Directive (DPD), Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), U.S. Gramm-Leach-Bliley Act (GLBA), and Asia-Pacific Economic Cooperation's (APEC) Privacy Framework.

OECD, EU and APEC Privacy Principles form the basis of many privacy laws throughout the world and are widely accepted. The United States of America (US) created Fair Information Practices (FIPs) that were formulated by the US Department of Housing, Education and Welfare (HEW) in 1973. The FIPs precede any other attempts by a group of countries. Later in 1980, OECD's Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data came into existence. The EU Data Protection Directive mandating Member States to promulgate laws in compliance with the Directive was issued in 1995. The

OECD Privacy Guidelines set out eight key principles for the protection of personal information. The APEC Privacy Framework is relatively more recent; it was endorsed by APEC Ministers and Leaders only in 2004.

Although there are commonalities between various privacy frameworks and guidelines, the way consumer privacy is perceived is different. For example, the European Union addresses privacy of personal information through one omnibus law and through an identified and independent data protection authority, while the United States addresses consumer privacy through sector specific and state laws on privacy of customer data that are administered by a variety of agencies. These include laws for protecting health information, and financial information among others. These laws are further supplemented by a variety of self-regulatory mechanisms and organizations.

The European Union has mandated that the Member States implement data protection in accordance with its Data Protection Directive (DPD). The Directive sets forth potential derogations such as consent and model contracts. These derogations have been extended to include Binding Corporate Rules (BCRs) The United States has a history of self-regulation, especially in its safe-harbor program with the EU. The seven principles of the safe- harbor program are,

- **NOTICE:** An organization must inform individuals about the purposes for which it collects information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or discloses it to a third party.

- **CHOICE:** An organization must offer individuals the opportunity to choose (opt out) whether and how personal information they provide is used or disclosed to third parties (where such use is incompatible with the purpose for which it was originally collected or with any other purpose disclosed to the individual in a notice). They must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise this option. For sensitive information, such as medical and health information, information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information concerning the sex life of the individual they must be given affirmative or explicit (opt in) choice.

- **ONWARD TRANSFER**: An organization may only disclose personal information to third parties consistent with the principles of notice and choice. Where an organization has not provided choice because a use is compatible with the purpose for which the data was originally collected or which was disclosed in a notice and the organization wishes to transfer the data to a third party, it may do so if it first either ascertains that the third party subscribes to the safe harbor

principles or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant safe harbor principles.

- **SECURITY:** Organizations creating, maintaining, using or disseminating personal information must take reasonable measures to assure its reliability for its intended use and reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

- **DATA INTEGRITY**: Consistent with these principles, an organization may only process personal information relevant to the purposes for which it has been gathered. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is accurate, complete, and current.

- **ACCESS:** Individuals must have [reasonable] access to personal information about them that an organization holds and be able to correct or amend that information where it is inaccurate. [Reasonableness of access depends on the nature and sensitivity of the information collected, its intended uses, and the expense and difficulty of providing the individual with access to the information.

- **ENFORCEMENT:** Effective privacy protection must include mechanisms for assuring compliance with the safe harbor principles, recourse for individuals to whom the data relate affected by non-compliance with the principles, and consequences for the organization when the principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which an individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with these principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

The APEC privacy Framework is based on the Accountability Principle under which the data protection obligations flow along with data in trans-border data flows. APEC enables economies to use both regulatory and self-regulatory elements to fashion a privacy approach that is credible while being consistent with a variety of cultures and legal frameworks.

