Cyber Security and Right to Privacy

Memorandum

Submitted to:
Standing Committee on Information Technology

9th July 2010
## Contents

1. The Indian Context .......................................................................................................................... 2
   1.1. Indian Economy Transforming to E-economy ................................................................................. 2
   1.2. Trans-border Data Flow – Outsourcing Environment ................................................................. 3
   1.3. e-Governance Projects .................................................................................................................. 3
2. National Security ............................................................................................................................... 4
   2.1. Paradox of Encryption .................................................................................................................. 4
   2.2. Encryption norms in India ............................................................................................................ 5
3. Cyber Security .................................................................................................................................. 8
4. Legal Regime for Cyber Security and Privacy .................................................................................. 10
   4.1. Information Technology (Amendment) Act, 2008 ..................................................................... 10
   4.2. Other Acts and Legislations ......................................................................................................... 11
   4.3. NASSCOM - DSCI – A Self Regulatory Organization ................................................................. 12
5. Right to Privacy - Concept ............................................................................................................... 14
6. Privacy Laws – brief facts ................................................................................................................. 17
7. Self-Regulation ............................................................................................................................... 19
   7.1. Privacy Codes ............................................................................................................................. 19
   7.2. Privacy Standards ....................................................................................................................... 21
8. Debate on Cyber Security and Privacy Issues ................................................................................. 22
9. DSCI Recommendations .................................................................................................................. 24
1. The Indian Context

1.1. 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 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. Some of the characteristics of Indian service industry growing multifold can be highlighted from following figures:

- **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 3\(^{rd}\) 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, citizens finds its way into massive databases held by the private sector, and the governments. Access to such data in such databases raises social concerns on how citizens’ personal information is used or shared; how it is protected; and who is accountable.

---

\(^1\) 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
1.2. Trans-border Data Flow – 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. Indian citizens will have similar concerns if their data is outsourced, or processed in cloud computing environment with clouds located anywhere in the world.

1.3. e-Governance Projects

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 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. Many issues on projects launched by UIDAI, and intelligence NATGRID with respect to profiling have been raised. These need to be addressed.
2. National Security

India continues to use the cyberspace more and more for government, and military applications. Indian embassies use email to exchange policy papers, and other secret information; missions host important data on intranet for internal use. Military uses computers extensively to store sensitive information, and share with listed users. Corporate and sensitive financial data of citizens is lying in e-governance systems such as companies, income tax, customs, excise, land records. All these need to be protected against unauthorized access. And if a breach does occur, access should be such as to render it difficult for the criminal to use it, e.g. through encryption.

India is a destination of choice for global sourcing. Most of the Fortune 500 companies outsource their IT and business processes to Indian service providers. For this to continue, India has to project itself as a secure destination. Best practices for security, encryption, data protection, privacy protection along with appropriate laws to give confidence to clients abroad are essential to see to it that the present business of US$ 60 billion can grow to US$ 225 by the year 2020, as projected by NASSCOM-Mckinsey report.

2.1. Paradox of Encryption

Globalization and the needs of economic growth require secure transactions using encryption which should be in line with the needs of various applications and the way these are being implemented in the United States, the UK, Europe and other countries of the world. The imperatives of globalization, with companies operating in most parts of the globe dictate that the same level of encryption should be used in the applications irrespective of the country that a user or corporate connects from. But it is also clear that law-enforcement agencies (LEA) in these countries also have stringent requirements for access to plain text data and that they must have ways and means of getting access to the encrypted data in times of need, and/or for sanctioned surveillance. In order to assure the protection of individual and civil liberties, many of these countries have developed processes and requirements which control government access to personal, non-public information. India as a nation, should have appropriate policies that both help the economic growth, while at the same time enabling LEA to access data much the same way it happens in the developed world.

