Summer 5-26-2017

An Exploratory Study on the Measuring of Privacy Policies

Lianfeng Yang
School of Economics and Management, Xiamen University of Technology,Xiamen, China

Qiuying Chen
School of Cultural Industries and Tourism, Xiamen University of Technology,Xiamen, China

Yonhong Hu
School of Economics and Management, Xiamen University of Technology,Xiamen, China

An Exploratory Study on the Measuring of Privacy Policies

Lianfeng Yang[1],*Qiuying Chen*[2],*Yonhong Hu*[3]
[1,3]School of Economics and Management, Xiamen University of Technology,Xiamen, China
[2]School of Cultural Industries and Tourism, Xiamen University of Technology,Xiamen, China

Abstract: With the development of Internet technology, individuals have become increasingly more dependent on the network. Personal information is collected by many firms when people surf online, but information collected is often misused by collectors, which may seriously violated the privacy of consumer. For this reason, a lot of government agencies and international organizations put great emphases on the development of privacy protection regulations. Companies from different parts of the globe have begun to issue privacy policies or statements on their websites, some detailed some simple. It is thus a vital task to evaluate these privacy policies and identify the degree of privacy protection. On the basis of previous studies, this article explores the dimensions of Internet privacy policy from the perspectives of personal information protection. Five dimensions of privacy policies including notice, choice, access, security and enforcement are identified and scale items for each dimensions are also proposed.

Keywords: privacy policy; privacy concern; dimensions of privacy policy; scale item

1. INTRODUCTION

Over the last three decades, the Internet has changed dramatically from a large network of computers that touched the lives of a few consumers to a new marketplace where millions of consumers shop for information, purchase goods and services, and participate in discussions. Information and communications technologies, including mobile technologies, that link to the Internet and other information networks have made it possible to collect, store and access information from anywhere in the world. These technologies offer great potential for social and economic benefits for business, individuals and governments, including increased consumer choice, market expansion, productivity, education and product innovation. However, while enabling it easier and cheaper to collect, link and use large quantities of information, these technologies also make these activities undetectable to individuals. Consequently, it can be more difficult for individuals to retain a measure of control over their personal information. Personal data is increasingly used in ways not anticipated at the time of collection, nonetheless, the security breaches are common. As a result, individuals have become concerned about the harmful consequences that may arise from the misuse of their information. Therefore, there is a need to promote and enforce ethical and trustworthy information practices in on- and off-line contexts to bolster the confidence of individuals and businesses.

In 1980, the OECD (the Organization for Economic Co-operation and Development) adopted the Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data ("1980 Guidelines") to address concerns arising from the increased use of personal data and the risk to global economy resulting from restrictions to the flow of information across borders. The 1980 Guidelines, which contained the first internationally agreed-upon set of privacy principles, have influenced legislation and policy in OECD member countries and beyond[1]. In 2013, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Trans-border Flows of Personal Data (2013) was issued.

The principal EU (European Union) legal instrument on data protection is Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), it was adopted in 1995. This directive settles down very strict rules for the protection of the rights and guarantees of freedom of

the European citizens and the protection of their right to privacy in relation to the obtaining and processing of personal data. In January 2012, the European Commission proposed a data protection reform package, stating that the current rules on data protection needed to be modernized in light of rapid technological developments and globalization. The reform package consists of a proposal for a General Data Protection Regulation, meant to replace the Data Protection Directive, as well as a new General Data Protection Directive which shall provide for data protection in the areas of police and judicial cooperation in criminal matters[2].

U.S. Federal Trade Commission had been studying online privacy issues since 1995. In its 1998 report, Privacy Online: A Report to Congress, the Commission described the widely-accepted fair information practice principles of Notice, Choice, Access, and Security. In its 1999 report to Congress, Self-Regulation and Privacy Online, that self-regulation be given more time, but called for further industry efforts to implement the fair information practice principles. In February and March 2000, the Commission conducted another survey of commercial sites information practices, using a list of the busiest U.S. commercial sites on the World Wide Web. After these surveys, the commission recommended the Congress enact legislation that would set forth a basic level of privacy protection for consumer-oriented commercial Web sites. It would establish basic standards of practice for the collection of information online, and provide an implementing agency with the authority to promulgate more detailed standards pursuant[3].

