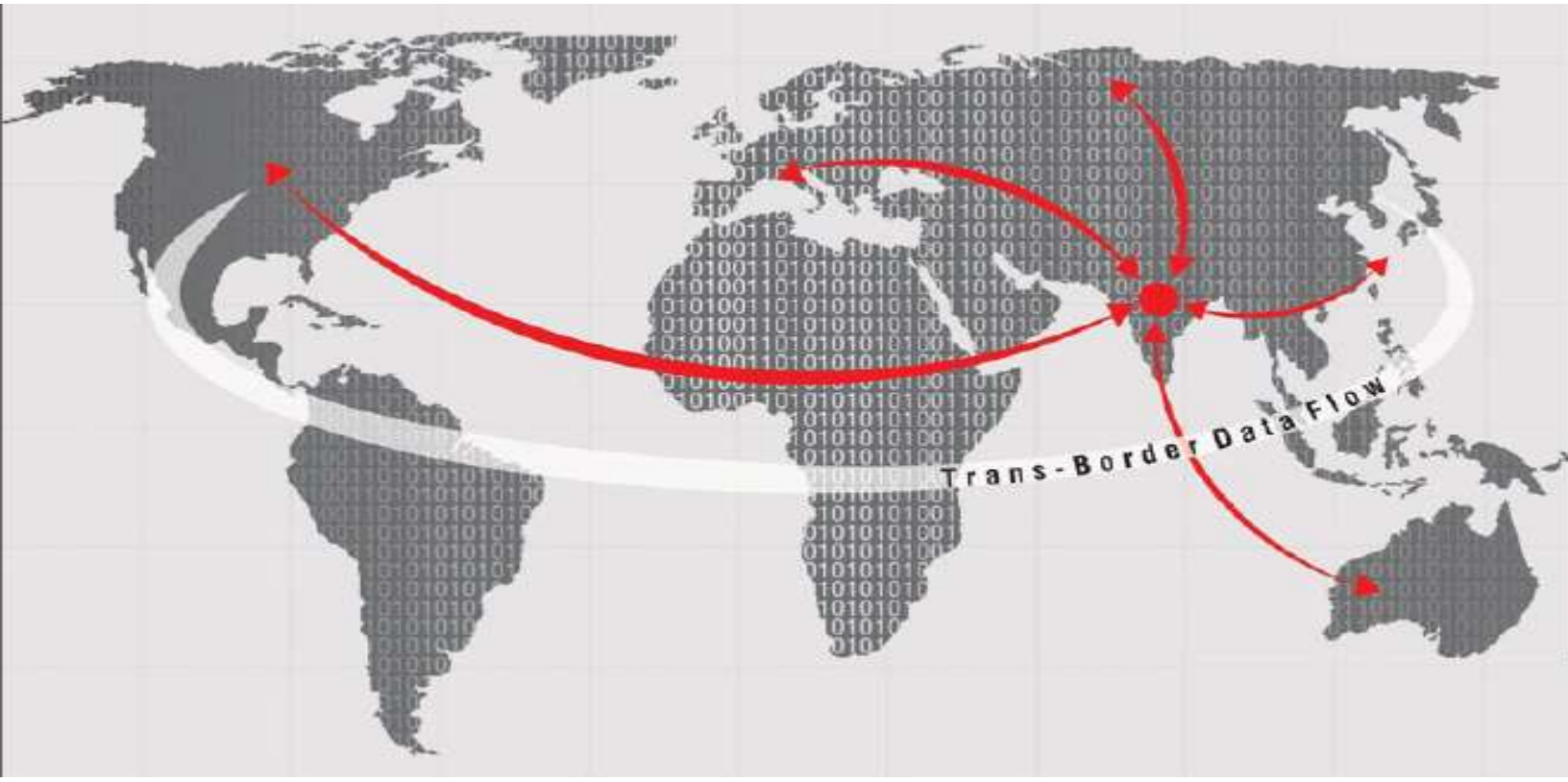
Data Protection - Security and Privacy

Information Technology Laws Workshop

Delhi University 19 – 21 March 2010

Kamlesh Bajaj, CEO, DSCI



DATA SECURITY COUNCIL OF INDIA
Niryat Bhawan, 3rd Floor, Rao Tula Ram Marg, New Delhi – 110057

