DOKUZ EYLÜL UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

PERSONAL DATA PROTECTION IN TURKEY: AN INFORMATION TECHNOLOGY FRAMEWORK INTENDED FOR PRIVACY RISK MANAGEMENT

by

Osman Okyar TAHAOĞLU

October, 2009
İZMİR

PERSONAL DATA PROTECTION IN TURKEY: AN INFORMATION TECHNOLOGY FRAMEWORK INTENDED FOR PRIVACY RISK MANAGEMENT

A Thesis Submitted to the
Graduate School of Natural and Applied Sciences of Dokuz Eylül University
In Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy in Computer Engineering

by
Osman Okyar TAHAOĞLU

October, 2009
İZMİR

Ph.D. THESIS EXAMINATION RESULT FORM

We have read the thesis entitled **"PERSONAL DATA PROTECTION IN TURKEY: AN INFORMATION TECHNOLOGY FRAMEWORK INTENDED FOR PRIVACY RISK MANAGEMENT**" completed by **OSMAN OKYAR TAHAOĞL**U under supervision of **PROF.DR.YALÇIN ÇEBİ** and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Doctor of Philosophy.

……………………………………
Prof. Dr. Yalçın ÇEBİ

Supervisor

…………………………………… ………………………………..
Prof. Dr. Alp KUT Asst. Prof. Dr. Salih Zafer DİCLE

Thesis Committee Member Thesis Committee Member

…………………………………… ………………………………..

Examining Committee Member Examining Committee Member

Prof. Dr. Cahit HELVACI
Director
Graduate School of Natural and Applied Sciences

ACKNOWLEDGMENTS

I would like to express my utmost gratitude and sincere thanks to my advisor, Prof. Dr. Yalçın ÇEBİ. His guidance, seamless support and friendship lead to the successful completion of my doctoral study. My cordial thanks and appreciation also extend to my thesis committee members, Prof. Dr. Alp KUT and Assist. Prof. Dr. Zafer DİCLE for their moral support, thought provoking and invaluable comments.

Finally, I would like to thank my mother whose love is boundless, my brother who was ready for help when ever needed and my loving wife for her continuous support, motivation and encouragement.

Osman Okyar TAHAOĞLU

PERSONAL DATA PROTECTION IN TURKEY: AN INFORMATION TECHNOLOGY FRAMEWORK INTENDED FOR PRIVACY RISK MANAGEMENT

ABSTRACT

Privacy has become an important value and right in and of itself where society has recognized the necessity of protecting citizens from its invasion. As a result of the significance of privacy, many disciplines including law, social-psychology, philosophy, economy and technology has approached the notion of privacy in their own areas where information technology used the term personal data protection in order to fulfill the confidentiality, integrity, availability, reliability, quality requirements of data owned by an individual.

Previous researches in Turkey analyzed the privacy rights from a public administration and law perspective and technical data protection mechanisms from a computer security perspective. In this study, current situation of data protection in Turkey, technical and non-technical aspects for a secure environment are investigated. An information technology framework is proposed in order to assure an end-to-end privacy during the full life cycle of personal data. The proposed solution is divided into three major domains; government, organizational and data owner domains. Consequently technology which is developed to protect privacy of data against the changing aspects of security concerns is described. Requirements engineering, risk management, incident calculation, compensation modeling, maturity modeling, privacy impact assessment are used in the framework analysis.

In this study it is shown that, technology originated threats on privacy can also be avoided by privacy enhancing technologies with a risk management approach. The proposed framework includes the starting point of a national wide privacy protection environment and detailed guidelines for companies, institutions and individuals.

Keywords: Personal data protection, privacy risk management.

TÜRKİYEDE KİŞİSEL VERİLERİN KORUNMASI: MAHREMİYET RİSK YÖNETİMİNE YÖNELİK BİR BİLGİ TEKNOLOJİLERİ ÇERÇEVESİ

ÖZ

Gizlilik ve mahremiyetin kendisi için bir değer ve bir hak olduğu ortaya çıktıkça toplumun kendi halkını koruma ihtiyacı ortaya çıkmıştır. Gizlilik ve mahremiyet öneminin bir sonucu olarak, hukuk, sosyal psikoloji, felsefe, ekonomi ve teknoloji gibi birçok disiplin kendi alanlarındaki bakış açısıyla konuya yaklaşmış, bilişim teknolojisi ise bir bireye ait bilginin gizlilik, bütünlük, erişilebilirlik, güvenilirlik ve kalite ihtiyaçlarını karşılamak için kişisel verilerin korunması terimini kullanmıştır.

Türkiye'de önceki araştırmalar mahremiyet haklarını kamu yönetimi ve hukuk perspektif incelerken, veri koruma mekanizmalarını bilgisayar güvenliği perspektifinden incelemiştir. Bu çalışmada Türkiye'deki mevcut veri koruma durumu, güvenli bir ortam sağlamak için teknik ve teknik olmayan yönleri araştırılmıştır. Kişisel bilgilerin tüm yaşam döngüsü boyunca uçtan uca gizliliğinin sağlanması için bir bilgi teknolojileri çerçevesi önerilmiştir. Önerilen çözüm üç ana alana ayrılmıştır; devlet, organizasyon ve veri sahibi. Dolayısıyla güvenlik kaygılarına, bu kaygıların değişen yönlerine ve verinin mahremiyetini korumak için geliştirilen teknoloji incelenmiştir. Çerçevenin analizinde ihtiyaç mühendisliği, risk yönetimi, olayı hesaplama ve tazminat modelleme, kurumsal olgunluk modelleme, mahremiyet etki analizi teknikleri kullanılmıştır.

Bu çalışmada, teknoloji kaynaklı mahremiyet tehditlerinin, yine mahremiyet arttırıcı teknolojiler ile risk yönetimi yaklaşımı ile önlenebileceği gösterilmiştir. Önerilen çerçeve, ulusal çapta mahremiyet koruma için bir başlangıç noktası ve şirketler, kurumlar ve bireyler için detaylı kılavuzlar içermektedir.

Anahtar sözcükler: Kişisel verilerin korunması, mahremiyet risk yönetimi.

CONTENTS

CHAPTER ONE

INTRODUCTION

1.1 Overview

Since the late nineteenth century, privacy has become an important value and right in and of itself, in the sense that society has recognized the necessity of protecting citizens from its invasion. Because of this significance of privacy, many disciplines including law, social-psychology, philosophy, economy and technology has approached the notion of privacy in their own areas (Kim, 2006).

The most productive research on privacy has been done in the field of law beginning with the first publication of "The Right to Privacy" by Warren & Brandeis (1890). The legal approach has dealt with privacy in terms of constitutional law, criminal law and decision making for various courts in United States (US) (McWhirter & Bible, 1992; Glenn, 2003).

Technological changes have been recognized as a threat against individuals' privacy. As a result of this growing threat; researches have focused on technology originated data protection issues (Regan, 1995). These results caused significant changes in Europe and US in the twentieth century.

Sociology has studied privacy from individuals' perspective. Westin's (1967) approach in "Privacy and Freedom" examines the four basic states (solitude, intimacy, anonymity, and reserve) and four functions (personal autonomy, emotional release, self-evaluation, and limited and protected communication) of privacy.

Margulis (2003) summarized four areas of privacy as the government role as a threat to and defender of privacy, consumer privacy, medical and genetic privacy, and workplace privacy.

In most cases, the psychological study on privacy usually uses the concept of boundary control through which people restrict and seek interaction to achieve a desired degree of access to the self or one's group by others at a particular time and in a given set of circumstances (Pedersen, 1997; Pedersen, 1999). As a result of researches in social science; privacy has been recognized as one of the important human rights all over the world.

From an economic perspective personal information has become a very important resource in economic activities for companies seeking target audiences. (Posner, 1984) Competition between companies force them to innovate new ways for customer loyalty and to develop new channels for reaching new customers. There are certain developments in marketing including mass marketing, Internet marketing, electronic marketing and mobile marketing that use personalized platforms for targets. Economic perspective forms the technological perspective. As a result, this causes aggressive data collection and data mining technologies to emerge. Beyond this, economic researches on privacy focus on legislations and policies of governments which regulate and set the rules of using personal data. Each nation and each sector have different approaches toward the regulation of data protection and data security. Strong regulation of privacy solely affects business and trade negatively. On the other hand weak regulation will not satisfy the individuals or citizens of a nation. The goal of privacy policy or regulation is by and large to balance the interests of the market and the protection of consumers (Bennett & Grant, 1999). It is seen that enhanced technological innovations encompassing listening, watching, and data collection functions raise concerns about privacy.

1.2 The Objective of This Study

Many dissertations have been prepared with inter-disciplines of science on privacy, data protection and security. Security domain is investigated broadly and deeply where many researchers have studied on protection technologies for confidentiality, integrity, availability, reliability, quality of data. Unfortunately these studies are mostly in Europe and U.S. During the literature review most of the researches made about privacy and data protection in Turkey are taken into consideration. The researches where limited numbers exist cover technological framework, public administration and legal aspects of privacy. Details of current situation in Turkey will be examined in the following sections. This field includes big academic and research potentials. Personal Data Protection realm is an open area for any discussion from technological, engineering, sociological, psychological and even though philosophical perspectives.

There has been very little attention paid to privacy issues in Turkey with respect to perspective of risk management covering national strategy, enterprise activities and individual's conformity. This study consists of technical, practical and legislative views of data protection. This study will help to better understand the reasons why a national wide personal data protection policy and technology strategy in Turkey is a requirement. The finding of this study is a framework of privacy based risk management for personal data protection in our country.

1.3 The Procedure of This Study

As suggested by the title "Personal Data Protection in Turkey", data protection concerns, current situation of data protection technologies in Turkey and its position as a developing country in the information age are investigated in this study. The analysis of privacy in terms of country wide, corporation wide and individual centric characteristics helps us to understand the technology used and being developed behind changing aspects of security concerns.

On the basis of the comparison on data protection in different nations and circumstances, security tensions and models for Turkey are examined.

This study has six main chapters; the introduction constructs the reason why data protection technologies and the need for such a research in Turkey are examined. Describing the boundaries of gap between the individual's data protection rights and the governmental practices give an opportunity to study in this area. This thesis may not be able to find final key solutions to close the gaps but it is sure that it will give a picture of the necessities for future studies.

The second chapter is the literature review of data protection and key definition of privacy beginning from the value, definition, characteristics of privacy. The second part of the chapter discusses the development of technology and its effects on individual privacy, including privacy tensions in information age

In chapter three, current data protection, security, internet technology related regulations in several countries including Turkey are discussed. In particular, the draft Act on Personal Data Protection will be the main focus of the analysis. Even though this is an engineering research, in order to choose the right technology solutions which are compliant with the regulations; data protection legislation field is also studied. The knowledge of Turkey’s national strategies and current regulations are used to find conflicts between theory and practices. This chapter also includes results of a survey conducted in health sector.

Benchmark is one of the best methods of assessing the current level of security and data protection state in Turkey. The circumstances that triggered data protection legislation in Europe and United States of America are studied in chapter three. The goal of exploring the concept of data protection and privacy in these nations is to show that meaning of privacy changes between societies. Each major international and national regulation which includes privacy rules is discussed in detail in the mentioned chapter. The initial indications of a data protection authority and regulation requirements are given. Diverse meanings of privacy should be analyzed for Turkish citizens and culture. The purpose of this analysis is to discover a model to achieve the security, privacy and protection needs of society.

Chapter four covers the requirement, motivation and dynamics of privacy. Several privacy technologies including Platform for Privacy Preferences and Privacy Enhancing Technologies (PET) are introduced in this chapter. Challenges and motivations for investment are discussed from an organizational point of view.

In chapter five, a risk management model based on assessing data protection realm for Turkey is introduced. The model will be based on current legislations, sector practices and individual's privacy rights. Requirements engineering methodology is used to build to this section. This multi domain privacy risk management model is described for each sector dynamics.

Also the model is applied for each sector such as finance, telecommunications, and health and inspect on applications where personal data is collected, stored and transmitted within or out of borders of this area. In this section, advent and development of communications technologies and their use in governmental bodies and corporations have been discovered where different aspects of security that these technologies have brought by their characteristics are also examined.

The conclusion chapter covers the findings that previous chapters produced about data protection technologies and concerns in Turkey where new communications technologies have played a pivotal role.

With respect to diverse personal data sharing applications, this comparative research will help better understand nationwide security model, its implementation and establishment. It will give recommendations on how these privacy and security concerns are changing in the context of physical privacy, information security, enterprise risk management, the disclosure of personal information in the public sphere, and the use of personal information without consent. Ultimately, this study will point out silent tensions of data protection in Turkey in the information age. The suggested model is open to discussion, test, simulation and development for other sectors, applications and services.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

In this chapter, simple meaning of *personal information* and *privacy* under the scope of human rights and relationship between public and government also with the complex meaning of privacy under the pressure of technological changes are described. The motivations of data protection for nations, public and organizations are reviewed by using the dynamics of privacy in literature. Re-evaluation of effectiveness, success and failure of internationally accepted regulations, methodologies and technologies for protection of personal data are made together with the similarities and dissimilarities of these methodologies between developed countries.

2.2 Personally Identifiable Information

2.2.1 Definition

Personally Identifiable Information (PII) is any data about an individual that is identifiable to the specific individual (Murphy, 1996). Such information includes, but is not limited to, an individual's name, address, telephone number, social security/insurance or other government identification numbers, employer, credit card numbers, personal or family financial information, personal or family medical information, physical characteristics, employment history, purchase or other transactions history, credit records and similar information (Karol, 2001). Personal data can be defined as all of the information that can express any opinion about an individual or corporate. The information collected by an organization about an individual is likely to be considered as personal information if it can be linked to an identified individual. Some personal information is considered sensitive. Some regulations define the following to be sensitive personal information; information on medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual preferences (AICPA & CICA, 2003). Sensitive personal information generally requires an extra level of protection and a higher duty of care.

Simplifying the relationship of information to the individual, personal information is the information around a person. Personal information means information space attached to an individual. According to Kang (1998), the relationship of information and an individual can be recognized in three ways.

1) An authorship relation to the individual: Information belongs to an individual who has purposefully created or prepared it (i.e. telephone conversation, personal diary, love letter, call center record or e-mail).
2) A descriptive relation to the individual: Information can designate a specific individual by depicting biological and social status or states of the individual (i.e. sex, birth date, or membership in political organizations).
3) An instrumental mapping relation to the individual: Information instrumentally pointing out specific individuals. The Social Security Number or National Identity Number does not describe the individual's state-of-being or actions, nor is it created by the individual. It is merely mapped to the individual by the government for record keeping purposes. Any personal information may include multiple of the three ways.

2.2.2 Value of Personal Information

2.2.2.1 Strategic Value

Several countries around the world are attempting to revitalize their public administration and make it more proactive, efficient, transparent and especially more service oriented. To accomplish this transformation, governments are introducing innovations in their organizational structure, practices, capacities, and in the ways they mobilize, deploy and utilize the human capital and information, technological and financial resources for service delivery to citizens. E-government can contribute significantly to the process of transformation of the government towards a leaner, more cost-effective government (United Nations, 2008). Turkey is ranked as 76th nation according to the E-Government Readiness Index 2008 and is getting ready for e-government services with the e-Transformation Turkey Project of the State Planning Organization (2006). The project considers personal data protection in strategy document as; "the privacy of personal information will be respected in the delivery of e-government services, and authorization limits for access to personal information will be defined".

2.2.2.2 Economic Value

The largest portion of the modern economy is made up of information-related activities driven by information technology industries (Choi & Whinston, 2003). Frichman & Cronin (2003) provide a definition of Information Rich Commerce and highlight several key factors influencing further developments in the e-commerce industry. "Information Rich Commerce" is a process where detailed consumer data, such as preferences, historical records, and different personal information, are used to customize the content offered to the customer including commercials, marketing offers, and new products etc.. This is done in order to add extra value to consumers and service providers (Nozin, 2005). These new techniques are used widely by merchants. Some researchers believe that new security risks grow from these new processes on the other side some researches insist on benefits of Information Rich Commerce will significantly outweigh the potential risks.

In the information age, information has a real economic value for any final product or service. The idea of valuable information, companies are investing in research and development, innovation and creative programs for processing data. These investments and activities add extra value to personal data as an economic aspect. For innocent purposes, companies use personal data to segment their existing customers. The segmentation for example may be in terms of age, gender, financial income, territory they live, and purchase trend. These innocent researches are used to control and guess future activities of customers. Therefore knowledge behind data processing is necessary for increasing sales and revenues. The abilities to collect, access, store, transmit, format, index and process data are powerful tools for companies. Any company with better capability of information processing techniques can manage its existing customers better than others. This advantage is enough to step forward and faster than its competitors to gaining new markets and potential customers.

The advances in information technology made it possible to collect and process personal information in every stage of service and sales. Pattern recognition of customer behavior and profiling can be decided very quickly and easily with the new technologies. Value of information can be measured by comparing the value of information with the media where it is stored. Success of rapid development of technology reduced the price of storage devices and now it is known by everyone that the value of information is greater than the value of physical media it is hosted. Nowadays it is not enough for any company or government agent to have data. They pay high amounts of money to transfer it into understandable data called information. Data mining, data warehousing, knowledge management and information management are some disciplines and programs that agents are investing. The term “information economy” properly reflects this natural trend and tendency of economic characteristics.

2.2.2.3 Personal Value

For economic efficiency, effectiveness and security, big companies and government agencies may exchange or reuse PII for purposes different from the original one in collecting it. Individuals are becoming more aware of the value of their own information. Privacy concerns will continue to rise more than before and it requires more attention than before.

2.3 Definition of Privacy

Privacy refers to something private or personal that an individual does not want to share with unfamiliar others. The difficulty of defining privacy lies with the impossibility of identifying the adjective terms of "private" or "personal" because those are differently defined according to an individual and a society. In other words, individual and social differences bring a very diverse conceptualization of the private or personal. At an individual level, some people care more for their private or personal life than others. In a similar way, at the societal level, some societies or their cultures value the concept of the private or personal, while other societies or their cultures value the public (Spiro, 1971).

In order to better understand the pure meaning and aspects of privacy, philosophical analysis of privacy concept is studied. This definition sets the bridge between privacy and individuals (consumer, customer, nation, etc.) as a human right. This background will help us to better design a consisting framework and choose security technologies for protection of privacy.

In the history, privacy was firstly used by Aristotle's definitions of political distinction between public and private realms. He described the sphere of political activities in villages and private sphere of households. Another track of privacy was seen in a book by Cooley (1880) where he mentioned privacy as "the right to be let alone".

Western culture has valued the right to privacy, whereas in the rest of the world where the concept of individualism has been underdeveloped, the right to privacy is also under-evaluated (McDougall & Hansson, 2002). It is very hard to find one definition for privacy covering the whole consensus of all people and cultures. It is frequently used in daily life of ordinary people in terms of different meanings. This concept was used by Warren & Brandeis (1890) to define needs for privacy after inventions of newspaper and photography. They described the difference between compensation of possible physical injuries and compensation of personal injury. In the following sections the mentioned personal injury term will be used as a fundamental concept and as a link to disclosure of personal information.

Privacy International is a human rights group formed in 1990 as a watchdog on surveillance and privacy invasions by governments and corporations, describes privacy in the context of personal data as (EPIC & PI, 2006);

1. Information privacy, which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as “data protection”;
2. Bodily privacy, which concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches;
3. Privacy of communications, which covers the security and privacy of mail, telephones, e-mail and other forms of communication; and
4. Territorial privacy, which concerns the setting of limits on intrusion into domestic and other environments such as the workplace or public space.

Longman Dictionary describes privacy as:

1. “The (desirable) state of being away from other people, so they can not see or hear what one is doing and”
2. “Avoidance of being noticed or talked about publicly. With this definition privacy is something with personality.”

2.3.1 Frameworks for Understanding Characteristics of Privacy

In order to understand the meaning of privacy for people the model described by Kim (2006) will be used. Privacy includes personal objects containing body, heart, and mind. Thus, privacy relevant to personal traits has a salient relationship with bodily, sentimental, and mindful dimensions.

Table 2.1 shows dialectics and dichotomies on the diverse features of privacy in terms of various aspects and criteria so that complicated concepts and meanings of privacy can be recognized lucidly (Kim, 2006). Dialectics is the assumption that in social life, people experience tensions between opposites and contradictions (Petronio, 2002). Dichotomy is the unity of dialectics including connection-autonomy, openness-closeness, and disclosure-privacy (Baxter & Montgomery, 1996).

Table 2.1 Dialectics of privacy.

Aspects of Privacy	**Criteria**	**Dichotomy**	
		Privacy	**Publicity**
Body *(Physical Privacy)*	Space (Territory)	Private Solitude (Closeness)	Public Society (Openness)
Heart *(Emotional Privacy)*	Individual Level	Concealment	Revelation
	Information Relationship	Secrecy	Disclosure
	Formal Relationship	Confidentiality	Exposure
Mind *(Spiritual Privacy)*	Identity (Life Style)	Autonomy (Independence)	Heteronomy (Dependence)

With respect to space or territory, *physical privacy* implies a private sphere that prevents others from invasion on someone’s territory. Private-public dichotomy of physical aspect of privacy indicates the sharing of a space or not sharing it. Physical aspect of a person is literally the basic and fundamental requirement for being let alone so that one’s physical being is not intruded upon by unfamiliar others. Physical privacy provides individuals with the safe and peaceful place or space to rest themselves in protection from outside threat or invasion. Boundaries of physical privacy have different meanings in different nations and cultures.

Emotional privacy can be examined in individual, informal and formal levels. Privacy dichotomy means concealment, secrecy, or confidentiality in the expression of personal affairs. On the contrary, revelation, disclosure, or exposure of individual life means sacrificing one’s privacy to share it with foreigners. The informal intimacy between lovers, peers, and family members can be continued in secrecy; otherwise, it can be broken in disclosure. Official relationships such as patients-doctors, clients-lawyers, customers-banks require confidentiality in the norms of society.

The emotional aspect means not to be embarrassed or uncomfortable in one's personal life. People in most cases do not want to reveal to unfamiliar others their own information, habits, loves, likes, tastes, and so on. Emotional privacy helps people develop closer relationships with friend and family member by sharing personal information sometimes secrets.

According to Benn (1984) the spiritual aspect emphasizes the self-determination and self-definition on matters of private and family affairs. Spiritual privacy allows individuals to reflect many thoughts and prepare some opinions before presenting them to the public. Without this kind of spiritual autonomy and independence, individuals cannot make their own judgments, decisions, and choices about their personal actions just as children are always dependent on their parents. No matter what the circumstances are, every person should have the right to decide the secrecy and confidentiality level of his own data. Individuals must be free from interferences or influences on their own decision-making process. This autonomy of judgment is called *spiritual privacy*.

As the importance of personal information has increased in the information society, privacy as a basic human right has moved concerns to the protection of invisible personal information from visible personal territory (Kim, 2006). Privacy is no longer only defined by physical, emotional and spiritual publize, but has become about personal information about any aspects of privacy.

When personal data protection of individuals is examined it is seen that any data about a person can be in any category of the Table 2.1. Since any information can be converted to electronic data, privacy of information cannot be assured easily. Disclosure of any information will have different effects on individuals in terms of physical, emotional and spiritual aspects. These definitions are simple but they are not enough to describe the practical reflections of privacy in daily life with the effect technology in the Internet Age.

The PII is used to link any data with an identified individual. The quality and sensitivity of the link is not in the focus area thus some scholars study on database privacy from this perspective. Fischer-Hübner (2001) describes the probability and risk of using anonymous data to identify an individual as “there is always a risk of re-identification depending on the entropy of the depersonalized dataset and additional data about the data subject. Developing reliable criteria to estimate this risk is a non-trivial task”.

