Appendix V

DSCI Privacy Framework (DPF) from Data Security Council of India

Introduction

The impact of globalization on "privacy" of an individual is growing day by day. Refer to Fig. 6.1 in Chapter 6 – the middle block in the figure mentions "privacy" in the context of identity theft (see ID theft discussed in Chapter 5). Privacy protection laws and legislations around the globe are discussed in Chapter 6. On the business side, "data privacy" is a major concern when information changes like never before in the global business era where applications are integrated, seamlessly connected and businesses run 24 × 7 around the world. Data privacy protection is now a business enabler for emerging economies such as India where a large amount of IT services work is getting outsourced. Implications of data breaches and loss of confidential information in businesses and corporate is explained in Chapter 9. Chapter 5 explains how individuals' "Privacy" is impacted by "Phishing attacks" and "identity theft." Data privacy has several dimensions (see Fig. V.1). Chapter 11 (in CD) provides a number of real-life case illustrations – many of those are about privacy breaches and data breaches. Clearly, we need strong measures to protect privacy in its many gambits. We need a dependable framework for data protection and in that context the data protection framework (DPF) from DSCI is introduced in this appendix. The idea is to present the data privacy framework that has emerged from India.

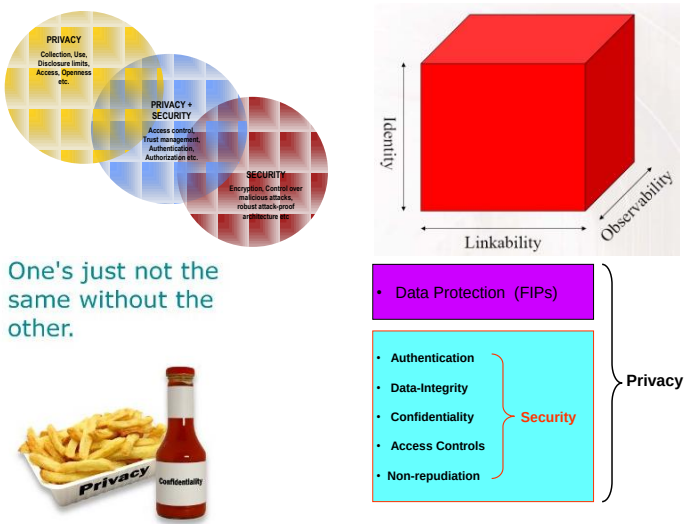

Figure V.1 Privacy: A multi-dimensional concept.

Privacy: A Multi-Dimensional Concept

The FIPs (Fair Information Practices) are explained in Chapter 6 (see Box 6.4). FIPs for data protection mentioned in Fig. V.1 are as follows:

1. Collection Limitation Principle.
2. Data Quality Principle.
3. Purpose Specification Principle.

4. Use Limitation Principle.
5. Security Safeguards Principle.
6. Openness Principle.
7. Individual Participation Principle.
8. Accountability Principle.

Rising Importance of "Privacy" in Healthcare Domain

In the healthcare business domain, "PHI," that is, personal health information is globally recognized as private data and in other businesses there is PI (personal information) and SPI (sensitive personal information) to be protected (see Fig. V.2).

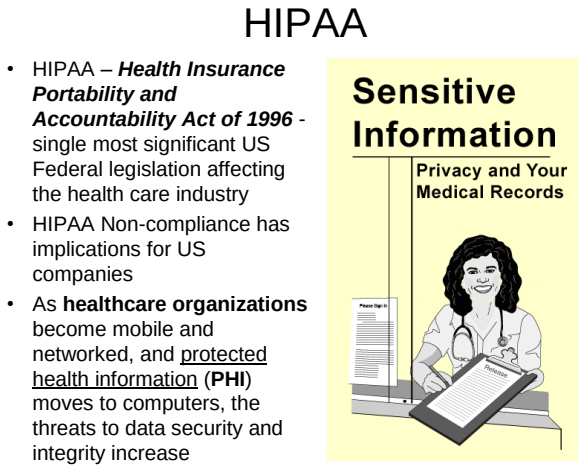

Figure V.2 HIPAA and PHI (protected health information).