P: +91-11-26155071 |**W:** www.dsci.in

1. Introduction

In today's world data collection is ubiquitous. So is data sharing. Google collects data of all users visiting it; Facebook collects data and shares data. These companies sell data to others which use it for marketing, in what is known as targeted marketing based on social behavior. Even though it is personal data of users, those collecting it are sharing it with others for business purposes. Companies are supposed to use Fair Information Principles like Notice, Choice and Consent and inform the users before collecting their data. Although companies do take some steps such as declaring their privacy policy, much is left to be desired as a fair practice. Countries around the world have enacted different laws to protect privacy of individuals.

In India, the Information Technology (Amendment) Act, 2008 was notified for implementation on 27 October, 2010. Although it is not a privacy law, it has some provisions that address data protection, including privacy. Section 43A in the Act mandates that all body corporates will implement 'reasonable security practices' to prevent unauthorized access to personal data of customers held by them. Failure to do so will make a company liable for compensation to an aggrieved person whose personal data including sensitive personal data may be compromised, during the time it was under processing with the company. It will be deemed as failure to protect such data whether because of negligence in implementing or maintaining reasonable security practices. In this paper we are focused on the personal data protection, or privacy, and not on what constitutes 'reasonable security practices' although that is an important subject.

The impact of globalization on privacy of identity is growing. The fact that more and more personal information is crossing borders in trans-border data flows means that data breaches often affect people in multiple countries, and may result in financial frauds – as in TJX case, a retailer in the United States. Nearly 100 million credit and debit cards belonging to people from various regions were exposed when hackers broke into its computer systems. They kept the information in personal computer servers in the U.S. and Eastern Europe and converted some of it into ready-to-use bank cards. Hackers sold the stolen credit card information to people in U.S. and Europe via the Internet.

Such crimes need to be addressed in national data protection laws. A strong data protection regime requires that cyber crimes of all types be covered to ensure data

security and data privacy. The amended IT Act does precisely that - it has tried to respond in a way that enhances trustworthiness of the entire cyberspace.

Social networking, in a short span of 3-4 years has caught the fancy of millions of users throughout the world even though it impacts security of organizations and privacy of individuals. Social web sites such as Orkut, Facebook, MySpace and many others have spawned up. People love to connect with one another, make friends, chat, and publish photographs of family and friends. They even post personal information for viewing by others. They can choose to keep such information secret, share it among their closed group of trusted friends, or make it public. However, these options, though available on social sites, are not fully understood by common users. But the consequences of ignorance or callousness can be serious. Behavioural patterns are quite disturbing though. On the one hand, citizens are paranoid about their privacy – they want and expect protection of all of their personal identifiers: name, address, mobile number, credit card details, PAN number, passport number, and social security number. On the other hand they reveal all of their personal information quite innocently and voluntarily on such sites to unknown people.

Information thus shared by people gets stored on the web site's servers located anywhere in the world. One does not know where the servers of Facebook, MySpace or Orkut are located? Where are their back up centres, their business continuity management servers? The personal information that we so zealously guard and protect, within our four walls or our perimeter so to say, is now out there in the open or in the cloud , as it is commonly called - on the servers of all such web sites. Which privacy laws are applicable? While all these sites must be taking adequate security measures, cloud computing does pose major security risks even as the promoters like Google, Facebook, and MySpace, try to assure the world that it is safe. Of course, there have been numerous incidents in the recent past when intruders have been able to gain access into some of them resulting in compromise of millions of records. There is no substitute to awareness creation, education and training of users, not as a one time exercise but as a continuous way of mitigating risks associated with technology adoption.

It may come as an eye opener to many if they try to understand how much do these global sites know about the users across the world. You just step into the website, and your habits based on surfing or transactions get locked. And perhaps for ever, unless, of course, the laws force them not to retain data beyond a certain period. For example, Google nows the following:

- Almost everything that is connected to the Web.
- 67% of all Web searches.
- 1% of what's sold on the Web.
- The traffic to more than 1.5 million Web sites.

- The physical locations of many things.
- The status of your machine if you install Google apps.
- The behavior patterns of Google registered users.
- Trying to know the physical location of any cell phone user who has installed Google apps, or accesses Google services from the phone.