There are various scenarios that may make use of encryption in e-commerce applications and where the LEA may need to have access to unencrypted data. The use of encryption for e-commerce applications in these scenarios implies that one is talking about users/employees of the corporates, their trading partners, collaborators, service providers etc. Citizens at large have access to encryption tools that are freely available over the Internet, and they may use encryption in their communications with one another. The government itself uses secure channels of communication in delivering services to citizens.
They will have to manage or direct the management of encryption in e-government systems; so access to unencrypted information and documents in those systems is of less concern. There are, however, business-to-business e-commerce systems where regulation may be required in the interest of national security, but that should be in keeping with global approaches for using appropriate encryption to ensure that India continues to use best practices for secure communications. National security concerns have to balance the global competitiveness of Indian industry or attractiveness of India as a processing location.

National security, thus, has a bearing on encryption policy, and it requires consideration of various technical issues, national security issues, business privacy, and international competitive pressures for the growth of e-commerce and e-governance applications. Continued economic growth of Indian industries and business in an increasingly global economy require availability of cryptography to all legitimate users that include employees and business associates of the corporate sector. There is no question that the government will have legitimate reasons based in national security and law enforcement to require companies to provide access to information in decrypted form. That being said, to maintain the international credibility of doing business in India such requests must be made pursuant to established processes with required element of proof, appropriate documentation and authority for the request and subject to appropriate oversight and redress.

It would be instructive to study the experience of other countries. In the US, pursuant to the Omnibus Crime Control and Safe Streets Act of 1968, it is required that the Administrative office of the United States Courts (AO) report the number and nature of orders authorizing or approving the interception of wire, oral, or electronic communication. Among the information elements that need to be included (Public Law 106-197 amended 18 U.S.C. 2519(2)(b)) are the number of wiretaps where encryption was encountered and whether such encryption prevented access to plain text by law enforcement. These reports are required to be filed annually, and a review of even the most recent filings of these reports is that encryption is not often found and where found only resulting in a problem in a few instances. Such reporting by intelligence agencies in India should be considered by the government. It is now believed that it enhances security to enable the use of encryption rather than the idea that strong control of encryption by governments is the best path. Any controls on encryption would actually limit or inhibit the use of encryption, which results in a less secure commercial infrastructure and a greater risk to security. It is the commercial secrets, intellectual property, and military secrets that are the target of cyber attacks. The US claims to have suffered losses of over a trillion dollars during the year 2008. Encryption can help secure against such losses.

2.2. Encryption norms in India

The encryption norms put forth by Department of Telecom (DoT) and Department of Information Technology (DIT) are as follows:
• ISP license issued in 1998-99 by DoT limits the level of encryption by 40 bit key length and for the use of more than this prescribed limit, written permission from DoT is required with mandatory deposit of decryption key with DoT. Also there is an obligation on ISPs to ensure that bulk encryption is not deployed.

• The IT amendment Act passed in 2008 which has amended the IT Act of 2000, and has come into effect from 27th of Oct 2009, has led to addition of Section 84 A, which says that the Central government may, for secure use of electronic medium and for promotion of e-Governance and e-commerce prescribe the modes or methods of encryption.

• Section 69 of IT Act 2000 empowers the, Central Government/State Government/ its authorized agency to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource if it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence or for investigation of any offence.

84 A of IT Amendment Act refers Govt. defining national Encryption Policy. Data Security Council of India in consultation with industry submitted its recommendation. DSCI has been requesting that encryption of higher strength should be permitted for the end users. When it comes to encryption, there are two things: one is the end user who is encrypting information, other is the systems that provide encryption, between the end user and the server. And then there is bulk encryption, i.e. point to point encryption provided by ISPs. DSCI in its recommendation to the encryption policy has highlighted all this. It has also deliberated on in situations like an imminent terrorist communication, etc, where government requires decrypted information.

To enable the encryption committee setup by Govt. of India, which has a presence from Law enforcement side also, DSCI along with USIBC organized a 3 days close deliberation with the committee. The Global experts in encryption technology and related legal aspects had visited for the deliberation. This initiative was supported by companies like Microsoft, Intel, RSA, RIM (Blackberry); and Indian companies like TCS, Infosys. This deliberation tried to convince the committee about the approach taken by western countries such as US and UK and made their submission to the committee on the same.

