Exploring Privacy Requirements and Their Online Managements

Da-Yu Kao

Department of Information Management, Central Police University,
Taoyuan City 333, Taiwan, ROC
camel@mail.cpu.edu.tw

Received 27 February 2014; Revised 15 January 2015; Accepted 20 May 2015

Abstract. Personal information is generated by many information systems around people. Online data transfer has become a research focus across a number of fields, including scientific research, government transparency and open data. The privacy requirements of OECD Guidelines, APEC Framework and EU Directives did influence the privacy legislation on Taiwan, Canada, and Australia. This paper describes Taiwan legislation on personal information protection, and sets out the ground rules for how an organization may collect, process, use or transmit information about any data subjects. This paper also proposes an ICT governance framework in online data privacy management. These privacy requirements are further explored from three categories: primary activities of manageable facets, secondary activities of relational stakeholders, and tertiary activities of positional concerns. These activities are explored from life cycle stage, data privacy issue, and privacy requirements. This framework supplements the existing conceptions of international privacy principles and their privacy requirements for personal information. Within the framework of this study, further studies may concentrate on big data and case study in online management strategies.

Keywords: privacy requirement, online management, personal information, standard operation procedure

1 Introduction

1.1 ICT and Personal Information

Information and Communications Technology (ICT) has a direct effect on data governance. ICT developments have enabled vast amounts of personal information process [13]. Personal information identifies one as an individual rather than one member of a group [11]. Personal information means information about an identifiable individual, including [14, 16]: individual data, contact information, social activities, medical health, and financial conditions. Organizations collect data from various sources or devices, and try to have benefits form independent applications. Every organization wants to use maximum of personal information than before. It has been labeled as the currency of digital economy. Therefore, organizations make huge investments in the controls of internal process to promote good data governance [4]. However, many executives have not paid sufficient attention to its critical role.

Users entrust social networks such as Facebook and LinkedIn with a wealth of personal information such as their age, address, current location or political orientation. They use Internet tools to build their identity. Digital identities are masks that people wear online to distort their identity [6]. Internet users present themselves online as they are in real life. They use avatars in online games to adopt behaviors which are different from their real personality. Such information systems have been widely adopted in our daily life from traffic services to online shopping platforms. Personal information is vulnerable to partners, adversary, and competitors. Organizations need to provide safe and secure services to citizens. The rapid growth of personal information has raised far-reaching problems about the future of online privacy [11]. Main challenges in organizations involve [4, 9, 10]:
(1) Governance: avoid increased financial penalties and reputational damage;
(2) People: implement adequate training for staffs with sufficient expertise;
(3) Process: embed privacy requirements into operational processes;
(4) Technology: adapt an information system in order to comply with relevant laws and regulations.

To combat these challenges, organizations should take some proper actions to avoid heavy sanctions. The ICT advancement plays an effective role in organizations to reach the desired level of reliability and productivity through ensuring integrity, availability and confidentiality. To establish a comprehensive framework practice that addresses the range of privacy issues, organizations can take steps to establish procedures that address all of the fair information practices.

1.2 Motivation

Since the ICT market is rapidly growing, new ICT forms tend to be employed in ways that primarily serve the interests of organizational elites. Online privacy has become an international issue, which is followed by the e-commerce development [7]. Personal information is increasingly regarded as a valuable resource in itself. In order to foster care for information systems, organizations should be readily consistent with maintaining security of them. Organizations should act in a timely manner to respond to the security breaches of information systems. The concern to improve performance efficiency has been primarily important to intensify its utilization. This study tries to [4, 10, 11]:
(1) clarify the logic understanding of privacy principles;
(2) explore the life cycle stage of personal information protection;
(3) outline the obligation of organizations;
(4) propose an ICT governance framework;
(5) emphasize the psychical control through data governance.

The literature reviews of privacy principles and their comparison are discussed in Section 2. Section 3 describes Taiwan legislation on personal information protection, privacy concerns from Taiwan legislation, and online managements for meeting privacy requirements. In Section 4, a proposed ICT governance framework in online data privacy management is divided into three categories: primary activities of manageable facets, secondary activities of relational stakeholders, and tertiary activities of positional concerns. This framework further points out data governance, capable people, efficient process and effective technology. Our conclusions are given in Section 5.

2 Literature Reviews

To implement online privacy protection, it is helpful to know some of the history behind privacy principles and associated developments in legislation [11]. Privacy principles and their comparison are introduced in this section. Associated developments of Taiwan legislation are discussed and analyzed later.

2.1 Privacy Principles for Personal Information

More issues are emerged in personal information protection perspective. How can we prevent harm to an individual whose personal information is at stake? Existing privacy principles associated with the collection, processing, use and transmission of personal data have formed the basis of personal information protection legislation around the world. A version of these principles was internationally agreed in 1980 in the form of the Organization for Economic Co-operation and Development (OECD) Privacy Principles: protection and security, accountability, individual participation, data quality, openness, collection limitation, purpose specification, and use limitation [12]. OECD Privacy Principles have been a core part of online privacy managements, but the manner in which they are implemented needs to be revisited or updated to reflect current practices or address changed circumstances in an Internet world [20]. The World Economic Forum held a global dialogue on personal information. In 2012, the World Economic Forum's dialogue clustered existing OECD principles into three broad categories [21]: "Protection and security," "Accountability and enforcement," and "Rights and responsibilities for using data." This initial clustering exercise has carefully enabled insight into the OECD principles (Fig. 1).