Is this invasion of privacy? In this paper we will discuss basic concepts of privacy, personal information, how these are viewed by various countries, and what kind of laws have been created to protect privacy, and what are generally acceptable privacy principles. Data Security Council of India – a Self-Regulatory Organization created by NASSCOM – is focused on privacy protection and data security primarily to ensure that India continues to remain a trusted global sourcing partner of major clients around the world. DSCI's Approach to privacy protection based on Best Practices is, however, equally applicable to service providers in the domestic marketplace. This will be briefly described.

2. Privacy and Legal Approaches to privacy protection

2.1. **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. A definition of Privacy, on the other hand is "the claim of individuals, groups, or institutions to determine when, how, and to what extent information about them is communicated to others" by Dr. Alan F. Westin (Privacy and Freedom, 1967).

2.2. **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 European Union (EU) Data Protection Directive (DPD), Organization for Economic Cooperation and Development (OECD) privacy guidelines, Fair Information Practices of the US, Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), U.S. Gramm-Leach-Bliley Act (GLBA) for the financial data in the Untied States, Asia-Pacific Economic Cooperation's (APEC) Privacy Framework etc..

2.3. **The European Union** views privacy of personal information as a fundamental right, while the United States has sector specific laws on privacy of customer data. These include laws for protecting health information, and financial information among others. Privacy regarded as a fundamental right, regulated by a comprehensive set of principles that apply to both business and government. In pursuance of the EU Privacy Directive 95/46 of 1995, comprehensive national privacy laws and offices of data protection, led by privacy commissioners, have been created in the EU countries. European companies are severely restricted from collecting and selling information without individual consent. Some of the privacy laws in the European countries are listed below:

- EU- Directive 95/46/EC on the protection of personal data (95/46/EC October 24, 1995)
- EU- Directive on Privacy and Electronic Communications (2002/58/EC July 12, 2002)
- EU- Electronic Communications Data Retention Regulations 2009
- UK – Data Protection Act 1984

- UK – Freedom Of Information Act (FOI) 2000
- UK – Environment Information Regulation (EIR)
- UK – Data Retention
- UK – Regulation Of Investigatory Powers 2000
- UK – Electronic Communications Act 2000
- Scotland - Freedom Of Information Act -2002
- Scotland - Environment Information Regulation
- Privacy and Electronic Communications (EC Directive) Regulations 2003
- Anti-Terrorism, Crime and Security Act
- France – Federal Data Protection Act
- Italy- Data Protection Act
- Finland- Data Protection Act
- Sweden- Personal Data Act
- Germany- Data Protection Act
- Switzerland – Federal Data Protection Act

2.4. **The United States** has a history of self-regulation, especially in its safe-harbor program with the EU. It has defined Nine Privacy Principles, namely, *Notice, Choice and Consent, Collection limitation, Accuracy, Use and retention, Access and Correction, Security, Monitoring and Enforcement, Accountability.* Privacy is largely viewed as a consumer and an economic issue. Americans are comfortable with having businesses handle their information, but skeptical about putting data with government. There are many laws restricting the government collection and use of information than laws restricting corporate use of collection and information. With so many state and federal laws and various agencies responsible for data protection – SOX, GLBA, HIPAA, California Data Breach Notification Law – privacy protection is a veritable patchwork of laws. In fact, nearly 600 laws for privacy data security exist in the US. Moreover, oversight is decentralized; and data protection is not a core mission of any government agency.

A partial list of privacy and data protection laws in the United States is as follows:

- Children's Online Privacy Protection Act – 1998 (COPPA)
- Gramm-Leach-Bliley Act (1999)
- Federal Trade Commission Act
- Freedom of Information Act - 1966 (FOIA)
- Privacy Act of 1974
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- Family Education Rights and Privacy Act (1974)
- Privacy Protection Act of 1980
- Video Privacy Protection Act of 1988
- Employee Polygraph Protection Act of 1988
- Driver's Privacy Protection Act of 1994

2.5. **APEC**: Self-regulation is part of the APEC Privacy Program, which has taken the approach of Accountability Principle under which the data protection obligations flow along with data in trans-border data flows. In order to accommodate different privacy laws in various countries, APEC has placed emphasis on the practical aspects of data flows, the manner of interface between various players including companies, regulators, and governments. Cross-Border Privacy Rules (CBPRs), along with information sharing, investigation and enforcement across borders among regulators will form an integral part of the APEC Privacy Framework. The CBPRs are akin to Binding Corporate Rules (BCRs) allowed to Multinationals under the EU Directive.

