



## RISE PROJECT

# Policy Paper: Privacy in India May 2010



---

**DATA SECURITY COUNCIL OF INDIA**

Niryat Bhawan, 3rd Floor, Rao Tula Ram  
Marg, New Delhi – 110057

P: +91-11-26155071 | W: [www.dsci.in](http://www.dsci.in)

---

## EXECUTIVE SUMMARY

---

### MESSAGE TO INDIAN POLICY MAKERS

- 1. Trust Relationship in Technology Transformation:** Trust relationships between government and citizens, businesses and citizens are critically important, as they provide an assurance to the end users about protection of their personal rights. While the Indian economy is gradually transforming into an e-economy, these relationships are increasingly challenged by technology innovations. Securing the growth of an economy, thus, requires redefining the trust relationships that govern these transactions with a view to protect the interest of end users.
- 2. Reflection of Culture Change:** Sustained growth of the country is gradually transforming the demographic patterns of the society towards urbanization, leading to migration of the population to the upcoming urban centers. This is one of the drivers behind individualism; moving away from hitherto collectivist nature for which Indian society is recognized. Rising Individualism Index (IDV) of a society is closely attributed to an increased awareness of personal rights. New generation, on the one hand, is increasingly opting for IT enabled services over the conventional channels; while on the other hand, it is becoming sensitive to the issues that impact their personal rights. The policy initiatives of a country should be sensitive to the changes in the societal perception and that should be reflected in the policy deliberations.
- 3. Internet Penetration:** Penetration of Internet in India is significantly rising, connecting citizens from all spheres to a web of new means of communication, new ways of service offerings, easy and efficient execution of transactions, and offering unprecedented opportunities of networking with individuals and organizations across the globe. A democratic country needs to do everything possible to protect its citizen's personal rights, no matter how communications, interactions and transactions are conducted.
- 4. Increasing Digitization of Personal Information:** As a result of the huge investment in e-Governance projects and increased reliance on IT enabled channels by industry like Banking, Finance, and Telecom; more and more services are being delivered over the Internet. Delivery of services to end users requires collection of personal information. This, however, attracts the attention of security threats that offer more targeted capabilities to compromise the information. The magnitude of the information that will get digitized in this country will make matters worse, as it will provide more avenues and yield more benefits to those who are likely to be benefitted by the use of information.

- 5. Assuring Personal Rights in the Age of E-Governance and E-Commerce:** Increasing attempts are being made by the government bodies and private organizations to bring the entire population under the fold of IT enabled services. Population of over 1.2 billion, diverse geographical locations, cultures and associated perceptions, and disparate economical value distribution lead to multifaceted challenges in protection of the personal rights. Managing this challenge will be a complex affair in the Internet age, and hence, requires all players including the Government, Regulatory Bodies, Civil Societies, and Private Organizations to act in collaboration with one another to protect the personal rights of an individual, with whom they are doing their daily transactions.
- 6. Weaker Section of the Society:** Rural population and urban poor—significant portion of them are still illiterate— will get networked through some flagship and specific e-Governance projects. Industries such as banking, insurance, and telecom are also trusting technology enabled services to take them to the remotest part of the country. Mobile is becoming a means to engage with this segment of the population. These industries are taking some initiatives to check whether the mobile technology can be used to execute a financial transaction. Although new channels will be delivering tremendous benefits, with less awareness of the flip side of the use of technology, and without adequate protection guaranteed, there is a great danger of catastrophic exploitation of this section mass.
- 7. IT Outsourcing Industry:** India IT and ITES service providers are growing at a phenomenal rate and establishing India as an IT powerhouse. They are increasingly exposed to the global compliance regimes for data protection. Data protection regimes increase liability of the service providers towards the data subject. They also demand to have a strong legal framework for data protection in the country where data is being transferred. IT and ITES industry, now an inspiration of millions and poised to earn \$ 225 billion by 2020, needs an ecosystem that ensures protection of data and an adequate legal model that promises adequate protection. This will help provide assurance to the clients across the globe, with legal mechanisms in their geographies and the data subject, whose personal information is at a stake.
- 8. Changing Attributes of Principles Democracy:** India has been greatly regarded for resorting to the core principles of democracy while many testing scenarios have emerged in the last 60 years. Even with very diverse cultures, scale and diversity of issues, size that poses challenge beyond management, India stand out in a global landscape that guarantees its citizens of their fundamental rights. The right to privacy, with the use of IT, assumed a meaning of protection of the personal information that is being gathered, processed, stored and transferred. Therefore, it is obvious that a democratic society should reflect this transformation and respond