In 2005, APEC (Asia-Pacific Economic Cooperation) issued the APEC Privacy Framework. This principal-based Framework, which aims at promoting electronic commerce throughout the Asia Pacific region, is consistent with the core values of the OECD's 1980 Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data, and reaffirms the value of privacy to individuals and to the information society. It promotes a flexible approach to information privacy protection across APEC member economies, while avoiding the creation of unnecessary barriers to information flows[4].

Besides the above famous legislations or regulations about privacy, The U.S. Public Policy Council of the Association for Computing Machinery (USACM) also suggested some recommendations about protection of privacy when developing system that make use of personal information, these recommendations have been central to any development of any legislation, regulations, international agreements and internal policies that govern how information is stored and managed[5]. The Safe Harbor Privacy Principles issued by the U.S. Department of Commerce on July 21, 2000[6] and The Personal Information Protection and Electronic Documents Act published by the Canada Department of Justice on September 15, 2014[7], both of them also stipulate a series of principles to protect information privacy.

In addition to these non-government associations and countries started to pass laws and guidelines regarding the use of private information gathered online, in order to easy customer's concerns about the online privacy, companies from different parts of the globe have begun to issue privacy policies or statements on their websites. These are descriptions of site's practices for online collection, use, and dissemination of personal information, but the elaboration extent of descriptions are very different. How to assess the effectiveness of the companies' privacy policies or statement? Can we develop a scale (or instrument) to score privacy policies or statement objectively?

2. PRINCIPLES OF PRIVACY REVIEW

The legal principles of privacy are guidance for companies to establish their privacy policies. Keith Mossman suggested 10 legal principles according to the previous studies in 1975. These principles are Mutuality, Consent, Relevance, Fiduciary Duty, Notice, Access, Confidentiality, Warranty, Accuracy, and Remedy[8]. Table 1 provides the main contents of these privacy principles.

Table 1. The Keith Mossman's Privacy Legal Principles

Principle	Description
Mutuality	Both data keeper and data subject have an interest in seeking that the record is used properly.
Consent	The data subject has a right to participate in deciding the content, use, and disclosure of the record.
Relevance	Certain types of information should not be recorded. Information should be recorded if it is necessary and relevant to proper purpose.
Fiduciary Duty	(a)The data keeper owes the data subject a duty of reasonable care by providing an adequate system for the security and safeguard of the record. (b)The data keeper owes the data subject a duty of fair dealing, assuring the reliability of the data for intended use and assuring precautions to prevent misuse of data.
Notice	There must be no personal data system whose existence is secret. The subject must have a way of being informed what information exists about him or her and how it is used.
Access	The subject must be accorded opportunity to challenge and to correct the record
Confidentiality	The record shall be disseminated only to third parties who demonstrate a "need to know." Such dissemination must be audited.
Warranty	Information shall be used only for purpose for which it was collected.
Accuracy	Records would be reviewed and obsolete matter reclassified, sealed, deleted, or destroyed.
Remedy	These rights should be implemented by (a) federal or state legislation, (b)a private right of legal action, and (c) federal enforcement agencies.

Source: Based on Keith Mossman(1975, pp.831)

The OECD Privacy Framework (2013) suggest 8 basic principles of national application: Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, and Accountability. Its detailed content is presented in Table 2.