2.2 International Comparison of Privacy Requirements

Privacy requirements have become critical in all aspects. It is also important to increase the performance of information system, follow security policy, and meet privacy requirements. Organizations around the world have differently defined their privacy requirements for personal information protection. Table 1 represents the derivation of privacy requirements as articulated by the principles and acts [15, 20]. These principles and acts map legal obligations for implementing the privacy requirements.

(1) Principle

- Organization for Economic Co-operation and Development (OECD) Privacy Guidelines in 1980 (Amended in 2010) [12];
- Asia-Pacific Economic Cooperation (APEC) Privacy Framework in 2005 [1];
- European Union (EU) Data Protection Directives in 2012 [8].

(2) Act

- Taiwan Personal Information Protection Act (PIPA) in 1995 (Amended in 2010) [17];
- Canada Personal Information Protection and Electronic Documents Act (PIPEDA) in 2000 (Amended in 2011) [3];
- Australia Privacy Law (APL) in 2008 (Amended in 2013) [2].

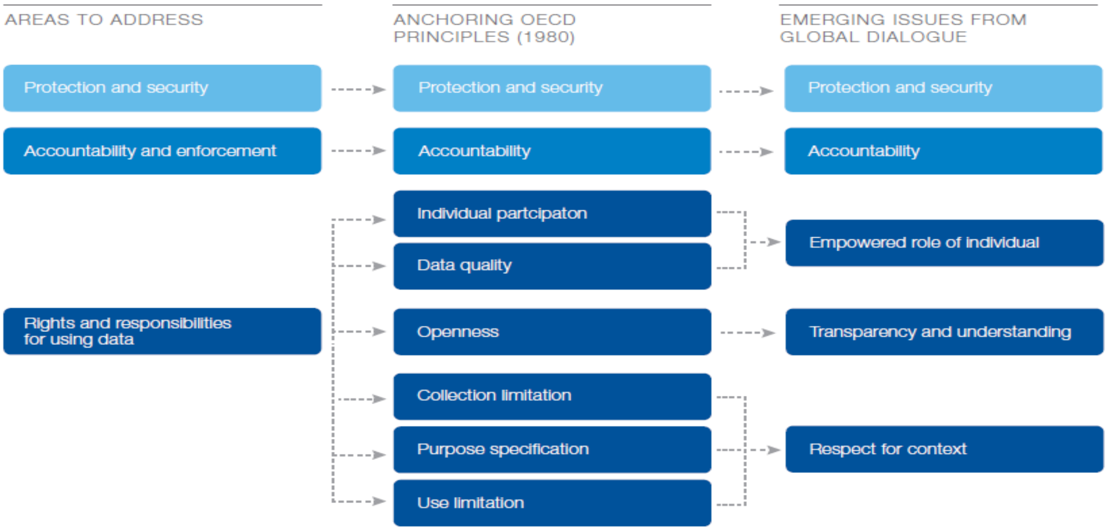

Fig. 1. OECD Privacy Principles for Personal Information (Source: World Economic Forum, 2013)

The following privacy principles are discussed (Table 1): such as Notice, Consent, Collection Limitation, Sensitivity, Access & Corrections, Data Quality, Anonymity, Accountability, Use, Limitation, Security & Safeguards, Enforcement, Disclosures, Openness, and Transborder Data Flow. Privacy requirements give us control over personal information by requiring organizations to obtain the consent to handle personal information about any individuals.

Table 1. International Comparison of Privacy Requirements

	Principle			Act			
First Adoption/ Last Modification	1980/ 2010	2005	2012	1995/ 2010	2000/ 2011	2008/ 2013	Quality
Privacy Requirements	OECD Guidelines	APEC Framework	EU Directives	Taiwan PIPA	Canada PIPEDA	Australia APL	
Notice	Yes	Yes	Yes	Yes	Yes	Yes	6
Consent	Yes	Yes	Yes	Yes	Yes	Yes	6
Collection Limitation	Yes	Yes	Yes	Yes	Yes	Yes	6
Sensitivity	N/A	N/A	Yes	Yes	N/A	Yes	3
Access & Corrections	Yes	Yes	Yes	Yes	Yes	Yes	6
Data Quality	Yes	Yes	Yes	Yes	Yes	Yes	6
Anonymity	N/A	N/A	N/A	N/A	N/A	Yes	1
Accountability	Yes	Yes	Yes	Yes	Yes	N/A	5
Use Limitation	Yes	Yes	Yes	Yes	Yes	Yes	6
Security & Safeguards	Yes	Yes	Yes	Yes	Yes	Yes	6
Enforcement	N/A	Yes	Yes	Yes	Yes	N/A	4
Disclosures	N/A	Yes	N/A	Yes	Yes	Yes	4
Openness	Yes	Yes	Yes	Yes	Yes	Yes	6
Transborder Data Flow	Yes	Yes	Yes	Yes	N/A	Yes	5

Note: 1. Privacy requirements are divided into the following two types: Principle and Act. 2. 'Yes' does match that statement, and others are 'N/A'.

