This is to certify that the
dissertation entitled

PERSONAL DATA PROTECTION IN E-GOVERNMENT:
GLOBALIZATION OR GLOCALIZATION?
A COMPARATIVE STUDY OF THE UNITED STATES, GERMANY
AND CHINA

presented by

Yuehua Wu

has been accepted towards fulfillment
of the requirements for the

Ph.D.	degree in	Communication Arts and Sciences – Media and Information Studies

Major Professor's Signature

4/29/10

Date

PERSONAL DATA PROTECTION IN E-GOVERNMENT: GLOBALIZATION OR GLOCALIZATION?
A COMPARATIVE STUDY OF THE UNITED STATES, GERMANY AND CHINA

by

Yuehua Wu

A DISSERTATION

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

Communication Arts and Sciences – Media and Information Studies

2010

ABSTRACT

PERSONAL DATA PROTECTION IN E-GOVERNMENT: GLOBALIZATION OR GLOCALIZATION?
A COMPARATIVE STUDY OF THE UNITED STATES, GERMANY AND CHINA

by

Yuehua Wu

The development and diffusion of information and communication technologies, particularly the internet, creates a worldwide trend of using ICTs and the internet to deliver public services. This new form of electronic administration -- e-government -- potentially offers great benefits to society in that it can enhance public service efficiency, quality, and cost-effectiveness. However, the development of e-government carries new risks. Compared to government functioning in the pre-computer era, e-government involves the generating, storing, processing, and transferring of much larger amounts of personal data. The development and expansion of e-government, therefore, affects individuals' right to privacy, in particular the right to information privacy. It is necessary to balance the societal benefits promised by e-government with individual rights to information privacy. Adequate personal data protection is also essential to boost public trust in online government and is thus crucial to the success of e-government.

This study provides a comparative overview of the national/federal laws and policies protecting personal data collected and processed in e-government in the US, Germany, and China, and a brief overview of the international legal and policy landscape. The first goal is to examine the overall regulatory frameworks adopted at the national and supranational level, with the hope that it will contribute to the current reflections on this topic worldwide. Drawing on governance and internet governance theory, a further

theoretical goal is to understand the governance mechanism of this issue and to evaluate the impact of national context on the governance modes adopted. The analysis will provide practical guidance for the governing of this issue and other internet policy issues.

Overall, the study found that national government regulations and the international regulatory framework do not keep pace with technological changes or with the current information practices of the public sector and relevant private parties. In many instances, the existing data protection laws were found insufficient to protect personal information in the e-government area. New laws or revisions of the existing data protection laws and enforceable global standards are desired to address the increasing information privacy concerns in this particular context.

With respect to governance models, the study found that traditional government regulation is currently a major governance mode for the issue under discussion, which counters the 'governance without government' perspective that is widely held for internet governance. Whereas international agreements provide guidance on the most basic principles for data protection, alternative regulation and code-based technological rules serve supplementary roles to the government regulatory framework at both the national and international levels. National government regulation seems to be seen as the most effective means to achieve meaningful protection of personal data in the context of e-government, which yet has to be accompanied by other governance modes as mentioned above to be a complete success. Meanwhile, the national context is found to impact the form and level of data protection and the choice of governance modes of this issue with respect to the specific context of e-government.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS

