A Novel Executable Framework for Protecting Personal Information at Risk: Taiwan Experiences

Da-Yu Kao, Central Police University, Taiwan
Cheng-Yu Peng, National Police Agency, Taiwan

The Asian Conference on Business & Public Policy 2014
Official Conference Proceedings

Abstract

Both government and commercial organizations are collecting personal data about individuals at an increasing rate. Online attacks against computer systems are also on the increase and are increasingly considered a risk for these organizations. It's about time to manage privacy and security of on-line information by reviewing their relevant laws and regulations. Privacy concerns have resulted in laws and regulations including Taiwan's Personal Information Protection Act (PIPA). By taking a proactive stance towards privacy invasion, organizations can help stave off excessive government intervention to tighten controls over what can be done with an individual's personal data. This proposed P-P (Performance Evaluation - Policy Management) framework is divided into two phases: Performance Evaluation and Policy Management. This framework is presented to provide guidance for managers tasked with implementing an organization's privacy policy. The study closes with recommendations for privacy and security best practices for information managers. We anticipate collateral benefits for law enforcement in the cybercrime investigation of data leakage.

Keywords: Personal Information Protection Act, Information Security, Performance Evaluation, Policy Management

1. Introduction

Due to the rapid growth of digital data, the demands for personal information as a thing of value have also increased. Users are often unaware of the fact that their data is being collected and processed for various reasons. These include consumer behavior analysis, personalized advertisement, opinion mining or profiling (Theoharidou and Gritzalis, 2007). There is a widespread lack of suitable strategies to respond to the digital revolution, and personal information protection strategies are in urgent need of reform. Due to the ease of rapid conversion, convenient transmission and widespread access, common information security mechanisms do not provide users with a high degree of control over their resources at runtime (Chakraborty, Shen, Raghavan, Shoukry, Millar, and Srivastava, 2014). Recent media attention to information protection issues has shown that people are increasingly concerned about their rights to protection of their personal information. On-line information privacy is important. People desire more control over their information and the subsequent use (e.g., collection, process, use, and transmission). A proactive stance against privacy invasion can also help stave off government intervention to tighten controls over what can be done with an individual's personal information. It's about time to manage privacy and security of on-line information by reviewing the relevant laws and regulations. It is increasingly becoming an organization's most important assets as well as a significant potential liability.

Since there is no comprehensive privacy statute that protects on-line personal information, it is about time to pay more attentions on privacy enhancement (Wang and Kobsa, 2009). A patchwork of laws and regulations is always insufficient to meet the demands of on-line privacy. Privacy has different aspects or dimensions: informational, physical, decisional, proprietary or relational. This study focuses primarily on informational privacy, which fits well within the general definition of privacy as a condition of limited access to an individual or information about an individual (Rothstein, 2014). Concerns of privacy harm have resulted in laws and regulations. Any discussion of the privacy laws in Taiwan, especially privacy of personal information, should start with the Computer-processed Personal Information Protection Act (CPIPA) in 1995. The Taiwan Legislative Yuan passed an amendment to the CPIPA on April 27, 2010 and promulgated as the Personal Information Protection Act (PIPA). The amendment broadens the scope of the act, and the definition of data is no longer limited to "computer-processed" data. The act applies to all individuals and organizations. The act imposes costs. 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 between personal right to control access to and use of personal information for legitimate and reasonable purposes.

The related works are discussed in Section 2. Section 3 presents a case scenario and its analyses. The P-P (Performance Evaluation - Policy Management) framework of privacy enhancement is proposed in Section 4. The conclusion is drawn in Section 5.

2. Reviews

This section gives a broad overview of the legal and practical issues. It also presents a literature review on the following personal information issues (Chakraborty, 2002;

TW Ministry of Justice, 2010): Urgent Needs to Enhance Privacy Control, Protective Guidelines of Personal Information, and Potential Features of Taiwan PIPA.