In consequence of this it is assumed that *information* and *data* mentioned in this study are directly about an identifiable person. Moreover, social perspectives and aspects of privacy are examined to set a strong baseline of privacy notion. Thus, the concept of privacy is not absolute, but rather changing in times and regions. In addition to this concept, technology makes it almost impossible to define the dynamics and borders of privacy. In this study, privacy is defined in various perspectives. In the following chapters *privacy* will be used in the context for *personal information* and the definition made here about the privacy realm of an individual will be used.

2.3.2 Balancing Availability and Privacy

Privacy concerns for an individual begin at the information flow out of the borders of a person’s control. The increasing sophistication of information technology with its capacity to threat the borders of personal information around individuals has introduced a sense of urgency in the demand for privacy and data protection. On the other hand, information about individuals has an economic value because it is transmitted as a kind of commodity in modern society (Davies, 1997). This is a challenge between privacy and availability as well as between human rights and economics.

Companies can not sacrifice making profit; they have to continue earning money. On the other hand governments can not give up holding citizen information because of national security strategies and public responsibilities. How has this dilemma been managed since now? The dominant trend in privacy protection is to provide citizens or customers with reasonable control over their personal information without the intervention of others, including government in the public area and companies in the private.

2.3.3 Threat Agents

The exploration of information and the importance of personal information have continuously increased the threat and invasion to privacy in the behaviour of both commercial and government agents (Rothfeder, 1992).

The corporate sectors become the main agents for privacy violations due to the increasing reuse or abuse of personal information for profit making in the marketplace. These concerns reflect that the main privacy concerns have moved to the abuse of personal information in the economic realm, from the disclosure of personal life in the social realm where mass media played the first role and technology plays the leading role at the moment (Kim, 2006).

Collecting customer data and updating the existing data is an ordinary and a must operation for corporate agents. As the competition increases, company agents in these sectors become more aggressive and customer information becomes more valuable. Answers to the questions below are investigated:

1. What is the value of privacy in the Information Age?
2. Who is the threat?
3. Who are the safeguards?
4. What is the role of government bodies and agents in privacy and security realm?
5. Can we solve security and privacy problems at one instant;
6. Is there a repeatable systematic solution or framework?

2.4 Communication Technologies and Privacy

2.4.1 History of Communication Technologies

When the historical developments of communication technologies are investigated the reason why Internet hosts most variety of risks and opportunities are seen. The relationship between communication structures and privacy concerns are given in Table 2.2 (Kim, 2006).

Table 2.2 Privacy concerns and communication channels.

Era	**Before Mass Media**	**Mass Media**	**Internet**
Communication Mode	Private Communication	Public or Mass Communication	Internet Communication
Production and Consumption	One-to-one	One-to-many	Many-to-many
Format	Letter, Telephone, Videophone Formats	Printing Press, Radio, Television	Internet, Digital Media
Agents of Privacy Concerns	Government	Mass Media	Corporations, Individuals, Government
Dimensions of Privacy Concerns	Political	Social	Economic

Before the mass media era, the main concern of privacy focused on the government that has the power to invade and occupy the private territory. At that time, privacy meant the protection from censorship and invasion by the administration of government.

The advent of newspapers converted the concerns of privacy at the end of nineteenth century. Thus, mass media represented by the printing press, radio, and television became the principal invader of privacy, replacing the government.

In the era of the Internet, the private sectors including companies and individuals become the main violators of information privacy, replacing the public sectors including government and mass media.

2.4.2 The Internet

The Internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location (Leiner et al., 2000). First researches on packet switching and time shared environments were the early stages of the Internet and nothing has revolutionized the computer and communications world like Internet before.

The Internet combines various modes of communication (personal, group, and mass communication) and different forms of content (text, visual images, audio, and video) into a single medium (Dimaggio, Hargittai, Neuman & Robinson, 2001). Internet is an interactive medium. Interactivity means that users have the ability to influence the flow of information or to modify its content. The integrating capability of Internet became very powerful and it penetrated into other media.

Internet with its uncontrolled boundaries becomes a decentralized repository for the process of information storage, share, distribute and produce. With this universal use it provides individuals with many benefits and advantages to make our living conditions more convenient than ever before. The Internet, as the network of networks, has been a backbone of today's communication infrastructure. It is a fast and efficient tool for searching, collecting, and transmitting information. Telephones, Personal Digital Assistances, televisions and other hardware nowadays have Internet capabilities.

As the Internet becomes more ubiquitous concerns rise about the individual's right to privacy. The conflict of willingness of using Internet and threats it hosts, reflect the need for a balance between privacy and availability of communication technologies.

2.4.3 Commercialization of the Internet

In the Information age, societies produce and distribute information in a large scale, just as it was with material goods in the industrial society (Schement & Lievrouw, 1987). Commercialization of the Internet involved not only the development of competitive, private network services, but also the development of commercial products implementing the Internet technology. World Wide Web technology allows users easy access to information linked throughout the globe. Products becomes available to facilitate the provisioning of that information and many of the latest developments in technology have been aimed at providing increasingly sophisticated information services on top of the basic Internet data communications (Leiner, et al., 2000). The Internet enables electronic trade and specific business models like business-to-business, business-to-consumer, business-to-employee, and business-to-government appeared.

Communication technologies support mobile life by enabling accessing information nearly from everywhere and any time. By the mobile technologies, teenagers can play online video games, listen music, employees access documents in their offices and can work, brokers can execute stock transactions, doctors can make operations, and managers can sign financial transactions while mobile. People can share any format of data (text, video, music, etc.) on line, peer-to-peer and anytime. Free communication principle of Internet makes it almost impossible to protect data as a consequence invasion of privacy is easier with mobile information technology.

2.4.4 Information Systems

An information system is a collection of people, processes, hardware, software and data. They all work together to provide information essentials to run an organization. The data flowing within or outside the borders of organization's processes is called as "information". After being processed this information, for example, is used by profit-orient-enterprises to keep records of events and by executive management in decision making processes. Internet, communication links, and databases connect us with information resources as well as information systems far beyond the surface of our desk. Any personal computer offers its users access to a greater quantity of information with higher speeds than was possible a few years ago. The rapid and significant increase in the utilization of computers enabled to store and process data easier.

On the other side it increased the threat and invasion to privacy. Businesses around the world encounter a serious dilemma: the use of computer and information systems has created an enormous potential for communication and service delivery; these systems, on the other hand, are an invitation to the computer hackers and the criminals (Wong, 1994).

Information flows through on organization on different types of systems including transaction processing systems, management information systems, decision support systems and executive support systems (O'Leary & O'Leary, 2002). Each level has different information requirements but a common requirement is the security in terms of confidentiality, integrity, and availability at any processing level. The other common feature of these levels is that data can be created, distributed, used, accessed, transferred, updated, stored, processed, archived and destroyed at the end of the retention period. This is called as the management of information life-cycle. Computers pose a potential danger to the privacy of an individual through all steps of life cycle. This is because computers have the ability to store a vast amount of data, the facilities to process and transfer these data at high speed, and the further capability to correlate these data with other data held.

In the past, privacy was not considered as a major issue since there were readily available means of restricting both electronic and physical access. Besides, the cost of misdirecting personal information was usually minimal and any lost customer data was replaced with backups. But now broadband technology enabled masses to be online and face up with privacy problems as well.

2.4.5 Privacy Tensions in the Internet Age

The importance of information privacy depends on the two driving forces: the new technological factor and the increasing value of information (Jeff, 1994). As technology has advanced, the way in which privacy is protected and violated has changed with it. In the case of some technologies, such as the Internet, the increased ability to share information can lead to new ways in which privacy can be breached. Generally the increased ability to gather and send information has had negative implications for retaining privacy. As large scale information systems become more common, there is so much information stored in many databases worldwide that an individual has no way of knowing of or controlling all of the information about themselves that others may have access to. Such information could potentially be sold to others for profit and/or be used for purposes not known to the individual of which the information is about (Wikipedia, 2008a). On the other hand, technology is also used to protect privacy. Monitoring, detective, corrective and surveillance systems are used for protection of public. It may be expected that fraudsters and hackers will always be one step ahead and technologies such as Internet will be used more for misuse of personal information than as a tool to protect personal data.

2.4.6 Increasing Risk Appetite of Technology

2.4.6.1 Data Collection

In the information society, it is easier to collect personal data of consumers while they purchase goods and services from restaurants, banks, shopping centres, schools, hospitals, etc. in their daily lives. People unavoidably expose their personal information by filling in paper and electronic forms, even without the recognition of giving such information. The data are processed automatically and filed into databases within second by computer power.

2.4.6.2 Controlling the Movement of Personal Information

Controlling the movement of personal information out of the control barriers of a person is crucial to the meaning of privacy. Control barrier filters and manages the flow of data and threat of privacy. Stealing a credit card number from computer system is an outward threat. While a disturbing incoming phone call from insurance company is an inward threat. The direction of threat is not the direction of data flow but represents the direction of privacy boundaries.

2.4.6.3 Physical Access versus Logical Access

Physical paper documents now can be scanned and copied to electronic media, making it possible to be transmitted easier. Life cycle of data has also changed. Production, formation, usage, storing, and destroying of data can all be done electronically. There is no need to physically be present with the data; it is enough to logically access the data from anywhere on earth. With the communication technologies fraudsters and hackers do not need a physical contact to lose privacy any more. Unlimited access to content makes the physical closeness useless. Networked information technologies make the current privacy problem different from the traditional one. Computers are connected to each other with Internet, extranets and intranets. Any information on one computer is accessible from others intentionally or unintentionally.

Data are transmitted across the Internet via “packets”, which are separate pieces of datum in a particular layer of Internet Protocol layers. Transferring data on Internet travels through several distributes layers, servers, routers, switches, computers and backbones. Once information is posted on the Internet, no matter how carefully guarded, it exists somewhere else, where virtually anyone can gain access to it (Lane, 1997). Physical access to data is no longer required; logical access is enough.

2.4.6.4 Logical Correlation of Information

Because of comparatively inexpensive and widely available resources personal information can be subject to risk when it is combined with other data (Cate, 2000). This information can be used to create new meaningful information. In this case, technology is used widely to index data with other data and it makes it possible to gather more data that can not be accessed before. Information in a database A is available in a simple form of its rows. Another database, B which has data relation directly with database A, can be combined together. When two rows of databases A and B are combined it may give an opportunity to create new information. As a web based e-mail account from Mypost.com can be given as an example. Mypost.com wants to advertise products when the user logs in. It also wants to advertise related products according to user's shopping pattern but it does not have much personal information about the user since he did not fill in the forms (database A) while creating his account. It would be a fantastic opportunity if Mypost.com could know his age and gender. Finding them directly may not be possible therefore it looks for other data (database B). The web pages which the user visits may give information about database B. Therefore Mypost.com will not hesitate to make collaboration with other companies to collect more data about his habits and find his age and gender. At this point possible innocent activities become salient.

2.4.6.5 Aspects of Privacy

Obviously several countermeasures to protect personal information are defined before. Threats were discussed and controls have been deployed before. Protection of secrecy and privacy in the Internet age is a serious problem. The changing features of privacy in terms of the advent of typical communications technologies are given in Table 2.3 in regards to the content of privacy, the zone of privacy, the agents and types of privacy violations, and the protection of privacy (Kim, 2006).

Table 2.3 Aspects of privacy in terms of communication technologies.

Era	**Before Mass Media**	**Mass Media**	**Internet**
Content of Privacy	Personal Territory	Personal Affairs	Personal Information
Zone of Privacy	Personal Space	Personal Life	Information Space
Types of Privacy Violations	Invasion	Disclosure	Abuse
Protection of Privacy	Safeguard of Personal Belongings	Freedom from Public Sphere	Control over Information Space

2.4.6.6 Personal Data in Mobile Environment

Mobile devices are widely used in today's business and private life. Thus number of mobile terminals has exceeded number of personal computers worldwide. People store personal data in hand-held devices and communicate privately through wireless networks and mobile broadband. Wireless handheld scanners are being used for real-time biometric identification by private sector and government (Whitaker, 2007). The amount of biometric and personal information stored on identification cards is increasing to include iris scans, fingerprints, health information, and information of dependents. It became easier to transfer personal data across frontiers between countries which have completely different levels of conception, approach and praxis on personal data. The increasing flow of personal information across national borders raised requirements concerns in international approaches to data protection and privacy.

2.5 Corporate Risk Management

Risk management in the widest sense is not a new topic for businesses. All corporations take risk and invest in their own industry but on the other hand operational and detailed risk analysis methods are not used as a tool to mitigate business and technology risk in every industry. This issue has captured considerable attention from corporate management in recent years, as financial risk management has become a critical corporate activity "risk management including technology risks" followed it (Basel Committee on Banking Supervision, 2004). Basel standards which are the international recommendations on banking laws have begun to force financial institutions for managing credit, operational and market risks. Regulators such as Securities and Exchange Commission (SEC) and Sarbanes-Oxley Act in the US have begun to insist on transparent disclosure of the exposure companies financial risks. In addition to these, Turkish Banking Regulatory Authority sets regulations for internal audit and risk management. Behind these fundamental regulations, the economic crisis which affects every country nowadays shows that commerce and trade systems all over the world are far away from being secure. Risk management practices failed during this crisis and none of the companies assessed the financial risk correctly. Thus personal data risks are not being assessed correctly either.

2.5.1 Risk Management Life Cycle

In literature, privacy risks fall in the area of operational risk and legal risks. Operational risk is defined as “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events” by Basel. National Institute of Standard and Technology defines risk management as the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. The risk must be systematically and continuously assessed (Stoneburner, Goguen, & Feringa, 2002).

There are several risk management approaches. Regardless of the main purpose (financial, operational, credit or information security etc.) of risk analysis; the elements and step of the management are alike. According to Crouhy & et al. (2006), risk management has eight elements; these eight elements will be modified for personal privacy.

1. The first element is developing a *risk management policy.* In our scope the policy includes the meaning of personal data for the corporation and covers the baselines of protection.

2. The second step is to establish a *common language* of risk identification which will be used in the company to assess and define risks, threats and vulnerabilities all over the business and IT processes.
3. The following element can be developed parallel with the policy and it includes *process maps* where personal data is used directly or indirectly.
4. The fourth element is to develop *comprehensive set of metrics*. These metrics are used to measure the impact on business, sensitivity of the personal data and probability of an event.
5. The fifth element is the company's risk management *approach* which defines the risk appetite and mitigation actions and cost-benefit plans.
6. The sixth element is the *reporting* mechanism for events and top risks to the management level. Periodic reporting ensures that management is aware of the current level of risks.
7. The seventh element is *monitoring and measuring* the events for making analysis and calculations. This is widely used for quantitative risk analysis.
8. The eighth element is monitoring *compliance* with the current legislations.

The Information Security Management Systems (ISMS) deals with a closed circular circle and aims to improve the systems (ISO, 2005a).

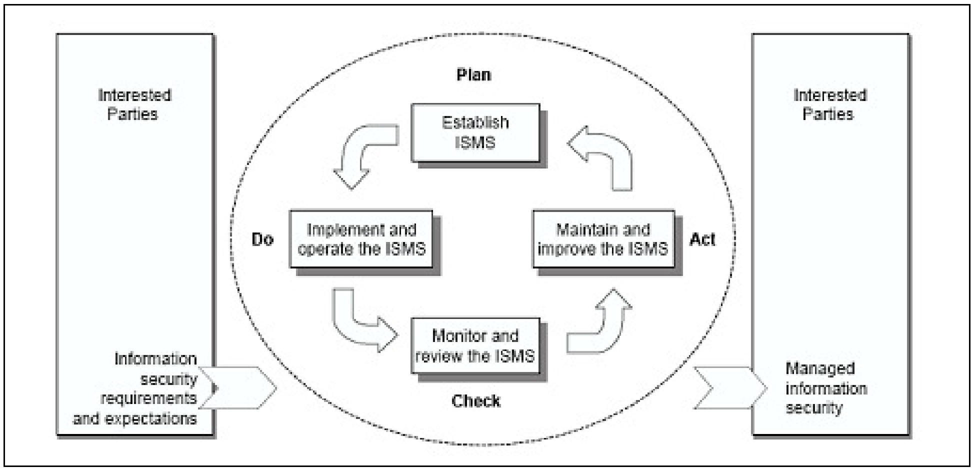

Interested Parties
Plan
Establish ISMS
Interested Parties
Do
Implement and operate the ISMS
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check
Information security requirements and expectations
Managed information security

Figure 2.1 Plan-do-check-act life cycle.

The plan-do-check-act life cycle (Figure 2.1) includes:

1. Plan: Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
2. Do: Implement and operate the ISMS policy, controls, processes and procedures.
3. Check: Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
4. Act: Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

2.5.2 Risk Assessment Types

There are two types of risk analysis methods; qualitative and quantitative methods. Qualitative risk analysis method, risks are evaluated in terms of subjective approaches. Generally data owners or managers assess the value and probability of risk. Quantitative risk analysis uses analytical and mathematical calculations rather than adjectives. Quantitative method are not easy to use and mostly it not possible to set an economical value for an asset and incident. On the other side, two methods are used together where applicable.

2.5.3 Risk Calculation

Annual Loss Expectancy *(ALE)* is common monetary measurement for risk assessment (Tsiakis & Stephanides, 2005):

$$ALE = (Rate\ of\ Loss) \times (\ Value\ of\ Loss\ ) \qquad (1)$$

$$ALE = (impact\_of\_event) \times (frequency\_of\_event) \qquad (2)$$

While the frequency represents the possibility of the event to take place within a year, impact of event and value of loss represent the monetary effect of the harmful incident. More quantitative values scan be calculated as well (Schechter, 2004):

$$Savings = (ALE_{baseline} - ALE_{with\_new\_safeguards}) \tag{3}$$

$$Benefit = S + profit_{new\_ventures} \tag{4}$$

$$ROI = Benefits / investment\_on\_controls \tag{5}$$

In practice it is not easy to find companies which calculate their security expenditures and the benefits but Return on Investment (ROI) can serve as a useful tool for comparing security solutions based on relative value (Wawrzyniak, 2006).

2.6 Privacy Impact Assessment

Privacy Impact Assessments (PIAs) are methodologies to help determine whether technologies, information systems and processes of a project meet privacy regulation requirements. It measures technical compliance with privacy legislation and defines the gaps between the practices and requirements. PIAs are used to identify privacy vulnerabilities and risks of new or redesigned programs, products or services. As an example; Canadian and UK governments use PIA as a tool to assess government projects against privacy risks. PIAs take a close look at how government departments protect personal information as it is collected, stored, used, disclosed and ultimately destroyed. These assessments help create a privacy-sensitive culture in government departments such as Officer of the Privacy Commissioner of Canada (2007). All federal departments, agencies and institutions conduct PIAs for new or redesigned programs and services that raise privacy issues. The governmental institutions which must implement PIA as a tool in new system designs are listed in the nations privacy act in detail.

2.6.1 Fundamental Principles of PIA

In order to have a standard privacy baseline for PIAs the ten fundamental principles mentioned in previous sections are used. Organizations must consider these principles and should assure that computer systems which collect, use, store and transfer personally identifiable information are assessed accordingly. Government organizations must perform a PIA in order to assess privacy risks in new programs, acquisition of new software programs and integration of distributed systems in different government agencies. Major changes to existing programs, changes in technology architecture, additional systems linkages, new channel release for a governmental service, database design change, a new plan to collect citizens' personal data and outsourced operations are some examples where PIAs must be initiated.

Usually two kinds of PIAs are used; preliminary PIA and full-cycle PIA. Preliminary PIA is used at the initial phase of a project to determine whether a full-cycle PIA is needed. If personal data is not used or processed or transferred in the corresponding system preliminary assessment may find there are no or minimal privacy risks. This approach saves resources and time for the project.

Another way to save resources is using self-assessment where individual government departments conduct their own PIAs. Therefore each governmental agency must have educated professionals from various departments (Information Technology, legal, business analysis, project management etc.) of the organization.

CHAPTER THREE

BACKGROUND OF DATA PROTECTION REGULATIONS AND NATIONAL APPLICATIONS

3.1 International Instruments for Data Protection

The genesis of modern legislation in this area can be traced to the first data protection law in the world enacted in the Land of Hesse in Germany in 1970. This was followed by national laws in Sweden (1973), the United States (1974), Germany (1977), and France (1978). The increasing use of automated processing of personal data over the past few decades has improved the risk of misuse of private information about individuals.

Privacy is protected in the Universal Declaration of Human Rights (United Nations, 1948) and the International Covenant on Civil and Political Rights (United Nations, 1966) as a fundamental right. In 1981, Council of Europe (CoE) and Organization for Economic Cooperation and Development (OECD) wanted to guide the member states by setting a set of rules to solve this rising problem. While European Convention on Human Rights guarantees the right to privacy, it also states the right to information (Council of Europe, 1959). Therefore regulating the protection of personal data processing might secure private data but on the other side might slow down the free movement of information and services which could have economic results. In order to solve this potentially conflicting situation CoE elaborated the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)" and other analogous directives. OECD has prepared a set of rules called Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data (OECD, 1981).

Both regulations are balancing acts between transferring of information and fair collection and use of personal data. Convention 108 defines the principles as; data can only be collected for a specific purpose, should not be used for any other reason, must be accurate and adequate for this purpose, and stored only for as long as it is necessary. Convention 108 also establishes the right of access to and rectification of data for the person concerned; *data subject*. CoE's Convention is a reference for today's data protection legislation framework. Following years, European Union (EU) and CoE have supported Convention 108, by enacting several regulations for private and public sectors including telecommunication, technology, financial, marketing, health, and insurance.

International governmental organizations have played active roles in privacy policy formation by guiding countries to adopt or amend data protection legislation with an eye to entering the European Union or the European information technology market. The EU's adequacy requirement has played an important role in the development of international standards (EPIC & PI, 2007). These laws are being adapted by many countries to remedy past injustices, to promote electronic commerce and to ensure laws are consistent with Pan-European laws.

3.1.1 Key Definitions and Terms

Even though definitions can change from country to country, key definitions are usually used as they are defined in the CoE regulations. Some key data protection definitions are given below (UK Data Protection Act, 1998); they will be used for discussing regulations as well as technical control.

Data: Information which recorded and is being processed by means of equipment operating automatically in response to instructions given for that purpose.

Personal Data: Data which relate to a living individual who can be identified from those data

Data Subject: The subject of personal data and solely owner of the personal data.

Database System Controller (data controller): The individual or corporate party which has taken permission from the data subject to process the data in a relevant filling system for pre-defined purposes and by pre-defined methods is the competent authority to specify the processing methods and can outsource the processing to a data processor or database system controller representative agent

Data Processor: In relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller;

Process: Data can be indexed, classified, stored, transferred or made anonymous.

Making data anonymous: Formatting the data so that the output information cannot pin-point the individual (data subject), cannot be associated with the data subject directly or indirectly and the source of raw data cannot be identified.

Authority: Independent regulatory office appointed by the data protection legislation that regulates data protection principles, protects personal information and investigates complaints from people who believe they have been denied rights

RACI: Illustrates who is responsible, accountable, consulted and informed within in a standard organizational framework.

Risk: The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss and/or damage to the assets. It usually is measured by a combination of impact and probability of occurrence.

Programme: A structured grouping of interdependent projects that includes the full scope of business, process, people, technology and organizational activities that are required (both necessary and sufficient) to achieve a clearly specified business outcome.

Project: A structured set of activities concerned with delivering to the enterprise a defined capability (that is necessary but not sufficient to achieve a required business outcome) based on an agreed-upon schedule and budget.