APEC Asia-Pacific Economic Cooperation

BMI Federal Ministry of Interior of Germany

BSI German Federal Office for Information Security

CASS Chinese Academy of Social Sciences

CNNIC China Internet Network Information Center

CoE The Council of Europe

DCP Dynamic Coalition on Privacy

EPIC Electronic Privacy Information Center

EU European Union

FIPs Fair Information Practices

FISMA Federal Information Security Management Act

ICANN Internet Corporation for Assigned names and Numbers

IETF Internet Engineering Task Force

IGF Internet Governance Forum

ISO International Organization for Standardization

ISPAB Information Security and Privacy Advisory Board

NIST National Institute of Standards and Technology

OECD Organization for Economic Cooperation and Development

OMB Office of Management and Budget

PIA Privacy Impact Assessments

PMA President's Management Agenda

PPSC Privacy Protection Study Commission

SILG State Informatization Leading Group

UN United Nations

US The United States

USDOJ United States Department of Justice

VPS Virtual Post Office

WGIG Working Group on Internet Governance

INTRODUCTION

The development and diffusion of information communication technologies (ICTs), particularly the internet, over the last two decades has great transformative power across almost all areas of society. In the public administration area, it has brought about great changes in how governments operate and serve their constituencies. From the 1990s, worldwide ICTs and the internet have been increasingly used to deliver public services. This new wave of public administration reform, termed as electronic government ("e-government"), is expected to bring many benefits to society. Implemented properly, e-government can enhance public service efficiency, quality, cost-effectiveness, and increase government information and service access. Enticed by these benefits, government organizations at various levels around the world are placing high hopes in e-government as an engine of economic, social, political, technological, and strategic transformation (2003a, p. 242). According to the United Nations (UN) Global E-government Survey (2008), 189 out of the 192 UN member states had some form of e-government online presence by the end of 2007. With massive financial and political commitments made to introduce e-government, an increasing number of countries have made progress in developing e-government, migrating from the simple provision of information online to more advanced areas of e-service delivery and citizen participation.

However, e-government carries new risks. The development and expansion of e-government affects individuals' right to privacy, in particular the right to information privacy. First, the use of internet technology in e-government enables very fast, easy, and low-cost ways to collect, store, and distribute personal data from citizens. New technologies like cookies also enable *hidden data collection* (Belanger & Hiller, 2006),

which happens because of users' unfamiliarity with such technologies. Consequently, e-government involves the generation, storing, and processing of much larger amounts of personal data than during the pre-computer era, which increases information privacy concerns. The increasing migration of e-government services to more advanced and sophisticated two-way interactional and transactional functions makes even more data collecting and processing necessary. Second, with the development of e-government and the exponential growth of data collection and storage, the aggregation and cross-referencing of personal data contained in government computer records are increasing in scale. Government agencies share information with other agencies for various purposes, such as eligibility verification, fraud detection, and data reconciliation (two agencies share data to update records) (Belanger & Hiller, 2006). Such cross-referencing is becoming a privacy issue when the amount increases markedly. Further, constructing government databases and sharing data between government agencies are encouraged by many governments in the e-government era for economical and efficiency purposes (such as in China's *General Framework of National Electronic Government* and some US e-government policy documents), which poses a serious threat to individuals regarding their information privacy.

In addition to the privacy threat brought about by e-government activities, the growing usage of personal information online and the vulnerable and insecure nature of the internet as a globally connected and easily accessible (open) network also increase the possibility of loss, theft, and errors of such data, which heightens the data security concern on the internet and in the particular context of e-government. While the openness and networked nature of the internet creates enormous benefits, it also opens new attack

vectors from remote locations for malicious purposes, which include breaches into information databases collected by government agencies. Moreover, the sophistication and effectiveness of cyber attacks have steadily advanced with the development of information technology. Thus the risks that government agencies face are significant[1].

In brief, the privacy and security of personal data in the context of e-government is becoming a very pressing issue to deal with. An adequate protection of personal data in e-government is of great significance for various reasons. First, individual privacy rights have been increasingly recognized as an important value worldwide. The development of e-government should be balanced with the need to guarantee individuals' right to information privacy. Meanwhile, as an important component of data privacy protection, the security of personal data must be guaranteed to avoid various damages to individuals, such as identity theft or other harms caused by unauthorized use, disclosure, disruption, or modification. Second, adequate personal data protection is essential to boost public trust in online government and thus crucial to the success of e-government itself. Empirical studies found that a lack of trust decreases e-government adoption and diffusion (e.g. Carter & Belanger, 2005; Das, DiRienzo, & Burbridge, 2009). Users will not actively engage in e-government, especially in conducting transactions with online government, before they have confidence that government and technology can protect their data privacy and security. Therefore, to fully unleash the true potential and value of e-government, government needs to address and reassure citizens about the privacy and security of their personal information online.

---

[1] Such risks also occur in the private sector. Yet anecdotal evidence shows that, compared to the private sector, government agencies have lower awareness of, or put lower priority on, this issue.