Brief comments on these privacy principles or acts are listed below [2, 17].

- The logic is ambiguous;
- The order of provisions is confusing;
- The key concepts are not clearly defined or fully clarified;
- The contents of right to information privacy have not been unambiguously announced;
- The obligations of organizations are not well articulated.

3 Discussions and Analyses

This section describes Taiwan legislation and privacy concerns on personal information protection, and further focuses on online management requirements.

3.1 Taiwan Legislation on Personal Information Protection

The public issues of privacy protection attract some attention in the years ahead. There is a shift trend from individual theft to organization theft. Hackers no longer steal our individual identities once at a time, but they steal large sets of customer or employee information from compromised organizations. For example, in 1998, the U.S. Congress enacted the Children's Online Privacy Protection Act to regulate the online collection and use of children's personal information [16]. Taiwan is one of the pioneering states in adopting statues for protecting personal information. More and more countries are either implementing or considering laws that heighten data security, breach notice, and general notice/choice obligations.

In 1995, the Legislative Yuan of Republic of China in Taiwan enacted the Computer-processed Personal Information Protection Act (CPIPA) to regulate the collection and use of digital personal information. Further, in 2010, this CPIPA is amended as Personal Information Protection Act (PIPA) to govern the collection, process, use and transmission of personal information. The PIPA provides comprehensive regulation of personal data for all data users. The previous CPIPA legislation only covered public agencies and specific industry sectors, and only in relation to the processing of data in electronic form. The PIPA scope is also broadened, and the definition of data will no longer be limited to "computer-processed data" [17].

Personal information protection act has gone into effect. Penalties for the unlawful disclosure of personal information are increased. Individuals or enterprises who profit from the collection, process, use or transmission of personal information will be fined no more than NT$1 million (up from NT$40,000) or face a term of imprisonment of up to five years (up from two years). Finally, the filing of legal proceedings is permissible under the new PIPA.

3.2 Privacy Concerns from Taiwan Legislation

Since information systems collect personal information, they are also subject to privacy laws and regulations if the respective individuals are identifiable. Due to the proliferation of innovative information technologies, various privacy issues have been raised and have attracted substantive attention in society [9]. The technical developments in information processing can be summed up in terms of increasing electronic interpenetration of organizational spheres. This process involves greater utilization of information processing across organizational boundaries. It both diminishes and enhances the personal privacy by automated control mechanisms. Much of contemporary, economic activity is based on the production and exchange of information [21]. Privacy concerns are raised when the personal information of individuals is obtained. Governments worldwide have promulgated legislation to protect individual privacy. The PIPA provides a boost to the protection of privacy and personality rights. This study tries to formalize how to follow the information security guidance on the quantity of personal information. Organizations have better to at least take certain measures in response to privacy protection.

With technological advancements, information may be collected, processed, used and transmitted more efficiently than ever before. Figure 2 illustrates some data privacy requirements in the life cycle stage of personal information protection [14]: collect, process, use and transmit. It increasingly becomes a part of organization assets [18]. Organizations should make personal information policies clear, understandable and readily available. To support proper privacy protection, certain properties must be ensured from each life cycle stage of personal information. These activities are explored from life cycle stage, data privacy issue, and privacy requirements (Table 2) [3, 17, 19].

(1) Collect: Individual Choice

The term "collect" means to obtain the individual notice or consent when organizations handle personal information by any direct or indirect means. An organization should notify all identified data subjects about the purposes for which personal information is collected and used. If the information is collected, it is essential to have the consent of the individual. The collection of personal information must be reduced to a minimum.

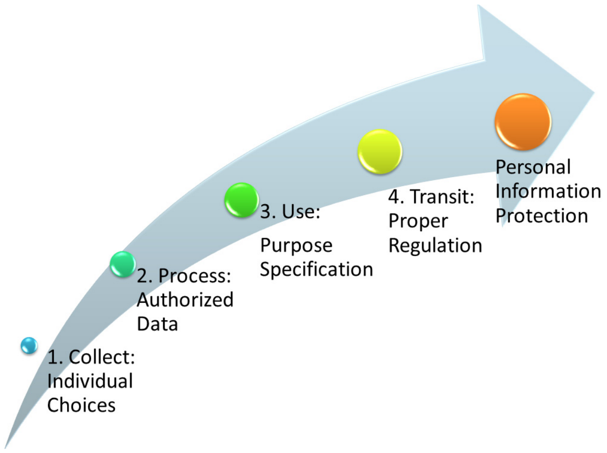
1. Collect: Individual Choices
2. Process: Authorized Data
3. Use: Purpose Specification
4. Transit: Proper Regulation
Personal Information Protection

Fig. 2. Data Privacy Requirements in the Life Cycle Stage of Personal Information Protection