Within industry and business, privacy is perpetually an important issue. It is an issue which regularly presents tensions between challenging obligations. Privacy is a fundamental right of individuals and is an important condition for the exercise in self-determination. At one level privacy is about corporate culture and how individual rights are valued. This leads to the thought of what levels of protection are required. However, privacy has many aspects such as:

1. **Informational privacy:** It is about data protection and the users' rights to determine how, when and to what extent information about them is communicated to other parties, and the execution of this right may be based upon their knowledge about what the other party's intention is. Consider "data privacy" as in Corporate businesses/outsourcing of work.
2. **Personal privacy:** It is about content filtering and other mechanisms to ensure end-users are not exposed to whatever violates their moral senses. In today's Internet era protection of individuals' non-public information is important.
3. **Communication privacy:** It is as in flow of information through computer networks; encryption of data being transmitted.
4. **Territorial privacy:** It is about protecting users' property ─ for example, the user equipment ─ from being invaded by undesired content such as an SMS or E-Mail/spam messages. Privacy is a vast and complex topic (see Fig. V.1).

DSCI and DPF

DPF© is DSCI Privacy Framework developed by *Data Security Council of India.* DSCI operating under the aegis of NASSCOM is a self-regulatory initiative in *data security and privacy protection.* It is envisaged as a credible and committed body to uphold a high level of data privacy and security standards.

The concept of "privacy," which traditionally meant intrusion in one's physical space, has become much larger in the cyberspace. Data privacy is evolving as a basic right of consumers. In certain countries, it is recognized as a fundamental right, guaranteed by the constitution and supporting legal framework. Although various countries share the goal of enhancing privacy protection of their citizens, majorly all the countries generally take a different approach to privacy.

To protect privacy of PI from unauthorized use, disclosure, modification or misuse, DSCI has conceptualized its approach toward privacy in the DSCI Privacy Framework (DPF©) which is based on the global privacy best practices and frameworks. Figure V.3 presents the key elements of the framework – there are nine disciplines or areas, organized in three layers. In the context of DPF, it is important to understand the two important terms: (a) data controller and (b) data processor. These terms are explained in the next section.

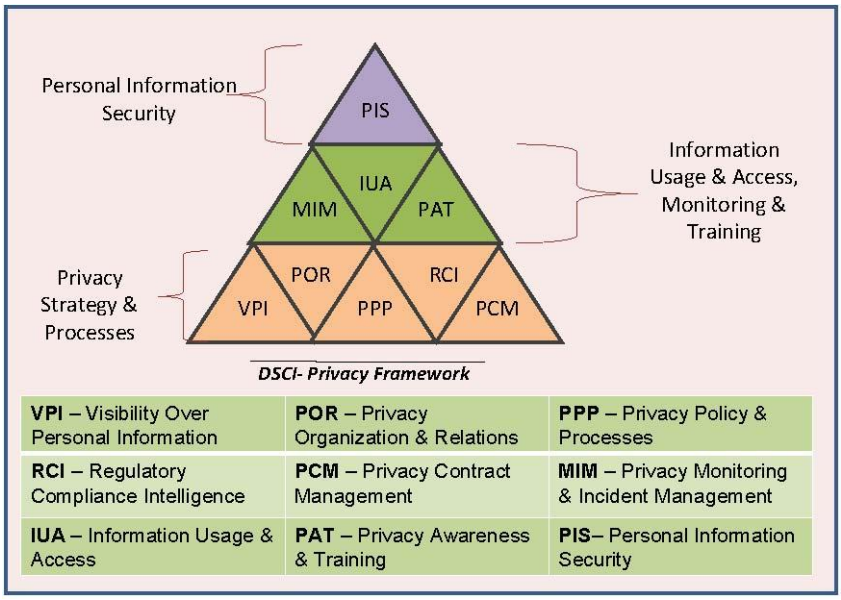

Figure V.3 The DSCI Privacy Framework.

Data Controller and Data Processor

To understand the implication of privacy requirements or regulations, there is a need to evaluate what role an organization is performing with regard to handling the PI. An interface with the end customer or user or consumer for collecting the personal data is one of the factors for identifying the role of an organization from the perspective of data protection. If an organization collects the data directly from the end customer, for the purpose of providing the business services offered, then it is called as the data controller. As the domestic industry segments in India such as banks, telecom, E-Commerce and E-Governance collect PI directly, they can be classified as data controllers.

If an organization receives the PI from any another organization for processing, as a part of services offered, it becomes the data processor. The IT services and BPO industry fall under this category. An organization that collects the PI of its employee also falls under the category of the *data controller*. The individual whose PI is collected – be it the end customer, consumer or even an employee is referred to as the *data subject*.

The data controller, who is the owner of the personal data being collected, should adhere to the privacy practices to provide an assurance to the end customer, and be in compliance with the applicable regulations. However, business realities such as outsourcing change the data protection dynamics. The data controller, who avails external services, extends the liabilities to and shares the same with the service providers. A service provider, termed as a data processor, thus, should also have the privacy initiatives to comply with data protection requirements of its clients.