However, as this issue is tied up with the National Security of the country, the final recommendation of the encryption committee is believed to be held up for want of resolution of debate on “access to plaintext by intelligence”, and how it’s creating uncertainty in business. For example, as per newspaper reports, DoT raised concerns over Blackberry devices, Skype and Google services. The DoT is said to have asked the companies to either ensure that data going through their networks be made available to

---

security agencies in a readable format or face a ban in India. It has also raised concerns over data services being offered by Tata Teleservices and Reliance Communications. All this has put a big question mark on outsourcing because global companies and Indian service providers use Skype and other VOIP services for secure business communications.

“DoT has asked the representatives of Research In Motion (manufacturer of Blackberry devices) and Skype to ensure that the content going through the telecom service providers is in readable format. They have to ensure that this is implemented within 15 days, failing which services that do not allow lawful interception on a real-time basis would be blocked/banned”.
3. Cyber Security

Cyberspace comprises IT networks, computer resources, and all the fixed and mobile devices connected to the global Internet. A nation’s cyberspace is part of the global cyberspace; it cannot be isolated to define its boundaries since cyberspace is borderless. This is what makes cyberspace unique. Unlike the physical world that is limited by geographical boundaries in space—land, sea, river waters, and air—cyberspace can and is continuing to expand. Increased Internet penetration is leading to growth of cyberspace, since its size is proportional to the activities that are carried through it.

Cyberspace merges seamlessly with the physical world. So do cyber crimes. Cyber attackers can disrupt critical infrastructures such as financial and air traffic control systems, producing effects that are similar to terrorist attacks in the physical space. They can also carry out identity theft and financial fraud; steal corporate information such as intellectual property; conduct espionage to steal state and military secrets; and recruit criminals and others to carry out physical terrorist activities.

Anyone can exploit vulnerabilities in any system connected to the Internet and attack it from anywhere in the world without being identified. As the Internet and new technologies grow, so do their vulnerabilities. Knowledge about these vulnerabilities and how to exploit them are widely available on the Internet. During the development of the global digital Internet and communications technology (ICT) infrastructure, the key considerations were interoperability and efficiency, not security. The explosion of mobile devices continues to be based on these insecure systems of Internet protocols.

It is increasingly cheap to launch cyber attacks, but security systems are getting more and more expensive. This growing asymmetry is a game changer. It has another dimension, too—individuals, terrorists, criminal gangs, or smaller nations can take on much bigger powers in cyberspace, and through it, in the physical world, as well. The effects of attacks on critical infrastructure such as electricity and water supplies are similar to those that would be caused by weapons of mass destruction, without the need for any physical attacks.

Proving attribution in cyberspace is a great challenge. In most cases, it is extremely difficult to attribute cyber attacks to nation-states, collecting irrefutable evidence. The very nature of botnets and zombies makes it difficult to do so, leading to the conclusion that “the Internet is the perfect platform for plausible deniability.”

Nations are developing cyber attack capabilities with a view to dominating cyberspace. However, unilateral dominance in cyberspace is not achievable by any country. But uncontrolled growth of cyber attack capabilities—in effect, cyber attack proliferation—is an increasingly troubling phenomenon. Yet another disturbing reality is that cyber attacks can be launched ever more easily, and propagated faster using the same broadband that nations are building for global e-commerce. Finally, the consequences
of a cyber attack are more likely to be indirect and more uncertain than most scenarios currently envision; we may not always recognize the damage inflicted by cyber attackers.

Yet another point to be appreciated is that it is the same vulnerabilities, and malicious codes to exploit them, that can be used to target for financial frauds, commercial or military espionage, or even to launch cyber wars. Growing number of significant actors not tied to, or even loosely affiliated with, nation-states have been observed to be responsible for a number of high profile attacks in India and abroad. Over the last few months, events in cyberspace such as the GhostNet attacks on governments and large multinational corporations, whether to steal intellectual property or attack free speech, bear this out. They are not restricted by geographical borders or national laws.