Table 2. Online Managements for Meeting Privacy Requirements

Online Personal Information Managements			Privacy Requirements						Quality
			Principle			Act			
Life Cycle Stage	Data Privacy Issue	First Adoption/ Last Modification	1980/ 2010	2005	2012	1995/ 2010	2000/ 2011	2008/ 2013	
		Privacy Requirements	OECD Guidelines	APEC Framework	EU Directives	Taiwan PIPA	Canada PIPEDA	Australia APL	
Collect	Individual Choice	Notice	Yes	Yes	Yes	Yes	Yes	Yes	6
		Consent	Yes	Yes	Yes	Yes	Yes	Yes	6
		Collection Limitation	Yes	Yes	Yes	Yes	Yes	Yes	6
		Sensitivity	N/A	N/A	Yes	Yes	N/A	Yes	3
Process	Authorized Data	Access & Corrections	Yes	Yes	Yes	Yes	Yes	Yes	6
		Data Quality	Yes	Yes	Yes	Yes	Yes	Yes	6
		Anonymity	N/A	N/A	N/A	N/A	N/A	Yes	1
Use	Purpose Specification	Accountability	Yes	Yes	Yes	Yes	Yes	N/A	5
		Use Limitation	Yes	Yes	Yes	Yes	Yes	Yes	6
		Security & Safeguards	Yes	Yes	Yes	Yes	Yes	Yes	6
		Enforcement	N/A	Yes	Yes	Yes	Yes	N/A	4
Transmit	Proper Regulation	Disclosures	N/A	Yes	N/A	Yes	Yes	Yes	4
		Openness	Yes	Yes	Yes	Yes	Yes	Yes	6
		Transborder data flow	Yes	Yes	Yes	Yes	N/A	Yes	5

Note: 1. Privacy requirements are divided into the following two types: Principle and Act. 2. 'Yes' does match that statement, and others are 'N/A'. 3. Online managements are explored into the following four types: data governance, capable people, efficient process, and effective technology.

(2) Process: Authorized Data

The term "process" means to deal with the authorized data. An individual can request an organization to provide the individual with access to personal information. The personal information is provided to persons who are authorized to record, input, store, correct, duplicate, retrieve, delete, or output information for the process purpose.

(3) Use: Purpose Specification

The use of personal information should be disclosed for specific purposes. Right of use includes the right to obtain a copy of personal data by the relevant application form [3, 8]. Inquiries and requests regarding access and correction can be directed to the organization. An organization must make a reasonable effort to ensure that any personal information collected, used, processed or transmitted on behalf of an organization. The use right should be reasonable for the organization's purposes in dealing with the data.

(4) Transmit: Proper Regulation

Data transmission is the physical transfer of an electromagnetic signal over a point-to-point or point-to-multipoint communication channel. Special care should be taken due to the legal and administrative rules. Some information might be easily linked to a particular individual, and could be readily available to the public by proper regulation. An organization must protect personal information under its control and make reasonable security arrangements against some risks (e.g. unauthorized access, copying, modification or disposal).

3.3 Online Managements for Meeting Privacy Requirements

Taiwan's PIPA sets out the ground rules for how a government or non-government organization may collect, process, use or transmit information about any person. It strikes a balance relationship among data stakeholders. For non-government organizations, the main end of increased efficiency is typically economic gains. For government organizations, improved efficiency serves other goals as well. Personal information can be collected, processed, used or transmitted by information systems explicitly and implicitly [17]. Information security is increasingly recognized a crucial concern in organization management for risk handling operation. Internal audit activities are often funded to tackle high risk areas of individual choice, authorized data, purpose specification, and proper regulation. Privacy has been recognized as a fundamental human right. Despite its importance, the concept of privacy is difficult to grasp. This win-win situation is undermined by privacy concerns. It is important to reconsider how these requirements can be appropriately practiced in nowadays framework [20]. Existing and emerging legislation, practices, and procedures should be brought into compliance with the above privacy requirements.

4 A Proposed ICT Governance Framework in Online Data Privacy Management

The proposed ICT governance framework in online data privacy management is divided into three categories (Fig. 3): primary activities of manageable facets, secondary activities of relational stakeholders, and tertiary activities of positional concerns. Primary activities of manageable facets include: data governance, capable people, efficient process, and effective technology. Those facets contribute to bridging the gap between online privacy management and legal framework from research and development [3, 7, 10]. It provides a basis for proper understanding of the current state of privacy requirement with a focus on the online management.