3.1.2 Fair Information Practices

To prevent the abuse of personal information, most policy concerns about the protection of personal information emphasize fair information practices in which personal information should be used in the right way and for the right purpose under the provider’s control. Fair information practices may change forms in various legislations but mostly have the similar key principles. These principles are studied and defined by Electronic Privacy Information Center in US as (Banisar, 2000);

1. Obtained fairly and lawfully;
2. Used only for the original specified purpose;
3. Adequate, relevant and not excessive to purpose;
4. Accurate and up to date;
5. Accessible to the subject;
6. Kept secure;
7. Destroyed after its purpose is completed.

3.1.3 Data Protection Legislations in Developed Countries

Some of the milestone regulations in data protection field are given in Table 3.1. Most of the developed and emerging nations have their own bills issued, enacted or ratified but the directives and laws listed set the background for motivation of regulation in all countries.

Table 3.1 Privacy laws and regulations.

Full Title	Legislation entry into force date	Issuing Organization/Country
Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data	1995	European Union
European Union (EU) Directive on Data Protection (95/46/EC)	1995	European Union
EU Directive on Privacy and Electronic Communications (2002/58/EC)	2002	European Union
Freedom of Information Act (FOIA)	1966	United States of America
Privacy Act of 1974	1974	United States of America
Gramm-Leach-Bliley Financial Services Modernization Act, (GLBA)	1999	United States of America
Health Insurance Portability and Accountability Act (HIPAA)	1996	United States of America
Children's Online Privacy Protection Act (COPPA)	1998	United States of America
International Safe Harbor Privacy Principles	2000	European Union, United States of America
Guidelines on the Protection of Privacy and Transborder Flows of Personal Data	1980	Organisation for Economic Co-operation and Development
Data Protection Act of 1998	1998	United Kingdom
Personal Information Protection and Electronic Documents Act (PIPEDA)	2000	Canada
Universal Declaration of Human Rights	1948	United Nations General Assembly

3.1.3.1 European Union

In 1981, the Council of Europe adopted the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. This convention and OECD’s guideline has a major impact on the development of national legislations around the world. EU and Council of Europe have supported the Directive 108, by enacting several regulations for telecommunication, private and public sectors. The European Parliament passed the Directive on Privacy and Electronic Communications (2002/58/EC) on July 12, in acknowledgement of the threat posed to personal privacy from the development of complex communication systems.

The Directive prohibits flow of information from a member country to a country without adequate level of protection, unless there is proof that due to certain conditions, this country constitutes a so called “safe harbour” for personal information.

Especially the data that falls in the definition “sensitive personal data” is identified to give a direction for the members. The United Kingdom (UK) Data Protection Act (1998) defines the sensitive data as:

1. The racial or ethnic origin of the data subject.
2. His political opinions.
3. His religious beliefs or other beliefs of a similar nature.
4. Whether he is a member of a trade union.
5. His physical or mental health or condition.
6. His sexual life.
7. The commission or alleged commission by him of any offence.
8. The commission or alleged commission by any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Each data protection act includes a statement for establishing a regulatory authority. The mentioned authority is responsible for building an infrastructure to make this act possible by preparing the supporting regulations, registry system and the audit mechanism. Each EU member gives different names for this authority like, regulator, commissioner, supervisor or commissioner. For example EU, UK and

Greece call their central authorities European Data Protection Supervisor, The Information Commissioner, and Data Protection Authority respectively.

3.1.3.2 United States

United States deal with Data Protection Legislation with a priority of economic approach. US prefer to balance the availability and privacy principles in a good equilibrium. Regulation movements did not particularly affect the US, where public awareness of, and concerns about, privacy issues were much less. The US public's attitude favoured the sharing of information, while in Europe restricting its dispersal was favoured in part due to the abuse of personal information experienced during World War II. There were also major commercial benefits from allowing disclosure and use of customer information. These uses were accepted by the US public as far outweighing any concerns about such sharing of information (Axelrod, 2007).

US approach data protection in terms of economic aspects and powers up movement of information through organizations and companies in order to keep alive e-business. On the other hand EU has an idealist approach because of their experiments in the World War II. Therefore an ideal and theoretical framework has been established to keep personal data safe in the borders of union which will be discussed afterwards.

In practice US doesn't have a central Data Protection Legislation. Instead, each sector is regulated with its own data protection acts, rules and procedures. In the US many laws have been established to control and mitigate security risk which has risen due to developments in surveillance technologies Some laws are HIPAA, Gramley Beach, Fair Credit Reporting Act, the Privacy Act, the Family Educational Rights and Privacy Act, the Right to Financial Privacy Act, the Cable TV Privacy Act, the Electronic Communications Privacy Act, the Video Privacy Protection Act, the Driver's Privacy Protection Act, and the Children's Online Privacy Protection Act. Common concepts of these laws are based on regulating the collection, storage, transfer, and use of personal information. These activities are covered by five core privacy principles: Notice, Choice, Access, Security, and Enforcement (Federal Trade Commission, 2000). Brief definition of US privacy laws which government has passed is given below:

1. Health Insurance Portability and Accountability Act (HIPAA): August 1996, allows for health information to be released and used for research based on a patient authorization, an approved waiver of patient, the de-identification of a person's health information as defined by HIPAA, and the de-identification through a limited data set.
2. The Gramm-Leach-Bliley Act Privacy of Consumer Financial Information (GLB): November 1999, is an act which allows commercial and investment banks to consolidate and includes privacy rules to protect the information from foreseeable threats in security and data integrity. Government framework includes components; financial privacy rule, safeguard rule and social engineering rule.
3. Children's Online Privacy Protection Act of 1998 (COPPA): October 1998, protects children when they are surfing the Internet from unnecessary collection of their personal data without parental consent.

It is understood that laws which are taken into force in the US have been prepared for protection of personal data and in more general personal life against corporations and private sector. There is no data protection law in practice that covers all sectors for data secrecy and protection as an umbrella laws. Instead, listed regulations are prepared for different sectors like finance, education, and telecommunication. It is seen that data protection and security issue are constitutional rights in the US. Ultimately, data protection is taken into hand from a practical perspective and as an economic realm in US.

3.1.3.3 Privacy Breaches in US Organizations

The US does not have an act directly for data protection and does not have an authority at present. Privacy Rights Clearinghouse, a nonprofit organization located in California, San Diego, reports the chronology of data losses and identity thefts according in US annually. According to the 2006 reports, 327 events took place where a hundred records have been affected (Rosenberg, 2007). There is no such organization in EU that takes records of incidents. The percentage of data loss and vandalism events reported from the private sector is 40% for notebook theft, 20% personnel errors and software malfunctions. Personnel errors and software malfunctions take the first order in public sector with a 44% ratio and computer theft follows by 21%.

The absence of a data protection act in the US should be taken into account and the relation of existence of such an act and the incidents occurred should be investigated. One of the duties of the regulator bodies should be to investigate this correlation.

“2007 Privacy & Data Protection Survey” conducted by Deloitte & Touche LLP and Ponemon Institute LLC provide compelling evidence that organizations continue to struggle with managing and protecting private data in US. 827 participants have responded in this survey. In the results, it is seen that incidents compromising personally identifiable information are occurring at an alarmingly high rate, with more than 85% of survey respondents reporting some type of reportable privacy breach in 2006 and 63 percent of privacy and security professionals surveyed had multiple reportable privacy breaches – between 6 and 20 breaches – in the same year (Deloitte, 2007).

The participants were asked to indicate the number of records lost or exposed in order to understand what respondent’s organizations are dealing with from a breach size perspective. When asked to report the number of records lost during the single “most significant breach” in the last year the responses naturally “group” into large breaches and small breaches.

Large breaches, involving over 1000 records were reported by (33.9%) of respondents. These ‘large’ breaches were distributed as follows (Deloitte, 2007):

1. Over 25,000 records – 9.9%
2. 5001-25,000 records – 12.8%
3. 1001-5000 records – 11.2%
4. Smaller breaches involving fewer than 1000 records were reported by 22.2% of respondents.

Over 21% stated they were not sure of the record count, 14.8% did not respond and 7.6% indicated that no records (0) were lost.

If a similar survey is prepared in Turkey it would be almost impossible to have response to this survey. Since there is no data protection legislation in Turkey, the organizations would not be able to answer these questions because:

1. They do not know the context and content of such breaches within their organizations.
2. There is no incident management program in their organizations.
3. There is no regulation in practice that forces the organizations to announce such events.
4. Information economy concept has not arisen in Turkey therefore privacy breaches are not investigated as properly.

3.1.4 Awareness

A survey done by the Council of Europe in 2003 shows that 70% of the European population has no information about that is being done in their own countries to protect personal data (European Opinion Research Group, 2003). In consequence of this, the Council of Europe has decided to celebrate the 28th of January as Data Protection Day in order to raise the awareness of individuals (Council of Europe, 2007). This proves that even though the countries have acted data protection legislations, have authorized commissioners for governance and deployed safeguards to protect individuals; that failed in raising awareness in the public. Training and educating the customers, individuals and students is the most critical and long lasting effort in building a sustainable safe environment.

3.2 Diversities between National Regulations

In order to deal with the potential threat of Information and Communication Technologies (ICT) to individual privacy and the ethical issues related to computer use, many Western countries have established data protection legislation to control the collection, storage, use and disclosure of Personally Identifiable Information (PII) by means of computers and telecommunications techniques (Wong, 1994). With the present expansion of ICT in Turkey, several potential problems are anticipated to cause loss of data where this will result with loss of money and confidence. The confidence of general public must be safeguarded. Any incident or fraud will make the public stay away from ICT services and this will cause break in the ICT industry.

On the other side, it can not be assured that the data protection law will be an ultimate solution and therefore conclude personal data privacy discussions. Public concern in the privacy environment in the developed countries is increasing, causing significant social, economic and political changes in related issues and legislation (Culnan, 1993).

For example; at the biggest airport of the UK, Heathrow; fingerprinting (biometrics) technology is used to ensure the passenger boarding the aircraft is the same person, the fingerprinting process will be repeated just before they board the aircraft and the photograph will be compared with their face. In view of the fact that there has been more than 20 years since the acceptance of data protection act in the UK, discussions still continue on practices such as biometrics (Cimato, Gamassi, Piuri, Sassi, & Scotti, 2006). Advancements in computer and telecommunications technology mean that data protection and privacy issues are no longer just national debates. These issues have been globalised by technology therefore legislation enacted in one country is capable of affecting trade and business with its partner counties (Regan, 1993).

3.2.1 Relation between Data Protection Legislation and Internet Penetration

Although each country aims to protect personal data it is shown that regulative approach, methods, priorities may change from nation to nation. Even though first milestones of international acceptance of data protection legislation are in the preceding time of evolution in communication technologies like the Internet a correlation can be searched whether there is link between existence of regulation and technology investments.

According to a report of Organization for Economic Cooperation and Development (OECD) total number of broadband subscribers in Turkey has reached 5 million by June 2008 (OECD, 2008). According to Turkish Statistical Institute, 24.5 % of households have access to the Internet at home while proportion of computer and Internet use of individuals are 38.1 % and 35.8 % respectively by the end of 2008 (Turkish Statistical Institute, 2008). Here, broadband corresponds to fast Internet, and includes several technologies (Asymmetric Digital Subscriber Line, Cable, Dedicated Lines). On the other hand, broadband penetration in Turkey is 6.01 coming very behind the average of OECD countries 19.95. It is known that the EU nations have travelled long on the data protection highway. Thus Council of Europe monitors the national laws of member states.

Any correlation between the broadband usage level of the countries and the data protection legislation in these countries may show us the possible ratification date of Turkish data protection act. Broadband access and Internet penetration ratio are among the indicators of a nation’s diffusion to information age and information society. The higher the penetration ratio, more people online. Broadband subscription rank of top 20 countries and current data protection legislation status are shown in Table 3.2 accordingly. Internet penetration has a significant effect on data protection regulations because secrecy of personal data draws more attention when it becomes a public problem. On the other side some countries like Germany and UK have enacted data protection regulations far before Internet became publicly available.

Table 3.2 Data protection legislation status of nations having high broadband access.

Rank	**Broadband subscribers, Dec 2007**		**Data Protection Legislation**	
			National Law entry into force date (day/month/year)	**Data protection authority existence**
1	USA	69,859,707	31/12/1974	N
2	Japan	28,302,152	16/12/1988	Y
3	Germany	19,579,000	01/01/2002	Y
4	United Kingdom	15,606,100	01/12/1987	Y
5	France	15,550,000	06/01/1978	Y
6	South Korea	14,709,998	07/01/1094	N
7	Italy	10,122,126	01/01/2004	Y
8	Canada	8,675,197	01/07/1983	Y
9	Spain	7,951,905	14/01/1999	Y
10	Netherlands	5,682,770	01/09/2001	Y
11	Australia	4,830,200	18/10/1988	Y
12	Mexico	4,548,838	01/05/2002	Y
13	Turkey	4,395,800	N/A	N
14	Poland	3,340,000	01/04/1998	Y
15	Sweden	2,755,014	24/10/1998	Y
16	Belgium	2,715,308	08/12/1992	Y
17	Switzerland	2,340,650	01/07/1993	Y
18	Denmark	1,906,557	01/07/2000	Y
19	Austria	1,622,023	01/01/2000	Y
20	Finland	1,617,100	01/06/1999	Y

Turkey is among the member states of the Council of Europe which has signed Convention 108 but has not enacted its national legislation with Andorra, Russia and Ukraine. Turkey is the only country that has a significant number of broadband users on the other side has no data protection legislation framework. This seems to be a high risk for transit, transfer and mobility of personal data within the borders and transborders of the nation. Number of broadband users and Internet penetration are shown in Figure 3.1 (International Telecommunication Union, 2007; Internet Worlds Stats, 2008).

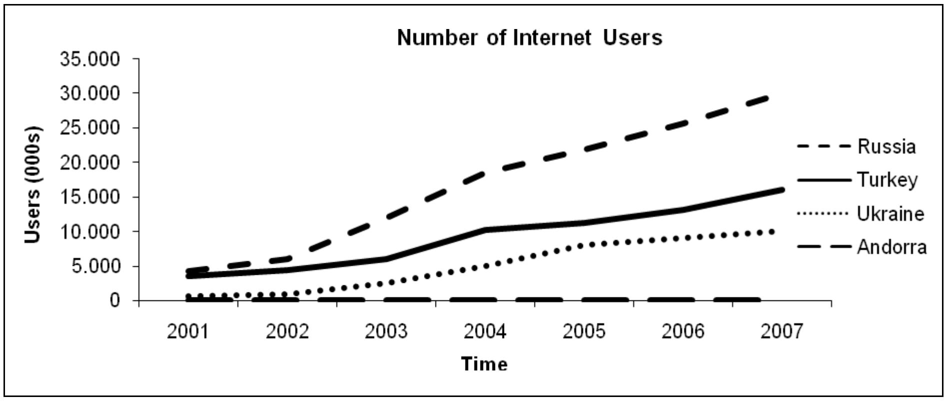


Figure 3.1 Number of Internet users of selected four nations for comparison.

Even though Internet connection distribution and access in Turkey are below the average of EU nations, Internet penetration has increased with an average of 28% between years 2002 and 2007. The increasing investment made by private organizations in broadband technologies is a proof of expectations about penetration on Internet. Penetration has not reached the saturation level and it will probably continue to increase in the following years. Besides, when the number of Internet users in Turkey is considered, it is seen that mass customers are already online.

3.3 Personal Data Protection and Privacy in Turkish Regulations

3.3.1 Turkey's Strategy, Policy and Regulations

Turkey signed the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data in 1981 but has not ratified it yet (Council of Europe, 2007). It has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms in 1954 and the International Covenant on Civil and Political Rights in 2003. Laws and regulations in which privacy is directly mentioned are given in Table 3.3.

Table 3.3 Data protection legislations in Turkey.

Regulation	Privacy Definition
Constitutional Law	Privacy of private life and freedom of communication
Criminal Code	Privacy of private life and penalty on recording, sharing and deleting personal information.
Electronic Signature Code	Protection of electronic certificate owner's personal information
Internet Crimes Code	Protection and governance for information related to the Internet usage
Banking Regulations	Protection of investors assets and account information
Health and Social Security Regulations	Privacy of human health diagnostics and integrity, availability and confidentiality of records
Privacy Ordinance in Telecommunications Sector	Privacy of communication and call details
The Draft Personal Data Protection Act	The draft act for protection of Turkish citizenry data, an umbrella code for privacy

3.3.2 Constitutional Law

Every Turkish citizen has rights protected by the Turkish Constitution about protection of private and family life. Article 20 of the Turkish Constitution deals with individual privacy and right to demand respect for private and family life. Article 20 prohibits the search or seizure of any individual, his private papers, or his belongings unless there is a decision duly passed by a judge in cases explicitly defined by law, and unless there exists an order of an agency authorized by law in cases where delay is deemed prejudicial. Article 22 preserves the secrecy of communication (Constitutional Law, 1982).

With Turkey's motivation to join European Union, Turkey passes several bills to comply with the member countries. EU requires from Turkey to "adopt a law on protection of personal data" and "establish an independent supervisory authority" (Council of The European Union, 2006).

The draft Personal Data Protection Act (DPA) has not been adapted yet in Turkey. The draft includes a series of rules about data privacy, data security and protection in the public and private sphere. In DPA sensitive personal data means personal data consisting of information as to name, surname, the racial or ethnic origin of the data subject, his political opinions, his physical or mental health or condition, his sexual life and financial profile.

3.3.3 Criminal Code

Criminal Code has been updated in 2005 and regulates felonies against private life and private sphere of individuals. Articles between 132 and 140 regulate the felonies on data protection, privacy of private life, wire-tapping recording, sharing and deleting personal information (Criminal Law, 2004).

3.3.4 Electronic Signature Code

The Electronic Signature Code (ESC) came into force in 2004. The Act was prepared under the guidance of the EU Directives and it defines the necessities for a digital signature framework. Telecommunication Authority established technical and organizational guidelines soon after the code. Electronic Certificate Service Provider (ECSP) firms are authorized to issue Qualified Electronic Signature (QES). Processing of personal data in QES is strongly taken into consideration. Thus data collection principles are defined seriously in the ESC which was not seen before. Under this law, ECSP are subject to the following obligations related to data protection (Electronic Signature Law, 2004):

1. ECSP collects personal data only to the extent, necessary for the purposes of issuing a certificate.
2. ECSP may not disclose the certificate to third parties without the consent of the certificate owner.
3. ECSP has to prevent third parties from collecting personal data without the written consent of the owner of such personal data. The certificate service

provider may transfer/use personal data only with consent of the owner of such data.

3.3.5 Internet Crimes Code and Regulation of the Internet

Media other than Internet is regulated by Turkish government. Radios, televisions, books, newspapers and magazines are regulated in terms of quality, content and context. Turkey gave signals of willingness for governing the Internet by preparing "Internet Crimes Code" in 2006. Argument on regulating Internet continues in Turkey where the discussion focuses on the question; Are we governing the Internet connection, usage of Internet or the Internet itself?

In response to the unpleasant events prompted by the scandals of child pornography, misuse of Internet as a threat for national wide security, privacy of personal life and exploitation of children, Turkish government has endorsed monitoring and regulation of Internet in Turkey. Although the main reason of the "Internet Crimes Code" is to prevent an expanded list of crimes such as pedophilia, children pornography, prostitution, inciting to suicide, and gambling, the law includes clauses about governing the content, context and access to information on Internet. The bill came to action in 2007. Utilizing the power of monitoring on Internet access within the borders of Turkey, the law provided judges the right to stopping access to suspicious web sites. Telecommunication Authority is responsible for monitoring operations. It empowers a new "Informatics Crimes High Board" to restrict access to such web sites by filtering mechanisms. In comparison with broad data sharing features and endless data storing capacities of Internet, this law seems to be an impractical and incomprehensive process. Several critics have been made about the law. Law is prepared for crimes on Internet but it seems that the argument will continue.

It must be discussed whether continuous monitoring and regulation of Internet will be effective in preventing misuse of Internet and child pornography or not. The mentioned law uses its full power to control Internet and surveillance of personal activities on the Internet. In fact, monitoring the Internet process may be a fantastic opportunity to protect personal information on the Internet. Web applications and services that give personal information host several vulnerabilities, because they access secret personal information by the use of interconnected networks. Overcoming this weakness requires plugging a large hole in today's security environment; the lack of an effective system of territory monitoring for the personal data security. This requires development of a new system of risk management which will enhance the effectiveness of personal data flaw business-to-customer and business-to-business.

3.3.6 Privacy Ordinance in Telecommunications Sector

In February 2004, the Telecommunications Authority enacted a new data security regulation, "Ordinance on Personal Information Processing and Protection of Privacy in The Telecommunications Sector" (ICTA, 2004). The purpose of this regulation is to define the procedures and principles related to guaranteeing personal information processing and protection of privacy in the telecommunications sector and in principle a summary of the European Union's 1997 directive on data protection in electronic communications. It regulates the security of communication network, responsibility to disclose the risks with regard to violation in the security of network, secrecy of communication, approval for processing of data, call number display, directory of participants; and spamming.

3.4 The Draft Personal Data Protection Act

The draft is a regulation that draws the boundaries of usage and processing practices of data. The draft law consists of five parts and 14 chapters. The first part describes the boundaries of objective, scope, definitions and processing of data with adequate and acceptable purposes for data processing. Second part includes the article about the rights of the data subject, necessary controls for processing the data and data transit to the third parties in or out of the borders. The third part includes the registry of database controller to a system managed by the Personal Data Protection

Authority (PDPA) and audit methods. The organization and responsibilities of the PDPA and the relationship with the data controller are defined in the fourth and the fifth parts.

3.4.1 Purpose and Convenience for Processing of Data

The article no. 4 of the act determines that the database controller is required to inform the data subject during the collection of the information about his purposes. Database controller must also have an authorization from the data subject. The statements used in such contract must be definitive and clear. The context of the gathered data must be sufficient and well proportioned with the service taken by the data subject from the database controller. In accordance with this definition, a merchant requesting the home phone number or e-mail from his customer during a purchase may be discussed as an "insufficient data" for the service. Similarly, a bank's credit customer may be asked to give extra information other than financial and guarantees that may not be necessary also.

Article no. 5 describes the suitable and appropriate legal circumstances of data processing. An articulate allowance and agreement is required at this point. The way of declaring and approval of such an agreement includes detailed legal definitions and is out of the scope of this paper. However it is clear that there must be a statement describing "the purpose of data processing, and the identities of the responsible data controllers" in the agreement (Başalp, 2004). In addition to this, an opportunity must be given to the data subject to choose to agree or disagree.

3.4.2 Scope for Individuals and Corporations

According to the act personal data is the all data that can be associated with an individual or corporate. Therefore each case of nonconformity will have different results and effects. A disclosure of an individual's data will be a privacy problem where a disclosure of a company data may result in financial loss and image loss.

3.4.3 Duties and Responsibilities of the Parties

The data subject has the right to know whether the database controller has a record about him or not. In practice a customer of a merchant will be able to reach the details of the database of the store or the chain store and will be able to request to update or delete it. The merchant will have to process this request except for the record that has to keep according to the labour laws. Merchant will establish a channel to accept the requests and will announce and operate the channel free of charge or for an acceptable fee.

3.4.4 Data Controller's Duty and Information Security

DBSC is responsible for deploying managerial and technical controls to protect personal data, process it with privacy and integrity, protect it away from misuse, unauthorized alteration, deletion and modification. The controls will be relevant technical and managerial countermeasures.

The relevant controls indicate computing a cost-benefit analysis, handling the data as an asset and analyzing the risk associated with this asset and ensuring the baseline of security level. The actions and countermeasures described in the act include parallel descriptions with the international standards "ISO27001:2005 Information Security Management System" (International Organization for Standardization [ISO], 2005a) and "ISO17799:2005 Information Technology-Code of Practice for Information Security Management" (ISO, 2005b).