2.6. **OECD, EU and APEC Privacy Principles** form the basis of many privacy laws throughout the world and are widely accepted.

2.6.1. The EU Data Protection Directive mandates that Member States promulgate laws in compliance with the Directive 95/46 issued in 1995.

2.6.2. The United States of America (US) - Fair Information Practices , US Department of Housing, Education and Welfare (HEW) in 1973.

2.6.3. OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data in 1980 - eight key principles for the protection of personal information.

2.6.4. The APEC Privacy Framework is relatively more recent endorsed by APEC Ministers and Leaders in 2004 – nine privacy principles

3. Privacy Principles

The underlying philosophy of privacy protection is that that the consumer be informed about the personal data that may be collected by the company whose services one is availing of, or the website that one is visiting. The company is expected to do so by declaring its privacy policy. Generally, the following eight principles cut across all

geographies: Notice, Consent, Collection Limitation, Use Limitation, Access & Corrections, Security/Safeguards, Data Quality and Openness. APEC, EU, and Canada include two more principles namely, Accountability and Enforcement. US Safe Harbor Program also includes these very principles (Notice, Choice, Onward Transfer, Access, Security, Data Integrity and Enforcement, openness, collection limitation, purpose specification, use limitation, data quality, individual participation, security safeguards, and accountability). Thus these twelve principles constitute the universe of privacy principles. These are covered in section 8.3.

4. Indian Legal Regime for Privacy

A citizen's right to privacy emanates from Article 21 on Liberty, as interpreted by the Supreme Court in a judgment. The IT (Amendment) Act, 2008 takes care of privacy rights of consumers by mandating that service providers protect 'sensitive personal information'. This could include all personal information, financial information such as bank account details, credit card number; biometrics; health information and any other information that is used to identify a person.

Data protection new clause 43A: The existing Act provides for penalty for damage to computers, computer systems under the title 'Penalty and Adjudication' in section 43 that is widely interpreted as a clause to provide data protection in the country. Unauthorized access to a computer, computer system or computer network is punishable with a compensation of upto one crore rupees. This section has been improved to include stealing of computer source code for which compensation can be claimed. (Computer source has been defined) Data protection has now been made more explicit through insertion of a new clause 43A that provides for compensation to an aggrieved person whose personal data including sensitive personal data may be compromised by a company, during the time it was under processing with the company, for failure to protect such data whether because of negligence in implementing or maintaining reasonable security practices. Further, 'reasonable security practices and procedures' will constitute those practices and procedures that protect such information from unauthorized access, damage, use, modification, disclosure or impairment as may be specified in an agreement between the parties or as may be specified in any law in force. In the absence of such an agreement or any law, the central government will prescribe security practices and procedures in consultation with professional bodies or associations.

Penalty for breach of confidentiality and privacy: Under section 72 it is presently restricted to those who gain access to an electronic record or document under the powers conferred under this Act. A new section 72A has been added that provides for punishment for disclosure of information in breach of a lawful contract. 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 with imprisonment of up to three years, and/or a fine of five lakh rupees. This is a strong deterrent, and also will bring those responsible for breaching data confidentiality, under lawful contracts, to justice. Along with section 43A, section 72A strengthens the data protection regime in the country. It will go a long way in promoting trust in trans-border data-flows to India.

Some of the other laws that have a bearing on data protection and privacy protection are as follows:

- 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

International Conventions

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

5. Global sourcing involves international data-flows

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

Global data-flows have become the norm. Whether one uses a social networking site or webmail to exchange information, it is not known where the data is stored. Personal information of users could be physically located anywhere around the world where huge data centers are getting established by service providers. And many of these services are now delivered out of 'cloud computing' models – some of which are global clouds. Again, the users do not know where their personal information is located, and which laws govern them. They are more concerned about the security and privacy of their personal data. So are the companies which are outsourcing their IT or business process operations to service provider.