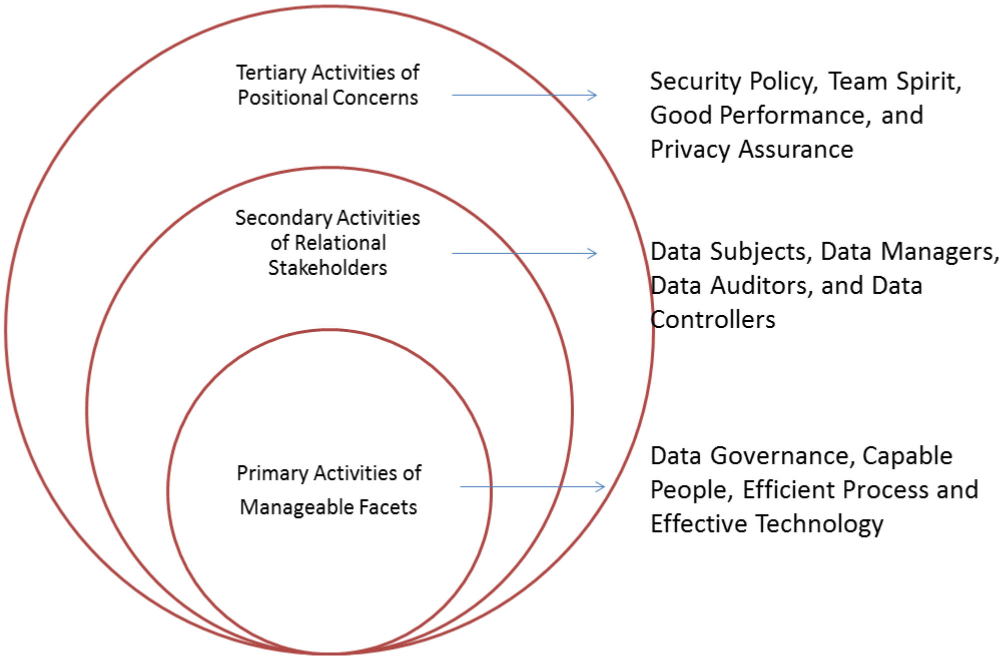
Tertiary Activities of Positional Concerns
Security Policy, Team Spirit, Good Performance, and Privacy Assurance
Secondary Activities of Relational Stakeholders
Data Subjects, Data Managers, Data Auditors, and Data Controllers
Primary Activities of Manageable Facets
Data Governance, Capable People, Efficient Process and Effective Technology

Fig. 3. Three Key ICT Activities in Online Management Framework

Secondary activities of relational stakeholders include data subjects, data managers, data auditors, and data controllers. The ICT governance framework is discussed to analyze online privacy management within an organization strategy development. It draws upon organizational management policies to derive four stakeholders that determine the privacy requirements and online managements of an organization.

Tertiary activities of positional concerns provide structure to governance deployment in the virtual workplace, which can be further explored by the following positional concerns: security policy, team spirit, good performance, and privacy assurance. This framework is vertical and horizontal integration in Fig. 4. This framework supplements the existing conceptions of people, process, technology and governance in vertical integration. It also incorporates manageable, relational and positional issues in horizontal integration. Organizations can use this framework as a reference of privacy requirement and online management.

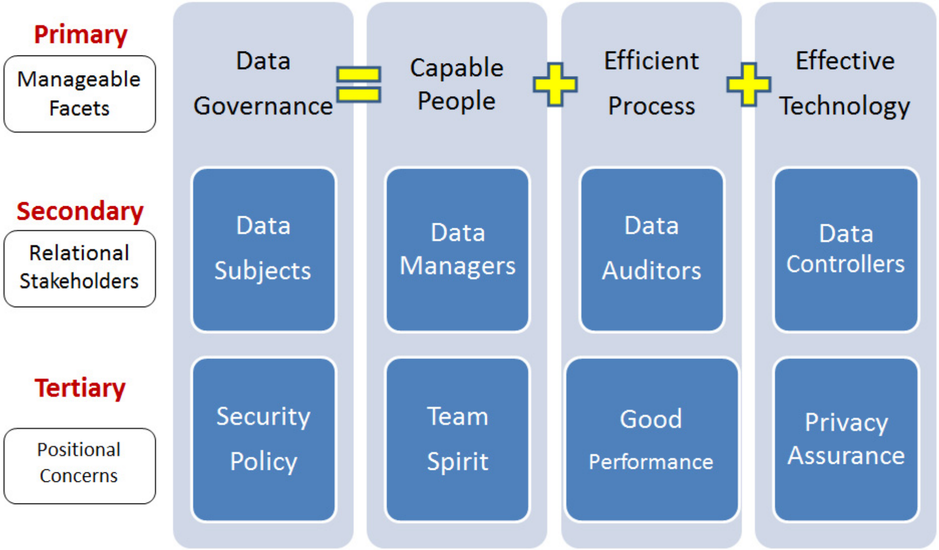

Fig. 4. A Proposed ICT Governance Framework in Online Data Privacy Management

4.1 Primary Activities of Manageable Facets

The manageable facet of data governance is implemented by capable people, efficient process and effective technology (Fig. 5). Every organization may face some problems. No single people, technology or process change can remove all of the constraints that prevent organizations from optimizing their performance and efficiency. Capable people, efficient process and effective technology can be addressed through a systematic review of data governance (Fig. 5). Data governance requires tighter integration between the above three core facets. These are critical to an organization's success [5]. Data governance, capable people, efficient process and effective technology play effective roles in information security but they require a balance among them. Their management activities are discussed below [1, 5, 7].