Table 2. The OECD's Basic Principles of National Application

Principle	Description
Collection Limitation	There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
Data Quality	Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
Purpose Specification	The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
Use Limitation	Personal data should not be disclosed, made available, or otherwise used purposes other than those specified in accordance with Purpose Specification except: (a)with the consent of the data subject, or (b)by the authority of law.
Security Safeguards	Personal data would be protected by reasonable security safeguards against such risk as loss and unauthorized access, destruction, use, modification, disclosure of data.
Openness	There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
Individual Participation	Individuals should have the right: (a)to obtain from data controller, or otherwise, confirmation of whether or not the data controller has data relating to them; (b)to have communicated to them, data relating to them; (c)to be given reasons if a request made under (a) and (b) is denied and to be able to challenge such denied; and (d)to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.
Accountability	A data controller should be accountable for complying with measures which give effect to the principles stated above.

Source: "Recommendation of the Council concerning Guidelines Governing The Protection of Privacy And Transborder Flows of Personal Data". OECD 2013,pp.14-16.

The European Data Protection Law (the "EDPL") was based on The Data Protection Directive and Convention 108. It summarized 5 key principles and 4 rules of data protection, Table 3 lists their names and commentaries in detail.

Table 3. The Key Principles of European Data Protection Law

Principle/Rules	Description
Lawful Processing	Accordingly, the processing of personal data is lawful only if it (a) is in accordance with the law; and (b) pursues a legitimate purpose, and (c) is necessary in a democracy society in order to achieve the legitimate purpose. Personal data may be lawfully processed if (a) the processing is based on the consent of the data subject; or (b) vita interest of the data subject require the processing of their data; or (c) legitimate interests of others are the reason for processing, but only as long as they are not overridden by interests in protecting the fundamental rights of the data subjects.
Purpose Specification and Limitation	(a) The purpose of processing data must be visibly defined before processing is started. (b) Under EU law, the purpose of processing must be explicitly defined; under CoE law, this question is left to domestic law. (c) Processing for undefined purposes is not compliant with data protection law. (d) Further use of data for another purpose needs an additional legal basis if the new purpose of processing is incompatible with the original one. (e) Transfer of data to third parties is a new purpose needing an additional legal basis.
Data Quality	(a) The data relevance principle: controller should strictly limit collection of data to such information as is directly relevant for the specific purpose pursued by the processing. (b) The data accuracy principle: a controller holding personal information shall not use that information without taking steps to ensure with reasonable certainty that the data are accurate and up to date. (c) The limited retention of data principle: to makes it necessary to delete data as soon as they are no longer needed for the purposes for which they were collected.
Fair Processing	(a) Fair processing means transparency of processing, especially vis-à-vis data subjects. (b) Controllers must inform data subjects before processing their data, at least about the purpose of processing and about the identity and address of the controller. (c) Unless specifically permitted by law, there must be no secret and covert processing of personal data. (d) Data subjects have the right to access their data wherever they are processed.
Accountability	(a) Accountability requires the active implementation of measures by controllers to promote and safeguard data protection in their processing activities. (b) Controllers are responsible for the compliance of their processing operations with data protection law. (c) Controllers should be able at any time to demonstrate compliance with data protection provisions to data subjects, to the general public and to supervisory authorities.
Security of processing	The rules on security of processing imply an obligation of the controller and the processor to implement appropriate technical and organizational measures in order to prevent any unauthorized interference with data processing operations. Data breach notification: the obligation of providers of electronic communications services to notify data breaches to the likely victims and to supervisory authorities.
The Rights of Data Subject	(a) Everyone shall have the right under national law to request from any controller information as to whether the controller is processing his or her data. (b) Data subjects shall have right under national law to: access their data from any data controller who process such data; have their data rectified (or blocked, as appropriate) by the controller processing their data, if the data are inaccurate; have their data deleted or blocked, as appropriate, by the controller if the controller is processing their data illegally. (c) Additionally, data subjects shall have the right to object to controllers about: automated decisions (made using personal data processed solely by automatic means); the processing of their data if it leads to disproportionate results; the use of their data for direct marketing purposes.
Enforcement Remedies and Sanctions	In order to ensure effective data protection, independent supervisory authorities must be established under national law. National law must set out appropriate remedies and sanctions against infringements of the right to data protection.