accordingly so that the core principles of democracy are adhered to, even though their nature change with societal and technological transformation.

- 9. Law Enforcement:** Law enforcement, historically, has been a challenge in this country; sometimes it may be seen falling short of protecting rights of an individual in the physical space. Protecting these rights in the Internet Age is a daunting task, as borders of jurisdiction expand across nations. The means that lead to infringement of individual rights are abundant; technology provides multiple avenues to the perpetrators. Increasing connectivity and networking offers an expanded surface that can be exploited. Guarantee of personal rights in the Internet Age, thus, requires competent legal system and an effective enforcement of the same
  
- 10. Privacy and National Security:** India acquired a unique geopolitical space that is surrounded by many challenges affecting its national security posture. These challenges became more evident in the last couple of years. It is legitimate to strengthen the internal security mechanism that assures its citizens a free and secure life. Collective security has a major bearing on the rights of an individual as national security measures, now a days, include measures such as gathering information, tracking of individual's transactions to identify likely suspicious behaviour, and monitoring user activities for crime detection and analysis. This endangers personal rights of an individual, who would like to tolerate, to an extent, the use of his information for the cause of national security, but will like to avert compromise of his rights. To avoid gross misuse of the personal information, there is a need for an equal balancing of national security requirements and personal rights.

## Contents

---

|   |           |
|---|-----------|
| <b>CHAPTER 1: Privacy in the Digital Age .....</b>                    | <b>1</b>  |
| 1. Data Collection.....   | 1         |
| 2. Impact of Globalization.....                                       | 1         |
| 3. Social networking.....   | 1         |
| 4. Information Sharing.....   | 2         |
| 5. Mammoth Information and its analysis.....                          | 2         |
| 6. Rising Privacy Concerns.....                                       | 2         |
| <b>Chapter 2: Privacy Issues in India.....</b>                        | <b>4</b>  |
| 1. Indian Economy Transforming to E-economy.....                      | 4         |
| 2. Privacy in New Age Transactions and Service Deliveries.....        | 4         |
| 3. Cyber Crime and Warfare .....                                      | 5         |
| 4. National Security and Privacy .....                                | 5         |
| 5. Security and Privacy Challenges in a Centralized UID Database..... | 6         |
| 6. Outsourcing.....   | 6         |
| 7. Legal and Regulatory Environment.....                              | 7         |
| <b>Chapter 3: Privacy Initiatives .....</b>                           | <b>9</b>  |
| 1. End User Education.....  | 9         |
| 2. Privacy by Design .....  | 10        |
| 3. Transborder Flow of Information and Privacy .....                  | 11        |
| 4. Self Regulation .....  | 12        |
| <b>Chapter 4: Policy Recommendations.....</b>                         | <b>13</b> |
| 1. Government of India.....   | 13        |
| 2. eGovernance projects.....  | 13        |
| 3. Civil Societies.....   | 14        |
| 4. Law Enforcement Bodies .....                                       | 14        |
| 5. Industry Regulatory Bodies.....                                    | 14        |
| 6. Industry Bodies .....  | 15        |
| 7. Outsourcing Industry .....   | 15        |
| <b>References.....</b>  | <b>16</b> |

## CHAPTER 1: Privacy in the Digital Age

---

- 1. Data Collection:** 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. Companies tend to sell data or analysis based on the data to others which use it for marketing, in what is known as targeted marketing based on online behaviour. 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.
- 2. Impact of Globalization:** The impact of globalization on privacy of an individual is growing. The fact that more and more personal information is crossing the 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.
- 3. Social networking:** 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.