Cybersecurity is not a technology problem that can be ‘solved’; it is a risk to be managed by a combination of defensive technology, astute analysis and information warfare, and traditional diplomacy. Cyber attacks constitute an instrument of national policy at the nexus of technology, policy, law, ethics, and national security.

There is an added dimension to this problem: the infrastructures are owned and operated by the private sector, and cyberspace passes through various legal jurisdictions all over the world. Each government has to engage in supporting its private sector for cybersecurity through effective public-private partnership (PPP) models, with clearly-defined roles for government and industry. Because cyberspace is relatively new, legal concepts for ‘standards of care’ do not exist. Should governments create incentives to generate collective action? For example, they could reduce liability in exchange for improved security, or introduce tax incentives, new regulatory requirements, and compliance mechanisms. Nations have to take appropriate steps in their respective jurisdictions to create necessary laws, promote the implementation of reasonable security practices, incident management, and information sharing mechanisms, and continuously educate both corporate and home users about cybersecurity.

When it comes to tracking cyber criminals, it is not only the laws dealing with cyber crimes that must exist in various countries, but the collection of appropriate cyber forensics data in various jurisdictions and their presentation in courts of law, which are essential to bring criminals to justice in sovereign countries. International cooperation is, clearly, essential to securing cyberspace.
4. Legal Regime for Cyber Security and Privacy

Privacy as a concept involves what privacy entails and how it is to be valued. Privacy as a right involves the extent to which privacy is (and should be legally protected). “The law does not determine what privacy is, but only what situations of privacy will be afforded legal protection.” In the legal parlance the issue of privacy comes up where an obligation of confidence arises between a ‘data collector’ and a ‘data subject.’ This may flow from a variety of circumstances or in relation to different types of information. An obligation of confidence gives the data subject the right not to have his information used for other purposes or disclosed without his permission unless there are other overriding reasons in the public interest for this to happen. That is, the information collected for a purpose should not be used for any other purpose. This is seldom the case here as is evident from telemarketing calls one receives on their mobile, unsolicited mails received and so on. And this has been the case in more mature democracies in the western world.

4.1. Information Technology (Amendment) Act, 2008

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, introduces the concept of “sensitive personal information”, and fixes the liability of the ‘body corporate’ to protect the same under section 43 A.

The IT (Amendment) Act, 2008 under section 43(A), makes a body corporate handling any sensitive personal data or information in a computer resource controlled/operated by it, liable to follow reasonable security practices – failure to do so may result in loss of information which will make it liable to pay compensation. Under section 72A punishment for disclosure of information in breach of a lawful contract is prescribed. Any person including an intermediary who has access to any material containing personal information about another person, as part of a lawful contract, discloses it without the consent of the subject person will constitute a breach and attract punishment. This will bring those responsible for breaching data confidentiality, under lawful contracts, to justice, and also act as a deterrent.

The above law is an omnibus that creates conducive environment for the growth of e-commerce and e-governance, while ensuring that cyber crimes do not go unpunished. It has created a strong data protection regime, along with privacy protection. Rules, to be notified, are expected to frame important privacy principles, even as they will prescribe the ‘reasonable security practices’ to protect ‘sensitive personal information’. Consumer privacy is thus effectively protected, both of domestic users and of clients who are outsourcing business processes and data to Indian service providers. Indian banks,
telecom companies, e-commerce sites and others, who collect personal data of their customers, are mandated to implement adequate security to protect their personal information.