2. Privacy Laws – brief facts

These early privacy rules were originally intended as a protection against unreasonable police searches of private property and an overly intrusive press. As a result of World War II and experiences with the Nazi regime, people became more afraid of leaving too much personal information in the hands of powerful government bureaucracies. They were confronted with a new tool however, in the hands of governments - the computers in the 1960s – that had the potential of holding data about them in a manner that could be exploited by the bureaucracies. The policy problem of limiting the compilation, access, and use of personal files from a purely bureaucratic task soon became a political-technological endeavour. It was called 'informational privacy' or 'fair information practices' in the US, while it went under the name 'data protection' in Europe. The discussion on the 'Big Brother state' was also growing around the same time. Parliaments started drafting laws to protect personal information against unlimited computer use. The world's first data protection law was enacted in the German state of Hessen in 1970. Shortly afterwards, Sweden (1973) and the United States (1974) followed suit. This was followed by West Germany enacting a law at the federal level in 1977; Denmark, Austria, France, Norway and Luxembourg introduced privacy protection laws in 1978. By early 1980s, seven more countries in Western Europe had enacted data protection laws; followed by ten more in the 1980s - among them Israel, Japan, and Canada. By the 1990s, 22 more states from all continents had joined the club.

Technical systems at the time were large mainframes that acted as centralized computer facilities. They were easy to control and supervise, and where the data, once entered, just remained there. The new order was thus a set of huge cabinets full of digitized data, in place of the earlier huge cabinets full of paper records and files.

The globalization of the economy in the 1980s was beginning to see an increase in trans-border data flows. But the various national data protection laws often contained differing procedural regulations with regard to transnational data transfers, leading to legal conflicts. An expert group in the Council of Europe, in early 1970s, identified the transnational character of the computer and the need for international regulatory harmonization. In the late 1970s, the Council of Europe and the European Parliament began discussions on how to remove these trade barriers while preserving data protection. It was clear that International harmonization of data protection was needed**.** This was in pursuance of one of the official goals of international economic policy, namely free trade. The Council of Europe's 1981 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data was the most binding international agreement for 15 years. The Convention included regulations on trans-border data flows and also allowed restrictions in cases where the data was to be transferred to a country with lower protection levels.

The OECD developed its 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in close coordination with the Council of Europe. Unlike the Council of Europe's 1981 Convention, the guidelines were not binding. Prior to this, very fierce conflicts between the United States and some

of the European governments had emerged. The Europeans perceived the very low or non-existing level of data protection in the United States as unacceptable. They viewed the American phrase 'free flow of information' as synonymous with their attempt to globalize the dominance of the US computer industry. The United States, on the other hand, accused the Europeans of protectionism by means of data protection.

The OECD Guidelines are only a short document listing basic fair information practices. The OECD followed up in 1985 with another declaration on transborder data flows that dealt with data flows within transnational corporations, trade barriers, and related aspects of data protection, and envisioned better cooperation and harmonization. The OECD was the only international organization that dealt with privacy and data protection for over a decade. It was only in 1990 that the UN General Assembly adopted the Guidelines concerning computerized data files. This too was voluntary, and because of no follow-up mechanism it had no real impact.

The EU data protection Directive is described as 'the most influential international policy instrument to date'. It contains regulations on the private and public sectors' use of personal data, applies to manual and automated data processing, has detailed rules on implementation and mandatory data protection commissioners, and creates a coordination body at the European level (the 'Article 29 Working Party') as well as a Commission-chaired committee that can make binding decisions.

3. Privacy in Indian Context

3.1. Indian Economy Transforming to E-economy

While India is leading in providing IT services to businesses across the globe; the domestic sector has emerged as a key IT investor. Leading the pack, Government agencies are spending more than $ 10 billion in several of e-Governance projects. Private sectors such as BFSI, Telecom, Manufacturing, Travel, etc. are increasingly relying on IT to process transactions and offer diverse channels to their end customers.

Indian Services industry growing multi-fold		
Outsourcing industry currently at $60 billion, will reach $225 billion by 2020[1]	*Cloud computing market - $110 million, will be worth $1 billion in next five years*[2]	
Payments going e-way[3]*, E-transaction 30% of total transactions and 75% of total value*	***Total Credit & Debit card** - 200 million in 2010*	
***Internet penetration** – 52 million – will become 3rd largest by 2013*[4]	***Broadband subscriber** - 9.24 million in May '10*	***Mobile Subscriber**- 654 million*[5]*-May '10*

This transformation may expose citizens to new age threats that not only have the potential to damage their financial interest, but also infringe their personal rights. Increasing commercialization involves identifying potential customers, marketing products and services, promotional activities, and cross-selling. The data gathered while providing such services is increasingly used for the purpose not intended. With the growth of digital age, more and more personal information of consumers, and citizens finds its way into massive databases held by the private sector, and the governments. Access to data in such databases raises social concerns on how citizens' personal information is used or shared; how it is protected; and who is accountable.