Source: "Handbook on European Data Protection Law". The Council of Europe and the European Court of Human Rights 2014,pp.62-77,81-126.

In APEC privacy framework, there are 9 information privacy principles: Preventing Harm, Notice, Collection Limitation, Use of Personal Information, Choice, Integrity of Personal Information, Security Safeguards, Access and Correction, and Accountability. Its detailed content is presented in Table 4.

Table 4. APEC Information Privacy Principles

Principle	Description
Preventing Harm	To prevent wrongful collection and misuse of personal information and consequent harm to individuals.
Notice	Controllers should provide clear and easily accessible statement about the fact that personal information is being collected, the purposes for collecting, the types of personal and organizations to whom personal information might be disclosed, the identity and location of the controller, choices and means the controller offers individuals for limiting the use and disclosure of, and for accessing and correcting their personal information.
Collection Limitation	The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of the individual concerned.
Use of Personal Information	Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes.
Choice	Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information.
Integrity of Personal Information	Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.
Security Safeguards	Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses.
Access and Correction	Individuals would be able to (a) obtain from the controller confirmation of whether or not the controller holds personal information about them; (b) have communicated to them, after having provided sufficient proof of their identity, personal information about them; and (c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.
Accountability	A data controller should be accountable for complying with measures which give effect to the principles stated above.

Source: "The APEC Privacy Framework". APEC 2005,pp.11-29.

The Federal Trade Commission (U.S.A) suggested in 2000 four dimensions of privacy online: Notice prior collection of data, Choice to share or use information, Access to data collected, and keeping data Secure[9]. It also identified Enforcement-the use of a reliable mechanism to impose sanctions for noncompliance with these fair information practices--as a critical ingredient in any governmental or self-regulatory program to ensure privacy online. Table 5 provides the main content of the Fair Information Practices Principles.

Table 5. FTC Fair Information Practices Principles

Principle	Description
Notice	Web sites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (e.g., directly or through non-obvious means such as cookies), how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site.
Choice	Web sites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided (e.g., to consummate a transaction). Such choice would encompass both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities).
Access	Web sites would be required to offer consumers reasonable access to the information a Web site has collected about them, including a reasonable opportunity to review information and to correct inaccuracies or delete information.
Security	Web sites would be required to take reasonable steps to protect the security of the information they collect from consumers
Enforcement	Legislation and seal program will ensure adequate protection of consumer privacy online.

Source: "Privacy Online: Fair Information Practices in The Electronic Marketplace". Federal Trade Commission 2000,pp.iii

3. DIMENSIONS OF PRIVACY POLITICIES

FTC's principles is most concise in all information privacy principles, and it is widely accepted[3]. We select FTC's principles as the basis. There are total 41 principles in all these studies about privacy principle. Excluding the same name principles① (double strikethrough in Table 6), there remain 27 principles as shown in Table 6.

Table 6. The All Principles in Above Stated Studies

FTC	Keith Mossman	OECD	EDPL	APEC
Notice	~~Mutuality~~	Collection Limitation	Lawful Processing	~~Preventing Harm~~
Choice	Consent	Data Quality	~~Purpose Specification and Limitation~~	~~Notice~~
Access	Relevance	Purpose Specification	~~Data Quality~~	~~Collection Limitation~~
Security	Fiduciary Duty	Use Limitation	Fair Processing	Use of Personal Information
Enforcement	~~Notice~~	~~Security Safeguards~~	Accountability	~~Choice~~
	~~Access~~	Openness	~~Security of processing~~	Integrity of Personal Information
	Confidentiality	Individual Participation	The Rights of Data Subject	~~Security Safeguards~~
	Warranty	~~Accountability~~	~~Enforcement~~	~~Access and Correction~~
	Accuracy		Remedies and Sanctions	~~Accountability~~
	Remedy			

Additionally, there are some principles that are general and difficult to be embodied in privacy policies or be only controlled by data keepers, such as Accountability which requires controllers to actively demonstrate compliance with principles and not merely wait for data subjects or supervisor authorities to point out shortcoming. The same as Mutuality and Preventing Harm. So these three principles (single strikethrough in Table 6) can be dismissed from the above remaining principles. In OECD's Implementing Accountability and EDPL's Rules on Security of Processing, they all suggest that a data controller should provide notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects. Given this important notice item, we should add Data Breach Notifications as an item in Notice (see Table 8).