In addition to becoming an important regulatory issue at the national level, the privacy topic in e-government also gives rise to complex issues of international regulation and cooperation because of the global nature of the internet and increasing cross-border data flows between governments and relevant parties. The non-territorial nature of the internet and globalization as exemplified by the increasing country interdependence and cross-border data flows creates pressure toward privacy policy convergence at least in some fundamental issues. At the same time, due to the conditional nature (e.g. social and cultural) and problem nature (local. vs. global) of the data privacy issue considerable divergence in terms of the policy instruments might persist. Because of the novelty of the problem and scant research in the specific e-government privacy area it is still an open question of how well national and international solutions could address this issue and what specific roles they should play. Although scholars, policy-makers, and privacy advocates have come to recognize and increasingly called attention to the data protection issue in the e-government context in the past years, studies on this topic are very limited and there is barely any literature systematically analyzing this issue at a global scale. One purpose of my dissertation is to fill this gap.

Meanwhile, over the past years, the rapid growth of the internet has caused heated discussion and debate in the internet community on how the internet could and should be governed. In the early years of internet development, people commonly referred to the internet as a new frontier beyond the reach of traditional government regulation. Even if government tried to intervene, the space was seen as ungovernable with traditional means (Barlow, 1996). Rather, forms of self-governance would take the role of traditional government. Yet as the internet is becoming widely accessible and a routine means of

communication, reliance on market and self-regulation has failed to adequately address and reconcile conflicting interests on many internet issues. Online privacy and data protection is one of these issues. While a broad spectrum of governance mechanisms is available, such as government intervention and regulation, self- regulation and co-regulation, and market decisions (Bauer, 2007), the key problem is which or which mix of governance mechanisms to apply for different public policy issues relevant to the internet[2]. The existing internet governance literature largely focuses discussions on domain names, technical issues and relevant institutional arrangements such as the Internet Corporation for Assigned names and Numbers (ICANN) (e.g. Bygrave & Bing, 2009; Mathiason, 2009). The discussion of governance structures that address specific public policy issues, such as on online privacy protection, is quite limited. More exploration and insights regarding what governance arrangements best serve a specific purpose can contribute to a deeper understanding of the internet governance issue. Therefore, in addition to providing a national and international overview and analysis of the data protection issue in e-government, the main theoretical research goal for my dissertation is to contribute to the open question of which governance mechanisms might be best suited to address this issue and how national context may shape the specific governance regime adopted.

A preliminary review of the literature seems to suggest that government regulation is currently a predominant mode governing the issue under discussion. So what is the actual fact in the sampled countries? Meanwhile, the internet component of e-government and the public sector as the major party to be regulated in this issue make the

[2] See (WGIG, 2005a) for the list of key public policy issues identified by the Working Group on Internet Governance as relevant to internet governance.

specific role and the effectiveness of government regulation in protecting personal data in the context of e-government an important question to be explored and answered (more detail see Chapter 2). In this study, therefore, I choose government regulatory instruments as the main subject of analysis. Within "government regulation" there are many ways how government policies can be structured, which is what I am predominantly interested in. Based upon government policy instruments at national and international levels, efforts are made to identify other forms of governance mode, if there is any evidence. At the international level, in addition to governmental agreements, a closer look at non-governmental actions/solutions ("alternative regulation") is also provided because the whole discussion of internet governance greatly emphasizes global-level multi-stakeholder cooperation and negotiation in relevant policy-making processes.

In brief, as an endeavor to fill the above-mentioned research gaps, the first goal of my dissertation is to present an overview of the current regulatory instruments protecting personal data in the e-government domain worldwide. This is done with in-depth case studies of relevant legislative and administrative actions in three countries and regulatory actions by important supra-national organizations. Reviewing relevant laws and policies can help us evaluate the current status of personal data protection in e-government and seek solutions to this issue more effectively. Building on the country cases, the international landscape, and the internet governance theory, the second goal of the paper is to explore the mechanism adopted to govern this issue. Understanding the governance mechanism could help facilitate future policy-making regarding data protection in e-government area and hopefully also provide a reference framework for other internet public policy issues. In sum, as one of the first assessments of this issue on a global scale,

this study could contribute to both national and international policy responses to this issue and to the broader topic of internet governance.