4.2. Other Acts and Legislations

Data Protection including protection of personally identifiable information are based on the amended IT Act, 2008, and the following supporting Acts and Legislations

**Act(s)**
- The Indian Penal Code, 1860
- The Indian Telegraph Act, 1885
- The Indian Contract Act, 1872
- The Specific Relief Act, 1963
- The Public Financial Institutions Act, 1983
- The Consumer Protection Act, 1986
- Credit Information Companies (Regulation) Act, 2005

**Special Legislation(s)**
- The Information Technology Act, 2000
- The Information Technology (Amendment) Act, 2008

**Sector-specific law(s)**
- TRAI- National Do Not Call (DNC) Registry
- RBI Guideline- Adhere to privacy principle to protect customer information

**International Conventions**
- International Covenant on Civil and Political Rights, 1966
- Universal Declaration of Human Rights, 1948

While all these laws give privacy protection to a consumer, a citizen’s right to privacy emanates from Article 21 on Liberty, as interpreted by the Supreme Court in a judgment. However, there is no comprehensive Privacy Law in India.

Considering the Indian legal regime, protecting public safety and a nation’s security is a necessary and important function of a civilized society. However, *liberty, equality and fraternity* are also essential to the functioning of prosperous and free societies. Technological advances in the collection and processing of information over the last few decades have positioned this resource as vital to the health, well-being and freedom of individuals. More specifically, abuses of personal information can cause untold harm, wasted resources, and generally lead to the detriment of society. For example, a society of individuals perpetually anxious about identity theft, misuses of their information, or unwarranted search and seizures cannot function at optimum levels.
4.3. **NASSCOM - DSCI – A Self Regulatory Organization**

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 shows that self-regulation in the form of co-regulation is important even with enactment of privacy laws.
5. Right to Privacy - Concept

In the 1890 seminal article by Samuel Warren and Louis Brandeis (later Supreme Court judge), they coined the phrase, the ‘right to be let alone’ as defining privacy. ‘Privacy’ has been internationally regarded as a fundamental civil liberty since the 1940s. The Universal Declaration of Human Rights (1948) contains a paragraph on privacy. The 1950 European Convention on the Protection of Human Rights and Fundamental Freedoms includes 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, but not limited to, 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 such data in such databases raise 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.

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), 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 that were formulated by the US Department of Housing, Education and Welfare (HEW) in 1973. 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 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.
6. 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. The use of computers in accounting and personnel management that emerged in the 1960s transformed the policy problem of limiting the compilation, access, and use of personal files from a purely bureaucratic task into a political-technological endeavour. Now, it became ‘informational privacy’ or ‘fair information practices’ (the US version) and ‘data protection’ (in Europe). The discussion on the ‘Big Brother state’ was also growing. Thus began parliaments’ first efforts in 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. A bit later, West Germany at the federal level (1977), Denmark, Austria, France, Norway and Luxembourg (all 1978) also introduced privacy protection laws. Up to the beginning of the 1980s, seven countries—all in Western Europe—had enacted data protection laws, and in the 1980s, ten more followed, among them Israel, Japan, Canada. By the 1990s, 22 more states from all continents had joined the throng, followed by a smaller number into the new millennium.

Technical systems at the time were envisioned as centralised large computer facilities that would be easy to control and supervise, and where the data, once entered, would remain. In other words, there were huge cabinets full of digitised data where before there had been huge cabinets full of files, but still, they were huge cabinets.

By the 1980s, the picture had already begun to significantly change. The globalisation of the economy had led to an increase in transborder data flows. On the other hand, one of the official goals of international economic policy was (and is) free trade. Personal data, as soon as it became more widely available than before, also became a valuable commodity. As early as 1970, an expert group in the Council of Europe identified the transnational character of the computer and the according need for international regulatory harmonisation. Due to the fact that various national data protection laws often contain differing procedural regulations with regard to transnational data transfers, difficult legal conflicts still arose, even though they rested on the same basic set of principles. In the late 1970s, the Council of Europe and the European Parliament began discussions on how to remove these trade barriers whilst preserving data protection. The objective soon became clear: International harmonisation of data protection was needed. The European Parliament even called for the ‘creation of a genuine common market in data-processing’. During the following years, several international treaties and documents were developed in an attempt to harmonise international data protection. The most binding international agreement for 15 years was the Council of Europe’s 1981 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. This ‘influential treaty’ mandated the signatories to translate (or incorporate) its rules into national law. Citizens of one country party to the
treaty now had the right to legally fight any misuse of their personal data in another country that had ratified the treaty. The Convention included regulations on transborder 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 are not binding, and they had been preceded by fierce conflicts between the United States and some European governments. The Europeans perceived the very low or non-existing level of data protection in the United States as unacceptable and suspected that behind it was an attempt to globalise the dominance of the US computer industry with the buzz phrase ‘free flow of information’. The United States in turn accused the Europeans of protectionism by means of data protection. The guidelines themselves 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 harmonisation. The OECD for a decade was the only supra-regional international organization that dealt with privacy and data protection. It was only in 1990 that the UN General Assembly adopted the, also voluntary, Guidelines concerning computerised data files, which had no follow-up mechanism and therefore no real impact.