**4. Information Sharing:** 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 backup 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 onetime exercise but as a continuous way of mitigating risks associated with technology adoption.

**5. Mammoth Information and its analysis:** 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 forever, unless, of course, the laws force them not to retain data beyond a certain period. Google knows 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 mapps.
- The behavior patterns of Google registered users.
- The physical location of any cell phone user who has installed Google mapps, or accesses Google services from the phone

**6. Rising Privacy Concerns:** 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 a 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)

## Chapter 2: Privacy Issues in India

---

- 1. Indian Economy Transforming to E-economy:** While India is leading in providing IT services to businesses across the globe; the domestic sector has emerged as a key IT investor. Leading the pack, Government agencies are spending more than \$ 10 billion in several of e-Governance projects. Private sectors such as BFSI, Telecom, Manufacturing, and Travel are increasingly relying on IT to process transactions and offer diverse channels to their customers. Internet penetration, although currently low at about 7.1 %, is rising exponentially. According to a Forrester report, a market research company, India will be third largest user of Internet by 2013. According to the Celnet report, 'Payments in India is going e-way', E-transaction currently account for 30% of the total transactions, 75% of the total payment value is found in the electronic form. Similarly, card circulation both credit and debit is on the verge of hitting 200 million this year. Indian IT and IT Services industry is growing multi-fold. According to Mckinsey-NASSCOM study, outsourcing industry currently at \$60 billion, will reach to \$225 billion by 2020. This transformation will increasingly bring Indian citizens under its fold, exposing them to the new age threats that not only have the potential to damage their financial interest, but also infringe their personal rights.
- 2. Privacy in New Age Transactions and Service Deliveries:** Increasing commercialization in India that involves identifying potential customers, marketing products and services, promotional activities, and cross-selling is seen to be relying on the personal information. It has been observed that the data gathered while providing services and selling products is increasingly used for the purpose not intended. This has been more visibly observed in the telecom sector, which later resulted in the implementation of National Do Not Call Registry (NDNC). However, implementation of it on the ground remained abysmal, leading to irritation, frustration and worries of the end users. Reserve Bank of India, the Central Bank of India, sensing the way the transactions are transforming and their impact on privacy of customers, issued a regulatory guidance that demands banking industry adhere to privacy principles. Privacy is slowly graduating into discussion landscape of India. This has been accelerated by the recent amendment of the Information Technology (IT) Act. Transaction heavy organizations such as Banking, E-Commerce, and Telecom that are leading the adoption of Information Technology are conforming to the world recognized privacy principles. Privacy policies of these organizations are visible on their websites, articulating their commitment to, and informing users about the likely usage of their information.

However, in comparison to the advanced countries, the privacy initiatives both by individual companies and the respective regulatory bodies have remained at the surface. In the United States, vertical specific regulations like HIPAA, GLBA strongly advocate protection of personal information, and enforce them vigorously through breach notification laws and regulatory bodies such as Federal Trade Commission (FTC). In India the industry specific regulatory bodies seem to be lagging in aligning their policies to evolving security and privacy challenges. The awareness of privacy issues in the Internet browsing, usage of new age services, social networking and executing online financial transactions seem to be not mature as observed in the European countries.

**3. Cyber Crime and Warfare:** Cyber criminals began in a small way to commit petty crimes, in different parts of the world. But with the expanding cyberspace, financial payoffs have increased, which, in turn, have led to the emergence of organized gangs spread over different cities across countries. Crime syndicates including terrorists are increasingly visible. So are fundamentalists of different religious, socialist and political groups, who are masquerading the cyberspace to cause aggrieved damages to nations. They have already graduated from defacing websites to causing real damage to their 'enemies'. New age cyber crimes increasingly attack the end users; increasing digitization of the end users' information aggravates this problem multifold. E-Governance applications are obvious targets of these attacks that come from cyber criminals or nation states, indulged into cyber warfare capabilities. Critical sectors like banking also offers lucrative target to them. This poses a great challenge to an individual, who is willingly or unwillingly, become a part of the cyber space. This lead to an unprecedented scene, where the significant section of population is exposed to grave threats that are international in nature.