According to the description, the Consent Principle is included in Notice② and is also relevant to Choice, so it belongs to duplication. The Relevance and Collection Limitation have the same meaning, i.e., the collection would be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means. But how to know they match? Telling you what information will be collected is simple and clear. Whether or not the means of obtaining are lawful and fair? We are also informed from how they collect it. So these principles are also included in Notice (See Table 8). Fiduciary Duty is about the security and safeguard of record, it is the same as Security. Confidentiality is about disclosure to third parties, it is also one item of Notice. Warranty is about purpose limitation, it is included in Purpose Specification which also claims to inform data subject of purpose before collecting. This is one item of Notice. Whether or not does the controller go beyond the purposes? Listing all the purposes for which personal data are collected is maximum guarantee for users. Likewise, the purposes are always expressed by narrating how to use personal data. So Warranty and Purpose Specification can be replaced by Notice's How to use. Accuracy, Data Quality, and Integrity of Personal Information have the same meaning, but how to achieve accuracy, completeness, and

① There is a little difference between the same name principles, more detailed discussion see below.
② The following appeared Notice, Choice, Access, Security, and Enforcement are all based on FTC.

update? One of the effective methods is admitting consumers to review information and to correct inaccuracies or delete information. So these three principles can be reflected from Access.

Additionally, the EPDL's Data Quality has a sub-principle known as the Limited Retention of Data, which specifies that keeping in a form which permits identification of data subjects for no longer is necessary for the purposes for which the data were collected or for which they are further processed. The data must therefore be erased when purposes have been serviced. So we can add an item known as the limited Retention to Notice.

Remedy, Remedies and Sanctions, and Enforcement are all about against infringements of the right to data protection. Use Limitation is equal to Choice. Openness suggests the identity and usual residence of the data controller should be readily available. It belongs to items which should inform consumers. Thus we can add an item known as Identity and Location to Notice which includes information on how to contact data controllers about their practices and handling of personal information. This item is also relevant to Accuracy, Data Quality, and Integrity of Personal Information in fact. When consumers know how to contact data controllers, they can put forward to correct, update, or delete. Individual Participation's (a), (b), and (c) mean that individuals have right to know whether or not their personal information is collected. This right can be reflected by informing consumers what information will be collected and how. When consumers know "Identity and Location", it will help consumers propose this right. Individual Participation's (d) is similar to Access. The Rights of Data Subject's (a) and (b) are similar to Individual Participation, and its (c) is relevant to Choice. Fair Processing's (b) is included in Notice , Fair Processing's (d) is equal to Access, and its (a) and (c) are difficult to verify by data subjects because they depend on supervisory authorities and self-regulation completely. So it is relevant to Enforcement. Use of Personal Information means that use of personal information cannot go beyond the purposes of collection, so it is constrained by the Notice of how to use.

In conclusion, the five principles which are suggested by Federal Trade Commission in *Fair Information Practice in the Electronic Marketplace: A Report to Congress* can be regarded as basic principles, from which we can conclude that there are five dimensions of privacy policy, namely Notice, Choice, Access, Security, and Enforcement, as shown in Table 8.

4. PRIVACY CONCERN

Internet privacy concerns represent individuals' perceptions of what may happen with the information they provide via the Internet. More specifically, many researchers have adopted the definition of privacy concerns as focusing on the concerns individuals have with the information privacy practices of organizations[10].The use of Web sites implies exchanging information between Internet users and site owners, whether in an explicit or implicit way. This leads to an increasing level of concern of the Internet users about their privacy. The major concerns have to do with the kind of information that Web sites collect, the way it is collected and the uses that business gives to the information collected[9].