Rationales for selecting the three country cases will be introduced in the methodology part in Chapter 2. However, a comparative overview of the countries' political, social, and economic contexts and e-government development status (see Table 1) might be helpful. While all the three countries face the common problem of designing and implementing protections for private information in the context of e-government,

Table 1 Country Profiles of the United States, Germany, and China

		United States	**Germany**	**China (mainland)**
Location		Northern America	Western Europe	Eastern Asia
Population		301.6 million	82.3 million	1318.3 million
Adult Literacy		99%	99%	91%
Per Capita GDP (nominal) (US$)		45,790 (10^{th})	40,079 (16^{th})	2,485 (99^{th})
Political Structure		Federal Constitutional Republic	Federal Parliamentary Republic	Single-party Communist State
E-government performance	E-government Readiness Ranking	4	22	65
	Web Measurement Index Ranking	3	33	47
Internet Infrastructure	Internet Users /100 persons	69.10	46.67	10.35
	Broadband /100 Users	19.31	17.03	3.85

Notes: (1) All the rankings refer to global ranking. (2) Data on population and per capita GDP refer to the year 2007. All the other numeral data refer to the year 2008. Per capita values were obtained by dividing the GDP data by the Population data. (3) The E-government Readiness Index used by the UN for its global e-government survey is composed of three components: Web Measurement Index, Infrastructure Index, and Human Capital Index.

Sources: World Development Indicators database, World Bank; unstats.un.org; the United Nations (2008)

the United States (US), Germany, and the People's Republic of China (China) are distinct from each other in various aspects ranging from their geographic location, cultural heritage, political system, economic development, internet infrastructure, and e-government performance. These differences make them all unique cases for the inquiry and meanwhile are expected to influence the form and level of data protection and the choice of governance modes with respect to data privacy and security in the context of e-government in individual countries.

One main finding of this study is that national government regulation and the international regulatory framework do not keep pace with technological changes and the current information practices of the public sector and relevant private parties in the context of e-government. In terms of the governance mechanism, traditional government regulation is found to play a major role in protecting the privacy and security of personal data in e-government. Meanwhile, international agreements provide guidance on the most basic principles for data protection. Alternative regulation (self-regulatory and co-regulatory approaches) and code-based technological rules primarily serve in supplementary roles to the government regulatory framework, while the latter playing a more prominent role than the former. Although further evidence is needed to draw conclusions on the most effective governance mechanism for the issue under discussion, we may conclude that in the long run effective coordination of the various aforementioned governance tools at different levels is critical to achieve an adequate and effective protection of information privacy in e-government. The study also found that the national context, such as the existing legal system and cultural traditions, impacts

which governance mechanisms are adopted by and how these mechanisms function in individual countries.

The dissertation is structured as follows. In the first chapter the concepts of e-government and information privacy are defined and the relevant literature is reviewed. The second chapter presents the conceptual framework, research questions, and the research approach. Chapter 3 provides some background information on the development of e-government in the three countries. Chapter 4 examines the primary national/federal data protection laws applicable to e-government in the three countries and Chapter 5 takes a closer look at additional relevant laws and policies. The case studies are expanded in Chapter 6 with a discussion of international efforts to protect privacy in e-government. The last chapter analyzes the governance frameworks established to address information privacy in e-government and draws conclusions and implications based upon the analysis.

CHAPTER 1

PERSONAL DATA PROTECTION IN E-GOVERNMENT

Conceptualizing E-government

Various definitions of e-government have been proposed in the pertinent research literature. For example, according to Koh, Ryan, and Prybutok (2005), e-government is the use of the internet and other digital technologies to simplify or enhance the methods by which citizens, employees, business partners and government organizations interact and conduct business. Generally, e-government is defined as the utilization by government of ICTs, in particular the internet and web technology, for the delivery of information and public services to its citizens (Bekkers & Homburg, 2007; Gant, 2008; United Nations, 2005). Differentiated by the main stakeholders involved, e-government includes electronic interactions of three main types: *government-to-government (G2G)*, *government-to-business (G2B)*, and *government-to-consumer/citizen (G2C)*. In these activities, two related functions can be distinguished: *back office* and *front office* (UN, 2008). *Back office* activities refer to the internal operations of government that support core processes yet are not accessible or visible to the general public. *Front office* activities refer to the electronic functions made accessible to the general public and the interactions between government and the general public. In this dissertation, the discussion of the protection of personal data in e-government covers measures regulating both the back office information practices and front office activities.