**4. National Security and Privacy:** 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 discussions. Though the proposal will finally get CCS approval, it will happen only after the ministry comes out with the detailed information about the inbuilt safety mechanism, according to the 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.

In the interest of sovereignty and integrity of India, security of the State, the IT (Amendment) Act, 2008<sup>1</sup> authorised the designated agencies of Government to

---

<sup>1</sup> [http://www.mit.gov.in/sites/upload\\_files/dit/files/downloads/itact2000/it\\_amendment\\_act2008.pdf](http://www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf)

assume a power to issue directions for interception or monitoring or decryption of any information through any computer resource. This has a major bearing on privacy of an individual. Rising terrorism threats that India is witnessing in the recent years justifies a need for such monitoring of traffic, the implementation of ambitious projects such as NATGRID or Lawful Interceptions as allowed by amended IT Act may lead to infringement of the privacy of individuals.

#### **5. 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 the residents of 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 Data Security Council of India (DSCI), 'Security and Privacy Challenges in the UID project'. Some of the data protection challenges are as follows:

- (i) 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
- (ii) 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.
- (iii) Large centralized databases are more prone to functional creep (secondary uses) and insider abuse.
- (iv) Significant risks associated with transmitting biometric data over networks where they may be intercepted, copied, and actually tampered with, often without any detection.

**6. Outsourcing:** 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. While the European Union views privacy of personal information as a fundamental right, the United States has sector specific laws on privacy of the customer data. Processing of personal information of citizens of these countries by service providers (IT/BPO companies) in India and in other countries through outsourcing raises concerns about the regulatory compliance. In view of the multiplicity of privacy legislations

worldwide, the service providers in India are faced with a major challenge of demonstrating compliance with the laws of countries where the data originate.

**7. Legal and Regulatory Environment:** The Indian legal system derives a strength to deal with cyber security and data protection measures from various enactments, namely, (i) The Indian Telegraph Act, 1885, (ii) The Indian Contract Act, 1872, (iii) The Specific Relief Act, 1963, (iv) The Public Financial Institutions Act, 1983, (v) The Consumer Protection Act, 1986 and (vi) The Credit Information Companies (Regulations) Act, 2005 and the IT Act 2000. 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. On the other hand, it helps to take legal action against an individual for the breach of confidentiality and privacy, under a lawful contract. The data protection regime in India emerges with these provisions.

**7.1. Reasonable Security Practices for Data Protection-** IT (Amendment) Act, 2008, adopts a route of ‘reasonable security practices’ for protection of ‘sensitive personal information’. The Act refrained from creating an infrastructure in terms of a privacy commissioner’s office as prevalent in the European countries. This would have led to the formation of a rigid bureaucratic mechanism impeding routine business functions. Instead, the Act tries to address the data protection concerns of its citizen by fixing the liability of the organization that is not able to implement the practices to an extent of unlimited liability. However, the definition of ‘reasonable security practices’ and ‘sensitive personal information’ are not yet notified by the Government of India. Data Security Council of India, a not-for-profit company set by NASSCOM, an industry body of Indian IT and BPO companies, in its consultation paper, recommended the Government of India define the Privacy Policy based on OECD privacy principles. There is a hope that Government, shortly, will come up with a set of rules for privacy. This will help align India’s legal regime with the global practices.