2.1 Urgent Needs to Enhance Privacy Control

Organizations are growing to incorporate almost everything available on the web. The ability to gather much information on individuals is largely because of advances in on-line technology. It is important for information system managers and professionals to understand the issues surrounding personal information protection in order to protect the rights of those from and about whom they collect data. We are facing a research challenge and an engineering challenge to make data protection a competitive advantage. We need formal frameworks not for their own sake, but for privacy assurances we can count on. We need models and tools to cope with diverse privacy attitudes. And, we need experiments to learn and gain insight from consumers' on-line privacy choices.

2.2 Protective Guidelines of Personal Information

The central rules of the PIPA are based upon a set of protective guidelines, which can be summarized in Table 1 (Bygrave, 2002; Online Trust Alliance, 2014):

Table 1: Protective Guideline of Taiwan PIPA

Purpose	Organizations	Individuals
Necessary	Fair Means	Individuals' Consent
Collected	Lawful Means	Informed Individuals
Processed	Security Measures	Responsible Individuals

(1) Purposes

Organizations must state their purpose for data collection, and explain how the personal information will be used. The use of personal information must be aligned with the stated purpose and be justifiable to meet that purpose.

- Necessary purposes: The collected amount of personal information should be necessary to achieve the purposes for which the data are gathered and further preceded.
- Collected purposes: Personal information should be collected for specified, lawful, legitimate purposes.
- Processed purposes: Personal information should be relevant, accurate and complete in relation to processed purposes.

(2) Organizations

- Fair and lawful means: Personal information should be collected by fair and lawful means.
- Security measures: Security measures should be taken to protect personal information.

(3) Individuals

- Individuals' consent: Organizations will be required to advise an individual that their information is collected, and shall obtain the written consent of the affected individual.
- Informed individuals: Persons should be informed of, and given access to information.
- Responsible individuals: Those who are responsible for handling personal information should be accountable for implementing controls in accordance with the above principles.

2.3 Potential Features of Taiwan PIPA

Personal information also has a dark side in the background. People are increasingly becoming a data source for various stakeholders (Thomas, 2014). Personal information includes a natural person's name, date of birth, national identification number, passport number, physical description, fingerprints, marital status, family, education, occupation, medical records, medical history, genetic information, sex life, criminal records, contact information, financial status, social activities, and other data which is sufficient to directly or in combination with other information identify an individual person. Certain types of information require greater control including medical information, genetic information, sex life, examinations and criminal records. Personal information in these categories may only be collected, processed, used or transmitted in specific circumstances. The act excludes personal information accessed during private and family activities and the posting of information or group photos on Facebook, twitter, blogs, or social network websites from prior consent requirement. The potential features of Taiwan PIPA can be explored from the following attributes (TW Ministry of Justice, 2010).

(1) Sanctions against Data Controllers

The act grants authorities various means to sanction data controllers who violate the act unless data controllers can prove that they took measures to prevent the violation.

(2) Impose Fines

Criminal liability is initiated where a data controller illegally collects, processes, uses, or transmits personal information in a way that is likely to harm an individual. Under the act, authorities may impose fines ranging from NT$ 20,000 to NT$ 500,000 on offenders. The act increases criminal penalties for violations with intent to profit. Where such illegal activity is undertaken with intent to profit, offenders face more severe punishments including imprisonment of up to five years and fines of up to NT$ 1 million.

(3) Recovery for Damages

An injured party may claim actual and non-pecuniary damages. The maximum damages may be claimed is NT$ 2 million. An injured party may also claim measures to restore reputational damage. The act allows for class action whereby 20 or more

claimants may collectively bring suit through a foundation or public interest association.

3. Case Study of Extortion Ring

The internet facilitates criminal activity both directly and by making it easier to seek out potential victims. The following scenario of extortion ring case, which is based on lots of personal information, is presented. This example is intended to help organizations better understand the risks of data loss. It is observed that personal information is very critical to explore their potential victims as far as any criminal rings are concerned. It is also an urgent need to explore a wide variety of contexts in which PIPA can be implemented to safeguard this information.