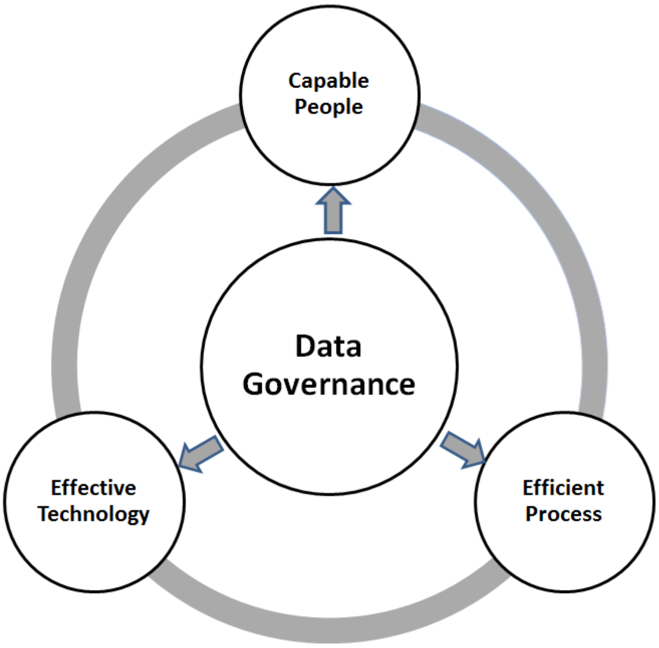

Fig. 5. Data Governance in ICT Framework

(1) Data Governance

Data governance is a process of planning to implement the use of information technology. It has become crucial for risk mitigation action. The activity of protecting data must be the first and foremost of achievement in any security programs. The pressure to secure personal information seems to demand tight controls. Data governance is not simply about managing an organization's data but also describing processes to handle information. It may be trusted, secured, and utilized by an entire organization.

(2) Capable People

Capable people are accountable for organization performance and consider how information systems work together to support performance objectives. This can only be achieved to minimize ongoing operating problems when efficient process and effective technology are in place to achieve the efficiency, availability and agility in an organization. Electronic access to personal information should be enabled. Operators of information systems have to ensure that data subjects are sufficiently informed about any incidental events. It is necessary to secure information systems in a way that only authorized entities have access to personal information.

The support for organizational process and policy changes requires significant training and proper communication with a carrot-and-stick performance practices. To accomplish a governance state, significant behavioral change will likely be required across workforce ecosystems. These following essentials help us find a proper way to handle capable people [11, 19].

- Help organization achieve success through the motive staff;
- Look for ways to enhance staff productivity;
- Write a staff handbook, and establish a streamline processes;
- Prioritize specific requirements;
- Meet the critical organization needs;
- Deliver exceptional outcomes.

(3) Efficient Process

Online privacy management and data handling are important issues for an organization. Information systems should be designed in accordance with the aim of processing as little personal information as possible. When concerns or questions are raised about online management, privacy requirements seek to establish an appropriate electronic process. The effectiveness of online management should be aligned with organization strategy through a well-defined process. The management requires the efficient process element to identify, measure, manage, and handle risk as well as to ensure integrity, availability, confidentiality and accountability.

(4) Effective Technology

There have been decades of debate on how personal data values and legal obligations can be embedded into information systems. An information system should provide data subjects with effective means of controlling their personal data. The effective technology is composed of tools, applications and infrastructure for process efficiency. The possibilities regarding consent and objection should be supported by technological means. While capable people and efficient process are critical to an organization's success, advanced collaboration technology can be truly transformational.

Techniques can provide guarantees that the implementations of ICT governance framework are sound. Effective technology provides individuals with new possibilities to collect data with the requirement of little human interaction from a technological perspective. The security of information systems should be reassessed periodically, as the requirements of cyber security vary over time. This raises serious concerns on personal privacy protection. Right technology utilization creates a foundation for continuous return on capital and cost-effective growth [7]. The technology facet is covered as an essential part of the online environment. This leads to a situation where computer programmers try to improve the application software in order to comply with the existing law.

4.2 Secondary Activities of Relational Stakeholders

Many security and privacy-protecting technologies have a plethora of different features. The complexity of these technologies needs to be reduced and analyzed from various stakeholders [13]. ICT governance in this context refers to the following four stakeholders in personal information management (Fig. 6): data subjects, data managers, data auditors, and data controllers. Personal information management is an important emerging area of study on how people store, handle, manage and re-find personal information to support their needs and tasks. Four-stakeholder analysis is a critical component to the successful delivery of online privacy management activity. Four stakeholders are affected below [1, 2, 8].