The definition of information security in the introduction of ISO standard is; information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes.

The essence of information security management system is based on risk management. The assessment of data, its context and importance for the corporation, the vulnerability analysis, identifying the effect and probability of a compromise on the data, measuring and controlling the risk, all include managerial and technical countermeasures. As a result of the assessment, the controls will be chosen from a set of practices, technologies and procedures. Some can be classified as;

- Protection of data from unauthorized access,
- Training personnel responsible for the processing of private data,
- Guaranteeing the secrecy of data and the responsibilities by signed contracts in the case of an outsource of operations or sharing of data with third parties,
- Other technical and managerial controls.

Assuming that ISO standard will be enough to comply with the act will be deceptive (Çebi & Tahaoğlu, 2007). This internationally accepted standard should be analyzed. Since risk management forms the framework of the standard, corporations must prepare a scope within their main business activity and aim to protect the data used in this scope. The applied countermeasures will increase the security level up to a certain point. The act also estimates similar solutions as the international standard and foresees the application of countermeasures by taking into account current technology and costs.

Therefore if corporations establish a security system and develop their systems by referencing the standard, they will make a progress to comply. On the other side, each corporation will decide on a different acceptable level of risk and this situation may bring new concurrency problems. Regulatory compliance and security requirement will be discussed in detail in the following sections.

3.4.5 Turkish Data Protection Authority

According to the act an authority called PDPA will be established. The PDPA will be responsible for operating registry system and auditing the database controller. The

PDPA will force the database controller to register to the inventory of data controllers. One of the mostly criticized part of the act will be the independence of the authority; with the current version of the draft the authority will not be enough independent in terms of budget therefore in terms of decision making.

The PDPA will prepare the regulations to guide the rules of the registry system, the attributes of the inventory. According to the EU directives; the registry inventory includes the name and surname of the database controller and its representative and DBSR, purpose for the data processing, the authorized parties, plans and the measures taken for the transmission of the data to the third countries.

3.4.6 Complaints and Public Bodies

According to the act the PDPA will start an investigation in the case of a complaint of a data subject. PDPA requests the data controller to take action to change the applications and comply with the act immediately but if the data controller is a public body a 30 day period is given to improve the practices. This is a reactive approach but information security needs more proactive approaches.

The scope of the act includes the protection of data owned by individuals and corporations which aims to audit the attempts to reach the origin of data subject from an anonymous data. The draft act in progress determines new regulations to the public and private sector to secure their systems with new practices. The act will aim to protect the subject data in a boundary but it does not give any suggestion or direction for the open databases which can be used together and to reach the subject data. Open databases can be associated and used to find the source of information.

3.5 Industrial Practices and Applications

In this section, applications and processes will be investigated where personal data is being processed primarily in health, government, finance, telecommunication, and retail sectors. Personal data including but not limited personal identification number, name, phone number, address, wealth, habits are collected, processed and sometimes shared between organizations. Specific processes in these sectors will be described and the effects of such a PDPA on these applications will be visualized.

3.5.1 Health

Medical information is one of the most sensitive personal data. Patients share information about their ailment to have a better treatment. On the other hand, many researchers in the medical domain agree that there is a paradox when limiting access to medical records. "*While our medical records contain information about us that is of the utmost sensitivity, yet this information is only useful to us when it is shared with the medical providers and systems under which we get our care. Indeed, our physicians need and expect access to our complete medical records in order to help diagnose diseases correctly, to avoid duplicative risky or expensive tests, and to design effective treatment plans that take into account many complicating factors*" (Rindfleisch, 1997). Rindfleisch's statement explains the requirement of sharing medical data and also points the vulnerability of genetic information abuse. In practice, medical information is widely accessed and used not only by doctors, but also by insurers, employers, physicians and laboratories.

3.5.1.1 Health Survey Results

In order to measure the awareness, due diligence and degree of responsibility of medical sector employees, a survey is conducted. The survey includes two parts; the first part includes nine questions with an answer of "yes", "no" or "no answer". The second part is one question with multiple-choices.

The researcher-administered survey is done face to face with 95 conveniently selected medical doctors, physicians and dentists working in 3 cities; İzmir, Ankara, İstanbul. According to the Ministry of Health of Turkey (2006); 46% of the total number of specialist and practitioner physicians work in these three major cities of Turkey. The survey includes an introduction text describing the purpose and method of questionnaire. The respondents are informed that their identities will be kept confidential therefore they are not forced to record their names on the form. Thus some respondents wrote their names, title and signature. Since it is obvious that medico-employees are conscious about their responsibilities on privacy of patients this statue can not be interrogated by the mentioned survey. On the other questions about how this statue is affected with the technology is asked. The aim of the survey is to challenge how aware the medical doctors are with the information technology is used for storing data, setting appointments, transferring data between departments and more.

Hypothesis 1: Physicians believe health information kept in electronic media is less secure than in conventional (paper) media.

Hypothesis 2: Physicians who process health information electronically (e.g. computers, notebooks) do not have enough user level security information.

Hypothesis 3: The data owner who is responsible for protection in a health information system is not defined in national or enterprise level.

Hypothesis 4: As data are being stored in electronic forms; physicians can no longer keep patients' health information secret within their own boundaries.

The questions in the survey are given in Table 3.4 where nine of them are direct questions with answers *yes*, *no* or *no idea*. The respondents can give the answer if they are sure or can check "no answer" if they do not know the current application in their hospital.

Table 3.4 Health survey questionnaire.

Question no	**Question**	**Answer**
1	Do you store the information in paper media?	y / n / no answer
2	Do you store the information electronically?	y / n / no answer
3	Is the computer program used for processing the electronic data developed by your institution / hospital (in-house)?	y / n / no answer
4	Is the computer program used for processing the electronic data developed by a third party (out-source)?	y / n / no answer
5	If you have data stored on paper media do you believe they are physically protected sufficiently?	y / n / no answer
6	If you have data stored on electronic media do you believe they are protected sufficiently?	y / n / no answer
7	Is the patient data stored for a certain time (eg 10 years) and then destroyed eventually?	y / n / no answer
8	Do you believe that you have sufficient technical knowledge about the most secure method to store data on your computer?	y / n / no answer
9	Do you believe that you have sufficient technical knowledge about the most secure method to transfer data outside the institution (e.g. another physician to forward, to work at home)?	y / n / no answer
	[illegible]	i) IT department ii) Physician itself iii) Hospital management iv) Ministry of Health

According to the respondents, 86% of the hospitals keep patient's data in electronic format while 73% still have hard copy filing system. There is a conflict in the answer of the question asking whether the hospital health information system is developed in-house or out-source but it can be expected that this is technical question which user of such a system may not know. On the other side these two questions show that the physicians are aware of the existence of an IT system; 51% says they have an in-house developed system and 63% believe it is out-sourced. The fifth and sixth questions gives an interesting result where respondents trust the confidentiality and security of electronic data (46%) more than physical data (36%). 53% or all people do not believe paper media is protected sufficiently. System users where in this case the physicians do not have enough information how to secure data in their own computers (60%) and how to transfer electronic files securely out of their institution (62%). This shows that even though they use computer systems for business purposes there is a big gap in user awareness and training.

Table 3.5 Health survey hypothesis results.

Hypothesis No.	**Hypothesis**	**Prove the Hypothesis**	**Interesting Fact**
1	Physicians believe health information kept in electronic media is less secure than in conventional (paper) media.	No	53% and 27% of respondents believe data in paper form and electronic form is not secured respectively.
2	Physicians who process health information electronicly (e.g. computers, notebooks) do not have enough user level security information.	Yes	60% of physicians do not have enough information how to secure data in their own computers (60%).
3	The data owner who is responsible for protection in a health information system is not defined in national or enterprise level.	Yes	There is no defined official or common consensus owner of the health information.
4	As data are being stored in electronic forms; physicians can no longer keep patients' health information secret within their own boundaries.	Yes	Physicians are not the only owner of health information anymore, The 10th question could not receive one answer.

Physicians put the responsibility of securing electronic health data respectively IT department (34%), hospital management (32%), the physician itself (29%) and Ministry of Health (16%). From the results (Table 3.5) it can be seen that exact data processor and custodian are not defined clearly; there is a gap in personnel awareness training, responsibilities and application end user training. These conclusions will be used to develop the personnel training, awareness and data ownership requirements in the national-wide privacy scheme.

CHAPTER FOUR

PRIVACY ENHANCING TECHNOLOGIES

4.1 Definition

The privacy protection models is not a new notion in the Information Technology world where many studies are made on protection of privacy using preventive, and detective technologies. Several models are studied and proposed to protect privacy using technology. Fischer-Hübner (2001) analyzes existing security models under several privacy criteria; protection of confidentiality, integrity of personal data, binding of access to personal data, defining necessity of personal data processing, right of self-determination for data subject. Olivier (2003) makes a classification as personal privacy-enhancing technologies, web-based technologies (including Platform for Privacy Preferences), identity management, network technologies. Olivier’s architecture is made of multiple layers of controls.

4.2 Platform for Privacy Preferences (P3P)

The Platform for Privacy Preferences (P3P) is the most widely endorsed approach to enhance privacy protection.

4.2.1 History

P3P (Cranor, Langheinrich, Marchiori, Presler-Marshall, & Reagle, 2002) is a protocol for automating the intercession of privacy policies between web sites and client browsers. It compares the server policies with the user preferences. In a P3P network web site that collects personal information should have a published P3P policy. P3P is an XML-style language with a very narrow set of predefined data types and purposes. In plain words, the privacy policy should be translated into P3P to enable its automatic analysis. When a session is established, the user preferences are compared with the web site policy using a P3P Preferences Exchange Language

(APPEL). Agents on the client side perform and process the policy to a human understandable form. Therefore users can make conscious decisions about their privacy. P3P is not an ultimate solution to protect the Internet users' personal data. Yet "the presentation of P3P policies might motivate changes in practice, as companies work to be more consumer-friendly. Alternatively, a proliferation of P3P policies that do not meet customer needs might be used as evidence to support arguments for stronger privacy legislation" (Hochheiser, 2002).

4.2.2 Privacy in Biometrics

By March 27, 2008 all domestic passengers who will pass through Terminal 5 of Heathrow airport will have four fingerprints taken, as well as being photographed, when they check in. According to Telegrapgh.co.uk (Millward & Rayner, 2008), this will be the first time at any airport; the biometric checks will apply to all domestic passengers leaving the terminal, which will handle all British Airways flights to and from Heathrow.

Biometrics technology is used to ensure the passenger boarding the aircraft is the same person, the fingerprinting process will be repeated just before they board the aircraft and the photograph will be compared with their face.

BAA, the company which owns Heathrow, declares that the biometric information will be destroyed after 24 hours and will not be passed on to the police. But it is sure that this data is a treasure for any intelligence service. On the other hand there are also fears that it will make innocent people feel like criminals. Since fingerprinting will be mandatory, there will be no choice of not being scanned. This technology is open to misuse and it is not proven yet to work properly and robust. The fingerprinting of domestic passengers is expected to be the first step in the increasing use of the technology for people coming to and from Britain (Millward & Rayner, 2008).

Fingerprinting is carried out in the United States in wide areas (Brettell, 2008). It is used at the US airports as part of immigration checks for international arrivals, baggage matching, airport personnel access and border controls, driver's licensing agencies, driver's commercial lines, employment eligibility confirmation.

U.S. National Biometric Test Center describes the use of biometrics in identification and authentication as; "*the direct delivery of government services to citizens inextricably requires human identification, both positive and negative: positive identification for efficiently preventing multiple persons from using a single identity; and negative identification to effectively prevent a single person from using multiple identities.*"

Positive identification does not require biometrics. A person can prove his identity by supplying other forms of identification, such as a birth certificate, driver's license or utility bill. Where, negative identification can only be done with biometrics. No document or password can establish that one does not have multiple identities, so in government applications where negative identification is required there is no reasonable alternative to biometric identification (Wayman, 2000). In the scope of this definition, the case in Heathrow airport is an example of shifting from positive identification to negative identification.

4.3 Data & Database Security

In some occasions it becomes extremely difficult to refine application access down to the data item level therefore data should be focused rather than applications. In order to success this method data classification and data access methodologies have to be prepared before. Information must be tagged according to the sensitivity (secrecy, confidentiality and privacy) level and applications must have the ability to decide how to use the tagged information.

1. Classify data within the organizations.
2. Prepare and implement data handling procedure.

3. Prepare and implement data access and restriction policy.
4. Prepare and implement data transfer through applications policy.
5. Prepare data life cycle architecture of personal data trough out the organization.

4.4 Black Box Logging

Continuous Assurance (CA) is technology-enabled auditing which produces audit results simultaneously with, or a short period of time after, the occurrence of relevant events. CA provides a wider set of assurance reports encompassing a broader set of variables, alarms and analytic procedures. CA systems can be used as an audit process for financial and technological audit. The ability of CA is to benchmark data content of a company's information systems in real time against expected values and conditions. Therefore instead of periodical audits, CA is more timely, comprehensive, accurate and supportive for the management process (Alles, Kogan, & Vasarhelyi, 2003).

A black box logging system can be used to monitor activities on personal data in the boundaries of a database. A black box solution can be connected to the database and any read, write, update request on the pre-defined attributes of the database can be logged. This enables us to be sure that any access is identified and the logs are unchanged. A digital signature time stamp or hash algorithm can be used to protect log files from alteration. These logs can be audited periodically to detect an abnormal access attempts to personal records.

4.5 Dynamics of Privacy for Businesses

Privacy is a business issue while good privacy practices are a key part of corporate governance and accountability. One of today's key business imperatives is maintaining the privacy of personal information. As business systems and processes become increasingly complex and sophisticated, more and more personal information is being collected. As a result, personal information may be exposed to a variety of vulnerabilities, including loss, misuse, and unauthorized access and disclosure. Those vulnerabilities raise concerns for organizations, the government, and the public in general.

Organizations are trying to strike a balance between the proper collection and use of their customers' personal information. The government is trying to protect the public interest but, at the same time, manage its own cache of personal information gathered from citizens. Consumers are very concerned about their personal information and many believe they have lost control of it. With identity theft on the rise, and fears of financial or medical records being accessed inappropriately, there is a pressing need to protect personal information. Individuals expect their privacy to be respected and their personal information to be protected by the organizations with which they do business. They are no longer willing to overlook an organization's failure to protect their privacy. Therefore, privacy is a risk management issue for all businesses (AICPA & CICA, 2003).

Most of the highly publicized data breaches have taken place in the US. This is not because organizations in EU and other countries do not incur such breaches, but it is more due to their not having to publicize such events or notify customers. Axelrod (2007) describes the current situation and the increasing amount of events resulting customer data breach as a crisis: The current data protection crisis has evolved mostly from the proliferation of vulnerabilities and threats stemming from the ever-increasing sophistication and complexity of computer systems and from years of neglect.

4.5.1 Challenges for Organizations

When privacy and data protection for organizations is mentioned, there is a complex range of standards to meet, both in terms of regulatory requirements and arising expectations from customers and employees. It is balancing act on the part of the organizations to make sure that the regulatory requirements are met while customer and market expectations are achieved. In today's challenging market, organizations must take complicated issues into account in order to comply (Deloitte, 2007):

1. Complex regulatory environments: privacy and data protection laws, customs and practices vary dramatically from country to country at the local, national and global levels.
2. Globalization: Businesses today are compelled to interact beyond traditional market borders, organically and through acquisitions, out sourcing and emerging markets.
3. The extended enterprise: Success today often demands that you open, if not remove, the walls around your business and broaden access to your organizations and its IT systems.
4. Rapidly changing technology: Every advance in data-handling technology, including the recent consolidation trend in ERP systems and data warehouse IT virtualization, bring new privacy and cross border data flow implications.
5. Outsourcing and off shoring business processes: Companies are outsourcing more activities than ever to third-party providers, which introduce an entirely new level of complexity to data risk and privacy issues.

Potential risks of having inadequate privacy policies and procedures are (AICPA & CICA, 2003):

1. Damage to the organization’s reputation, brand, or business relationships.
2. Legal liability and industry or regulatory penalties.
3. Charges of deceptive business practices.
4. Lost customer or employee trust.
5. Squandered resources.
6. Denial of consent by individuals to have their personal information used for business purposes.
7. Lost business and consequential reduction in revenue and market share.
8. Disruption of international business operations.

4.5.2 Motivation for Security Investments for Organizations

Bringing an organization's systems into compliance with privacy requirements, which themselves are becoming ever more stringent, is a huge task. It will take many years and cost high amounts to achieve fully, given that customers, authorities and organization itself agree to take on the task in the first place. However, with the increased attention and involvement of lawmakers and regulators, there may not be much choice. This is one of the main differences between security and privacy. Security has been on stage for long years but has never found chance as privacy has found. Privacy and personal data protection have taken interest from lawmakers and seems that it will continue to expand for the following years. Once privacy has been a congressional issue, since the results may be excessive every effort will be used to achieve goals. There can not be a better motivation for data protection technologies to emerge.

4.5.3 Mainframe Systems

There is no doubt that computer systems have become seriously complicated since the first mainframe computer IBM System/360 which was introduced in 1965. In the 1960s, most mainframes had no interactive interface. They accepted sets of punch cards, paper tape, and/or magnetic tape and operated solely in batch mode to support back office functions, such as customer billing. Access to applications and data was much more controlled for these centralized processors, since systems were generally monolithic and user populations were more easily contained. Teletype devices were also common, at least for system operators (Axelrod, 2007). Users were able to process both business and scientific problems, or a combination of the two, with equal effectiveness (IBM, 1964).

By the early 1970s, many mainframes acquired interactive user interfaces and operated as timesharing computers, supporting hundreds or thousands of users simultaneously along with batch processing. Users gained access through specialized terminals or, later, from personal computers equipped with terminal emulation software. Many mainframes supported graphical terminals and terminal emulation by the 1980s (Wikipedia, 2008b). Even though at this time security was strong enough to control users by giving access through terminals that were known by an identifier and by location. They were hooked up to well defined and dedicated networks. Data were held centrally very different than today's dedicated database servers and data were protected using mature access control products (IBM's RACF and Computer Associate's ACF2). Nowadays most mainframes have partially or entirely phased out classic user terminal access in favor of web user interfaces and they have connection to Internet, intranet and other servers with the server farm of organizations. Today's access administration requirements need a level of granularity and flexibility. Consequently, it is a struggle to try to adapt mainframe security products to today's decentralized, distributed and often federated environment (Axelrod, 2007).

Decentralized new computing environments have problems different than mainframes. Availability of each node within distributed system, integrity of transactions transmitting through different nodes, accuracy of data stored in databases and user access management with various roles and profiles. Identity and right management is not a well solved problem for all systems. Federated environment is a new trend to solve this common problem for both systems. Transferring the responsibility for administering access to applications and enterprise resources to the end user, which can be any other division of the company other than IT department, is a commonly used approach in Identity and Access Management tools (Axelrod, 2007).

In contrast to centralized mainframe systems and departmental computer based systems, web based and PC based applications are usually developed short in security. It is always hard to find qualified programmers who are educated well in building security in applications from very beginning of system development life cycle of software products. In practice, IT analysts, developers and project managers who want to spend more time and effort on security, reliability and accuracy of software products are usually overridden by IT managers who want to launch software products into production with competitive features included (Axelrod, 2007).

To make security control matters worse, the past few years have seen an explosion in the use of e-mail, Internet access, instant messaging (IM), portable devices, laptops, personal digital assistants, smart phones and wireless access. These are additional conduits for the intentional or accidental distribution of unprotected sensitive information. Consequently the risk of leaking sensitive information is usually seen to be greater for newer technologies. When the concentration of sensitive data transferred using such resources may be much less than on traditional production systems, they are vulnerable to get lost or stolen. This combination of factors has left organizations with a multitude of areas open to possible compromise.

In the past, privacy was not considered as a major issue since there were readily available means of restricting both electronic and physical access. Besides, the cost of misdirecting personal information was usually minimal and any lost customer data was replaced with backups (Axelrod, 2007). An important difference is it is relatively easier to steal vast numbers of personal information via electronic means, which were not available in the past.

4.5.4 Security and Privacy

Security and privacy of information and data have always been confusing terms for anyone. Security of information is defined as "preservation of confidentiality, integrity and availability of information" in International Standard ISO/IEC 27001 (ISO, 2005a). Security includes these three properties of information:

1. Confidentiality: information is not made available or disclosed to unauthorized individuals, entities, or processes.
2. Integrity: safeguarding the accuracy and completeness of assets.
3. Availability: being accessible and usable upon demand by an authorized entity.

Privacy is about individuals having control over the collection, use, and disclosure of their personal information. Thus, privacy of data involves the establishment of rules governing the collection and handling of personal data. Unlike privacy, confidentiality in most cases, it is about keeping business information from being disclosed to unauthorized parties. Confidentiality is usually driven by agreements or contractual arrangements (AICPA & CICA, 2003). These definitions will be investigated in detail in following sections but it is a common target of privacy and security to protect information fairly.

4.5.5 Security Investment

Huge growth in automation of information systems enabled vast number of end users to access online resources and applications. Therefore security expense has taken an important percentage of IT budget. Organizations have started security investments from the very beginning of mainframe time and this budget increased with the development of PC, Internet, mobile phones and mobile computers in the early 1990's. Privacy risks have begun to draw attention in 2000 in terms of IT and organizational management system expenses. Private sector, government and academia have responded to meet the requirements of legislation and regulations. The relationships between security and privacy risks and corresponding expenditures are given in Figure 4.1 (Axelrod, 2007). Increase in investments in security does not mean that people are living in a more secure electronic environment. Thus security risks arise as well.

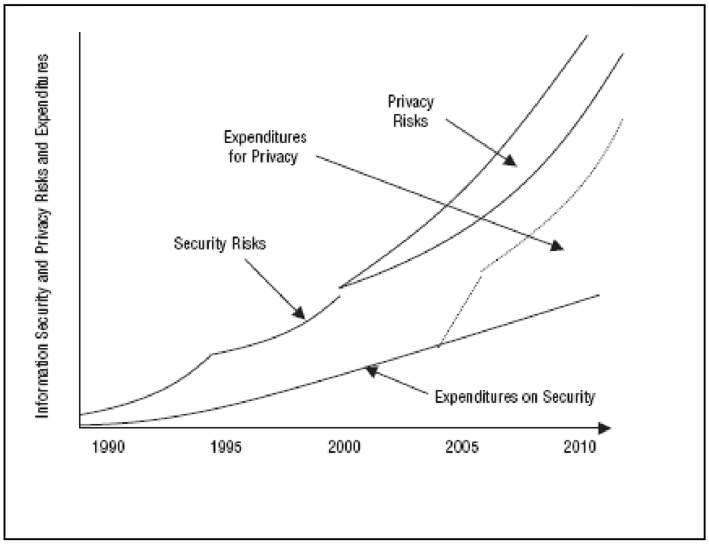


Figure 4.1 Security risks and expenditures.

4.5.6 *Demand and Supply for Security*

In order to better understand the economic aspects of privacy in terms of security privacy requirements must be investigated and studies must be made on the management of its services; in other words economics. Demand-supply curve approach is illustrated in Figure 4.2 (Axelrod, 2007). Here the supply curve and the various demand curves for various security services and products are plotted.