3.1 Scenario: CIB Arrests Four Suspects for Online Extortion

The scenario of this case is:

(1) Original Police Complaint

A large on-line retailer in Taiwan had experienced a leak of customer data dating back to 2011. The extortion ring contacted the organization in November 2013. They threatened to release personal information of the organization's customers unless they paid ransom. The organization contacted law enforcement and said that several unidentified individuals had been threatening to release the above-mentioned data on the internet for potential misuse by criminals. Although the organization sent out a press release to contain the incident, they continued to receive threats.

Communication with the organization included email. Email clients often contain header information showing the origin and route of the message. The CIB was able to trace through the email headers back to the extortion ring. On January 27, 2014, Criminal Investigation Bureau (CIB) mobilized 20 police officers to conduct raids in Taiwan, and arresting 4 suspects (Taiwan Criminal Investigation Bureau, 2014).

(2) Data Loss

The customer information fell into two categories. Personal identification data (which can be used to transact with government or non-government organizations under an assumed identify) and financial data (which can be used to conduct secure electronic payments and related financial transactions). Both types of information would be of interest to criminal actors.

(3) Promulgate PIPA in Taiwan

Monetary fines and penalties are traditionally integral to punishment / deterrence in most democratic societies. Prior to Taiwan's revised PIPA (which took effect in October 2012), criminal and civil liability arising from leakage of information was not a strong part of the legal system. With possible fines of up to US $500,000, PIPA significantly raised the costs of information disclosure whether intentional or unintentional. In this case, the extortion ring was able to hold this penalty over the victim's heads in order to coerce them into paying ransom. Although the original fines

were designed to deter or prevent data loss, in this case, they had the unintentional effect of enabling the extortion ring.

3.2 Case Analyses: New Threats on the Internet

Nowadays, instead of writing letters or making a telephone call, people communicate with each other on Facebook, Twitter, Line, Whatsapp or other online social networking websites. We should use our skills and expertise to restore privacy and freedom to the internet. The following analyses of personal information are conducted to address the changing role of the internet (Jaishankar, 2011; Jone, Bejtlich and Rose, 2006; National Institute of Justice, 2007).

(1) Find Online Victims

Every day, privacy on-line is eroded against our will. People are losing control over the dissemination of their information. This has assisted many criminals in planning extortion and other crimes. How can extortion rings find victims? Computer networks contribute to a greater flow of information. The internet provides a comprehensive tool that is accessible to everyone. The internet has the advantage of protecting offenders' identity, and allows offenders to monitor victims' activities.

(2) Shared Information

Extensive amounts of personal information are shared on the internet. With more people turning to the internet to have fun, find love, research topics, perform analysis and conduct business, offenders have started focusing more heavily on hacking, data extortion, money laundering, credit card scams, pornography, and unconventional sexuality.

(3) New Threats

Connecting computers to the internet is inherently risky. It is almost difficult to prevent the data leakage from happening. Our world is changing. The rate of changes shows no sign of slowing down. Cyber technology and personal information is neutral, but their usage can generate great value or create significant harm.

4. Proposed Framework

People want the benefits that information sharing can bring. A proper on-line privacy protection solution is necessary to enhance privacy in on-line service. Do organizations analyze the vulnerabilities (or problems) they have before addressing them? Creating and implementing a proper privacy enhancement framework become common sense. However, this kind of common sense issues are ignored due to a lack of understanding their importance. This proposed P-P framework in Table 2 is divided into two phases (Cotter, 2004; National Institute of Justice, 2007; USA White House, 2011): Performance Evaluation Phase and Policy Management Phase. Each phase is explored from the following issues: concern, strategy, and principle.

Table 2: The P-P Framework of Privacy Enhancement

Phase I	Performance Evaluation Phase	
Concern	Individuals' Privacy	Customers' Openness
Strategy	Internal Capability	External Environment
Principle	1.Internet Data Quality 2.Collection Limitation 3.Use Limitation	1.External Openness 2.Transmission Confidentiality 3.Information Sharing
Phase II	Policy Management Phase	
Concern	Controllers' Security	Auditors' Protection
Strategy	Prevention Measure	Detection Measure
Principle	1.Media Security 2.Identification and Authentication Mechanism 3.Least Privilege	1.Information System Monitoring 2.Access Control 3.Protection of Information at Rest

4.1 Performance Evaluation Phase

Individuals do not abandon their right to personal privacy or data protection. The purpose of performance evaluation focuses attention on the protection of personal information. In the following, we demonstrate the internal capability from individuals' privacy concerns, and external environment from customers' concern viewpoint (National Institute of Justice, 2007; USA White House, 2011).