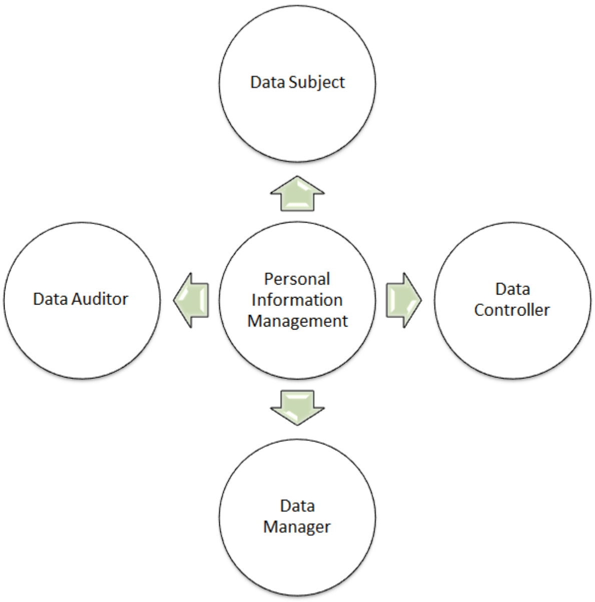

Fig. 6. Four Stakeholders in Personal Information Management

(1) Data Subjects

Data subjects are the individuals who are the subject of personal information. An organization needs a framework in information technology to obtain reliable data from data subjects, and to develop high quality of system information performance for data subjects [10]. Data subjects should be allowed to access their data and make corrections to any inaccurate data.

(2) Data Managers

Data managers must lead, inspire, and encourage staffs. Sometimes they have to hire, fire, or evaluate them. Making personal information an organization asset is almost a major culture shift for most organizations. Data managers have to set up their teams, and build the sense of team spirit within an organization to function effectively as a whole.

(3) Data Auditors

Data auditors may review the origin, creation or format of data to assess its value and utility. To ensure the reuse of organizational knowledge, adequate recordkeeping is essential. A data audit refers to the auditing of data to assess its quality or utility for the purpose of privacy management.

(4) Data Controllers

Data controllers decide the manner in which personal information gets processed. They determine the purposes and means of data processing. Online applications, services and processes are increasingly carried out in a digital working environment. Data controllers must have a lawful basis or legitimate interest in information management as it affects the organization operations. They are also responsible for implementing appropriate measures to protect the personal information against unauthorized disclosure.

4.3 Tertiary Activities of Positional Concerns

Personal information is supposed to be circulated between and modified by different users within an organization. Organizations should adjust developing strategies and evaluation focus timely. All privacy-intrusive breaches must be subject to controls or sanctions, because privacy protection is a key factor of success operation. The personal information issues in online management should periodically introduce new concepts and terminology to respond to emerging issues and to keep its message fresh [18, 19]. It guarantees that personal data are handled in such a manner as to ensure that they are safe from unforeseen, unintended, unwanted or malevolent use.

(1) Security Policy

A security policy is a legal statement that declares an organization's policy on how it gathers, discloses, and manages personal information. It fulfills a legal requirement to protect data privacy. The content of a security policy depends upon the applicable law. The development of security policy is believed to [14, 15]:

- Understand the privacy requirements;
- Ensure about the legality of a decision;
- Transform security policy into an efficient application;
- Deliver a data governance solution within organizations;
- Reduce ICT costs of maintaining personal information protection.

(2) Team Spirit

Having a good support team in place is an important step in online privacy management. Building team spirit is always one of the major objectives in an organization to achieve as a data manager. Team spirit is about supporting a team. Organizations should assess the ICT internal staff's abilities to perform tasks. ICT staffs should efficiently support future organization growth. Yet the problems of the past incapable people, inefficient process and ineffective technology hold many organizations back from keeping forward [7]. Organizations must ensure that their ICT support teams work as one to maintain consistent quality of service at a consistent quality level. ICT support teams must follow repeatable steps for each event, and ensure that critical functionality is maintained in efficient process. The following is useful for data managers and team spirit [15, 20].

- Create and maintain an understanding for team spirit;
- Realize the need of continuous change for data subjects;
- Use social networks to encourage clear communication;
- Ensure an enabling support culture.

(3) Good Performance

Good performance is always followed by some efficient processes. Poor process management has created many problems. Process inefficiencies can rob an IT organization of its agility, divert human resources from strategic pursuits, and introduce vulnerabilities that lead to downtime [7]. Data auditors conduct a data examination to assess the performance of standard operation process. The audit process is a willingness to improve operating activities. This involves profiling the data and analyzing the impact of poor quality data. In efficient process facet, the development of standard operation process for data auditors includes [2, 7]:

- Ensure data integrity;
- Create a help desk support;
- Support the end-to-end stewardship processes;
- Determine a mature, sustainable operation process;
- Provide a solution to maximize the competitive advantage.

(4) Privacy Assurance

Privacy deals with personal information that identifies the preferences of a person. The identity of an individual plays a role if it influences his or her choice. The choices reveal personal preferences [6]. It represents some unique essences in the virtual workplace. Privacy requirements are dedicated to protecting organizations and individuals against data loss or identity theft [16]. Any collected personal details are available to that organization. Data subjects are worried about how their information is handled, how privacy is assured, and what information is provided to others. The need for network accessibility and the use of social networks were identified as a requirement. The follow-up controls must be subject to review periodically in effective technology facet [13, 14].

- Identify the enabling technologies;
- Develop skilled resources;
- Determine standardized integrated tools;
- Maintain streamlined network accessibility.
- Evaluate the dependent systems which must be governed.