6. Recent Privacy issues internationally

There are numerous judgements on privacy protection of consumers especially in the European countries. Some of the important ones involving MNCs such as Google, Facebook are presented below:

6.1. To track fund flows to terrorist organizations, the **United States** had worked out an **arrangement with SWIFT for data sharing in real-time**. However, Members of the European Parliament felt that such an accord between EU and the US failed to protect the privacy of EU citizens. The European Parliament, last month rejected an agreement to share bank transfer data between the EU and United States that was meant to fight terrorist financing. The Parliament voted 378 to 196 to throw out the interim, nine-month accord that took effect on 1 February. Thirty-one MEPs abstained. (European Voice.com 11 Feb 2010)

6.2. **Google:** Three Google Executives on privacy violations were convicted by an Italian Judge in Milan court on 24 February 2010 because they were found guilty of failing to comply with Italian privacy code in allowing a disparaging video to be posted online. Prosecutors argued that Google broke Italian privacy law by not seeking the consent of all the parties involved before allowing it to go online. The video at the centre of the case was posted on Google Video in 2006 shortly before the firm acquired YouTube. But the video was removed as soon as it was brought to its attention and that the firm also provided information on who posted it. This decision was described by Google as an "astonishing" attack on freedom of expression on the Internet.

Further, if the European Union data-Protection regulators have reduces the image storage time from 12 months to 6.In such a scenario, Google may not be able to map Europe again with photos for its Street View service. It had negotiated with EU authorities, agreeing to one- year storage from the day the images were

published on Street View. Google can't reprocess its data quicker as shorter periods won't be possible as its of software restraints.

Again, under the German privacy concerns on the Street View, Google have to offer residents the chance to remove pictures before they are published. It will have to add a tool to allow quick removal once the images are published and it will announce when its cars will be driving by to take pictures.

6.3. **Facebook:** In November 2009, Facebook issued a proposed new privacy policy, and adopted it unaltered in December 2009. This new policy declared certain information, including ***"lists of friends",*** to be "***publicly available***", with no privacy settings; it was previously possible to keep access to this information restricted. Due to this change, the users who had set their "list of friends" as private were forced to make it public without even being informed, and the option to make it private again was removed. After Facebook's recent privacy settings "adjustment" in December 2009, the social network reported on 1 February 2010 that 35% users who had never before engaged with their privacy settings took the initiative to do so instead of accepting the updated suggestions put before them by the social network.

6.4. **Technology leading to more invasive marketing:** Technology is used in widespread and that itself has created lots of challenges in the field of privacy. There are numerous cases of clash between the privacy and technology. On considering the new technologies like Full Body Scanner which captures, record, and store detailed images of individuals undressed. RFID devices track the consumption habits for targeted marketing. Though privacy is a valuable interest but threatened more than ever by technological advances.

7. Privacy issues in India:

7.1. Times of India reported on 11 Feb 2010 that the Home Ministry could not get the Cabinet Committee on Security's (CCS) nod to set up its ambitious **NATGRID -- National Intelligence Grid** -- as questions over safeguards for individual's privacy are learnt to have forced it to hold the proposal for further discussion.

Though the proposal will finally get CCS approval, it will happen only after the ministry comes out with detailed information about the inbuilt safety mechanism, according to government sources.

The proposed NATGRID -- a world-class integrated national security database -- will facilitate quick access to information on an individual -- like details of his/her banking, insurance, immigration, income tax, telephone and Internet usage.

7.2. Security and Privacy Challenges in a Centralized UID Database: Government of India has launched a massive project to issue unique identification numbers (UID Nos.) to all residents in the country – close to 1.2 billion – by capturing their personal particulars along with biometrics such as fingerprints, iris scan and facial image. This has thrown up several privacy challenges. Data will be captured by thousands of registrars and sub-registrars throughout the country, sent over networks for storage centrally. Central data will be accessed for de-duplication whenever a new entry of UID is to be created. This poses privacy challenges at all stages of collection, processing and storage. These have been analysed in detail in a paper prepared by DSCI (Security and Privacy Challenges in the UID project). Some of the data protection challenges are as follows:

- Large centralized databases, accessible over networks in real-time, presents significant operational and security concerns. If networks fail or become unavailable, the entire identification system collapses
- Large centralized databases of biometric PII, hooked up to networks and made searchable in a distributed manner, represent significant targets for hackers and other malicious entities to exploit.
- Large centralized databases are more prone to functional creep (secondary uses) and insider abuse.
- Significant risks associated with transmitting biometric data over networks where they may be intercepted, copied, and actually tampered with, often without any detection.