**7.2. Body Corporates-** IT (Amendment) Act, 2008 demands ‘Body Corporate’<sup>2</sup> implement ‘reasonable security practices’ for protection of the personal information. The Act defines “Body Corporate” as any company that includes a firm, sole proprietorship or any other association of individuals engaged in commercial or professional activities. This leaves a debate open on whether Government bodies fall within the ambit of the “Body Corporate”. If government and its bodies are immune from the legal protection assured to the citizens, it will leave all e-Governance projects including the flagship projects such as the UIDAI out of the scope. This will seriously impact the endeavour of

---

<sup>2</sup> [http://www.mit.gov.in/sites/upload\\_files/dit/files/downloads/itact2000/it\\_amendment\\_act2008.pdf](http://www.mit.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf)

assuring privacy to the end users as government agencies are front runner in offering online services, hence, gathering mammoth personal information, storing, processing at centralized locations. Extending the scope of privacy specific regulations to the government bodies will bring them at par with the private industry in terms of their accountability and liability towards protecting the sensitive personal information.

**7.3. Data Breach-** As compared to some of the leading western countries, especially in the US, the legal regime mandates reporting of the data breaches, which gives a very transparent picture of the data breaches happen across the country, there is lack of such a mechanism in India. However, till date there was not a case of major data breach reported. Going forward, without this kind of mechanism, it would be difficult to have a national level picture on data breaches. For effective enforcement of the privacy policies, usefulness of this kind of a mechanism cannot be denied. The IT (Amendment) Act, 2008 enables CERT-In with a power of calling information from the organization. However, it remained to be seen how CERT-In will like to use this power to establish a breach notification mechanism in the country.

**7.4. Keeping pace with technology-** As life in the technology enabled age changes with a greater speed, attributes of the personal rights change accordingly. A dynamic regulatory mechanism is, therefore, required, which responds swiftly along with the technology changes. This need is recognized by the Government of India while drafting the amendment. It comes with an idea of 'rule making' under the Act. While amendment of statute requires assent of the Parliament, which is a long drawn process, the rule notification is a governance process that does not require approval of the Parliament.

## Chapter 3: Privacy Initiatives

---

**1. End User Education:** Among the various measures that are advocated to build a privacy culture in India, education of end users is particularly important. Majority of them would be the first time users of the IT systems. With technology being seen as a means to achieve financial inclusion, there has been increased investment in the e-Governance projects. Simultaneously, growing private investment in the technology will bring the entire population of the country under the fold of cyber age. This is being done irrespective of how equipped the end users are to understand the dangers of the cyber space. End user's awareness of how his or her personal information is being collected, used, processed, shared and stored and how organizations and individuals can misuse this information will go a long way in creating a privacy culture. End user's awareness of the legal protection available to guard his or her personal rights, in case of any breach pertaining to the personal information, will definitely serve as an effective check on organizational practices in respect of processing the personal information. High level end user awareness will also help deploy trust mechanisms. In that case, they will be able to use the facility that enables them take trust decisions while executing his or her transactions. The success of a policy advocacy that demands such a technical measure from the entities that are involved in processing of a transaction is critically dependent on the end users' awareness for effective implementation. Recently there has been a significant change in the legal regime of India in respect of data privacy. This should be complemented with an adequate awareness of all entities that are part of executing transactions that include body corporates, government bodies, end users, law enforcement bodies and judiciary.

End user awareness needs enough attention of technology policy initiatives. Government of India should commit adequate resources, develop an ecosystem and appropriate partnership, and outline a well conceived plan that assures continual awareness of the end users. Messages pertaining to security of the data, privacy in the cyber age needs a loud and comprehensive platform that targets different categories of audiences and achieve the desired outreach. Civil liberty bodies should also take this cause in their initiatives. Exploitation of new age services channels serves a significant cause for these bodies to act in the interest of the citizens. Industry, which relies on the end user's confidence for their growth, while transforming their business using IT, should put significant efforts to create the trust relations with user community. Individual effort of a company, joint efforts of the industry bodies and their partnership with Government should incorporate the task of educating users. All channels that connect the end users must be utilized while

taking security and privacy messages to them. The awareness and education program should cater to all user types that include home users, students, farmers, workers, bank customers, professionals, and law enforcement officials. The program should be able to deliver general and customized messages based on the user community, type of transactions and channels used to deliver.