***More** than 1.1 million records **of New York State residents were impacted by over 400 data breaches in 2009 –** (US Govt. Monitor)*
***More** than 342 million records **containing sensitive personal information have been involved in data breaches from 2005 – 2009, as per Privacy Rights Clearinghouse –** (US Govt. Monitor)*
***Cost Implications of Data Breach is** $305 per record **for a single breach in a high profile regulated organization** – (Forrester)*

3.2. National Security and Privacy

Projects of national significance like Census 2010 which include National Population register, Unique ID project, National Intelligence Grid - will facilitate quick access to information on an individual centrally - like details of his/her banking, insurance, immigration, income tax, telephone and Internet usage. This data can then be used for profiling an individual and raises questions on safeguards of individual's privacy. Some of these projects also capture information either on biometrics such as fingerprints, iris

[1] NASSCOM- McKInsey Survey
[2] Economic times article: Cloud-computing-biz-may-touch-1-bn-in-5-years/articleshow/6080458.cms
[3] Celnet Report
[4] Forrester Research, leading market Analyst firm, 'Global Online Population Forecast, 2008-2013
[5] Mobile subscribers crossed 617 million mark in May: TRAI, 28 Jun 2010, Economic Times, Benitt & Colmn group

scan and facial image of citizens of India or other non-recoverable personal information. This information, if compromised can impede the privacy of citizen throughout his lifetime.

In the interest of sovereignty and integrity of India, security of the State, the IT (Amendment) Act, 2008[6] has authorized the designated agencies of the government to issue directions for interception or monitoring or decryption of any information through any computer resource. This has a major bearing on privacy of an individual as well as the business, which uses reasonable security practices to protect customer information, since the encryption keys may have to be shared with such government agencies, whenever required under a lawful process.

Rising terrorism threats that India is continuously witnessing for the past few years justifies the need for such monitoring of traffic through the implementation of ambitious projects such like NATGRID . These justifications, though in national interest, may however lead to infringement of the privacy of individuals.

3.3. Trans-border Data Flows – Outsourcing Environment

Data Protection has emerged as a major challenge in cross-border data flows. Clients are demanding more security as their worries about the cyber crimes, privacy and identity theft grow. Regulatory and law-enforcement agencies of countries where clients are located require a proof of compliance by the IT/ITeS service providers (SPs) with their security and privacy regulations. Different countries have different laws to deal with data security and data privacy.

Privacy laws are prevalent in the western world which protect the privacy of their citizens. India's privacy law, if and when enacted, should likewise protect a citizen's personal information, irrespective of whether it is processed in-house or outsourced - either in the domestic market or in the international market.

3.4. Existing Privacy laws in India

In India the industry specific regulatory bodies seem to be lagging in aligning their policies to evolving security and privacy challenges. However, recent IT (Amendment) Act, 2008, for the first time, has introduced the concept of "sensitive personal information", and has fixed the liability of the 'body corporate' to protect the same under section 43 A. Some of the other laws from which privacy can draw strengths are:

- Article 21 fundamental right to liberty, has been interpreted to include right to privacy in Supreme Court judgements
- Indian Contract Act
- Consumer Protection Act
- Sector - specific laws of telecom and Banking:
    - TRAI- National Do Not Call (DNC) Registry

[6] http://www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf

- RBI Guidelines- Adhere to privacy principle to protect customer information

4. Privacy and Self-Regulation

Voluntary disclosure of privacy policy was used by most organizations to reach out to the people that their Personally Identifiable Information (PII) was secure with them. Such statements merely reflected organizations' commitments to a set of Privacy Principles. It was in 1981 that OECD Guidelines on the Protection of Privacy and Transborder flows of Personal Data, in close coordination with the Council of Europe, were issued. In 1985, OECD issued another declaration on transborder data flows that dealt with data flows within transnational corporations, trade barriers, and related aspects of data protection, and envisioned better cooperation and harmonization. However, such commitments in the form "Codes" or "Guidelines" would indicate a self–regulatory function. The organization showed that it had considered privacy protection at some level; however, it was more in the nature of good public relations to state a set of commitments. Privacy commitments may inform data subject about certain rights to access and correction, to opt–out of disclosures, and so on.