Other Security Issues:

- Falsification of content, eavesdropping, physical attacks, man-in-the-middle attacks etc.
- Security and Privacy Challenges at various lifecycle stages: collection, transmission, storage
- Additional challenges: Introducer system, POA, POI documents authentication
- Biometrics for de-duplication : vulnerable to loss – loss of identity forever
- Security vulnerabilities in Biometrics: spoofing, replay attacks, substitution attacks, tampering, masquerade attacks, Trojan horse attacks ….
- Biometrics Encryption - possible solution

8. Data Security Council of India (DSCI)

DSCI believes that data protection and privacy should be based on the tenet that if a corporate can have BCRs or CBPRs to show compliance with the data protection

requirements of an originating country - irrespective of where it is processed - a service provider in India should be also able to demonstrate compliance with data protection requirements similar to those of the country where the client is located, and/or where the data is originating, by following the best security and privacy practices and standards. DSCI considers the Best Practices Approach as a practical and realistic way to enhance global adherence to data security and privacy standards. These practices can also be used in meeting with the privacy and security of 'sensitive personal information' through the implementation of 'reasonable security practices'.

8.1. DSCI Best Practices for data protection are based on global best practices, security standards, and OECD Privacy Principles that will enable a service provider in India to be not only in compliance with regulatory requirements of clients' countries, but also make them really secure. Likewise, privacy too will be fully protected through best practices that include declaration of privacy policy, compliance audit for privacy, and privacy impact assessments. DSCI Security Framework (DSF) - comprising 16 Best Practices, and DSCI Privacy Framework (DPF) - comprising 9 Best Practices have been established for data protection.

8.2. DSCI Best Practices

In order to strategically define and address privacy issues, using a risk based approach, DSCI has proposed that the data controllers (exporting data to service providers in India) and the data processors (data importers, i.e. service providers in India) develop a privacy program that should include the following best practices:

Organizational Privacy Vision (OPV) - Privacy vision and strategy should be defined at the organizational level for the implementation of privacy program. Privacy vision, strategies, business drivers, scope of the privacy program should be defined and documented. The scope and objective should be communicated to the privacy working group. Responsibility for the protection of personal information should be delegated to a privacy officer. Roles and responsibilities of the privacy officer and the working group should be defined and documented as part of Organizational Privacy Vision.

Visibility over Personal Information (VPI) - Clear understanding of how personal information is being collected, used, transferred (or shared), stored and destroyed. Appropriate controls should be in place to address the clear visibility of the flow of personal information within an organization or when it is outsourced to a third party. At each stage of the information flow, starting from the collection till the stage it is

destroyed, it should be the responsibility of an organization to ensure that the information is used for its intended purpose only.

This could be carried out by,

- Taking out the inventory of all records containing personal information, whose information is being used
- What kind of personal information is being used or processed (e.g., Financial, Healthcare etc.)

The controls put in place should ensure that organizations take necessary actions in the event of the information not being used for its intended purpose.

Regulatory Compliance Intelligence (RCI) – Review of existing compliance mechanisms and identify areas where immediate compliance requirements are necessary. An organization should put in place procedures for analyzing information related to privacy regulatory changes thereby identifying areas where compliance requirements are necessary. These procedures should also be able to address the questions as to which courts should have jurisdiction over specific issues (choice of jurisdiction) and which system of law should govern specific issues.

Privacy Policy and Procedures (PPP) - Policies and procedures based on rationalized requirements and operational environment. An organization should assess the gaps between the current privacy practices and fair information practices, including pertinent privacy laws, regulations, and guidelines and prepare policies and procedures to address the identified gaps. These could include but not limited to, collection of personal information, management and use and disclose of information.

In Collection,

- Information will only be collected with the consent of an individual
- Information will only be collected that is necessary in order to carry out the intended task
- Information will only be collected in a fair and lawful manner.