The Strategic Approach<sup>3</sup> of the Department of Information Technology for Cyber Security identifies major actions and initiatives to promote a comprehensive national awareness program. This initiative, concentrating on cyber security, needs a major revamp to bring focus on the privacy.

**2. Privacy by Design:** As per Ontario's Privacy Commissioner, Dr. Ann Cavoukian's concept 'Privacy by Design'<sup>4</sup>, the future of privacy cannot be assured solely by compliance with the regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation. *Privacy by Design* now extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) Accountable business practices; and 3) Physical design and infrastructure. Privacy by Design advocates a proactive approach, which relies on preventive measures of an organization to gain confidence of the end users.

While IT provides a legitimate platform to both government and private organizations to extend their reach, integrates with a large section of user groups to the national economy, the systems and applications should be built in a way that they offer a real time protection of the sensitive personal information. Privacy should assume its role in life cycle processes of an organization right from the design, deployment and operation. E-Governance standards should be revisited to incorporate the privacy principles. Project design and requirements should spell privacy requirements in clear terms, ensure their implementation and monitor the enforcement of controls that are attributed to privacy. Transaction heavy applications like banking that processes sensitive personal information should embed privacy in their designs. Organizational practices should provide a high level of assurance to the end users that:

- (i) their information is being gathered for a designated purpose,
- (ii) a limit imposed on collection,
- (iii) prescribe and ensure usage of information,
- (iv) end user is updated on actions being performed on his or her information,
- (v) adequate safeguard is deployed to protect information

---

<sup>3</sup> <http://www.mit.gov.in/content/strategic-approach>

<sup>4</sup> <http://www.privacybydesign.ca/>

Data Security Council of India has come up with a privacy framework known as DSCI Privacy Framework (DPF<sup>®</sup>)<sup>5</sup>, which helps the organizations establish a privacy function that is based on visibility of information, intelligence over regulatory compliance, and privacy principles, policies and processes. It advocates establishing central privacy organization and its healthy relations with the business units. It takes a note of various Privacy Enabled Technologies, and recommends adequate controls for information usage and access. DPF<sup>®</sup> rely on Monitoring and Incident Management processes to deal with the data breaches. It also believes that privacy specific awareness and training is an important aspect of the privacy initiatives of an organization. Different frameworks, practices, technology measures and processes that embed into an organization's culture lead to a situation where privacy is treated as a hygiene factor in its operations.

**3. Transborder Flow of Information and Privacy:** Flow of information including personal information across borders has greatly increased in recent years, and it is bound to increase in the coming years. This flow of information contributes a lot to the economy of nations. While protection of personal rights is important for securing the interest of citizens, the economic and social values of information flow need to be appreciated. The success of the Indian outsourcing industry lies in the principle of market that demands organizations to take the benefit of the services which come with huge cost saving, with embedded quality and required scalability. Globalization also involves a great deal of information flow. Multinationals operating across the globe transfer data of their customers, suppliers, employees including their personal data to different geographies they operate in.

Nations across the globe are seen increasingly sensitive towards the protection of personal right of an individual in the new age that. Policy initiatives being taken across the globe—India also joined the league by IT (Amendment) Act, 2008— are trying to provide necessary protection to their citizens. In doing so, these legislations and policy initiatives may hinder the flow of information within or across national borders.

The market is strongly in favor of transborder flow of information across the nations. This has been proved in various studies. OECD declaration on transborder Data Flow<sup>6</sup> recognises the growing importance of transborder data flows and the benefits that can be derived from transborder data flow. It advocates its member states avoid the creation of unjustified barriers to the international exchange of data and information.