E-government can take various forms, ranging from the simple provision of government information to advanced interactive transactions and citizen participation in

governmental processes. Many e-government studies have attempted to structure this broad range of possibilities into "stages" of e-government development (e.g. Hiller & Bélanger, 2001; Koh, Ryan, & Prybutok, 2005; Moon, 2002; Siau & Long, 2005; United Nations, 2005). These studies generally distinguish four to five stages of e-government according to levels of sophistication of the utilized technology and services. A typical classification is the differentiation of (1) *one-way information delivery*, (2) *two-way communication and interaction*, (3) *transaction*, (4) *integration*, and (5) *participation*. At the most basic level, e-government activities focus on publishing basic information on the web, whereby the web content is usually static. At intermediate level(s), governments use websites to support two-way communication and process transactions online. Individuals are allowed to perform electronic transactions such as making payments, filling out and submitting applications, or renewing licenses. At advanced levels, governments use the web to integrate services across different agencies and provide tools for public feedback and political participation (Wu & Bauer, 2009).

Conceptualizing Privacy and Information Privacy

It is difficult to present a single definition for privacy despite its central position in Western philosophy and in various disciplinary research fields. Definitions of privacy vary according to context and environment (Privacy International, 2007a). Originally, Warren and Brandeis (1890) defined the right to privacy as the right "to be left alone". Various other definitions were proposed after this first explicit legal statement. Instead of looking for a specific definition, one useful approach to understand privacy is an approach using different privacy dimensions. Burgoon et al. (1989) distinguished four types of privacy violation: *physical*, *interactional*, *psychological/informational*, and

impersonal. Another scholar DeCew (1997) divided privacy into three dimensions: *informational*, *accessibility* and *expressive* privacy. More recently Braman (2006) differentiated four aspects of privacy as *spatial* (home and body), *communicative* (mediated communication), *relational* (communication with professionals and spouse), and *data* (disclosure and/or use of personal information) privacy. Other similar categorizations also exist, such as the four facets of *information privacy*, *bodily privacy*, *privacy of communications*, and *territorial privacy* (Privacy International, 2007a). In all these categorizations, *information (data) privacy* is a key dimension of privacy, which is defined by Westin (1967) as the amount of control that individuals can have over the type of information, and the extent of that information revealed to others. In this dissertation, the discussion of privacy is limited to *information privacy*, which, in Europe, is often referred to as *personal data*.

The concept of information privacy emerged in the 1960s and 1970s, at about the same time that *data protection* entered the vocabulary of European experts (Bennett, 2002). The emergence of the concept was closely connected to the information processing capabilities of computers. One of the early information privacy concerns arose from the misuse, or abuse, of census data, which could be found in much of the world, including in the US and in many European countries like Germany (Electronic Privacy Information Center, n.d.). In the 1970s and 1980s, for example, there were strongly-voiced information privacy concerns in Europe over national censuses and widespread public debate about privacy rights in relation to new computer technologies. In Germany, a public outcry against a national census law in the 1980s led to the amendment of the *German Data Protection Act* in 1990 to include the right of informational self-

determination regarding government uses of information. In brief, although debates on information privacy protection are not new, advances in ICT threaten individuals' privacy more easily and pervasively than ever before because of the increased ability to collect, assemble, and distribute personal information, in particular on the internet.

Regarding personal information, Smith, Milberg, and Burke (1996) identified four dimensions of concerns about organizational privacy practices, which include information practice by government agencies*: (1) unauthorized secondary use of personal information, (2) improper access of personal information (internal and external), (3) collection of personal information, and (4) errors in collected personal information.* These dimensions indicate that information privacy practices cover data collection, data use, data disclosure, and data quality. The dimension of external improper access of personal information and the other dimensions also contain the component of data security. In this study data security is discussed in the context of privacy protection or the general personal data protection. That is to say, for the purpose of this study, personal data protection equals personal information privacy protection, which includes the protection of data privacy and data security.