In Management and Use,

- Information as to how information is being collected and who else it might be given to should be communicated
- Reasonable steps to ensure the personal information collected, use or disclose is accurate, complete and up-to-date. This may require updating the information from time to time.

In Disclose of Information,

- Access to the information is limited to a “need to know” and/ or consent basis.
- Information will be disclosed only if deemed as relevant

Personal Information Security (PIS) – Measures for protection of personal information against risks, such as loss of confidentiality, integrity, unauthorized destruction, usage, or other misuses. Appropriate controls should be in place to protect personal information residing on servers, database, in the form of hard copy etc.

Controls could be but not limited to,

- Appropriate logical access controls on the servers, databases etc
- Physical access controls. Access to the data center could be given to authorized personnel only
- Storage of records containing personal information. Encryption tools could be used when storing or transferring personal information
- Destruction of records containing personal information. Means to modify the records containing the personal information in such a way as to render the personal information contained in the records unreadable or undecipherable, including, without limitation:
  1. Shredding of the record containing the personal information; or
  2. Erasing of the personal information from the records.

Privacy Awareness & Training (PAT) – Training strategy for creating awareness on privacy and data protection. This should address the continuous training of all the personnel involved in the privacy program, including the employees, contractors and individuals. There should be mechanisms to measure the effectiveness of the training programs.

Awareness & Training program would ensure but not limited to,

- Timely detection and reporting of privacy incidents and thereby minimizing the impact from such incidents
- compliance with organization's privacy policies
- demonstrates organization's concern for protection of personal information
- Helping employees recognize and respond appropriately to privacy incidents

Information Usage and Access (IUA) – Measures in limiting the use of personal information for the purpose identified. Providing access to personal information on a need to know basis with proper authentication, authorization and accountability defined. An organization should have appropriate controls to use the information only for the purpose identified.

Controls to access the information should include but not limited to,

- Access to records containing personal information should be given only need basis with proper approval and authorization
- Appropriate logical access controls on the servers, databases etc
- Physical access controls. Access to the data center could be given to authorized personnel only
- Accountability should be established when giving access to personal information

Privacy Contract Management (PCM) – Contracts with third party vendors, business partners for the protection of personal information. An organization could enter into a written agreement with third party vendors, business partners requiring that they provide at least the same level of privacy protection as required. Every third party vendor, business partners should enter into a privacy contract consisting of privacy agreements with an organization before any personal information is transferred.

These contracts should include but not limited to,

- Acknowledge that an organization cannot, by contracting out; relieve it of its privacy obligations.
- To ensure compliance with relevant regulations and requirements, each contract for personal information services should require the third party vendor, business partners to comply with the privacy practices specified in or under the contract.
- The contract should contain scope and inventory of personal information, general contractual obligations of an organization, address general contractual obligations of third party vendor, business partners.

Monitoring and Incident Management (MIM) – Privacy program monitoring and incident management process provides timely and effective feedbacks on the overall privacy program. This process should include necessary steps that an organization can adopt to manage a privacy incident, thereby minimizing the impact from such incidents. As part of this process, privacy incident response plan should be documented to provide a well-defined, organized approach for handling any potential threat pertaining to personal information of employees, clients, contractors and business partners.

This process should include but not limited to,

- Incident detection and recording
- Classification and initial support
- Investigation and diagnosis

- Incident closure
- Incident ownership, monitoring, tracking and communication

An organization should monitor compliance with its privacy policies, procedures and other requirements. Regulatory compliance should also be monitored and documented.

A privacy program roadmap is essential to address implementation through these key concepts.

8.3. DSCI Privacy Principles

The proposed privacy Principles are explained below,

8.3.1. Preventing Data Misuse

Personal information protection should be designed to prevent any data misuses. Further, acknowledging the risk that individual harm – tangible or intangible – may result from such misuse of personal information, specific measures should take account of such risk, and adequate remedial measures should be implemented for collection, use and transfer of personal information.

8.3.2. Notice

Data controllers should provide clear and easily accessible statements about their privacy policies and practices; the fact that personal information is being collected and the purposes of collecting personal information; usage of the collected personal information, retention and disclosure. Additionally, the identity and location of the data controller, including information on how to contact them about their practices and handling of personal information should be made available.