Smith et al. (1996) developed the concern for information privacy and identified data-related dimensions of privacy concerns, namely (1) Collection, which concerns that extensive amounts of personally identifiable data are being collected and stored in database; (2) Error, which concerns that protections against deliberate and accidental errors in personal data are inadequate; (3) Unauthorized secondary use, which concerns that information is collected from individuals for one purpose but is used for another, secondary purpose(internal secondary uses and external secondary uses) without authorization from the individuals; (4) Improper access, which concerns that data about individuals are readily available to people not properly authorized to view or work with this data[11].

In 1998, Wang, et al. established seven different privacy concerns related with act at improper way as follows. (1) Improper access, which is related to infiltrate an internet consumer's private with notice or

acknowledgment from the consumer; (2) Improper collection, which is related to collect a consumer's private information from the Internet without notice to or acknowledgment from the consumer; (3) Improper monitoring, which is related to monitor a consumer's Internet activities without notice to or acknowledgment from the consumer; (4) Improper analysis, which is related to analyze a consumer's private information without proper notice, and to derive conclusions from such an analysis; (5) Improper transfer, which is related to transfer a consumer's private information to other businesses without notice to or acknowledgment from the consumer; (6) Improper storage, which is related to keep private information in a non-secure manner resulting in a lack of trustworthiness of the stored information, or lack of authentication control for information access; and (7) Unwanted solicitation, which is related to transmit information to potential Internet consumers without their acknowledge or permission[12].

Miyazaki and Fernandez (2000) established users' information privacy concerns related primarily to Unsolicited customer contacts and Customer information distribution, i.e., consumer information will be shared (i.e., rented or sold) to third parties that have marketing-related interests such data, and Security concern, i.e., involved in online shopping pertains to unauthorized third-party access personal and financial information [13].

Liu and Arnett (2002) suggested that security; the extent of data collection, use, and disclosure; internal and external secondary data use; customer choice; and data access are major privacy concerns of global e-commerce[14].

Drawing on social contract theory, Malhotra et.al (2004) proposed the concerns of online consumers center on three major dimensions, namely (1) Collection, i.e., a person is concerned about the amount of individual-specific data possessed by others relative to the value of benefits received; (2) Control, which is an individual's concern for information privacy center on whether the individual has control over personal information as manifested by existence of voice (i.e., approval, modification) or exit (i.e., opt-out); and (3) Awareness of privacy practices, which refers to the degree to which a consumer is concerned about his/her awareness of organization information privacy practices, this awareness factor incorporates two types of justices, i.e., interactional and informational justices. Interactional justice includes issues of transparency and propriety of information made during the enactment of procedures. Information justice relates to the disclosure of specific information[15].

The above studies about privacy concern reveal the aspects to which consumers pay attention. We can compare them with dimensions of privacy policies, and find out whether or not the later can cover the former as shown in Table 7.

Table 7 Relationships between the Dimensions of Privacy Policies and Privacy Concern

Privacy concern \ Privacy policies		Notice	Choice	Access	Security	Enforcement
Smith et al. (1996)	Collection	√				
	Error			√	√	
	Unauthorized secondary use	√	√			
	Improper access				√	
Wang et al. (1998)	Improper access	√				
	Improper collection	√				
	Improper monitoring	√				
	Improper analysis	√	√			
	Improper transfer	√				
	Improper storage				√	
	Unwanted solicitation		√			

Miyzaki et al. (2000)	Unsolicited customer contacts		√			
	Customer information distribution		√			
	Security concern				√	
Liu et al. (2002)	Security				√	
	Data collection, use, and disclosure	√				
	Internal and external secondary data use		√			
	Customer choice		√			
	Data access			√		
	Collection	√				
	Control		√		√	
	Awareness	√	√			

Note: "√" stands for Privacy policy's dimension can cover Privacy concern's dimension.