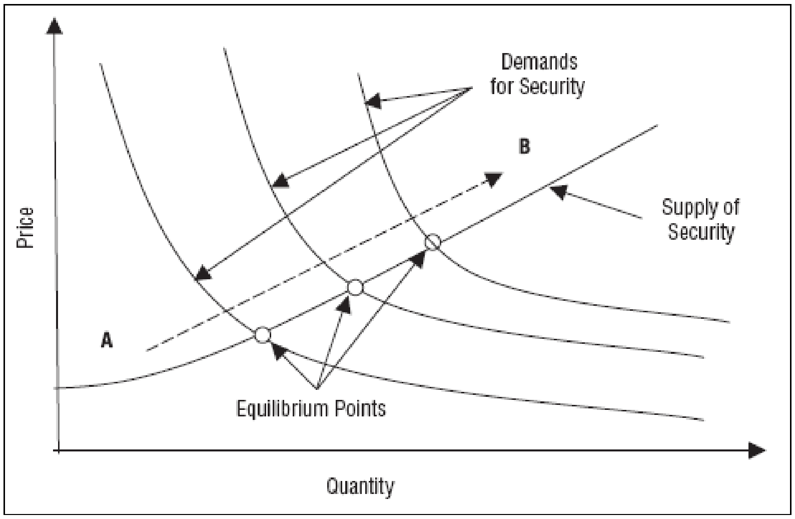


Figure 4.2 Security risks and expenditures.

Since time is not a dimension of figure, demand for security services and products increase by the regulations taken into action. If one service is examined, as the quantity decreases the price increases. As demand curves move upward, the equilibrium point move higher. The demand curves are shifting toward the upper right corner of the graph, indicating that, for example, if price were to remain the same, the quantity demanded would increase. At the same time, suppliers of security products will supply more products if the price increases. The equilibrium points are at the intersections of the demand and supply curves and they are shown to be moving upward in the direction from A to B. This indicates that, over time, the market for security products will increase in size, and will likely be relatively independent of price.

4.5.7 Security versus Survivability

There may be different methods to calculate the cost of security. Some functions of security are quantitative while some are qualitative, more information will be given about the types of controls. Axelrod (2007) uses terms security as preventing or avoiding attacks and breaches or deterring potential perpetrators, whereas describes survivability how to reduce the impact of a successful breach or attack through rapid and effective response. Expenditure relationship between them is given is Figure 4.3 where minimum point for both parameters are shown.

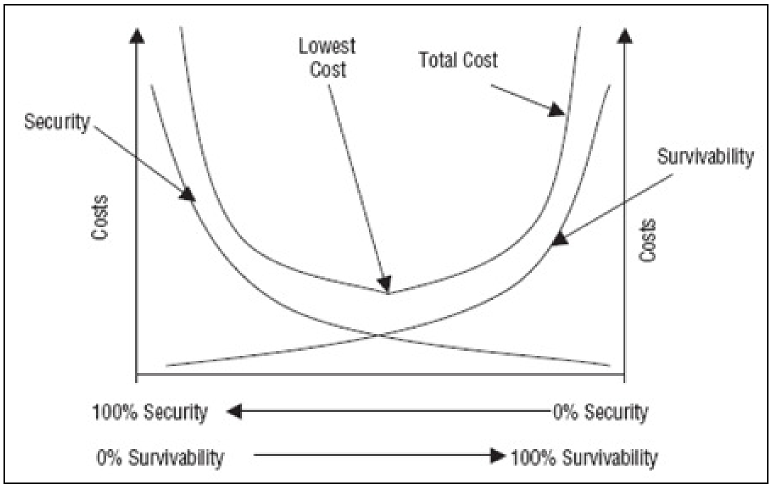


Figure 4.3 optimization of aggregate security and survivability cost.

For a given amount of spending, as more is spent on security, less needs to be spent on survivability to achieve the same level of risk mitigation.

CHAPTER FIVE

INFORMATION TECHNOLOGY FRAMEWORK FOR PRIVACY RISK MANAGEMENT

5.1 Introduction

In this chapter, the framework constructed on a set of government, organizational and individual functions and facilities regarding the regulatory, business and IT requirements are presented. This model is developed by the Requirements Engineering method (Nuseibeh & Easterbrook, 2000). Requirements engineering is widely used in software and system design and it enables an iterative process and ensure a systematic way to include all technical requirements in the framework. The framework is considered to include structured links between theory and practice. The framework includes definitions, graphical presentations, navigation descriptions, implementation guidelines, audit guidelines, maturity measurement models and templates for presenting each stage. This is supposed to be the first model studied in data protection research field in Turkey where the gap involving legislative requirements and the technical security controls is closed to some extent. Attorneys know what must be done to protect individual privacy and security experts know which controls can be implemented in enterprise systems and users computers for a secure environment but connection between these two ends is missing.

5.2 Design of the Framework

The effort is spent on finding fundamental solutions to the question; “how can compliance be assured?” Assurance is implemented in national boundaries taking into consideration the organizations’ and individuals’ requirements. Organizations and enterprises adapt their businesses and technical processes with the privacy objectives. They need motivations and funding for aligning business strategies with the data protection principles where individuals need more awareness to own and secure this personal data. This complex and wide requirements set is simplified in my design from there dimensions. Privacy principles form one dimension of the framework. Government, organizational and data owner forms the entities or stakeholders dimension of the Privacy Framework (PF). The third dimension called the "Security Measures" is this applicable managerial and IT controls. This presentation makes it traceable to follow the responsibilities of the entities in every domain and process.

5.3 The Privacy Framework

The underpinning concept of the Privacy Framework is that control in Information Systems is approached by considering at personal information that is needed to support the business objectives, and by considering the level of protection for compliance with the data protection legislations. In order to satisfy business objectives, information needs to conform to certain criteria, which Privacy Framework refers to as business requirements for personal data protection. Level of control is a balance between conformance and performance. Our privacy framework uses and improves the methodologies defined in Control Objectives for Information and related Technology (COBIT) (IT Governance Institute [ITGI], 2005) framework uses and Privacy Framework of American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants (AICPA & CICA, 2003). While COBIT is an internationally accepted method for IT governance this approach is used and developed for governance framework of personal data and privacy.

The Privacy Framework contains a set of privacy principles and related criteria that are essential to the proper protection and management of personal information. These privacy components and criteria are based on internationally known fair information practices included in many privacy laws and regulations of various jurisdictions around the world and recognized good privacy practices. In some researches these principles are called as components. For example Namli (2007) uses seven principles to protect the privacy of healthcare records. In order to have a standard privacy baseline for the Privacy Framework; OECD, EU and Canadian privacy regulations are investigated for common criteria. The selected 10 fundamental principles are given in Table 5.1.

Table 5.1 Ten principles of privacy assessment

Principle Name	Description
Accountability	Personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these principles. Each government organization is responsible for personal information under its control and shall designate an individual who is accountable for the organization's compliance with privacy regulations.
Identifying purposes	Individuals must be informed during the collection of personal information.
Consent	Knowledge and consent is required for the collection, use, or disclosure of personal information. Information and database controllers should provide clear and easily accessible statements.
Limiting collection	Minimum required information shall be relevant to the purposes of collection and obtained by fair and lawful means.
Use and retention	Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information should only be kept as long as necessary.
Accuracy	Personal information shall be as accurate, complete, and up-to-date.
Safeguards	Information shall be protected against risks such as unauthorized access, copying, disclosure, use or modification.
Openness	Personal information management policies and practices must be available to the public.
Individual access	An individual shall be able to ask the status of his/her own information and have access for any update.
Challenging Compliance	An individual shall be able to address a challenge concerning compliance with the above principles.

Entities of the framework are defined as:

1. Government is the set of regulations and authorities solely responsible for governance of personal information with the borders of a country.
2. Organizations include private enterprises, government organizations, schools, universities, hospitals, factories etc.
3. Public includes public of a nation, staff of an employee, visiting parties, tourists in a country.

These entities are presented in privacy domains. Each domain includes several processes in which personal data are used as input, output or processing elements. Each process covers at least one requirement and can be achieved by multiple security controls. Security controls are the actions which can be procedures or technical controls, where the entities take to achieve the principle.

The PF illustrates the link between regulatory and business requirements, which subdivides into three domains with the processes, provides the applicable security controls. This ensures the protection of privacy from international obligations to individual’s right to be alone. First, government needs to establish controls and role models to define the ultimate goal of implementing organizational policies and public confidence by (but not limited);

1. Set up an independent Authority and entrust the protection of personal information.
2. Provide necessary funding for the inner organization and systems of the Authority.
3. Leaving the Authority independent for making decisions on complaints.
4. Authorize the Authority to conduct audits and investigations in every industry.
5. Deploy a secure e-Government infrastructure and motivate government bodies to integrate with.
6. Institute a Privacy Impact Assessment framework to determine risk management and risk appetite approach to the data processors.
7. Supervise the diversity in between every sector and prepare applicable industrial guidelines.
8. Raise the awareness of public for privacy threats transparently.

Second, government bodies’ and private enterprises’ responsibilities are defined under model for Organizations. To achieve for benefits of personal data protection and compliance with the regulations, organizations must establish security systems in their information infrastructure. This can be realized by investing in process areas but not limited to;

1. Define the responsibilities of data processor on customer and employee information.
2. Plan on risk management and risk treatment.
3. Measure the capability.
4. Implement managerial and technical confidentiality controls.
5. Monitor compliance continuously and sustain current protection level.

Third, it must be in mind that the main focus of this effort is to protect the individuals and data owners essentially. Many surveys made by data protection commissions and Council of Europe (Council of Europe, 2007) have identified that lack of awareness and transparency on public is one of the most important drivers of a secure society. Confident public focus areas include but not limited to;

1. Declare and protect personal information as a fundamental right.
2. Be aware of the surveillance requirements in public and private locations.
3. Be aware of the surveillance actions made in electronic and virtual environments.
4. Defend rights as an employee in working environment.
5. Secure and useful access to and use of Internet being aware of privacy violations rising in new technologies.
6. Have opportunity to declare and force marketing preferences (opt-in and opt-out choices).

Figure 5.1 summarizes the framework model used in three domains, but these activities need to be defined in depth to represent the requirements and connection between domains.

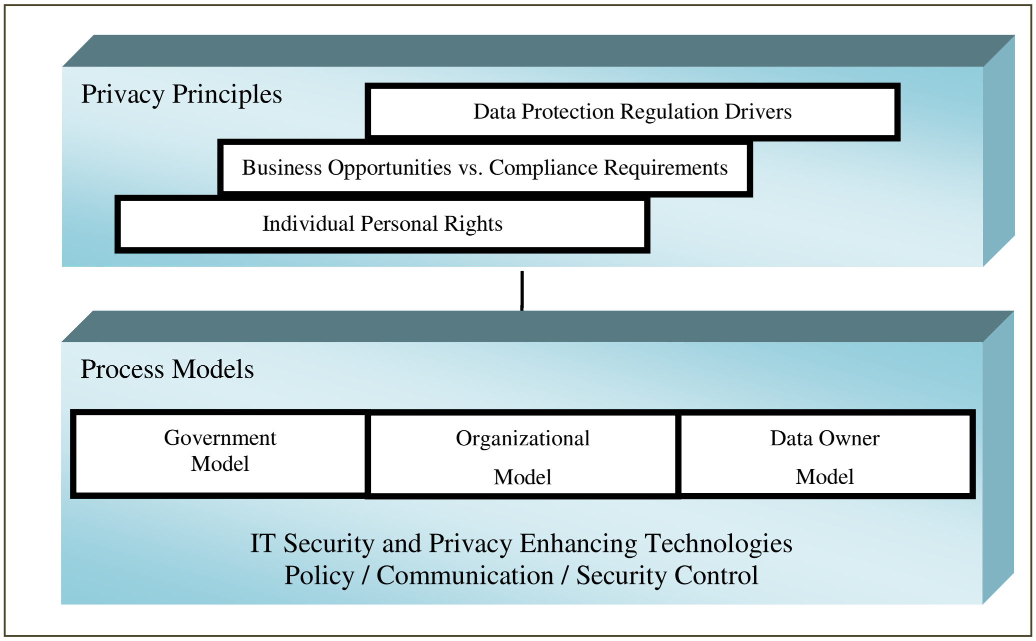

Privacy Principles
Data Protection Regulation Drivers
Business Opportunities vs. Compliance Requirements
Individual Personal Rights
Process Models
Government Model
Organizational Model
Data Owner Model
IT Security and Privacy Enhancing Technologies
Policy / Communication / Security Control

Figure 5.1 Summary of privacy framework model.

While privacy principles provide a generic method for defining the privacy requirements, defining a set of generic regulatory, business and personal goals provides a basis for determining governmental, organizational and data owner models against data protection problems. The output of the framework is a set of privacy policies, communications and security controls. Privacy policies are written statements that convey management's intent, objectives, requirements, responsibilities, and/or standards. Communications refers to the organization's communication to individuals, internal personnel, and third parties about its privacy notice and its commitments therein and other relevant information. Security controls are the safeguards and can be procedural technical control.

5.3.1 Requirements Engineering for the Privacy Framework with a Top-down Approach

Olivier's (2003) privacy architecture is used and developed to define the interaction between managerial and technical security controls. Assurance and quality systems always come from a top to bottom approach. Data protection requirements as well, must come from upper levels to force corporations to invest in security. This upper level of corporations' requirements can be regulatory requirements. The bottom level belongs to the individual's (data subject). For the purpose of this section, let *Rr, Ro* and *Rd* represent the regulatory, organizational, and data subject requirements while *Cg, Cc* and *Cp* represent government, corporation and public controls (safeguards) respectively (Figure 5.2).

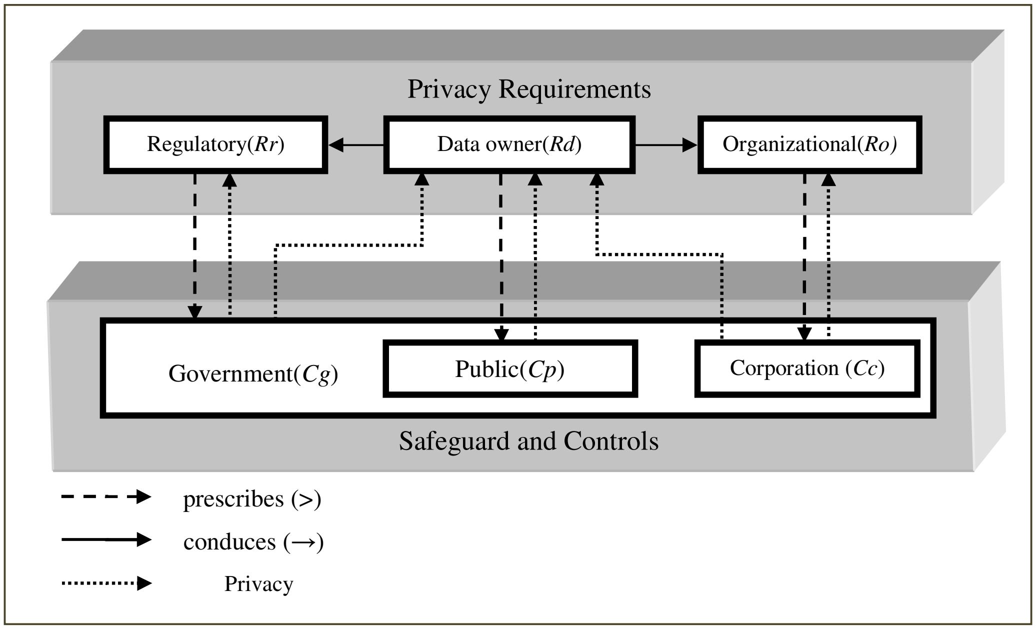


Figure 5.2 Privacy framework model

Let x > y, with x and y two of these elements, mean *x* prescribes y. Requirement *x* can cause safeguard *y* by providing configuration parameters for *y*, or by choosing one of a number of available alternative solutions on safeguard set of *y*. Often this means that domain *x* has to be informed about the permitted ranges and available alternatives on set *y*. However, there are also external parameters (i.e. financial costs, budget limits, and technological options) which affect the implementation but interaction of the domains will only be defined. It can be concluded that *Rr* > *Cg, Ro* > *Cc, Rd* > *Rp*. This is an expected result. Thus any requirement in one level has to force related element in the same domain to invest in security controls. Regulatory requirements makes the governmental bodies to invest in security while setting strategic direction and preparing national policies. The feedback of prescription is assurance and assurance of data owner's requirements can be assured by the entire security technologies. It planned that governmental security controls domain including, citizens identity management, network control, security policies, surveillance systems covers the entire subsystems; it can be illustrated as $\{Cp, Cc\} \in Cg$.

On the other side, let $x \rightarrow y$ mean requirement x conduces requirement y to exit and come into action. Clearly, data subject's requirements implies and created the requirements of national and industrial requirements; $Rd \rightarrow Rr, Ro$. Since the primary principle is to protect the personal data of the individuals it's obvious that all the necessary requirements will rise from the public.

5.3.2 The Privacy Components

The assurance, prescription and conductance feedback diagram is given in Figure 5.3. The interaction is given to show that the framework includes complex governmental and organizational requirement while they all work for the data owner domain. Although the interaction between the domains is complex it is not limited by the criteria given in Figure 5.3, and the framework will be kept as simple as possible in order to develop a practical architecture.

The PF ties the privacy requirements defined with the border of privacy principles and the security architecture and functions. The PF process models enable IT activities and the resources that support them to be properly used for data protection.

The PF components interconnect with each other in order to support regulative, business and technical needs of each process domain. Every component in the PF is used as a tool to bridge the gap between requirements of different domains. These components will be described in detail.

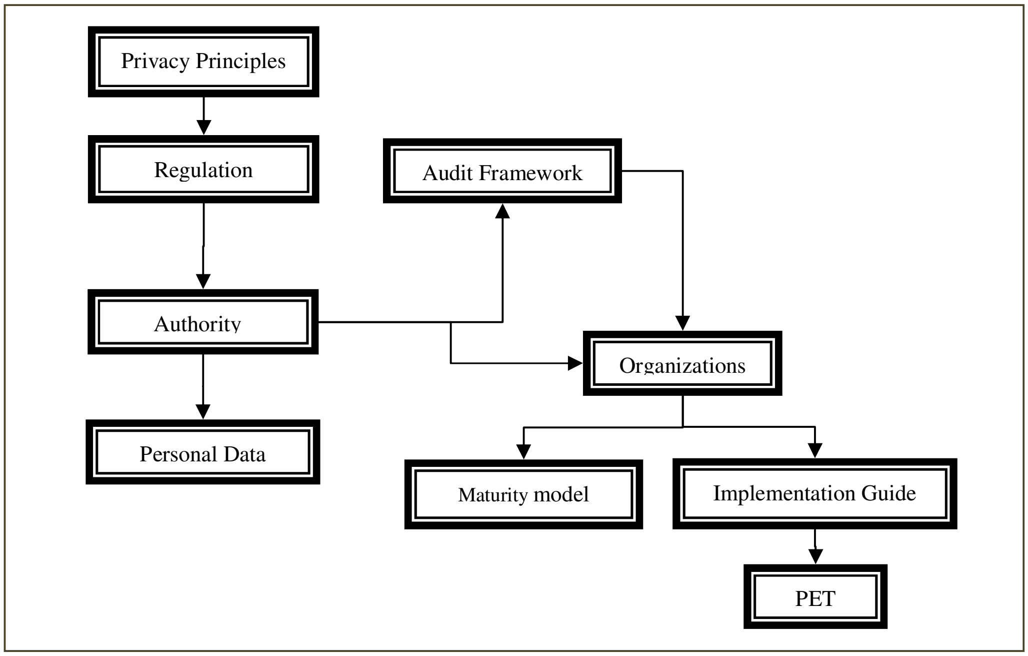


Figure 5.3 Interrelationship of privacy components.

The PF is built by security objectives in the form of regulatory, business and technology needs linking the requirement to applicable controls. The navigation shown in Figure 5.4 makes it possible to address each requirement with a security control (and PET) in a systematic approach. This illustration will be used to link privacy requirements and key controls for government, organization and public domains in the following sections.

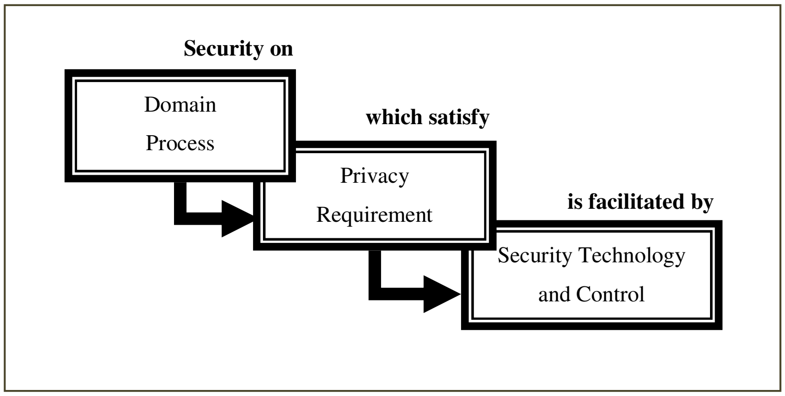


Figure 5.4 Privacy framework navigation.

It must be noted that the security objectives are designed in a generic way independent from industrial and technical differences, while accepting the reality that some environments may need different coverage. The framework contains statements of desired results to be achieved by implementing the enablers. Security requirements are clear definitions and set of controls to ensure protection of personal data in a secure, efficient, effective and economic way. The conceptual framework can be defined by three vantage points:

1. Privacy principles.
2. Data protection entities (government, organizations, public).
3. Security controls (procedures, PETs and trust services).

These three vantage points are depicted in the Privacy Framework cube in Figure 5.5.

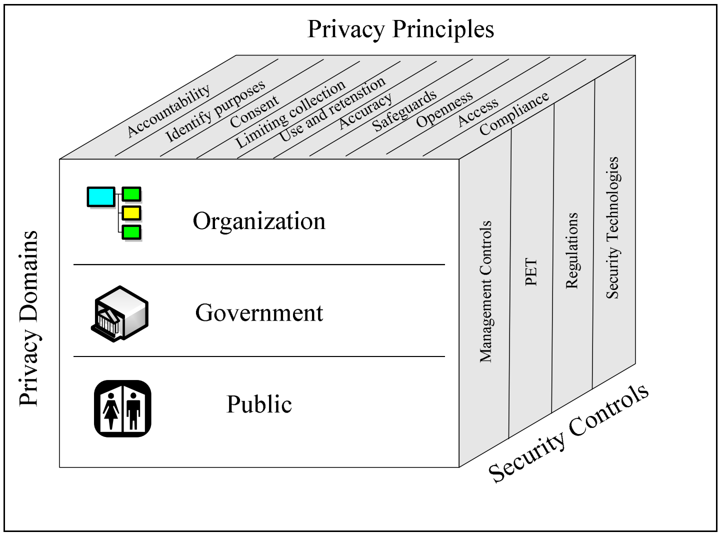


Figure 5.5 The privacy framework cube.

For each of the process domains, a high level security point is defined; each point is located to satisfy at least one privacy requirement, derived from regulatory statements. Navigation enables to justify the reason why a security control (e.g. logging, password management, encryption, etc.) is deployed together with the related privacy requirement.

5.4 Privacy Framework - Government Domain

Privacy governance for government and authorities is the responsibility of governors and the managers of the data protection authority, and consists of setting direction to the sector, motivation and protection of the data owners that ensure that there is a framework that ensures organizations are compliant with the data protection regulations and industrial standards. Therefore government domain includes obligations and duties for government agencies, private sector and citizenry. This domain observes organization of a data protection authority. Internal procedures for registration to the authority and audit system of data controllers must be organized and disclosed to the public. Public and private agencies must be audited once a year and results of the audit reports must be published for public attention. Any compliant coming from customers and employees of a company must be responded with in a certain time. The answers must be open and guiding for the requester. Organizations will not be able to understand and implement privacy and security controls in short period. As described before it took more than 10 years to deploy national-wide data protection practices in EU countries. Government domain must have a yearly budget deployed at independent and various departments. This budget must be used to financially support and sponsor companies to invest in security. Research and development in PET and management methods must begin to strengthen the national baseline for data protection. Agencies like The Scientific and Technological Research Council and universities can be entrusted to promote this research activity. Execution of transborder data exchange must also be regulated in this domain. Government must prepare the rules to guide the Turkish enterprises which transfer personal data to foreign countries for trading and commercial purposes. In addition to this, government domain must ensure the continuity of data protection mechanisms deployed in Turkish companies in order to guarantee the privacy of personal data imported into Turkey from foreign nations. Finally, confidence must be assured that collection, processing and retention are executed fairly for the Turkish citizens’ own data.