Information Privacy in E-government

Causes for Information Privacy Concerns in E-government

With the pervasive use of ICTs and the internet, the importance of e-government is increasingly acknowledged in many countries around the world. E-government initiatives are being carried out at all levels of government: local, regional, and national. The worldwide development of e-government, however, is accompanied by a side effect -- increasing threats to citizens' information privacy, which could seriously hinder this

developing trend. Compared to the private sector, public administration might create more serious privacy concerns considering the large scale, completeness, and sensitivity of the personal information in government databases, and the increasing cross-referencing practices initiated by e-government in order to achieve its efficiency goal and other benefits.

McDonagh (2002) summarized three information privacy problems arising from e-government applications:

(1) *Collection problems*: Automatic collection of personal information without reference to data subjects by use of cookies, collection of e-mail addresses and inclusion of e-mail in mailing lists.

(2) *Use and disclosure problems*: Data sharing and cross-referencing across government agencies due to development of integrated portals; data transmission between the public and private sector; use and disclosure of personal information through the public key directory and certificates revocation lists; unknowing information recording by government due to the use of digital certificates.

(3) *Security problems*: security of private keys and possible identity theft.

Appropriate data protection policies and measures should address each of the above aspects when e-government activities are being carried out.

A closer look at these information privacy problems in e-government might be necessary to help us understand this issue. As introduced earlier, e-government operations are divided into 'front office' (government portal) and 'back office', that is, the 'counter' services of contacting citizens on one hand, and the services of file-handling

on the other hand (European Union, 2003). The 'front office' administration collects various personal data that are necessary to provide the service required by the citizen. The administration of 'back office' then uses these data to provide the required service. To prevent any unlawful use or circulation of citizen's data within the 'back office', specific responsibilities on data handling should be defined clearly. In terms of data collection at the 'front office', the volume and sensitivity of personal information collected by government websites largely depends on the sophistication level of the e-government application (McDonagh, 2002). The most basic e-government function of one-way information delivery does not require the release of much personal information. At the more complex levels, however, such as the interactive and communicative features between citizen and government and those transactional services, government websites could collect large volumes of personal information that are often very sensitive, which may imply great potential of information privacy infringement. Requirements, therefore, should also be provided against unnecessary/unlawful data collection at the 'front office'.

In addition to collecting necessary personal data from citizens to provide required services (e.g., personal information is required to file tax online), government portals are also used by citizens to have access to other online administrative procedures, which include, for instance, browsing government information. As we know, every time someone visits a (government) website, he or she leaves an electronic footprint (personal data). Thus for any e-government service or function, there is the issue of possible retention of personal data on government portals.

Other than the data collection and data retention issues, a general trend of constructing and interconnecting public information databases exists in the public sector

for the purposes of efficiency and cost-effectiveness. There is also an increasing exchange of personal data between public administrations. Serving as a 'one-stop shop' for citizens is the goal of e-government development in many countries, which means that back-office procedures of many different government departments would be integrated (Sutton, Zhang, & Hart, 2007). With respect to the integrated stage of e-government, the UN (2008) also called for worldwide efforts towards an *e-government-as-a-whole* concept or goal, which "focuses on the provision of services at the front-end supported by integration, consolidation and innovation in back-end processes and systems to achieve maximum cost savings and improved service delivery" (p. xv). This phase was referred to as the 'second generation e-government paradigm' in the UN global report. Underlying this 'connected governance' concept (United Nations, 2008) is a seemingly unavoidable trend of increased sharing and cross-referencing of personal data across agencies, which poses a serious threat to personal privacy. It is clear, therefore, that as e-government initiatives become more complex, integrated, and pervasive, the likelihood of privacy invasion and data misuse by various parties will increase, thus the issue of ensuring privacy of personal information in the e-government arena will become more pressing.