4.1.1 Internal Capability: Individuals' Privacy Concerns

Protecting privacy is a vague concept. Different organizations might have completely different interests and views. The notion of privacy involves a basic sense of human dignity, which can be compromised by the proliferation of sensitive information about oneself. Trust, respect, and personal integrity are at issue. In order to deal with the issues on the internal capability of privacy concern, some proposed principles are listed below.

(1) Internal Data Quality

Personal information should be relevant to the purposes for which they are to be used, and should be accurate, complete and kept up-to-date. Individuals often seek assurance that their data is well protected.

(2) Collection Limitation

The purposes for collecting personal information should be specified. There should be limits to the collection of personal information. Any data should be obtained by lawful and fair means with the knowledge or consent of the individual.

(3) Use Limitation

Personal information should not be disclosed, made available to others except with the consent of the individual or by the authority of law.

4.1.2 External Environment: Customers' Openness Concern

In order to deal with the issues on the external environment of customers' openness concern, some proposed principles are listed below.

(1) External Openness

When controllers of sensitive datasets release data, they often reveal more information. There should be a general policy of openness about developments, practices and policies with respect to personal information. Means should be readily available of establishing the existence of personal information, and the main purposes of their use.

(2) Transmission Confidentiality

Organizations can protect the confidentiality of transmitted personal information. This is often accomplished by encrypting the communications in transmission or by encrypting the information before it is transmitted.

(3) Information Sharing

Organizations can provide automated mechanisms to assist data controllers and auditors in determining whether individuals or customers match access restrictions, such as contractually-based restrictions, for personal information. Organizations can protect digital media and mobile devices outside the organization‘s controlled areas. Organizations can choose to prohibit or strictly limit remote access to personal information.

4.2 Policy Management Phase

Organizational policies may play an important role in cyber security domain. To combat the problem an organization has to resort to the policy management phase of prevention and detection measures. In the following, we demonstrate the prevention measure from data controllers' security concern and detection measure from data auditors' protection concern (Cotter, 2004; National Institute of Justice, 2007).

4.2.1 Prevention Measure: Controllers' Security Concern

In order to deal with the issues on the prevention measure of data controllers' security concern, some proposed principles are listed below.

(1) Media Security

Organizations can restrict access to digital media containing personal information, including digital media (e.g., CDs, USB flash drives, backup tapes) and non-digital media (e.g., paper, microfilm). This could also include portable and mobile devices with a storage capability. Moreover, organizations can label digital media and output containing personal information to indicate how it should be distributed and handled.

(2) Identification and Authentication Mechanism

The requirement for the authentication mechanism depends on the impact level of the personal information and the system as a whole. Users should be uniquely identified and authenticated before accessing personal information.

(3) Least Privilege

Concerning personal information, the organization can ensure that users who access personal information only have access to the minimum amount of personal information, along with only those privileges (e.g., read, write, execute) that are necessary to perform their jobs.

4.2.2 Detection Measure: Auditors' Protection Concern

The value of data auditors is to help organization's routine surveillance and computer monitoring. That can be implemented from the basis of the surveillance data reported at the daily, weekly, monthly or six-month review. If organizations have any problem, the report of routine surveillance can be analyzed from daily auditing records. In order to deal with the issues on the detection measure of data auditors' protection concern, some proposed principles are listed below.

(1) Information System Monitoring

Organizations can employ automatic tools to monitor computer systems at network boundaries for unusual events. The log is accessed by a small number of system administrators when they troubleshoot operational problems or incidents. All access to the log occurs only from the organization‘s own systems. No remote control services are allowed.

(2) Access Control

Organizations can control access to personal information through access control policies and access enforcement mechanisms. Access control describes the collection of mechanisms that permits administrators of a system to exercise a directing or restraining influence over the behavior, use, and content of a system.