8.3.3. Choice and Consent

Choice and Consent, requires that the data controller describe the choices available to the individual and obtain implicit or explicit consent with respect to the collection, use, and disclosure of personal information.

8.3.4. Collection Limitation

The collection of personal information should be limited to the purposes identified in the notice and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.

8.3.5. Accuracy

Accuracy requires that the personal information that data controller holds should be accurate, complete and relevant, and kept up to date for the purposes identified in the notice.

8.3.6. Use and Retention

Use and Retention Principle requires that the data collector limit the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The data collector retains personal information for only as long as necessary to fulfill the stated purposes and the data is destroyed, when it is no longer required, in accordance with the identified procedures.

8.3.7. Access and Correction

Access and Correction Principle requires that the data controller provide individuals with access to their personal information for review and update. Personal information should be 'readily available', i.e., individuals should be able to obtain information without unreasonable cost and within reasonable time.

8.3.8. Disclosure to third parties

Disclosure to third parties requires that the data controller disclose personal information to third parties only for the purposes identified in the notice and only with the implicit or explicit consent of the individual. Additionally, the data controller should make sure that the third-party adheres to all applicable privacy Principles and/or regulations. As an alternative, the organization can enter 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 principles. However, this Principle may not be applicable when disclosing personal information to Government or law enforcement authorities.

8.3.9. Security

The Security Principle requires that the data controller should protect personal information that they hold with appropriate safeguards against risks, such as loss of confidentiality, integrity, unauthorized destruction, usage, or other misuses. Such safeguards should be proportional to the risk associated with the personal information misuse and harms it could result in, and should be subject to periodic review and reassessment.

8.3.10. Monitoring and Enforcement

This Principle requires that the data controller monitors compliance with its privacy policies, practices and applicable laws and regulations, and has procedures to address privacy-related inquiries and disputes.

8.3.11. Regulatory Compliance

This Principle requires that the data controller should have procedures in place to address different laws with respect to handling of personal information. These procedures should be able to address the questions as to which courts should have jurisdiction over specific issues (choice of jurisdiction) and which system of law should govern specific issues (choice of law).

8.3.12. Accountability

A data controller should be accountable for complying with measures that give effect to the privacy Principles. When personal information is to be transferred to another person or organization, whether domestically or internationally, the data controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization (or data processor) will protect the information consistently with these Principles. However, this would not prevent the data processor also being held accountable.

9. Conclusion

Privacy protection will grow in importance as people use more and more online applications for banking, e-commerce, and e-governance everywhere, including in India. This is because any privacy breaches resulting in data loss may compromise large number of records. This amounts to identity theft, since data stolen can be used for committing frauds, including financial frauds. One can have an idea of the enormity of possible online frauds because of identity thefts by looking at some of the numbers as presented below:

- 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, according to reports by the 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

Privacy concerns in the expanding online transactions in India are bound to increase. Some of the figures are astounding by the sheer volumes that are being handled in the projects:

- UIDAI Project – capturing the personal information of 1.2 Billion people in India. Will present the biggest challenge to privacy of citizens.

- Mobile - More than 490 million subscribers Cross **1 billion by 2014.** Their personal data is to be protected from any abuse.
- ***Internet is replacing*** other channels to ***execute banking transactions***
- Retail e-payment likely to grow by 70 % - **$ 180 billion by 2010**
- About **100,000 railway e-Tickets** by IRCTC
- E-transactions currently account for 37 % of total transactions. However, **total amounts to 75 % payment value in electronic form**
- Card circulation (credit & debit) will hit **210 million** by 2010

The IT (Amendment) Act, 2008 will have to be implemented effectively to protect consumer privacy. Organizations will be required to implement the Best Practices for Security and Privacy as outlined above.

REFERENCES

- http://ec.europa.eu/justice_home/fsj/privacy/
- https://www.privacyassociation.org/
- http://www.dataguidance.com/
- http://www.europeanvoice.com/
- http://thegovmonitor.com/world_news/united_states/new-york-highlights-data-privacy-day-22437.html
- http://www.readwriteweb.com/archives/facebook_pushes_people_to_go_public.php
- www.securityfocus.com/news/
- http://old.gartner.com/DisplayDocument?id=918012