There are various other privacy concerns with regard to personal data in the context of e-government. For example, e-government causes more data exchange between the public and private sectors due to the increasing e-government out-sourcing practice. Public records available online for open government also pose potential risks of disclosure and unauthorized access. Moreover, data mining – a technique for extracting knowledge from large volumes of data – is becoming unprecedentedly easy and being

increasingly used in both the government and the private sector (GAO, 2005), which has raised increasing privacy concerns. Cross-border data flow is also growing partly because of the development of e-government. For instance, in the *Communication on Interoperability for Pan-European E-government Services* (2006) published by European Commission, the importance of developing cross-border e-government services was highlighted, which indicated a necessity of more cross-border data flow. Creating a new problem of information privacy invasion, the increasing cross-border data flow makes it a pressing issue to internationally address the interoperability of personal data protection mechanisms by different governments.

Although the public sector is the primary data controller in the context of e-government, private parties might also get involved. First, private parties as internet service providers have the possibility to retain personal data of individuals who are engaged in e-government activities online. Second, as mentioned above, there is increasing government out-sourcing of e-government operations. It is possible that online administrative procedures are provided by private companies. Some government data handling work might also be contracted to private companies. Therefore, in addition to regulating government's information practice, the activities of relevant private parties should also not be ignored.

Apart from data collection, data use, and data disclosure problems, there is also the data security problem. Drawing upon the previous literature, Dias and Rafael (2007) summarized six general security requirements in e-government: (1) *Authentication*, as the ability to properly and securely identify system users, or protection against faked identity/origin; (2) *Authorization*, as the ability to grant access privileges to the resources

based on the user's identities; (3) *Confidentiality*, as the capacity to prevent information from being accessed by unauthorized users or systems; (4) *Integrity*, as the ability to prevent information from being intentionally or unintentionally modified or destroyed; (5) *Availability*, as the ability to grant access to resources within a reasonable period of time, or protection against failure of IT systems; (6) *Non-repudiation*, as the ability to prevent any user from later denying his intervention in a given process or transaction. All these aspects should be taken into account when making policies and taking specific measures to protect individuals' personal data in e-government. These security requirements are especially crucial when citizens conduct online transactions with government.

An Overview of the Literature

Personal information privacy in the digital age has increased in salience and is becoming one of the most hotly discussed topics in various fields, such as in the fields of public policy, law, and internet study. Yet most of the existing information privacy studies focus on the commercial sector or on the privacy issue in general without differentiating public and private sectors (e.g. Banisar & Davies, n.d.; Baumer, Earp, & Poindexter, 2004; Bennett, 2002; Buchanan, Paine, Joinson, & Reips, 2007; Farrell, 2003; Zwick, 1999). As a comparatively new area for the personal data protection issue, e-government has been attracting increasing attention from government entities, researchers, and citizens during the past few years. Despite the increasing attention, very few studies have been conducted on this topic so far.

Although there are not many studies investigating the public perceptions of privacy concern specifically posed by e-government, there are many studies reporting the public's online privacy concerns or privacy concerns posed by government in general.

For the latter, for example, a national privacy survey in New Zealand (UMR Research, 2008) showed that citizens' concern about government departments sharing personal information rose from 37% to 62% between the 2006 and 2008 surveys. Although the study did not differentiate online and offline government, it is reasonable to assume that the data sharing initiated by the digital form of government is one major concern behind the number. Moreover, with a lack of trust towards their *brick-and-mortar* government in protecting their personal information, it is hard to believe that the public will trust their online government more.

The rapid growth of the internet has led governments in both developing and developed countries to use the technology to deliver services to the public. Most people visit e-government websites to get information, yet there is strong interest expressed by citizens in using e-government to conduct more sophisticated e-government activities such as interactions and transactions. What makes people hesitate to turn their interest into action is, to a great extent, their concerns about the privacy and security of their personal information they submit to government websites. According to a study by the Council for Excellence in Government (Hart-Teeter, 2003), when non-e-government users in the US named the reason why they had not yet moved their interaction with government online, two of the top three reasons involved concerns about privacy and security. The international portion of this survey suggested that international internet users had views of e-government that were similar to those of American internet users. The difference was more in degree than in kind.