5.4.1 Governmental Privacy Framework Requirements

Business and IT “requirements set” which governments and data protection authorities are accountable are given below.

G1. Privacy on

Defining a national strategy and data protection plan

that satisfies the privacy requirement of

to strike an optimum balance of business opportunities and privacy requirements as well as ensuring a roadmap for community for compliance with data protection regulations

is facilitated by

i) develop national security policy and approach
ii) develop long term strategic plans and short term action plans
iii) keep and inventory of technological infrastructure
iv) Need for communication between government institutions
v) monitoring the incidents and events in the industry
vi) define personal data ownership in government organizations
vii) establish cooperation between private and public sectors
viii) reflect private sector’s opinions to developing privacy strategy

G2. Privacy on

Defining an information infrastructure

that satisfies the privacy requirement of

of optimizing the effort for data protection in national boundaries

is facilitated by

i) information data flow in government organizations
ii) design information data flow in all industries
iii) define data ownership rules
iv) define data classification rules
v) guidelines for personal data usage rules
vi) prepare record retention period and destroy methods
vii) explain how data subjects may access to their personal information
viii) limit costs and time period associated with obtaining access
ix) recommend and prevent identification and authentication methods for confirmation of an individual’s identity to organizations

G3. Privacy on

Keeping up-to-date with the technology

that satisfies the privacy requirement of

protection of public from emerging threatening technology and taking the advantage of new technology for protection of privacy

is facilitated by

i) capability of current technologies
ii) following the new emerging technologies
iii) monitoring future regulations worldwide
iv) monitoring applications and products in each industry
v) independent security testing of new technologies in laboratories
vi) realistic expectations of technology for monitoring of violation of privacy

G4. Privacy on

Organizing the data protection authority

that satisfies the privacy requirement of

authority

is facilitated by

i) establish and protect independence criteria of authority
ii) job descriptions in authority, other governmental and independent organizations
iii) determine the channels to receive and handle unresolved complaints and disputes between data owner and data controller
iv) disclose the ways to escalate unresolved complaints and disputes between data owner and data controller

G5. Privacy on

Transborder data flow

that satisfies the privacy requirement of

installation of sustainable safe harbors for personal data transfer between nations during commerce, legal actions and intelligence coordination

is facilitated by

i) propose data transfer standards
ii) transborder data exchange agreements
iii) coordination with political, regional and economic organizations of nations

G6. Privacy on

Identifying and allocation of funds for data protection investments

that satisfies the privacy requirement of

need for necessary funding and motivation of institutions for compliance with data protection regulations

is facilitated by

i) allocation of funds for government organizations
ii) motivation of private sector for making investment on data protection
iii) recording of costs made by organizations per annum
iv) establishing a calculation methodology for return in investment in security
v) benchmarking investments in each industry

G7. Privacy on

Managing privacy incidents and cases

that satisfies the privacy requirement of

judgment and penalty methods must be in place to solve privacy incidents and complaints

is facilitated by

i) establish complaint system for customers
ii) disclosure obligations for public and private bodies
iii) keep inventory of incident records
iv) prepare a value calculation model for incidents per person
v) prepare a compensation escalation model for incidents
vi) coordinate and escalate issues between government bodies
vii) publish mechanism of penalty and sanction to organizations
viii) report and announce decisions made by the authority
ix) take remedial action in the event that any party misuses personal information

G8. Privacy on

Assurance and audit of data processing

that satisfies the privacy requirement of

ensure the data protection safeguards are implemented by the data processors and the assurance of these systems

is facilitated by

i) declaration of audit methods and scope for each industry
ii) publishing annual audit plans
iii) preparing independent audit guidelines for organizations

5.4.2 PIA and the Role of the Authority

As previously defined an independent authority is responsible for the governance of data protection practices in each country. The authorities are responsible for building infrastructures to make the acts possible by preparing the supporting regulations, registry systems and the audit mechanisms. Preparing PIA assessment guidelines which is mentioned in the literature review chapter is one of the responsibilities of the authority. The role of the authority in PIAs is establishing a framework to assess the impacts effectively and make sure that privacy issues are clearly covered by the assessment. Authority acts a consultant and program director body for organizations. During the annual risk assessment planning, each organization is expected to submit their draft plan to the authority. The authority may provide comments and recommendations to these departments. These recommendations help the organizations to decide the scope of their privacy assessment plans and to appoint necessary resources for PIAs.

Authorities are also responsible for auditing whether government organizations and agencies are giving importance to personal data privacy and assures that PIAs are conducted as planned. It may not always be possible to make on site audits in organizations but authorizes use self assessment and reporting techniques to audit such organizations.

5.4.2.1 PIA Life Cycle

Several system and methodologies are integrated to form PIA framework. The building blocks of a PIA framework as given in Figure 5.6 are policy and guideline documentation, a risk assessment life cycle, audit system and awareness program for the related parties. The PIA policy helps to improve the awareness of privacy within government institutions. It has focuses on the potential privacy issues of a number of government programs. A PIA is a tool that helps ensure privacy protection is a core consideration when a project is planned and implemented. The whole process aims to force organizations to conduct PIA in case of new system development, integration and acquisition.

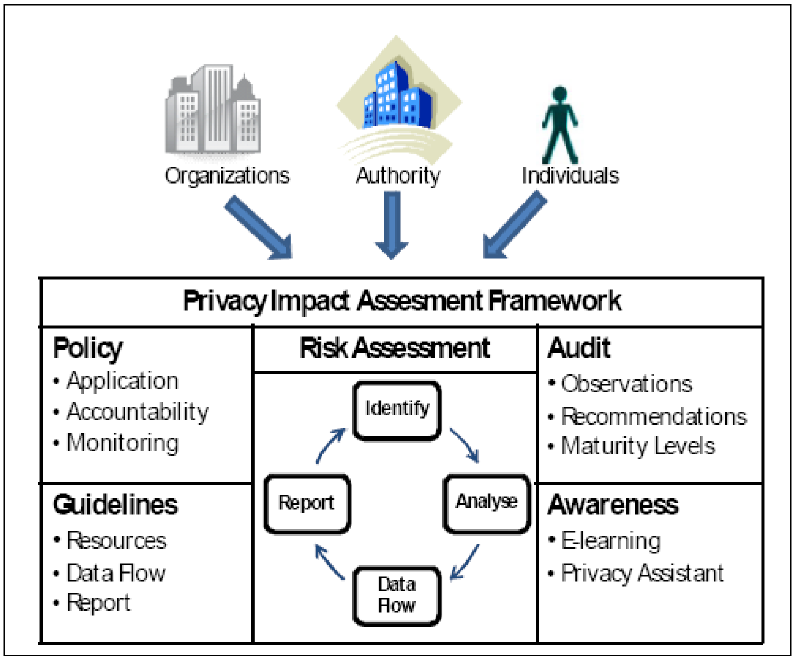


Figure 5.6 Privacy impact assessment framework components.

Guidelines prepared by the Authorities intend to provide instructions for completion of PIA. It includes checklists to determine whether a full PIA is required, measurement tools to identify required set of skills and expertise (security, legal, operational, and technology), and questionnaires assuring that PIA seeks for the entire Privacy Act principles. Risk management process must include at least these key steps (Treasury Board of Canada Secretariat, 2002):

1. Scope of the PIA must be determined. It must not be too wide thus it will be impractical to assess the entire system but also must not be too narrow where personal data may be out of scope. As a result of this Preliminary Privacy Impact Assessment process organizations decide conducting a full PIA. This step can be repeated if a design change takes place in the project.
2. Data flow must be analyzed. A detailed data flow diagram must be prepared covering the business processes and system architecture. The purpose of this step is to depict the personal information flows.

3. Privacy Analysis must be conducted from a risk management perspective. The privacy analysis examines the data flows in the context of applicable privacy policies and legislation. Checklists are used in this stage to identify major privacy risks and or vulnerabilities.
4. PIA report must be published. A document including the evaluation of the privacy risks, implications and possible mitigating and reducing countermeasures is published as a result.

The PIA report is designed as an effective communications tool used by a variety of stakeholders. If PIA system is a product then the individuals would be the customers of this system. Therefore result reports of PIAs must be available to the public. On the other hand, a national wide privacy protection framework can only be achieved by raising the awareness of individuals of the citizenry. Online leaning can be the most effective and economic way of an awareness program. Individuals must be able to ask to the Authority for assistance.

Periodic audits must be performed periodically to review that privacy directives are applied by organizations. Audits must assess; PIAs are done for necessary projects, risks are reported to the organizations' managers, recommended countermeasures are implemented, result reports are accurate, available and understandable for public. The Authority must be able to conduct on-site and off-site audits specific for each sectors (finance, communication, health, government, education etc.).

5.5 Privacy Framework - Organizational Domain

For many organizations (government bodies, companies, institutions, education bodies etc.), personally identifiable information is the most valuable, but often least understood asset. In unregulated markets, organizations usually prefer to use personal data freely without taking the attention of data owners on the security guards taken. The reason behind can be guessed easily; to use personal data as an unrecognized asses and make more profit. On the other hand, successors of the future recognize the benefits of information security and use it for the sake of their customers and to drive their stakeholders' value. These organizations also understand and manage the privacy risks, such as increasing attacks on customer information, regulatory compliance and lack of technical or managerial controls.

Privacy governance for organizations is the responsibility of top management and the board of directors, and consists of the support, resource allocation and organizational structure that ensure that the organization is compliant with the data protection regulations and industrial standards. Furthermore, privacy framework integrates and institutionalizes good practices to ensure that the organizations information systems support the data protection business principles. Privacy Framework enables the organizations to implement full control on the information which they are responsible, thereby maximizing long-term business benefits and gaining competitive advantage in the industry.

Organizations must be satisfied with the accuracy, integrity and confidentiality of personal data in the databases. Managers must also optimize the acquisition and use of security resources, including software, hardware, infrastructure, and security staff. To achieve its objectives, management must understand the current level of its enterprise architecture and decide what controls it should provide. Privacy Maturity Levels can be used to determine the current capability of the organizations.

The PF provides good practices across organizational domain and presents key security controls on activities and processes of the enterprise in a manageable and logical structure. PF's good practices represent the expectations for data processors and data controllers. These practices will help the companies to optimize IT security investments and provide a measure to judge whether the allocated resources are enough to satisfy the customers or not. For the PF to be successful there must a link between the IT security controls and business privacy requirements. PF Requirements in the organizational domain represents and summarizes these critical success criteria.

5.5.1 Enterprise Privacy Governance

Establishing an effective privacy governance framework includes defining enterprise structures, processes, management, roles and responsibilities to ensure that security investments are aligned with security strategies and policies. Organizations must deploy privacy best practices by initiating a privacy program. This program includes projects in different department and covers the areas; establishment of a data protection and security governance framework and strategy, data management, resource management for security systems, risk management and performance management. Although most of the decisions are taken at the management level, the security safeguards will be deployed at management, human resources and mostly IT departments.

Operational management of IT uses processes to organise and manage daily IT activities. The PF provides a generic process model including all necessary functions normally found in most IT departments, providing a common reference model which addresses where security safeguards must be deployed to protect customer and personnel information.

5.5.2 Organizational Privacy Framework Requirements

An effective privacy program requires that organizations and individuals be aware of their rights and obligations that, in some cases, carry the force of law. Depending on the policies of the organization, specific agreements between the organization and the individual, these aspects of privacy may be the right of the individual or organization, or its obligation to the other party. The following “requirements set” outlines some of the rights and obligations with respect to maintaining the privacy of personal information for an organizational perspective.

E1. Privacy on

Strategy and consistency with laws

that satisfies the privacy requirement of

enterprise data protection strategy set and compliance with regulations

is facilitated by

i) determine applicable laws and regulations in the jurisdictions in which the entity operates
ii) define employee security policy
iii) escalate management responsibility on enterprise policies
iv) making security a business objective in the organization
v) review the entity's privacy policies and procedures to ensure they are consistent with the applicable laws and regulations
vi) changes in business area and regulatory environment must be followed and overseen closely
vii) review business processes, people assigned responsibility for security, implemented technology, and contracts in case of any change in business environment
viii) destroy records no longer necessary in accordance with the retention policies

E2. Privacy on

Customer data protection

that satisfies the privacy requirement of

customers must be satisfied on personal data privacy to enable continuous commerce

is facilitated by

i) define an accessible customer privacy policy in a plain language
ii) ensure that customers' preferences are implemented
iii) conflicts in the records about an individual's preferences are addressed
iv) ensure use of personal information, throughout the entity and by third parties, is in accordance with an individual's preferences are met
v) notify the individual and document in case of new purposes
vi) explicit consent(opt-in) is requested from individuals affirmatively when sensitive information is collected
vii) monitor collection of personal information is limited to declared purposes

E3. Privacy on

Internal data protection strategy and communication to personnel

that satisfies the privacy requirement of

staff awareness on data protection responsibilities are adequate

is facilitated by

i) documenting privacy policies (in writing) with respect to ten principles
ii) make readily available to internal personnel and third parties who need them
iii) educate and train internal personnel initially who have access to personal information or are charged with the security of personal information about privacy awareness, concepts, and issues
iv) conduct continuous awareness and training programs
v) data usage, access procedures are communicated at least annually to the entity's internal personnel
vi) communicate Code of ethics and Disciplinary actions
vii) review, test and audit privacy policy, methods of collecting personal information and privacy notice
viii) communicate the responsibilities during and after an internal/third party audit in the company
ix) changes in privacy policies are communicated to such personnel shortly after the changes are approved

E4. Privacy on

Enterprise documentation management

that satisfies the privacy requirement of

to ensure the proper use of data in a standard and structured approach all over the enterprise processes

is facilitated by

i) documentation standards are prepared
ii) document developing and maintenance procedures
iii) management approval for privacy policies and procedures and review on changes
iv) responsibility and accountability for quality assurance and documentation are assigned to a person or group
v) responsibility and accountability are assigned to a person or group for managing, enforcing, monitoring, and updating the entity's privacy policies
vi) communicate names of person or group and their responsibilities to internal personnel
vii) ensure documentation set includes, user procedures, manuals, guidelines, training materials, audit report, test records

E5. Privacy on

Organizing the set of necessary skills

that satisfies the privacy requirement of

suitable management, technical and legal skills for establishing a data protection framework and sustain it for the future

is facilitated by

i) management responsibility for employment
ii) define formal job descriptions including responsibilities, educational and professional requirements and organizational reporting for key privacy management positions
iii) assign IT security, audit and information security team
iv) allocate a privacy or data protection officer responsible for data protection activities
v) supply legal advice and expertise
vi) supply technical expertise
vii) management best practices and consultancy
viii) assign responsibilities defined by the law and authority in the organization
ix) supervise segregation of duties for critical positions
x) define RACI responsibilities and ownership approach

E6. Privacy on

Managing the security investment

that satisfies the privacy requirement of

allocation of necessary funding for data protection investment

is facilitated by

i) request funding support from government
ii) seek investment alternatives
iii) measuring the ROI of security investment
iv) annual operational spending on security
v) annual management review for the assignment of personnel, budgets, and allocation of other resources to its privacy program
vi) benchmark of security fund in total IT fund with the competitor

E7. Privacy on

Human resources privacy

that satisfies the privacy requirement of

enterprises must protect staff information and ensure privacy

is facilitated by

i) recruitment practices
ii) roles and responsibilities in human resources department
iii) physical and logical control on employee files
iv) protection of performance, education and health files
v) job change and termination procedures
vi) responsibilities after job change
vii) assessing risk associated with outsourcing human resources operations
viii) notice the security obligations of individuals
ix) educate staff for reporting security compromises, privacy breaches and vulnerabilities

E8. Privacy on

Outsourcing and external service management

that satisfies the privacy requirement of

to meet legal and contractual requirements of third party services

is facilitated by

i) assessment of privacy risk for outsourced operations and services
ii) risk management for data flow and control on privacy
iii) defining privacy responsibilities in contracts
iv) regular monitoring and audit for compliance
v) manage risks associated with electronic commerce
vi) consider risk transfer and insurance alternatives
vii) require third parties to confirm (initially and annually) their understanding of and agreement to comply with the entity’s privacy policies
viii) inform data owners if third parties provide lower levels of protection
ix) limit the third party’s use of personal information other than purposes
x) communicate the individual’s preferences to the third party

E9. Privacy on

Risk management framework

that satisfies the privacy requirement of

privacy risk must be assessed, evaluated, communicated and mitigated accordingly and continuously

is facilitated by

i) risk management policy
ii) asset inventory
iii) threat and vulnerability assessment
iv) business risk assessment
v) technical risk assessment
vi) risk action plan
vii) risk treatment and measurement plans
viii) security control implementation
ix) classify the sensitivity of classes of data
x) ensure continuous improvement of the system
xi) Take corrective and preventive actions systematically

E10. Privacy on

Risk management for outsourced and third-part services

that satisfies the privacy requirement of

privacy risks must be managed by data controller and data processor accordingly

is facilitated by

i) third-part contract and service level agreements
ii) non disclosure agreements
iii) qualification for data transfers
iv) threat and vulnerability assessment
v) business risk assessment
vi) technical risk assessment
vii) risk action plan
viii) responsibilities in case of an incident
ix) internal organizational accountability and responsibilities
x) responsibilities after the end of contract and service
ix) confirm that third parties from whom personal information obtained from third parties is collected fairly and lawfully
x) inform data owners personal information is disclosed to third parties only for the purposes identified in the notice
xi) audit third parties

E11. Privacy on

Defining and measurement of privacy maturity levels

that satisfies the privacy requirement of

to ensure the continuous improvement of systems for data security

is facilitated by

i) measurement of current capability maturity level for key processes
ii) setting maturity targets for protection of personal data
iii) determine gaps for maturity level and compliance level
iv) define improvement opportunities
v) initiate programs and projects
vi) assess maturity level of third part entities if personal data is disclosed

E12. Privacy on

Infrastructure and Systems Management

that satisfies the privacy requirement of

to provide security during design, acquisition, implementation, configuration, and management of the infrastructure

is facilitated by

i) govern the development, acquisition, implementation, and maintenance of information systems and the related technology used to collect, use, retain, and disclose personal information
ii) ensure that the entity’s backup and disaster-recovery planning processes are consistent with its privacy policies and procedures
iii) test changes to system components to minimize the risk of an adverse effect on the systems that process personal information, anonymization all test data
iv) handle errors and omissions, security breaches, and other incidents
v) provision legal and contractual privacy requirements in service-level agreements
vi) prevent the spread of malicious code in the organization network

E13. Privacy on

Application software security

that satisfies the privacy requirement of

to provide error free and secure application and software

is facilitated by

i) adding security and data protection requirements during the design phase
ii) application software security testing
iii) development and acquisition policies
iv) application development methodology and life cycle
v) server security
vi) client (end-side) security
vii) change management
viii) Source code protection
ix) design of interfaces
x) project and software documentation
xi) Coding, maintaining, testing, evaluating, and authorizing system components before implementation

E14. Privacy on

Network infrastructure

that satisfies the privacy requirement of

to provide secure network infrastructure for supporting safe harbor of personal data

is facilitated by

i) deploy logical internal and external network security controls
ii) manage access and privilege management
iii) standardize system integration with external networks
iv) provide network device maintenance
v) hardware installation and security
vi) change management
vii) system software patching
viii) monitoring the network and detect actual and attempted attacks or intrusions
ix) network contingency planning
x) deploy intrusion detection
xi) firewall architectures and connections with public networks
xii) protect or encrypt information transmitted over the Internet or other public networks
xiii) periodically undertake vulnerability and penetration testing

E15. Privacy on

Change management

that satisfies the privacy requirement of

to ensure the sustainability of data protection systems in all times while preventing operational and environment changes

is facilitated by

i) analysis, implementation and monitoring of changes in IT systems
ii) assess planned changes to systems and procedures for their potential effect on privacy
iii) assess change impact assessment on personal data
iv) require the documentation and approval by the privacy officer and business unit manager before implementing the changes
v) release management by a listing of all software and the respective level, version, and patches that have been applied
vi) authorization for emergency changes
vii) documenting and logging the changes

E16. Privacy on

System access

that satisfies the privacy requirement of

logical access to data, unauthorized use, disclosure and modification must be managed by the data controller

is facilitated by

i) authorize employees to access personal information based on job responsibilities
ii) justification and reason for access to personal data
iii) identification, authorization, authentication are used to grant access to data
iv) role based access control
v) access control lists
vi) encrypt sensitive personal data
vii) enterprise rights management systems
viii) manage passwords
ix) allocate IT security management team
x) prepare an IT security plan
xi) deploy internal and external access monitoring systems
xii) review user accounts periodically
xiii) restrict access to offline storage and backup media
xiv) deploy enhanced security measures for remote access

E17. Privacy on

Physical and environmental boundaries

that satisfies the privacy requirement of

physical access to data, unauthorized use, disclosure and modification must be managed by the data controller

is facilitated by

i) maintain physical security is maintained over personal information stored in hard copy form
ii) deploy surveillance and monitoring systems
iii) maintain measure to protect data centers against environmental factors and disasters
iv) protect on-site and off-site backup storage
v) secure electronic assets from vandalism
vi) review of physical access logs and journals
vii) maintain physical control over sensitive reports
viii) maintain physical control over personnel files

E18. Privacy on

Database records

that satisfies the privacy requirement of

personally identifiable data must be secured by the data processor and data controller

is facilitated by

i) controls on database for integrity, accuracy and completeness
ii) data back-up and recovery
iii) on-site and off-site back-up controls
iv) accountability for data ownership
v) data input correction and output validation on databases
vi) design and control on interfaces to access data
vii) logging and journaling direct access to database
viii) integrity of data between distributed platforms
ix) additional training of database administrators and experts
x) attribute based encryption for sensitive data
xi) isolation of sensitive transactions and messages
xii) data dictionary and data map of personally identifiable information

E19. Privacy on
Assurance data processing security **that satisfies the privacy requirement of** to ensure the achievement of the internal control objectives set for the personal data processing business and IT functions **is facilitated by** i) monitoring internal controls, ii) assessing the effectiveness of internal security safeguards iii) reporting the audit findings periodically iv) self assessment of every departments within the organization v) second part audits for outsourced services and products vi) independent review and audits vii) using certification and accreditation as a proof for compliance

5.5.1 Using Risk Management in the Privacy Framework

The risk management model of the PF can provide organizations with strategic advice on privacy risk management, facilitate to mitigate privacy risk, and turn privacy into a competitive advantage. For organizations which collect, use, retain, and disclose personal information, the challenge is to enhance the trust relationships with consumers, customers, employees, and third parties, as well as to comply with privacy laws and regulations and good fair information practices. Since their resources are limited but the expectations are increasing rapidly, they have to find solutions to assess and decide the balance between privacy and availability. Risk management activity is a sub set of corporate privacy programme and is a continuous process.

The authority can use similar models with JO Model. In order to succeed, the primary requirement is to research incidents in the country. Data about publicly announced personal data leakage incidents must be collected. Court cases must be recorded as well. Complaints of consumers must be analyzed to classify causes and routes of incidents. After a repository of incidents is formed calculations can be re-evaluated. Afterwards a national calculation and compensation model can be operated. This model can be used to penalty the liable corporations, to reward incident preventions and to calculate return of investment in security countermeasures.