5 Conclusions and Future Works

An increasing number of users utilize Internet services as an essential part of their daily lives. Users increasingly store, collect, and exchange data on the Internet. The area of personal information is fast-evolving. Identifying the potential privacy violation is almost a difficult problem as any security breaches of personal information might have unexpected consequences. According to the analysis of privacy concerns from Taiwan legislation, this paper explores privacy requirements of personal information (Table 1), explores the life cycle stage of personal information protection (Fig. 2), and proposes an ICT governance framework (Fig. 4). If the proposed ICT governance framework is effectively implemented and maintained, the following benefits will be realized: (1) Improved achievement of organization goals; (2) Appropriate security measures to protect personal information; (3) Improved data governance trust between people, process, and technology; (4) Continuous improvement of stakeholder communication; (5) Improved effective processes through ICT-enabled access; (6) Improved return on effective technology investment.

Due to the decrease in calculation and storage costs, new challenges to big data have emerged. Big data refers to datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyze. Both government and non-government organizations are making increasing use of big data analytics. Within the framework of this study, further studies may concentrate on big data and case study in online management strategies.

Acknowledgments

This research was partially supported by the Ministry of Science and Technology of the Republic of China under the Grant MOST 103-2221-E-015-003-.

References

[1] Asia-Pacific Economic Cooperation, “APEC Privacy Framework,” April 26, 2015. Available at: http://www.apec.org/Groups/Committeeon-Trade-and-Investent/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

[2] Australian Law Reform Commission, “For Your Information: Australian Privacy Law and Practice (ALRC Report 108),” April 26, 2015. Available at: http://www.alrc.gov.au/publications/report-108

[3] Canada Minister of Justice, “Personal Information Protection and Electronic Documents Act 2000,” April 26, 2015. Available at: http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

[4] D. A. Chevers, and J. E. Chevers, "The Impact of Information Technology Material Weakness on Corporate - Governance Changes in Family-Owned Businesses," *International Journal of Business and Social Science*, Vol. 5, No. 6(1), pp.87-96, 2014.

[5] G. Danezis, J. D. Ferrer, M. Hansen, J. H. Hoepman, D. L. Metayer, R. Tirtea, S. Schiffner, "Privacy and Data Protection by Design – from Policy to Engineering," Heraklion, Greece: European Union Agency for Network and Information Security (ENISA), pp. 16-31, December 2014.

[6] C. Dartiguepeyrou, "The Futures of Privacy," France: Foundation Telecom, pp. 47-94, February 2014.

[7] Emerson Network Power, “Integrating People, Process and Technology to Transform Data Center Operations and Performance - A White Paper on Data Center Efficiency,” pp. 1-12, 2013.

[8] European Commission, “Proposal for a Regulation of The European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation),” April 26, 2015. Available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[9] M. Kaushik, A. Jain, "Challenges to Big Data Security and Privacy," *International Journal of Computer Science and Information Technologies (IJCSIT)*, Vol. 5, No. 3, pp. 3042-3043, 2014.

[10] G.A.T. Krisanth, I. M. Sukarsa, and I. P. A. Bayupati, "Governance Audit of Application Procurement Using COBIT Framework," *Journal of Theoretical And Applied Information Technology*, Vol. 59 No. 2, pp. 342-351, 2014.

[11] T. M. Lenard, P. H. Rubin, *Privacy and the Commercial Use of Personal Information: The Case of Customer Proprietary Network Information*, Washington, D.C.: Technology Policy Institute, pp. 1-12, 2007.

[12] Organization for Economic Co-operation and Development, “OECD Privacy Principle,” April 26, 2015. Available at: http://oecdprivacy.org/

[13] B. H. Patel, A. N. Shah, "Overview of Privacy Preserving Techniques and Data Accuracy," *International Journal of Advance Research in Computer Science and Management Studies*, Vol. 3, No. 1, pp.135-140, 2015.

[14] C. Y. Peng, *Online Data Security Model of Personal Information Protection*, Master Thesis, Graduate Institute of National Department, College of Social Sciences, National Taiwan University, 2013.

[15] A. P. Shah, *Report of the Group of Experts on Privacy*, Planning Commission, Government of India, 2012.

[16] G. Stevens, *Privacy Protections for Personal Information Online*, Washington, DC: Congressional Research Service, pp. 1-12, 2011.

[17] Taiwan Ministry of Justice,” Personal Information Protection Act,” May 26, 2010. Available at: http://pipa.moj.gov.tw/

[18] S. Tamura, “Electronic Governance Systems,” *Anonymous Security Systems and Applications: Requirements and Solutions*, Pennsylvania: IGI Global, pp. 219-243, 2012.

[19] USA White House, “National Strategy for Trusted Identities in Cyberspace - Enhancing Online Choice, Efficiency, Security, and Privacy,” April 26, 2015. Available at: https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

[20] World Economic Forum, “Unlocking the Economic Value of Personal Data-Balancing Growth and Protection,” *Rethinking Personal Data Project, Workshop Summary*, Brussels, 2012.

[21] World Economic Forum, “Unlocking the Value of Personal Data: From Collection to Usage,” *Collaboration with The Boston Consulting Group*, Industry Agenda, 2013.