---

<sup>5</sup> [http://dsci.in/index.php?option=com\\_content&view=article&id=80&Itemid=100](http://dsci.in/index.php?option=com_content&view=article&id=80&Itemid=100)

<sup>6</sup> [http://www.oecd.org/document/8/0,3343,en\\_2649\\_34225\\_2373500\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/8/0,3343,en_2649_34225_2373500_1_1_1_1,00.html)

If a party (service provider, who receives the data) involved in the Transborder flow of information deploys adequate measures to secure the data, and shares the proportionate liability with the other party (client organization, who sends the data) through a contractual agreement, and this agreement is valid under legal framework of the nations involved, then flow of the information should not be restricted. Once a responsible person or entity/independent body verifies that the level of protection by the recipient in the Destination State is similar to that in his own State, international transfers should begin.

- 4. Self Regulation:** Although adequate legal protection is required to protect the personal rights, and there is strong case in favour of the intervention of public powers to assure the protection, the role of Self-regulation in data protection increasingly has been established as an effective step. Self regulation reduces administrative bureaucracy and promises to bring efficiency in the data protection processes. A self-regulatory initiative has become now a useful instrument that not only supplements a legislative framework of an organization but also brings a required dynamism in the protection. United States has a long tradition of self-regulation. The best practices approach as a practical and realistic way to enhance global adherence to the data security standards.

Data Security Council of India (DSCI), has been set up by *the National Association of Software Services Companies of India (NASSCOM)*, as a non-profit organization and an independent self-regulatory organization to promote the data security and data privacy standards and frameworks as best practices among the Indian IT and ITeS.

## Chapter 4: Policy Recommendations

---

For the success of policy initiatives that can really create an impact, entities, including government and private, need to work in tandem. Each of these entities, in their respective capacity, can bring the necessary change that promotes a culture of privacy. This paper has proposed policy recommendations to the key entities that are in a position to make a difference in current state of the privacy.

### 1. Government of India

- (i) Rule making under the amended IT act, which is under progress, should set guiding principles for privacy in line with the globally recognized privacy principles.
- (ii) Include all government agencies which collect, process, store, transfer, disclose and use personal information of the end users in the definition of the “Body Corporate” as defined under Section 43A of the IT (Amendment) Act, 2008
- (iii) Establish a national ecosystem that is continuously engaged for the data protection cause
- (iv) Foster collaboration and partnership with all stakeholders including private sector for promotion of this cause
- (v) Dedicate sufficient resources and investment on technology research, for promoting academic projects, and creating an infrastructure for this cause
- (vi) Focus on awareness and education of the end users
- (vii) Issue guidelines and standards that provide practical guide government departments, e-Governance projects and private sectors
- (viii) Establish a mechanism for data breach notifications that mandates organizations to report the data breaches

### 2. E-Governance projects

- (i) Revisit design, architecture, and deployment of projects from privacy perspective. Conduct routine privacy impact assessment
- (ii) Ensure that project implementation and operations adhere to the guidelines and standards for privacy
- (iii) Ensure that privacy is ensured in entire lifecycle of data i.e. data collection, use, processing, and storage
- (iv) Implement adequate measures for security and vulnerability management of systems that engage in processing of personal information

- (v) Build an organization culture that respects privacy of the end users
- (vi) Ensure that privacy policies and practices are defined and implemented
- (vii) Ensure that significant effort is dedicated on end user's education that enables them to take trust decisions while they are transacting online
- (viii) Establish vigilant monitoring for privacy; deploy a mechanism to address end user's grievances

### **3. Civil Societies**

- (i) Attributes of humanity and democracy principles change with technology. Civil societies should proactively take data privacy in their agenda
- (ii) Closely monitor government proposals and initiatives that would potentially impact privacy
- (iii) Vigilant review or monitoring of private organization's practices that processes personal information
- (iv) Contribute to the education of end users, and lobby with the government for policy response

### **4. Law Enforcement Bodies**

- (i) Update themselves with latest trends, technology changes, transactions, end user relations
- (ii) Augment skills to deal with technology matters that impact the end users under cyber security concepts and how cyber crimes are perpetrated, and develop investigative techniques for such crimes
- (iii) Keep pace with changing legal regime for effective use of legal provisions that guarantee protection to end users against the crimes that infringe their personal rights or use their personal data to perpetrate any crime
- (iv) Focus on end user's education by making them aware of cyber crimes that are targeted on sensitive personal information