The data processor, however, may not be required to adopt all privacy principles that the controller has adopted. Principles such as notice to the end customer, collection limitation and consent of the data subject may not be applicable to the data processor. However, for identifying the role of an organization from the perspective of privacy there requires a careful study of the nature of its business and its relations with the end customers, clients and service providers.

DSCI Privacy Principles

DSCI recommends nine principles in the context of the Indian industry, namely

1. Notice.
2. Choice and Consent.
3. Collection Limitation.
4. Use Limitation.
5. Access and Correction.
6. Security.
7. Disclosure to Third Party.
8. Openness.
9. Accountability.

The principles such as "Notice," "Choice and Consent" and "Access and Correction" are the user-centric elements which help an organization to provide comfort to the end customer (data subject) about their intent and policy with regard to the use of the PI. The principle "Access and Correction" assures the data subject that his/her information is accurate, he/she is given access to the information that an organization has gathered and stored in its systems and he/she has been provided with a mechanism to correct his/her data. These two principles – (a) Collection Limitation and (b) Use Limitation – together demand due diligence and care from an organization while collecting and using the personal data. The principle "security" stipulates the technical and organizational measures for securing the data. To ensure privacy in the business ecosystem, which increasingly uses third parties, the principle "Disclosure to Third Party" demands that the principles of data protection should be upheld in these relationships. The principle "Openness" reflects transparency of an organization with regard to the use of PI. The principle "accountability" stipulates that the data controller is accountable for complying with the measures that give effect to the principles stated above.

Structure of the DSCI Privacy Framework (DPF)

The nine practice areas, described in Fig. V.3, are organized in the following three layers:

1. **Privacy strategy and processes:** This layer aids in establishing the strategic and tactical elements for privacy. Creating visibility over the personal data helps understand how the data is handled by an organization. The central privacy organization should track the PI processed by an organization's processes, functions, projects and operations. It should establish sound relationships with different entities of an organization for coordinating and collaborating on privacy. The privacy policy should guide and provide direction for the privacy implementation. It should be supported by appropriate processes that promise consistency in effectiveness of privacy measures. Regulatory compliance intelligence, along with contract management for privacy, ensures alignment of the privacy initiatives to changing regularity requirements and proportionality of the measures to the liability exposure.
2. **Information usage, access, monitoring and training:** This layer ensures that adequate level of awareness exists in an organization. A significant level of measures is deployed to limit information usage and access. Also a mechanism is deployed for privacy monitoring and managing incidents that may compromise privacy.
3. **Personal Information Security:** This layer derives strength from an organization's security initiatives. However, it demands a focus on data security. DSCI has developed its Security Framework (DSF©), which can be leveraged for ensuring security of the PI.

How the Framework Adds Value to Organizations

The DPF© framework comprehensively covers all aspects of organization's (data) privacy requirements; it does that by providing a discipline-specific approach to security. The privacy best practices are organized in nine practice areas as mentioned below:

1. Visibility into Personal Information (VPI).
2. Regulatory Compliance Intelligence (RCI).
3. Information Usage and Access (IUA).
4. Privacy Organization and Relations (POR).
5. Privacy Contract Management (PCM).
6. Privacy Awareness and Training (PAT).
7. Privacy Policy and Processes (PPP).
8. Privacy Monitoring and Incident Management (MIM).
9. Personal Information Security (PIS).

The guidelines provided in DPF© are aimed at helping organizations in their privacy initiatives. DSCI's Privacy Best Practices address the privacy requirements of an organization. They address the requirements either from the perspective of "data controller" or "data processor." The nine best practice areas of the DPF©, in conjunction with DSCI Privacy Principles, provide an approach to establish an effective privacy function for data protection.

DSCI's DPF© discusses the basic concepts of different roles performed by various organizations; applicability of privacy principles and the best practices can be used to fulfill the principles to protect PI in transborder data flows.

DSCI Contact Details for Further Information and Implementation Guidance

DSCI is implementing its framework at both IT outsourcing industry as well as domestic industry. Organizations interested in implementing the framework can contact Director – Data Protection at DSCI. The details are provided below:

Director – Data Protection
DATA SECURITY COUNCIL OF INDIA (DSCI) | A NASSCOM® Initiative
L: Niryat Bhawan, 3rd Floor | Rao Tula Ram Marg | New Delhi - 110057, India
P: +91-11-26155071 | F: +91-11-26155070 | | E: info@dsci.in | Website: www.dsci.in