The purpose of privacy policy is to eliminate consumers' concerns about online privacy. From table 7, we can conclude that the dimensions of privacy policies can cover all privacy concern's dimensions, in other words, if the privacy policy made by a company according to principles of privacy is implemented strictly, consumers' privacy concern would be dismissed. So the dimensions of privacy policies we developed are adequate.

5. MEASUREMENT OF DIMENSIONS OF PRIVACY POLICIES

The Notice principle is the most fundamental of the fair information practice principles, because it is prerequisite to implement other fair information practice principles such as Choice or Access. Notice principle requires an entity to give consumers clear and conspicuous notice of an entity's information practices before any personal information is collected from them, according to part 3 states, its scale items are shown in Table 8.

When a consumer's personal identifying information is used beyond the use for which the information was provide, data collectors would offer the consumer with other choices. Under the Choice principle, data collectors must afford consumers an opportunity to consent to secondary uses of their personal information, such as the placement of consumers' names on a list for marketing additional products or the transfer of personal information to entities other than the data collector. There are two types of choice, namely "Opt-in" and "Opt-out"[3]:

"Opt-in" choice requires an affirmative act by the consumer (such as checking a click-box or sending an email or a letter) before the information can be used in a particular manner; i.e., the default is that the information will not be used.

"Opt-out" choice allows the consumer to take an action (such as checking a click-box or sending an email or a letter) to prevent the information from being used in a particular manner; i.e., the default is that, absent action by the consumer, the information will be used.

Access refers to an individual's ability to access data about him or herself, i.e., to view the data in an entity's files, and to contest that data's accuracy and completeness. Access is essential to improving the accuracy of data collected, which benefits both data collectors who rely on such data, and consumers who might otherwise be harmed by adverse decisions based on incorrect data. Access measures privacy policy about a consumer's ability to review, correct, or delete at least some personal information about them.

Security means personal data should be protected by reasonable security safeguards against such risks as

loss or unauthorized access, destruction, use, modification or disclosure of data. Data security is not just achieved by having the right equipment--hardware and software--in place. It also requires appropriate internal organizational rules. So security involves both managerial and technical measures to provide such protection. In practices, there are many general statements about security in privacy policies, which are not specifically related to transmission or storage of information, such as "We take steps to ensure the security of your information", or "We provide security for all information we collect". So we classify security as two levels, namely (1) the first level contains statements which have been described above, and (2) the second contains steps to Ensure, meaning to take reasonable steps to protect the security of the information they collect from consumers, including (1) taking any steps to provide security for information during transmission, such as "We use SSL to protect your credit card information", or "We encrypt your information when send it to us", and (2) taking any steps to provide security for information after receipt, such as "We store all our customer information on a secure server", or "We use firewalls to prevent unauthorized access to our databases and servers". Only those privacy policies in which these two steps are satisfied should be awarded score.

Enforcement refers to the use of a reliable mechanism to provide sanctions for noncompliance as a critical component of any governmental or self-regulatory program to protect privacy online. The key enforcement mechanisms to emerge in industry's self-regulatory efforts are the privacy seal program, such as TRUSTe, BBBOnLine (Best Business Bureau Online Seal), and ESRB (Entertainment Software Rating Board Seal) . These programs require their licensees to implement certain fair information practices and to submit to various types of compliance monitoring in order to display a privacy seal on their web sites. If widely adopted, they promise an efficient way to alert consumers to licensees' information practices and to demonstrate licensees' compliance with program requirements.

The measurement items of dimensions of privacy policy are presented in Table 8.