The EU data protection Directive is unanimously 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.
7. 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.

7.1. 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.
7.2. 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 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.
8. Debate on Cyber Security and Privacy Issues

In this borderless cyber world the laws should reflect demonstrable and enforcement capability, these should be measurable and should make organizations accountable for their acts. Specifically law should deliberate on issues of:

1. Secure data transmission between businesses for enhancing customer confidence of the end users, thus boosting the growth of industry as well as economy
2. Appropriate Encryption policy with balance between national security and secure business communications
3. Government as a big buyer should force secure product development and purchase only the same. Consumers are entitled to products that are “fit for purpose” and “free of defects” as per the globally prevalent trade practices. These practices make IT product vendors accountable for not building security in their products, so as to allow consumer make informed choice at the point of purchase
4. 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
5. Critical-infrastructure protection: Establishment of an international clearing house for critical-infrastructure protection to share threats, vulnerabilities, and attack vectors
6. Balancing of Interests of businesses and surveillance for security; same for citizens

In case of ‘right to privacy’ following set of questions needs to be debated:

1. Is Right to Privacy a fundamental right?
2. Does a citizen voluntarily give their Personal Information 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 applications 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. Security scanners particularly that of ‘Full Body Scanner’, that potentially lead to breach of privacy of an individual.
9. DSCI Recommendations

DSCI makes the following recommendations to the Hon’ble Standing committee on Information Technology (2009-10) for their consideration:

The proposed bill may

1. have light weight regulations based on global security and privacy principles that value economic benefits of data usage and flow, while guaranteeing privacy to citizens
2. avoid bureaucratic structures that could hinder business interests, and lose the spirit of intent in operational implementation
3. ensure that profiling of citizens by correlating existing databases will not be allowed in the name of national security
4. rely on self-regulation of businesses that promote practices, making the privacy program relevant to technology advancements
5. 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
6. notify and implement through Self-Regulatory Organizations like industry associations
7. allow businesses self declare the codes of practices that they have implemented to protect the privacy rights of the customers
8. establish a mechanism, in the form of public private partnership, to resolve the disputes and grievances of consumers
9. provide for appropriate encryption policy for secure business transactions that promote business and the overall economy of the country. The policy should cover industry standards and take into account disclosure of information in plaintext when required to do so by LEA under a due process
10. include mechanism for Incident response and establishment of appropriate mechanisms for cooperation. Such measures must include provisions to respond to counter cyber terrorism, including acts of sabotage of critical infrastructure and cyber espionage through information warfare
11. enable rules to ensure incidents are shared between public and private enterprises as well as give opportunities for research communities enabling them to develop tools and best practices
12. cover acceptable legal norms for dealing with cyber crimes regarding territorial jurisdiction, sovereign responsibility, and use of force to reconcile differing national laws concerning the investigation and prosecution of cyber crimes, data preservation, protection, and privacy.
13. address the problem of existing cyber laws that do not carry enforcement provisions;
14. mandate trainings and awareness of judiciaries and law enforcement agencies to handle cyber crimes and preservation of evidence through the use of forensic capabilities.
15. lead to establishment of international clearing house for critical-infrastructure protection to share threats, vulnerabilities, and attack vectors
16. support current and future technological trends and have the ability to remain dynamic based on the threat environment, through the support of rules and guidance

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.