5.5.1.1 Privacy Incident Calculation and Compensation Model

As discussed in chapter one; risk management is targeted at measuring risk and as a result choosing the alternatives for mitigating, accepting or transferring risk, PIA is used to measure the privacy risks and Corporate Risk Management is a method to measure security and privacy risks for organizations. These described methods will be used as a baseline to manage security risks and calculate the impact of incidents.

Moreover risks cannot be eliminated completely. Incidents and events take place due to the residual risks. It is not always easy to calculate the cost of privacy event and data leakage. Japan Network Security Association (JNSA, 2008) developed a model to for estimating amount of compensation if a certain portion of privacy data is leaked (Iwaihara, Murakami, Ahn, & Yoshikawa, 2008). The model is called JNSA Operation Model for Individual Information Leak (JO Model). Economic-Privacy Map (E-P Map) is used to quantify the extent of the effect. The value of leaked privacy data of an individuation is evaluated in terms of (a) economical loss and (b) emotional pain as given in Figure 5.7.

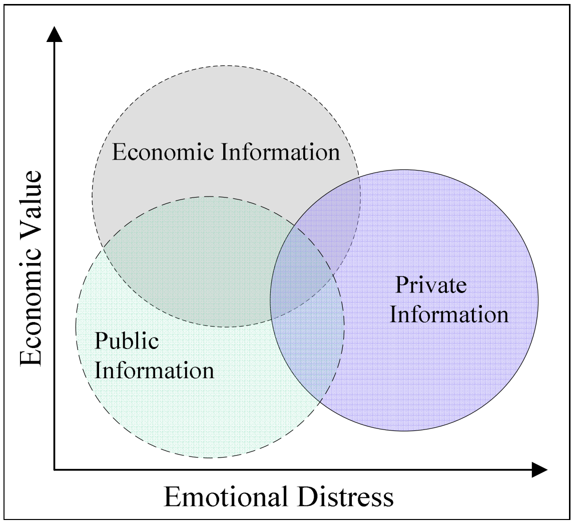
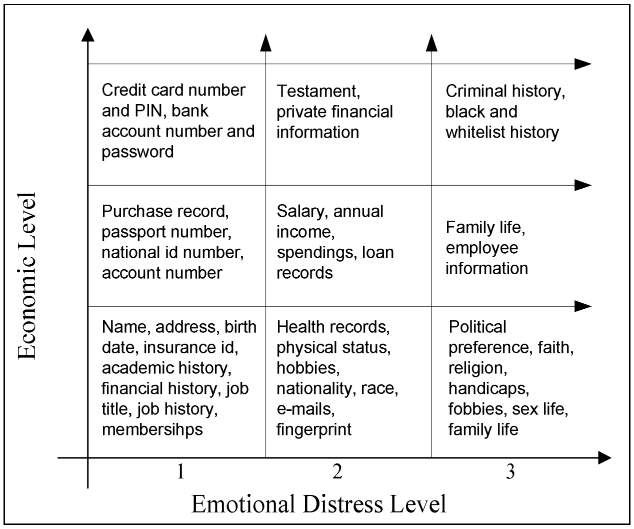


Figure 5.7 Economic-privacy map.

JNSA evaluates the level of values for economics and privacy by the use of previous events and incidents. Since they can make surveys annually their experience increase every year and the knowledge database enables to simulate the model every year.

5.5.1.2 Degree of Information Sensitivity

Let x and y be value for economical loss and emotional loss respectively. The JO Model limits the parameters by an integer from 1 to 3 in order to ease the input value to the calculation. The types of information leakage are given in Figure 5.8.



Credit card number and PIN, bank account number and password	Testament, private financial information	Criminal history, black and whitelist history
Purchase record, passport number, national id number, account number	Salary, annual income, spendings, loan records	Family life, employee information
Name, address, birth date, insurance id, academic history, financial history, job title, job history, membersihps	Health records, physical status, hobbies, nationality, race, e-mails, fingerprint	Political preference, faith, religion, handicaps, fobbies, sex life, family life

Figure 5.8 Valuation of information leakage types.

Assigning value to information is a subjective decision. Thus the figure given makes it more objective than previous approaches. Besides, the final value of disclosed personal information is not obtained yet. The *degree of information sensitivity factor (DegSen)* is defined as;

$$DegSen = (10^{x-1} + 5^{y-1}) \qquad (6)$$

As an example; a record of an individual consists of the attributes: real name, address, birth date, sex, phone number, medical records, bank account and password. Characters “x” and “y” will be assigned for selected attributes in Table 5.2.

Table 5.2 Information sensitivity factor.

Possible information leakage	***(x, y)***	***ISF value***
real name, address, birth date, sex, and phone number	(1,1)	2
medical records	(2,1)	11
bank account and password	(1,3)	26

5.5.1.3 Degree of Ease

The *DegEase* value represents the degree of ease to identify an individual by using the leaked private information. For example; by using a mobile phone number it is not possible to directly point an individual so extra databases and resources are required to address a real person. On the other side national id number may be enough to point a real person where national id number is a unique 11 digit number given for every Turkish citizen. The value of identification is given in Table 5.3.

Table 5.3 Degree of ease in identification.

Determination standard	**Degree of ease in identification of individual**
Easy to identify (Full name and address are included)	6
May be identified after certain effort or cost(Name or address are included)	3
Difficult to identify	1

5.5.1.4 Degree of Corporate Responsibility

As described in the legal framework of the data protection legislations, specific types of personal information is called sensitive. Corporations which process sensitive personal data have more social responsibility that the others. As being in a specific industry, they guarantee the appropriate protection and the degree of corporate responsibility (*CorpRes*) is classified in Table 5.4. Although value of information is will be used in the formulation, the degree of responsibility is used to enforce the corporate and public bodies. Large companies with high level of brand and name recognition must invest in security more than other companies.

Table 5.4 Degree of corporate responsibility.

Determination standard		**Degree of corporate responsibility**
Higher than normal	Organizations in specific types of industries, public institutions, companies traded on a stock exchange.	2
Normal	Other small or non-critical companies, associations.	1

5.5.1.5 Appraisal of Post-incident Response

It may not always be possible to prevent information disclosure incidents but detective and corrective actions can be taken if incident response procedures are made available before. The appraised value of pos-incident response *(AppResp)* is given in Table 9 below.

Table 5.5 Factor of post-incident response.

Determination Standard	**Appraisal of Response**
Appropriate controls taken	1
Inappropriate controls, unaware of the risks and vulnerabilities	2

5.5.1.6 Calculation of Leaked Personal Information Value

The leaked privacy information value (*LPIV)* is computed by using basic information value *(BasVal)*, degree of information sensitivity and degree of ease in identifying the individual:

$$LPIV = BasVal \times DegSen \times DegEase \tag{7}$$

$$(\ 1.000 \leq LPIV \leq 105.000\ ) \tag{8}$$

The basic information value is used as a correction value which is 500 in our calculation. Thus minimum and maximum values of leaked information are one thousand and 105 thousand respectively. The correction value can be adjusted accordingly to assess the minimum level of personal information for a nation. *LPIV* is designed to approximate the amount of compensation in national currency (US dollar, Euro, Japanese yen, Turkish Lira etc.) paid to each leakage victim. The *LPIV* is further adjusted to reflect other factors such as the social status of the information holder and evaluation on the response after the incident.

Once the value of lost information is calculated several actions must be taken. The recovery process and investment for compensation will also require financial and operational effort. *Compensation for damages (CFD)* can be projected as:

$$CFD = LPIV \times CorpRes \times AppResp \tag{9}$$

As it can be seen, corporate responsibility of a company and precautions taken by the company directly affect the compensation factor. An incident in health sector will not have the same results as in logistics and vice versa. The JNSA risk evaluation, value calculation and compensation models can be basis of risk evaluation for circumstances where semi-quantitative risk assessment is required. Such a calculation will enable the calculation of the security investment needed, as well as ROI in security. On the other hand, JNSA calculation must have a deterrent level control. A deterrent level must be set by the regulator and authority to prevent companies to choose the way not to invest in privacy protection technologies and instead pay any fine when an event occurs. The mentioned level can be a constant in unit of currency or it may change from industry to industry area.

5.6 Privacy Framework - Data Owner Domain

There is no doubt that personal data protection is a fundamental right. The challenging side is ensuring that citizens are aware of this important asset and they are taking the necessary steps to protect their own data. For the national privacy programme to be of practical effect, it must be known and accessible to the citizens. Accordingly, government should:

- Publicise the privacy protections it provides to individuals.
- Educate personal information controllers about the privacy protections.
- Educate individuals about how they can report violations and how remedies can be pursued.

5.6.1 Public Privacy Framework Requirements

The privacy "requirement set" for individuals is given below. These safeguards are controls which every individual must be careful and accountable for the protection of their own personal data.

P1. Privacy on
Communication and awareness **that satisfies the privacy requirement of** public awareness on data protection **is facilitated by** i) adhere to applicable laws and regulations, and other agreements with the organization ii) preparing annual awareness plan for the public iii) training and educating children at schools iv) raising awareness for privacy on Internet v) awareness campaigns for public to protect this own data vi) customer query for information request vii) response for a service to complaints

P2. Privacy on

Solutions for data owner requests

that satisfies the privacy requirement of

ensuring a standard approach for processing the data owner's information request

is facilitated by

i) information request definition
ii) request for an accessible request channel for data owner
iii) declaration for functionality and cost for each request
iv) defined data processor responsibilities
v) record the date when the personal information is obtained or updated

P3. Privacy on

Rights and obligations as an employee

that satisfies the privacy requirement of

being aware of worker rights and being accountable for responsibilities at working environments

is facilitated by

i) be aware of the organization's privacy policies
ii) confirm (initially and annually) their understanding of and agreement to comply with the employer's entity's privacy policies
iii) provide accurate and appropriate information suited to the purpose for which the information is needed
iv) job performance vs. personal privacy
v) logical and physical surveillance
vi) request information that personal information is collected only for the purposes identified in the notice
vii) request for types of information which will collected; financial, health , demographic

P4. Privacy on

Rights and obligations as a citizen

that satisfies the privacy requirement of

being aware of public rights against governments

is facilitated by

i) notify the organization of inaccuracies in or changes to personal information used by the government agencies
ii) be aware of surveillance systems in public areas
iii) request security and quality in e-government applications
iv) use legally accepted identification and authentication
v) request information when personal data is transferred to foreign countries by the government

P5. Privacy on

Rights and obligations as a customer

that satisfies the privacy requirement of

being aware of public rights against companies

is facilitated by

i) right to access own data and request for update

ii) informed about the purposes for which personal information is collected

iii) informed about the purpose for collecting sensitive personal information is part of a legal requirement

iv) notify the organization of inaccuracies in or changes to personal information used by the organization

v) authentication and non-repudiation precautions taken before notice is given to customer

vi) informed about the situations in exceptional situations where personal information will be disclosed

vii) provide notice in a timely manner to let customers decide objectively

viii) provide privacy policy regularly according to the regulatory requirements

ix) request for change about the choices with respect to the collection, use, and disclosure of personal information

x) informed about the consequences for refusing to provide all or some personal data

xi) request for implicit or explicit consent when personal information is disclosed to third parties

P6. Privacy on

Trust and confidence while using new technologies

that satisfies the privacy requirement of

individuals must be protected against new threats developing in online technology

is facilitated by

i) individuals must be aware of user generated content threats and new Internet usage (Ex: Web 2.0)

ii) malicious code and danger in peer-to-peer applications must be communicated

iii) personal data protection and intellectual property rights obligations in file sharing environments must be observed

iv) internet users must request privacy preferences in online applications (e.g. control on cookies)

5.7 Set of Controls and Countermeasures

Technologies within organization routinely use or share information in ways that are not necessarily well understood or under their direct control. Therefore after a series of investments in technology, the IT architecture of companies becomes complicated and it becomes impossible to control flow of data within the enterprise information systems. This vulnerability continues when the organizations decides to outsource some of its IT functions. That's where the ramifications begin.

Quick fixes can not be solution for personal data protection in organizations. A cohesive plan must be prepared and implemented systematically. Any design gap in the privacy governance architecture will not only cause data breaches but also frustrate the costs invested on security.

Privacy control is defined as the set of policies, procedures, guidelines, organisational structures and technologies designed to provide reasonable assurance that privacy requirements are business are achieved and disclosure, un authorized alteration and modification are prevented, detected and corrected. Some controls require investment on hardware or software while some need only method change. The method given in Figure 5.9 can be used for decision making before deployment of a control.

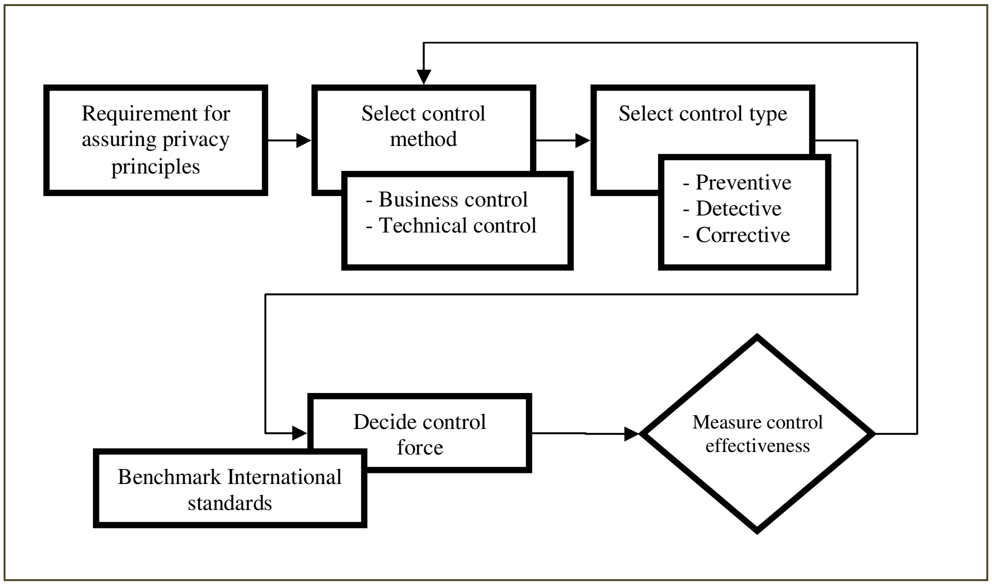


Figure 5.9 Control decision guide.

5.7.1 Control Types

5.7.1.1 Control Types by Ownership

At the business process level, controls are applied to specific business activities. Most business processes are integrated with IT applications, resulting in many of the controls at this level being automated as well. These controls are known as application controls. However, some controls within the business process remain as manual procedures, such as approved policies, provisioning access requests, segregation of duties, end-of-day checks, training programs, and manual reconciliations. Therefore business controls can be manual controls and automated application controls. They both are the responsibility of the business managers to define and request development and operation of application controls from the IT department.

IT departments provide IT services to support business processes. Usually the economic and accustomed approach is to use shared services like network, server farm, database, for multiple departments. The controls applied to all IT service activities are known as technical controls. The reliable operation of these general controls is necessary for reliance to be placed on application controls (ITGI, 2005). For example, change management, automated integrity checks, input data checks, interface controls.

5.7.1.2 Control Types by Functionality

Preventive controls attempt to keep deviations from occurring in the first place. In network management, for example, one engineer requests to access a computer but another administrator grants it. This is the segregation of duties. Unless the two parties collude, the person accepting the access can not grant access, authorize, use and then clear the access logs.

Detective controls attempt to detect deviations when they occur, so that action can be taken. Periodic reconciliations between independent processes will make it likely that deviations in one of the processes will be revealed. In the case of network access, management is informed about the request and its result by e-mail.

Corrective controls actually fix deviations. The restoration of backup files on a computer compromised by an attack is a corrective control. Also log file protection and log file check-sum are also corrective controls.

While the general taxonomy of preventative, detective, and corrective controls is useful in practice, it is not perfect (Panko, 2006). For instance, if fraudster and hackers realize that detective controls are in place, this may deter them from misbehaviour, preventative controls must be deployed. The best practice is to use them in a holistic implementation where applicable.

5.8 Economic Evaluation of the Framework

The regulation of the processing of personal data interferes in the free market by enforcing individuals’ rights and imposing standards of processing on organisations, therefore it is perhaps not surprising that anyone who regulates personal data processing may be required to provide an economic justification for their existence. Free market economics relies on competition to drive down prices, but needs adequate regulation to ensure fairness of trading and consumer protection. There appears to be a generally held belief that Data Protection is a “good thing”, but very little evidence as to whether the costs of compliance are balanced by the overall economic benefits to society (Harris, 2004). The tangible costs of data protection includes; cost of management and operations of the data protection authority, notification fees to the data processors, investments made to comply with the national regulation. The intangible costs include; impact of regulation on the free economy, limitation in data sharing between companies, and bureaucracy.

Mainly there two major items of expenses in implementing data protection legislations. The first item is the total costs of setting up the data protection authority including the annual general, administrative and operational expenses the authority. The second item is the expense of each organisation which will invest in privacy enhancing technologies.

The costs and incomes of the authorities in the UK, France, Ireland and Guernsey Channel Islands are given in Table 5.6. It should be noted that each supervisory body may be responsible for different functions in each country.

Table 5.6 Costs and Incomes of authorities in 2003.

Country	**Authority**	**Spending €** **[per thousand head]**	**Income €** **[per thousand head]**
UK	Information Commissioner’s Office	14,000,000 [240]	12,500,000 [212]
France	CNIL	6,500,000 [108]	n/a
Republic of Ireland	Data Protection Commissioner’s Office	1,600,000 [404]	450.000 [115]
Guernsey	Data Protection Supervisory	288,000 [4,800]	35,000 [583]

Total expenses are directly related with the population's requirements and interests on privacy. This may change from country to country even though between provinces within the same country. When France is taken as a reference Turkey's budget for a data protection supervisory should be €7.7 million at minimum and €108 per thousand head for a 71.5 million population.

In January 1994, the UK Home Office undertook a survey about the economic impact of the EU directive on 625 organisations, drawn from central government, local government, charities, private sector organisations and trade associations. The conclusions of that initial study were that set-up costs would amount to €3.34 billion and that annual expenditure on data protection would rise to €460 million (UK Home Office, 1994). Another assessment in 1997 estimated the start-up costs to be €1.720billion, representing slightly more than 0.1% of GDP for the UK for that year; the annual costs were estimated to be €1.110 billion, representing just less than 0.1% of the GDP (UK Home Office, 1997). For Turkey a start-up cost can be estimated to be TRY1.03 billion in 2010. This estimation is made assuming that the authority will begin in 2010, %0.1 of GDP for the forecast of 2010 according to the Mid-term Economic Programme of Turkish Republic (2009).

In 2005 European Commission published the report "Economic Evaluation of the Data Protection Directive (95/46/EC)" which is prepared by Ramboll Management. The objective of the report is to supplement the evaluation of the Data Protection Directive initiated by the Commission by measuring the economic impact of the Directive on data controllers. The economic evaluation of the Directive is based on case studies of the following five sectors: pharmacies, retail, NGOs, IT service providers and customs authorities in five EU Member States: Denmark, France, Germany, Italy and the United Kingdom. The case studies include evaluation of the following additional costs necessary to comply with the directive:

- Costs linked to learning about the requirements of the Directive
- Costs in adjusting the internal organisation to comply with the Directive
- Running costs of compliance

- Quantity and costs of Human Resources involved in the compliance
- Costs of external advice and support

According to Ponemon Institute (2004) report, 44 large US based organizations' privacy spending range from less than $500 thousand to over $22 million annually. These figures comprise all costs:

- Direct cost: The direct expense outlay to accomplish a given activity.
- Indirect cost: The amount of time, effort and other organizational resources spent, but not as direct cash
- Opportunity cost: Cost resulting from inefficient or ineffective compliance, including cost of failure/non-compliance.

A lot of focus has been given to the importance of protecting privacy. The other side of the coin is the value of information sharing. Responsible sharing of personal information lays a stable foundation for productive and successful economy. This enhances customer satisfaction and generates surplus and efficiency for the businesses and reduces fraudulent practices. Financial institutions and its customers benefit from sharing information. Customers benefit from about $17 billion of cost savings and 320 million hours of time savings annually from sharing of information by financial institutions with its affiliates and third parties (Ernst & Young, 2000).

5.9 Privacy Maturity Model for Organizations

In order to establish a reasonable benchmark for the evaluation of management control framework a Privacy Maturity Model is used. The Privacy Maturity Model is derived from multiple maturity models. Some of them are Software Engineering Institute's Software Capability Maturity Model (Sommerville, 1995) and Ernst&Young's Revenue assurance model (Ernst & Young, 2008).

The model given in Figure 5.10 identifies five progressive maturity levels from initial to optimized, ranking each organization according to its standardization of processes. The model is an indicator of the degree to which each entity is likely to be policy compliant. Organizations with strong cultures of confidentiality and an entrenched awareness of privacy issues are expected to have higher process levels. The main processes which must be assessed are listed below:

1. Organization
2. Awareness and communication
3. Policies and standards
4. Processes and tools
5. Skills and expertise
6. Responsibility and accountability
7. Performance measurement
8. Strategy and policy

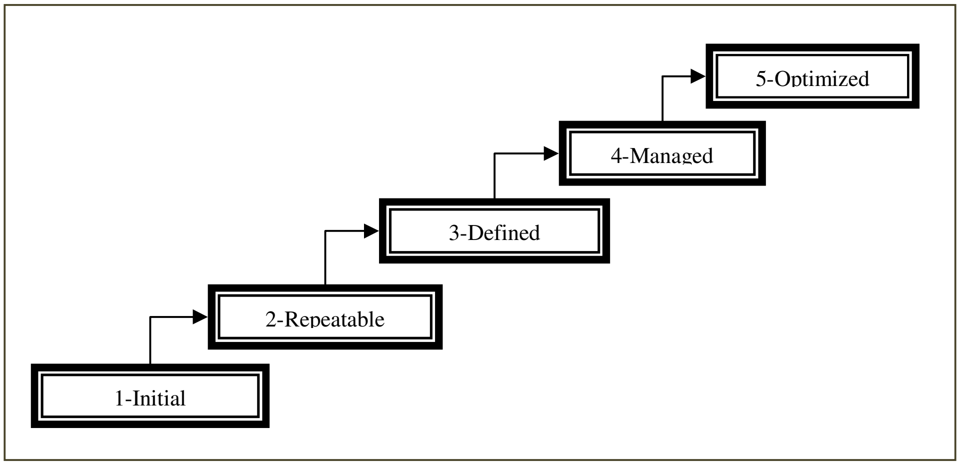


Figure 5.10 Privacy maturity levels.

5.9.1 Optimized Level

An optimized level is the maturity of an organization which is committed to continuous compliance with data protection rules, applications and business requests. Data protection has a budget and PET technology is deployed accordingly. PIA is an integral part of the organization and PIA assessment are planned and applied throughout the year. Organization is managing the external privacy risks. The organization formalized strategy, is aware of data protection regulations in sectoral details and management sets the key performance indicators for from data protection team and request integration with the group companies and third parties. Data protection officer primarily undertakes an advisory role. His team has auditing and incident management skills. Every employee takes risk management and privacy training in a formal basis.

5.9.2 Managed Level

A managed level is the maturity of an organization which has a defined policy, risk management and measurement system. Monitoring and measurement are made as quantitative where applicable. Current security level is reported to the management thus governance is on agenda. Detective and corrective actions for data protection are taken in the organization. Organization is aware of the external privacy risks. The organization formalized strategy, is aware of data protection regulations in sectoral details and management request these activities from data protection team. The organization can manage data protection team activities. Risk management and PIA activities are spread into the organization and data protection team monitors the compliance with organizational policies. Data protection officer has an annual budget and team has technical skills and subject matter expertise.