Over a period of time, privacy codes of practice evolved, which were usually operating in absence of a regulatory framework. Some of these privacy codes graduated to the level of privacy standards, and ultimately resulted in the establishment of privacy laws. The first such code was the Canadian Model Code for the protection of Personal Information in September 1995, which was subsequently approved as a "National Standard of Canada" by the Standards Council of Canada in March 1996. The standard was organized around 10 Privacy Principles. Its development was led by the Canadian Standards Association (CSA) with very active participation of the industry; it was known as the CSA Model Code.

Same course of events took place in Australia where the standard was based on the CSA Model around a set of National Privacy Principles in 1988. This was superseded by a Privacy Act later.

In 1999, the Japanese Standards Association released JIS Q 15001, which adapted the Environmental Management Standard, ISO 14001 to personal data protection. This again led to the establishment of a Privacy Act in 2005.

Privacy codes of practice are administered in these countries by the industry bodies in the co-regulation model.

4.1. Privacy Codes

Codes of practice have long operated in various countries, as part of self–regulation. Five kinds of privacy codes, according to the scope of application, have existed: the organizational code, the sectoral code, the functional code, the technological code and the professional code.

1. **The organizational code** applies to one corporation or agency which is bounded by clear organizational structure. High profile organizations such as the multinational organizations that are under the scrutiny from the media or privacy advocates, or who may have received a large number of consumer complaints, would come under this category.

2. **The sectoral code** is developed by trade associations for adoption by their memberships. These instruments were developed more extensively, in the absence of a law, in Canada. These model codes were adopted from the OECD Guidelines or the CSA Model Code. Sectoral Codes have emerged within industries that operate on a global scale, such as those of the International Air Traffic Association (IATA) and the Federation of Direct Marketing Association (FEDMA).

   The major defining feature of the Sectoral Code is that there is a broad consonance of economic interest and function, and by extension a similarity in the kinds of personal information collected and processed. Sectoral codes permit, therefore, a more refined set of rules tailored to the issues within each industry.

   The idea of the Sectoral Code was taken one step further in Japan when the Ministry of Trade and Industry (MTI) published guidelines on the content and substance of industry codes of practice, and on procedures for development and implementation.

3. **The functional codes** are defined by the practice in which the organization is engaged, e.g. direct–mail and telemarketing.

4. **The technological code** can be defined not by function, but by technology. As new potentially intrusive technologies have entered society, codes have been developed to deal with the specific problems associated with their application and distribution. For example, the code of practice on Closed Circuit Television Cameras (CCTV) in Britain. In 1992, the Canadian Banks developed a code for the governance of Electronic Funds Transfer. This code attempted to regulate the issuance of debit and personal identification numbers, the content of agreements between the issuer of the card and the card holder, and so on. Smart card technology is also amenable to specific regulation through privacy codes of practice.

5. **Professionals' codes** developed by professional societies such as for information processing professionals, for survey researchers, for market researchers and for a range of health and welfare–related professionals.

Privacy codes of practice differ from mere privacy commitments in that they may embody a set of rules for employees, members or member organizations to follow. They also provide important guidance about correct procedure and behavior based on the information privacy principles and procedures for implementation, complaint resolution, and communication.

4.2. *Privacy Standards*

A Privacy Standard extends the self–regulatory code of practice in important ways. Standard means a common code and conformity assessment procedure that might more effectively determine that an organization "says what it does, and does what it says".

Idea of a more general privacy standard was first attempted in Canada in 1995 – based on the OECD Guidelines. This was known as the CSA Model Code.