Table 8 Measurement of Dimensions of Privacy Policy

Principles \ Studies or laws	FDC	Keith Mossman	OECD	EDPL	APEC
Notice					
What Information Collected	√				
How Collected	√				
How Used(or Purposes for collecting)	√				
Whether Disclosed to Third Parties	√				
Whether Third Parties Collecting Data Through the Site	√				
Identity and Location			√	√	√
Data Breach Notifications			√	√	
The limited Retention			√		
Choice					
Opt-in	√				
Opt-out	√				
Access					
Review Personal Information	√				
Correct(or Delete) Personal Information	√				
Security					
Statement	√				
Steps to Ensure	√				
Enforcement					
Self-Regulation	√				

If we assign every item with one point, a relative complete company's privacy policy can get maximal score 15. Based on this grading system, we can evaluate a company's privacy policy respectively, then according to experience data, the company can be awarded a corresponding grade.

6. CONCLUSIONS AND LIMITATIONS

After a comprehensive analysis on primary studies of privacy, we have concluded five dimensions of privacy policies from principles which are proposed by those studies (or laws) and verified by consumers' privacy concern. We have also developed a measurement to scale a privacy policy, which will help to draft privacy policies for a company and to assess a company's privacy policies for consumers. As stated by Smith et al. (1996)[9], many areas of information system research may be impeded by the lack of validated instruments for measuring some important construct, the development of measurement for privacy policy may facilitate relationship research between website's privacy policy and others construct about consumers' online behavior.

Some Limitations of this study should be mentioned.First,we propose the notion of privacy policies'dimestion is exploratory research, its theoretical basis is insufficient,we only transfer the principles of information privacy to dimentions of privacy policies,it seems a little simple.Second, the dimentions of privacy policies may be incomplete and Enforcement dimention's scale item may be expanded after there are better methods to supervise data collector to ensure effective data protection.

REFERENCES

[1] OECD. (2013). The OECD Privacy Framework.

[2] European Union Agency for Fundamental Rights, Council of Europe. (2014). Handbook on European Data Protection Llaw. Belgium:The Council of Europe and the European Court of Human Rights 2014.

[3] FTC Congress Report.(2000). Privacy Online: Fair Information Practices in The Electronic Marketplace. Federal Trade Commission 2000.

[4] APEC Secretariat.(2005). The APEC Privacy Framework.

[5] ACM US Public Policy Council. (2014). Pivacy and Security. usacm.acm.org/privsec/index.cfm.

[6] U.S. Department of Commerce.(2000).Safe Harbor Privacy Principles. http://export.gov/safeharbor/eu/.

[7] Minister of Justice.(2014).Personal Information Protection and Electronic Documents Act.http://laws-lois.justice.gc.ca/.

[8] Mossman, Keith.(1975). A New Dimensions of Privacy. American Bar Assoication Journal,61: 829-833.

[9] Celestino Robles-Estrada, Juan A. Vargas-Barraza, Ma. Dolores del C. Sepúlveda-Núñez.(2006). Are Privacy Issues Important in Mexican Online Markets? An Empirical Investigation into Published Online Privacy Statements of Mexican Web Sites. In:AIS Electronic Library,ed. BLED 2006 Proceedings.

[10] France Bélanger, Robert E.(2011). Crossler. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly, 35(4): 1017-1078.

[11] H.Jeff Smith, Sandra J.Milberg, Sandra J.Burke.(1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. MIS Quarterly, 20(2): 167-196.

[12] Huaiqing Wang, Matthew K.o. Lee, Chen Wang.(1998). Consumer Privacy Concerns about Internet Marketing. Communications of the ACM , 41(3): 63-70.

[13] Anthony D. Miyazaki, Ana Fernandes.(2000). Internet Privacy and Security: An Examination of Online Retailer Disclosures. Journal of Public Policy & Marketing,19(1): 54-61.

[14] Chang liu, Kirk P.Arnett.(2002). Raising a Red Flag on Global WWW Privacy Policies. The Journal of Computer Information Systems,43(1): 117-127.

[15] Naresh K.Malhotra, Sung S.Kim, James Agarwal.(2004). Internet Users' Information Privacy Concerns (IUIPC):The Construct ,the Scale,and a Causal Model. Information Systems Reseach,15(4): 336-355.