5.9.3 Defined Level

A defined level is the maturity of an organization which has defined its data protection policy and thus has a baseline for improving this active model and practice. Formal procedures are in place to ensure that formal procedures are followed in all levels of organization and during every project. The organization formalized strategy and is aware of data protection regulations. The organization has defined the responsible data protection team or officer. Training of the staff and employees is on an ad hoc basis.

5.9.4 Repeatable Level

A repeatable level is the maturity of an organization which has formal management, policy, monitoring and privacy control procedures in practice. It is called as repeatable level because the organization can successfully repeat and continue the data protection activities. However, there is a lack of a formal data protection approach and risk management model. Current security and confidentiality assurance level is dependent on individual managers and staff. The organization has no formalized strategy but is aware of data protection regulations. The organization initiates an early formalization of the data protection team or officer. Skill set of the staff is in development stage.

5.9.5 Initial Level

An initial level is the maturity of an organization which does not have effective management procedures or project plans. If formal procedures for data control exit, there are no organizational mechanisms to ensure that they are used consistently. The organization may successfully develop software but the characteristics of the data protection and the management process will be unpredictable. The organization has no formalized strategy and is an aware of data protection regulations. The organization has no data protection team or officer.

CHAPTER SIX

CONCLUSION

6.1 Conclusion

In this dissertation the goal was to develop a framework including comprehensive understanding of how security technology can be used to ensure personal data protection. The aim was to describe how security technology can be chosen properly to manage data privacy. A literature review is presented in general concepts of data protection and privacy, data protection legislations in selected nations and current situation in Turkey. Several industries are chosen to prove how serious are privacy problems in practice. Privacy Enhancing Technologies are described in brief to show that current security technology is sophisticated and qualified enough to prevent, detect and monitor today's privacy problems.

Protection of personal data can be achieved by the current up-to-date technology where security software and security functions are enough to safeguard the confidentiality of data by using mechanisms like Public Key Infrastructure, symmetric or asymmetric encryption, virtual private network, identification, authentication, authorization, access control, auditing, etc. Security countermeasures including prevention, detection, deterrent and correction controls are mature and practically available to the industry for protecting data. On the other side legal authorities are clear and resolute about their decision to put force on protecting the privacy of individuals. In spite of the technically available solutions and pressure of authorities, data processors are under strict pressure but data owners must oversee the expense and costs of security investments. While balancing the availability and secrecy of information organizations must measure the return of investment in privacy technology. It is shown that the link between the socio-legal requirements and the implementation of technology is missing in Turkey.

In order to build and strengthen this link; the necessity of privacy is pointed out from a freedom and human right point of view and then the pure definition of privacy for an individual or customer is determined. The devastating impacts of advancement in ICT on privacy of data are described. Several examples of threats are given from various sectors. Requirements engineering method is chosen to identify the needs of the laws, sectoral rules and individuals in an objective and systematic means. Risk management approach is used to filter and select the controls which are genuinely desideratum. These structures formed the building blocks of the Privacy Framework for government authorities, private organizations, public bodies and individuals themselves.

The three domain of privacy framework is formed by requirements engineering therefore requirements, controls and objectives given in each domain can be used in business decision making, engineering modeling, assessment or audit. The government model can be used to organize the internal processes and structure of a data protection authority. PIAs measure technical compliance with privacy legislation and defines the gaps between the practices and requirement while help to determine whether technologies, information systems and processes of a project meet privacy regulation requirements. PIA approach can be used by authorities to manage organizations' privacy protection investments and help them get prepared for periodic audits. Risk management method targets measuring risk and as a result choosing the alternatives for mitigating, accepting or transferring risk. Moreover risks cannot be eliminated completely. Incidents and events take place due to the residual risks. It is not always easy to calculate the cost of privacy event and data leakage. The proposed incident calculation formulas are corrective actions which can be used to manage incidents and compensate loses of persons.

The organizational model can be used to systematize the internal processes and the hierarchy of the organization. Individual model can be used personally to educated families for a safe Internet and make them feel safe while online. As a summary, the baselines of personal data protection policies are set for Turkey from the findings explored during the thesis.

6.2 Limitations of the Study

The proposed model could not find an opportunity for a full test bed or experiment field since it may take long years to plan, implement and examine its effectiveness. A three years period is required to fully implement a data protection framework on the two high level domains where usually regulations give a one year period for the preparation of sub guidelines where guidelines usually respite another one year period for organizations to implement the data protection framework and finally the third year is needed to audit the organizations. In parallel, individual domain can be initiated at the same time as the government and organization domains. Unlike the top two domains, this domain will spend more time to educate the society and it is proved that raising awareness in the public took long period for the EU.

6.3 Further Studies

The Privacy Framework can be reorganized from a data owner's perspective. The proposed framework can be implemented practically. A customer gateway can be designed to help data owners monitor, control personal data, receive notifications, and give consent about direct and online marketing. This gateway can be regulated by the government and also used by corporations. Our entity domains will build the baseline and minimum requirements of such a gateway.

Another research area can be registration to this gateway; including identification and authentication mechanisms for every entity. Data owners can authorize data controller, processors and third parties to disclose or access PII. Such a research can investigate whether full control on personal data can be possible or not.

Every industry sector including public, health, finance, education telecommunication and technology can be researched in detail. A survey on health sector employees is made but more can be done on members and customers of these flagship sectors. The survey is conducted to analyze how the secrecy of health information has changed from the boundaries of physicians to the information systems. This survey can be expanded to physicians in other provinces, physicians by special category, patients and information system personnel of health systems. Every survey can give opinion about the variance and similarities of importance of personal data in daily and work life of people.

Privacy maturity model introduced in chapter 5 has also new research opportunities; maturity levels of government institutions, universities and private sectors can be evaluated. Private companies can be asked to supply their current status on personal data protection in order to calculate their rank within their own sector. Surveys can be conducted on each sector to analyze the privacy maturity levels.

REFERENCES

AICPA & CICA. (2003). Privacy framework, including the *American institute of certified public accountants, inc. and Canadian institute of chartered accountants trust services privacy principle and criteria.*

Alles, M., Kogan, A., & Vasarhelyi, M. (2003). Black box logging and tertiary monitoring of continuous assurance systems. *Information Systems Control Journal*, (1).

Axelrod, C. W. (2007). The dynamics of privacy risk. *Information Systems Control Journal,* (1), (51).

Banisar, D. (2000). *Privacy & Human Rights: An international survey of privacy laws and developments.* Washington: Electronic Privacy Information Center.

Basel Committee on Banking Supervision. (2004). *Basel II international convergence of capital measurement and capital standards, a revised framework.* Basel: Bank for International Settlements Press & Communications.

Başalp, N. (2004). *Kişisel verilerin korunması ve saklanması*, Ankara: Yetkin Yayınevi.

Baxter, L.A., & Montgomery, B. M. (1996). *Relating: Dialogues and dialectics.* New York: Guilford Press.

Benn, S. I. (1984). Privacy, freedom, and respect for persons. In F. D. Schoeman, (Ed.). *Philosophical dimensions of privacy: An anthology* (223-244). Cambridge: Cambridge University Press.

Bennett, C. J., & Grant, R. (Eds). (1999). *Visions of privacy: Policy choices for the digital age*. Toronto: University of Toronto Press.

Brettell, K. (2008). *U.S. increases fingerprints IDs at airports.* Retrieved September 24, 2009, from http://www.reuters.com/article/domesticNews/idUSN 2538685320080325.

Cate, F. H. (2000). Principles of internet privacy. *Connecticut Law Review, 32* (3), 877-896.

Choi, S., & Whinston, A. B. (2003). The IT revolution in the USA: The current situation and problems. In E. Giovannetti, M. Kagami, & M. Tsuji, (Eds.). *The Internet revolution.* (203-222). Cambridge: Cambridge University Press.

Cimato, S., Gamassi, M., Piuri, V., Sassi, R., & Scotti, F. (2006). Privacy issues in biometric identification. *Touchbriefings on Information Security,* 40-42.

Constitutional Law. (1982). *Grand national assembly of Turkey, Turkish constitutional law.* Retrieved September 24, 2009 from http://www.tbmm.gov.tr/anayasa.htm.

Cooley, T. M. (1880). *A treatise on the law of torts on the wrongs which arise independent of contract.* Chicago: Callaghan and Company.

Council of Europe. (1959). *Convention for the protection of human rights and fundamental freedoms.*

Council of the European Union. (2006). Council decision of 23 January 2006 on the principles, priorities and conditions contained in the accession partnership with Turkey (2006/35/EC). *Official Journal of the European Union, (22),* 34-50. Retrieved February 17, 2009, from http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_022/l_02220060126en00340050.pdf.

Council of Europe. (2007). *Human rights and legal affairs-Council of Europe.* Retrieved February 17, 2007, from http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection.

Cranor, L., Langheinrich, M., Marchiori, M., Presler-Marshall, M., & Reagle, J. (2002). *The platform for privacy preferences 1.0 (P3P1.0) specification. W3C recommendation.*

Criminal Law. (2004). *Grand national assembly of Turkey, Turkish criminal law.* Retrieved July 16, 2009 from http://www.tbmm.gov.tr/kanunlar/k5237.html.

Crouhy, M., Galai, D., & Mark, R. (Eds.). (2006). *The essentials of risk management.* New York: McGraw-Hill.

Culnan, M.J. (1993). How did they get my name?: An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly, 17* (3), (341-361).

Çebi, Y., & Tahaoğlu, O.O. (2007). Personal data protection in Turkey: Technical and managerial controls. *In Proceedings of Security of Information and Networks (SIN 2007), Gazimagusa (TRNC), North Cyprus,* 220-227.

Davies, S. G. (1997). Re-Engineering the right to privacy: How privacy has been transformed from a right to a commodity. In P. E. Agre, & M. Rotenberg, (Eds.). *Technology and privacy: The new landscape.* (143-165). Cambridge, MA: The MIT Press.

Deloitte. (2007). Privacy & data protection survey - Deloitte & Touche LLP audit & enterprise risk services and Ponemon Institute LLC.

Dimaggio, P., Hargittai, E., Neuman E. R., & Robinson, J. (2001). Social implications of the Internet. *Annual Review of Sociology*, (27), 307-336.

Electronic Signature Law. (2004). *Official Gazette No: 25355.*

EPIC, & PI. (2006). *Privacy and human rights 2005. Electronic Privacy Information Center & Privacy International.*

EPIC, & PI. (2007). *Privacy and human rights 2006. Electronic Privacy Information Center & Privacy International.*

Ernst & Young. (2000). *Customer benefits from current information sharing by financial services companies, December 2000.*

Ernst & Young. (2008). *Global revenue assurance survey - taking revenue assurance to the next level, 2008.*

European Opinion Research Group. (2003). *Eurobarometer survey on the protection of privacy.*

Federal Trade Commission. (2000). *Privacy online: Fair information practices in the electronic marketplace: A report to congress.* Retrieved July 28, 2009, from http://www.ftc.gov/reports/.

Fischer-Hübner, S. (2001). *IT-security and privacy: Design and use of privacy-enhancing security mechanisms (lecture notes in computer science).* Berlin: Springer Verlag.

Frichman, R. G., Cronin, M. J. (2003). Information-rich commerce at a crossroads: Business and technology adoption requirements. *Communications of the ACM, 46* (9), 96-102.

Glenn, R. A. (2003). *The right to privacy: Right and liberty under the law.* California: ABC-CLIO.

Harris, P.R. (2004). The European perspective - is data protection value for money? *In Proceedings of the 26th International Conference on Privacy and Personal Data Protection.*

Hochheiser, H. (2002). The platform for privacy preference as a social protocol: An examination within the U.S. policy context. *ACM Transactions on Internet Technology (TOIT), 2* (4), 276-306.

IBM. (1964). *Press Release, System/360 Announcement.* Retrieved November 21, 2009 from http://www-03.ibm.com/ibm/history/exhibits/mainframe/mainframe_PR360.html.

ICTA. (2004). *Information and communication technologies authority, ordinance on personal information processing and protection of privacy in the telecommunications sector, Official Gazette No: 25365.*

International Organization for Standardization. (2005a). *ISO/IEC FDIS 27001, international standard – information technology – security techniques – information security management systems – requirements.*

International Organization for Standardization. (2005b). *ISO/IEC 17799, international standard – information technology – security techniques – code of practice for information security management.*

International Telecommunication Union. (2007). *Internet indicators: subscribers, users and broadband subscribers.* Retrieved February 18, 2009, from http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx.

Internet Worlds Stats. (2008). *Turkey internet usage and telecommunications report.* Retrieved December 20, 2008, from http://www.internetworldstats.com/eu/tr.htm

ITGI. (2005). *IT Governance Institute, control objectives for information and related technology 4.0.*

Iwaihara, M., Murakami, K., Ahn, G., & Yoshikawa, M. (2008). Risk evaluation for personal identity management based on privacy attribute ontology. In *Conceptual modeling - ER 2008 (lecture notes in computer science).* Berlin: Springer Verlag.

Japan Network Security Association. (2008). 2006 information security incident survey report - version. 1.0.

Jeff, H. S. (1994). *Managing privacy: Information technology and corporate America*. Chapel Hill: University of North Carolina Press.

Kang, J. (1998). Information privacy in cyberspace transactions. *Stanford Law Journal* (50), 1193-1294.

Karol, T. (2001). Cross-border privacy impact assessments: An introduction. *Information Systems Control Journal*, (3).

Kim, Y. C. (2006). *Privacy and communications technologies in U.S. history: A comparison of concepts of privacy in relation to changing communication technologies, PhD thesis.* Pennsylvania State University.

Lane, C. A. (1997). *Naked in cyberspace: How to find personal information online.* Wilton: Pemberton Press.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., et al. (2000). *A brief history of the Internet,* Retrieved November 11, 2008, from http://www.iicm.tugraz.at/thesis/cguetl_diss/literatur/Kapitel02/References/Leiner_et_al._2000/brief.html?timestamp=1226850959229, 16.11.2008

Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. *Journal of Social Issues, 59* (2), 243-261.

McDougall, B. S., & Hansson, A. (Eds.). (2002). *Chinese concepts of privacy.* Leiden: Brill.

McWhirter, D. A., & Bible, J. D. (1992). *Privacy as a constitutional right: Sex, drugs, and the right to life.* New York: Quorum Books.

Millward, D., & Rayner, G. (2008). *Heathrow airport first to fingerprint.* Retrieved January 17, 2009, from http://www.telegraph.co.uk/news/uknews/1580993/ Heathrow-airport-first-to-fingerprint.html.

Ministery of Health of Turkey. (2006). *Turkey's hospitals activities based on province and some indicators.*

Murphy, R. S. (1996). Property rights in personal information: An economic defense of privacy. *Georgetown Law Journal, 84* (7), 2381-2417.

Namli, T. (2007). *Security, privacy, identity and patient consent management across healthcare enterprises in integrated health enterprises (IHE) cross enterprise document sharing (XDS) affinity domain.* Middle East Technical University.

Nozin, M. (2005). *A privacy framework to provide users with control, accuracy and audit.* Ontario: University of Ottawa.

Nuseibeh, B. & Easterbrook, S. (2000). Requirements engineering: a roadmap. *In Proceedings of the Conference on The Future of Software Engineering, Ireland,* 35-46.

OECD. (1981). *Guidelines governing the protection of privacy and transborder data flows of personal data.* Retrieved February 17, 2009, from http://www.oecd.org/document/18/0,3343,en_2649_201185_1815186_1_1_1_1,00.html.

OECD. (2008). *Broadband statistics subscribers per 100 inhabitants, by technology.* Retrieved February 5, 2009, from http://oecd.org/sti/ict/broadband.

Officer of the Privacy Commissioner of Canada. (2007). *Privacy impact assessments.* Retrieved July 26, 2009, from http://www.privcom.gc.ca/fs-fi/02_05_d_33_e.asp.

O'Leary, T., & O'Leary, L. (2002-2003). *Computer essentials.* New York: McGraw-Hill.

Olivier, M. S. (2003). A layered architecture for privacy-enhancing technologies. *South African Computer Journal, 31,* (53-61).

Panko, R.R. (2006). Spreadsheets and Sarbanes–Oxley: Regulations, risks, and control frameworks. *Communications of the AIS,* 17 (9).

Pedersen, D. M. (1997). Psychological functions of privacy. *Journal of Environmental Psychology, 17* (3), 147-156.

Pedersen, D. M. (1999). Model for types of privacy by privacy functions. *Journal of Environmental Psychology, 19* (4), 397-405.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. New York: State University of New York Press.

Ponemon Institute. (2004). *The cost of privacy study. IBM and Ponemon Institute.* Retrieved November 21, 2009, from ftp://ftp.software.ibm.com/software/tivoli/pdf/privacy-study.pdf.

Posner, R. A. (1984). An economic theory of privacy. In F. D. Schoeman, (Ed.). *Philosophical dimensions of privacy: An anthology* (333-345). Cambridge: Cambridge University Press.

Regan, P. M. (1993). The globalization of privacy: Implications of recent changes in Europe. *American Journal of Economics & Sociology, 52* (3), 257-274.

Regan, P. M. (1995). *Legislating privacy: Technology, social values, and public policy.* Chapel Hill: University of North Carolina Press.

Rindfleisch, T.C. (1997). Privacy, Information Technology, and Health Care. *Communications of the ACM, 40* (8), 93-100.

Rosenberg, B. (February 1, 2007). *Privacy rights clearing house - chronology of data breaches 2006: Analysis.* Retrieved July 26, 2009, from http://www.privacyrights.org/ar/DataBreaches2006-Analysis.htm.

Rothfeder, J. (1992). *Privacy for sale.* New York: Simon & Schuster.

Schechter, S. E. (2004). *Computer security strength & risk: A quantitative approach, PhD thesis.* Harvard University.

Schement, J. R., & Lievrouw, L. (1987). *Competing visions, complex realities: Social aspects of the information society.* New Jersey: Ablex Publishing.

Sommerville, I. (1995). *Software engineering* (5th ed.). Essex: Addison–Wesley.

Spiro, H. J. (1971). Privacy in comparative perspective. In J. R. Pennock & J. W. Chapman, (Eds.). *Nomos XIII.* (121-148). New York: Atherton Press.

State Planning Organization. (2006). *Information society strategy 2006-2010.* Ankara.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk management guide for information technology systems - recommendations of the National Institute of Standards and Technology.* Gaithersburg: NIST Special Publication.

Treasury Board of Canada Secretariat. (2002). *Privacy impact assessment guidelines: A framework to manage privacy risks.* Retrieved July 29, 2009, from http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld-eng.asp.

Tsiakis T., Stephanides G. (2005). The economic approach of information security. *Computers & Security, 24* (2), 105-108.

Turkish Republic. (2009). *Mid-term Economic Programme.* Retrieved November 22, 2009 from http://mevzuat.dpt.gov.tr/bkk/27351-M.htm.

Turkish Statistical Institute. (2008). *Science, technology & informatik, ICT usage statistics.* Retrieved November 16, 2008 from http://www.turkstat.gov.tr/.

UK Data Protection Act. (1998). *UK Parliament - Office of public sector information.* Retrieved July 16, 2009 from http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1.

UK Home Office. (1994). *Costs of implementing the data protection directive, paper by the United Kingdom.*

UK Home Office. (1997). *Regulatory impact assessment of Directive 95/46/EC, paper by the United Kingdom.*

United Nations. (1948). *The universal declaration of human rights.* Retrieved November 16, 2008 from http://www.un.org/en/documents/udhr/.

United Nations. (1966). *International covenant on civil and political rights.* Retrieved November 16, 2008 from http://www.un.org/millennium/law/iv-4.htm.

United Nations. (2008). *UN e-government survey 2008, from e-government to connected governance.* New York: United Nations publication.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4* (5), 193-220.

Wawrzyniak, D. (2006). Information security risk assessment model for risk management. In t*rust and privacy in digital business (lecture notes in computer science)* (21-30). Berlin: Springer Verlag.

Wayman, J.L. (2000). Federal biometric technology legislation. *IEEE Computer, 33* (2), 76-80.

Westin, A. F. (1967). *Privacy and freedom.* New York: The Association of the Bar of the City of New York.

Whitaker, G. (2007). *Mobile identification for the UK police project Lantern.* Retrieved February 18, 2009, from http://fingerprint.nist.gov/standard/archived_workshops.

Wikipedia. (2008a). *Privacy.* Retrieved November 15, 2008 from http://en.wikipedia.org/wiki/Privacy.

Wikipedia. (2008b). Mainframe computer. Retrieved November 24, 2009 from http://en.wikipedia.org/wiki/Mainframe_computer.

Wong, E.Y.W. (1994). Data protection legislation in Hong Kong: A practical perspective. *Journal of Information Technology Management, 5* (3), (59-63).

APPENDIX A. GLOSSARY

ALE. Annual Loss Expectancy.

AppResp. Value of pos-incident response.

BasVal. Basic information value.

CA. Continuous Assurance.

CFD. Compensation for damages.

COBIT. Control Objectives for Information and related Technology.

CoE. Council of Europe.

Consent. Agreement by the individual for the entity to collect, use, and disclose personal information in accordance with the privacy notice. Such agreement can be explicit or implied. Explicit consent is given either orally or in writing, is unequivocal and does not require any inference on the part of the entity seeking consent. Implied consent may reasonably be inferred from the action or inaction of the individual.

Convention 108. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

Cookies. Cookies are pieces of information generated by a Web server and stored in the user's computer, ready for future access. This information can then be used to identify the user when returning to the Web site, to personalize Web content, and suggest items of potential interest based on previous buying habits. Certain advertisers use tracking methods, including cookies, to analyze the patterns and paths through a site.

CorpRes. Degree of corporate responsibility.

DegSen. Degree of information sensitivity factor.

DPA. The draft Personal Data Protection Act.

ECSP. Electronic Certificate Service Provider.

Entity. An organization that collects, uses, retains, and discloses personal information.

E-P Map. Economic-Privacy Map.

ESC. The Electronic Signature Code.

ICT. Information and Communication Technologies.

Individual. The person about whom the personal information is being collected (sometimes referred to as the data subject).

ISMS. The Information Security Management Systems.

ISO. International Organization for Standardization.

JNSA. Japan Network Security Association.

JO Model. JNSA Operation Model for Individual Information Leak.

LPIV. Leaked privacy information value.

OECD. Organization for Economic Cooperation and Development.

Opt in. Personal information may not be collected, used, retained and disclosed by the entity without the explicit consent of the individual.

Opt out. There is implied consent for the entity to collect, use, retain, and disclose personal information unless the individual explicitly denies permission.

P3P. Platform for Privacy Preferences.

PDPA. Personal Data Protection Authority.

PET. Privacy Enhancing Technologies.

PF. Privacy Framework.

PIA. Privacy Impact Assessment.

PII. Personally Identifiable Information.

Policy. A written statement that communicates management's intent, objectives, requirements, responsibilities, and/or standards.

QES. Qualified Electronic Signature.

ROI. Return on Investment.

Sensitive personal information. Personal information that requires an extra level of protection and a higher duty of care, for example, information on medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual preferences, or information related to offences or criminal convictions.

Staff. Employees, contractors, agents, and others acting on behalf of the entity and its affiliates.

System. A system consists of five key components organized to achieve a specified objective. The five components are categorized as infrastructure (facilities, equipment, and networks); software (systems, applications, and utilities); people (developers, operators, users, and managers); procedures (automated and manual); and data (transaction streams, files, databases, and tables).

Third party. An entity that is not affiliated with the entity that collects personal information or any affiliated entity not covered by the entity's privacy notice.