(3) Protection of Information at Rest

Organizations can protect the confidentiality of personal information at rest, which refers to information stored on a secondary storage device, such as a hard drive or backup tape. This is usually accomplished by encrypting the stored information.

5. Conclusion

Information security today must account for highly interconnected global including critical transactions taking place over the internet. Privacy violations on the internet present a significant problem, and we should try our best to minimize these in order to have a better and more secure future in cyber space. Securing information has become one of the biggest challenges nowadays. Despite laws, legislations and technical

attempts to solve the personal information protection issue, we still need to constantly defend and preserve people's data against any unauthorized disclosure. Individuals or customers have a right to ask for adequate privacy controls. An organization can use a well-designed framework to develop consumer trust, and to make better investment decisions about technology infrastructure. This proposed P-P framework is very delicate and requires deep understanding of both internal and external aspects. That framework includes the proper measures to conduct protection actions, and provides managers guidance in dealing with privacy policy. The main contributions of this study lie in analyzing the internet privacy violation, conceptualizing a novel privacy-enhanced framework, providing the privacy strategy on the internet, and improving the ability on information security. The study closes with recommendations for privacy and security best practices for information managers. That also benefits the cybercrime investigation of data leakage.

Acknowledgements

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

References

Bygrave, L. A. (2002). *Data Protection Law – Approaching the Rationale, Logic and Limits.* MA: Kluwer Law International.

Chakraborty, S., Shen, C., Raghavan, K. R., Shoukry, Y., Millar, M. and Srivastava, M. (2014). *ipShield: A Framework For Enforcing Context-Aware Privacy.* 11th USENIX Symposium on Networked Systems Design and Implementation. https://www.usenix.org/conference/nsdi14/technical-sessions/presentation/chakraborty. Retrieved May 25, 2014.

Cotter, A. M. (2004). *Law Society of Ireland - Information Technology Law*. London: Cavendish Publishing Limited.

Jaishankar, K. (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. FL: CRC Press.

Jone, K.J., Bejtlich, R. and Rose, C.W. (2006). *Real Digital Forensics: Computer Security and Incident Response.* New York: Person Education.

National Institute of Justice. (2007). *Investigations Involving the Internet and Computer Networks.* Washington DC: USA Department of Justice.

Online Trust Alliance. (2014). *Data Protection & Breach Readiness Guide.* https:/otalliance.org. Retrieved April 24, 2014.

Rothstein, M. A. (2014). Privacy and Technology in the Twenty-First Century. *University Of Louisville Law Review*, 52:333-344.

Taiwan Criminal Investigation Bureau. 2014. *Criminal Investigation Bureau News.* http://www.cib.gov.tw/News/Detail/29454. Retrieved April 24, 2014.

Thomas F. D. (2014). *Big Data – the Untamed Force.* Deutsche Bank research. http://www.dbresearch.com/PROD/DBR_INTERNET_EN-PROD/PROD0000000000334340/Big data - the untamed force.PDF. Retrieved May 25, 2014.

Theoharidou, M. and Gritzalis, D. (2007). A Common Body of Knowledge for Information Security. *IEEE Security & Privacy*, 4(2): 64-67.

TW Ministry of Justice. (2010). *Personal Information Protection Act.*Taipei: TW Ministry of Justice.

USA White House. (2011). *National Strategy for Trusted Identities in Cyberspace - Enhancing Online Choice, Efficiency, Security, and Privacy.* Washington DC: USA White House.

Wang, Y. and Kobsa, A. (2009). "Privacy-Enhancing Technologies," In Gupta, M. and Sharman, R., eds., *Social and Organizational Liabilities in Information Security.* PA: IGI Global, 203-227.

Yeung, D. and Lowrance, J. (2006). "Computer-Mediated Collaborative Reasoning and Intelligence Analysis," In S. Mehrotra et al. eds., *IEEE International Conference on Intelligence and Security Informatics, ISI 2006*. CA: Springer Press: 1-13.

Contact email: camel@mail.cpu.edu.tw