### **5. Industry Regulatory Bodies**

- (i) Understand specific privacy needs of respective industry by dedicating significant efforts on how industry practices and use of technology affects privacy of the end users
- (ii) Issue specific and more granular set of guidelines and standards that control industry practices pertaining to processing of personal information
- (iii) Establish a mechanism to address grievances of the end users

## 6. Industry Bodies

- (i) Act in the interest of the end users, as industry growth that rely on the new age channels is critically dependent on the trust of the end users
- (ii) Work closely with the government in policy related matters that impact privacy of the end users and subsequent changes in the organizational practices
- (iii) Conduct research study on the impact of changing technology trends or use of specific technology solutions on the personal rights
- (iv) Awareness of the member companies on privacy of the end users
- (v) Advice on organizational practices that upheld privacy principles

## 7. Outsourcing Industry

- (i) Obtain a complete visibility over the personal information received or exposed to as part of outsourcing
- (ii) Establish sound organizational practices that are based on globally recognized privacy principles
- (iii) Build a Risk and Compliance Intelligence mechanism that closely tracks global data protection regimes, and their impact on trans-border data flows
- (iv) Implement adequate measures to secure access and usage of personal information
- (v) Build a vigilant and responsive privacy culture in the organization for a swift response to data breach incidents

## References

---

1. *Digital Person: Technology and Privacy in the Information Age* by Daniel J. Solove, New York University Press
2. *Privacy by design* by Ann Cavoukian, Information and Privacy Commissioner of Ontario, Canada
3. *Consumer E-Commerce Market in India 2006/07, Internet and Mobile Association In India: [www.iamai.in/Upload/Research/final\\_ecommerce\\_report07.pdf](http://www.iamai.in/Upload/Research/final_ecommerce_report07.pdf)*
4. *Payments in India is going e-way, Celnet report: <http://reports.celent.com/PressReleases/20081008/IndiaEPayments.asp>*
5. *Forrester Forecast: Global Online Population To Hit 2.2 Billion By 2013: <http://www.forrester.com/ER/Press/Release/0,1769,1296,00.html>*
6. *Sharma, Vakul. Information Technology-Law & Practice (2nd Edition): Universal Law Publishing Co. Pvt. Ltd, New Delhi, 2007*
7. *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security and Privacy <http://www.privacybydesign.ca/pbdbook/PrivacybyDesignBook-ch7.pdf>*
8. 'Security and Privacy Challenges in the UID project', Position paper of Data Security Council of India, [http://dsci.in/images/security\\_and\\_privacy\\_challenges\\_in\\_the\\_uidai\\_project-v6.1\\_final.pdf](http://dsci.in/images/security_and_privacy_challenges_in_the_uidai_project-v6.1_final.pdf)
9. *OECD Declaration on Transborder Data Flows [http://www.oecd.org/document/8/0,3343,en\\_2649\\_34225\\_2373500\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/8/0,3343,en_2649_34225_2373500_1_1_1_1,00.html)*
10. *Government Monitor: Public Sector News and Information [http://www.thegovmonitor.com/world\\_news/united\\_states/new-york-highlights-data-privacy-day-22437.html](http://www.thegovmonitor.com/world_news/united_states/new-york-highlights-data-privacy-day-22437.html)*
11. *Times of Indian <http://timesofindia.indiatimes.com/india/CCS-seeks-tighter-privacy-safeguards-in-NATGRID-proposal/articleshow/5557716.cms>*
12. *Overall Spectrum Management and review of license terms and conditions, TRAI: [www.trai.gov.in/WriteReadData/trai/upload/.../704/pr16oct09no71.pdf](http://www.trai.gov.in/WriteReadData/trai/upload/.../704/pr16oct09no71.pdf)*