The OECD Guidelines not only apply to Europe but also to North America, and the Asian developed countries. However, they are completely voluntary, and do not constitute international law. Its regulation is weak. On the other hand, the EU Data Protection Directive is stronger and applicable to Europe only. It is the national data protection laws, even if harmonized to the EU Directive, which are the most precise legal regulations that are enforced by Supervisory Authorities. Their reach is, however, limited to that country. Thus, the more binding the regulatory instrument, the shorter its reach.

The regulatory regime of Safe Harbor (SFH) consists of several layers:

1. The EU sets the substantive data protection standards
2. The companies voluntarily commit to them
3. It limits the scope of privacy adequacy ratings from whole countries to individual companies
4. Private or public bodies provide arbitration service
5. Public enforcement is carried out by a US agency
6. The EU Commission has the last word and can terminate the whole agreement if compliance or public supervision in the US is not working.

It is the SFH arrangement that combines transactional self–regulation on the one hand, and nation-state–based intergovernmental public regulation on the other hand, to produce a complex, multi-layered regime.

In the privacy led by business associations, enforcement in general is not very strict, but Industry Associations are playing an increasing role in educating their members about privacy based practices, through specialized seminars, training services, and newsletters. This form of self–regulation more closely resembles the "managed compliance" approach than the enforcement approach. But if trade associations have mandatory membership, it can act as a strong support for self–regulatory privacy protection instruments.

The experience of Canada, Australia, Japan and the United States where privacy codes, privacy standards and privacy seals have been developed and implemented, have graduated to the level of becoming part of the privacy laws that have got created. However, all of them see the role of self-regulation as an important element in ensuring privacy. The experience supports the conclusion that the voluntary approaches are not something to be ignored, but rather an integral part of privacy.

5. Privacy Debate: Issues

Privacy as a subject has evolved from the world war times and is continuously updated. Hence, when government of India decides to write such privacy law to protect the citizen data following questions should be debated:

1. Is it a fundamental right?
2. Does a citizen voluntarily give his PI to government databases; or there is threat of services being denied to them?
3. Large databases maintained by different agencies can be correlated to create profile of individuals – information collected for one purpose used for other purposes. Application creep. Examples of such personal information include but are not limited to following:
    - Health information – AIDS, genetic history, breast cancer, fertility, virginity, psychological details, etc.
    - Political beliefs – voting information of any individual
    - Internet browsing, search, download and upload history
    - Financial health / status
    - Life insurance details
    - Sexual preferences – gays, lesbians
    - Criminal record
    - Caste – caste based politics, reservation, etc.
4. Banks can deny credit on the basis of such correlation; house loans can be denied; medical policies may not be issued based on prior information of diseases, lifestyles…; jobs can be denied with information profiling from social networking sites.
5. Biometrics once collected for unique identification can be used for tracking criminals.
6. CCTV monitoring at public places – so useful in tracking terrorists after incidents - violates privacy.
7. Creating hindrance to data flow or usage in the name of privacy. Not respecting economic value of data.
8. WiFi data collection, use of cookies to collect personal information and analyze personal preferences, use of search keywords for targeted advertisements, street view application that encroach personal privacy, Software updates asking for personal data for cross selling products and services.
9. Social networking site, claiming ownership of user updates, like Facebook did in 2009, but reverted back.
10. Data Retention – national security regulations asking ISPs, network service providers and intermediaries retain user traffic information as well as message content – leading to breach of citizens' privacy. The country like Germany ruled out such retention.
11. Security scanners particularly that of 'Full Body Scanner', that potentially lead to breach of privacy of an individual.

6. Proposed Privacy Act – DSCI Recommendations

The Department of Personnel and Training (DoPT) need to ensure that the privacy bill should

- have light weight regulations based on global privacy principles that value economic benefits of data usage and flow, while guaranteeing privacy to citizens
- avoid bureaucratic structure that could hinder business interest 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
- provide legal recognition to the role of self-regulatory bodies, promoted by industry associations, in enforcing codes for the privacy in the interest of citizens' rights
- notify and implement through Self-Regulatory Organizations like industry associations
- 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

Self Regulation with a support from legal sanctity and reforms should be the path for the privacy policy, where Self-Regulatory Organization defines the process and codes of practices, which are vetted and recognized by the government through the proposed laws. Co-regulation should be the guiding spirit.