As noted earlier, studies on the personal data protection issue in e-government are very limited. The relevant literature mostly only mentions, among other things, the

security and privacy concerns of personal information as one of the major barriers to e-government development and calls for attention or actions from the government (e.g. Assaber, Hossain, & Srivastava, 2007; Heeks, 2006; Kudo, 2008; Palanisamy, 2004; Torres, Pina, & Royo, 2005). A few papers are found specifically addressing the privacy issue in e-government, yet with scattered emphases and mostly within national boundaries. For example, Hiller and Bélanger (2001) in their report posited that privacy concerns increase as e-government evolves through stages and presented a series of recommendations to the US federal government with respect to privacy in e-government.

Regarding empirical studies, by using online tax filing service as example, one recent paper (Hu, Brown, Thong, Chan, & Tam, 2009) explored the predictors of people's intention to continue using two-way interactive e-government services that involves transmission of sensitive personal information and found security (perceived security) a very crucial factor. Two other empirical studies by Becker (2005) and West (2008a) assessed privacy policies posted at government websites and found great deficiency in both quantity and quality. Specifically, by using an analysis of 1,667 national government websites in 198 nations around the world, the e-government survey conducted by West found that only 30 percent of government websites show privacy policies and 17 percent have security policies. This suggests that information privacy in e-government has not yet gained high attention worldwide. In this regard, the US National Research Council (2007) pointed out in its report that because the benefits of privacy often are less tangible and immediate than the perceived benefits of other interests, such as public security and economic efficiency, citizens' privacy is at an inherent disadvantage when decision makers weigh privacy against these other interests.

Internet-centered information and communications technologies pose unique privacy issues that differ from those previously addressed by privacy research, which requires us to rethink the traditional definitions of privacy. Further, the new nature and features of e-government as well as that of personal data use in that process bring new challenges to the law and policy enforcement regarding privacy protection. In this sense, it is necessary that an examination of privacy protection and law enforcement capabilities regarding the e-government area be conducted as the communication technology and e-government advance. Yet the literature on legal and policy responses to this issue is very limited and, to the author's knowledge, there is barely any literature systematically examining the legal/policy responses to this issue at a global level. McDonagh (2002) and Wong (2005) evaluated the regulatory efforts on information privacy protection in e-government, yet they only examined the legal status in one single country, Australia and Hong Kong respectively. More recently Otjacques, Hitzelberger and Feltz (2007) described the results of an international study on the way public organizations manage identity-related data and the sharing of such data in the e-government area. Their examination was limited to the member countries of the European Union (EU), where countries are comparatively more homogeneous in social and political systems than countries from other regions. Although the issue of personal data protection was touched upon, the topic was narrowly defined and the examination of this issue was quite brief.

Considering the limitations of the literature and the significance and increasing urgency of this topic, a deeper look at the governance framework of the personal data protection issue in e-government is greatly desired. Furthermore, the e-government privacy literature lacks comparative studies. Considering the fact that the conception of

privacy is socially and culturally conditioned, privacy protection is a very good issue for comparative studies to reflect how this internet policy issue is approached in different countries, or how national context shapes governance mechanisms adopted to protect information privacy in e-government. A comprehensive overview of the governance framework of this issue at both the national and international levels can contribute to the literature by adding to the scant research on this topic, and more importantly, contribute to the reflection on this issue by providing more insights into its governance mechanism and provide some practical guidance on protecting personal data in e-government.

CHAPTER 2

CONCEPTUAL FRAMEWORK, RESEARCH QUESTIONS, AND METHODOLOGY

Government regulation is widely believed to be an effective tool to protect information privacy because of its power of enforcement and general applicability (see the conceptual framework later in this chapter for more detailed discussion on government regulation). Regarding information privacy in the particular context of e-government, however, two special features or components are worth extra consideration: the platform of the internet and the public sector being the major potential privacy intruder. It is commonly argued, though not completely true, that government has less power in regulating the internet. Moreover, the major role of government itself in this issue (as the primary party to be regulated) may impact the governance mechanism adopted to address this issue. For example, it is possible that self-regulation by the public sector in general is more trustworthy than self-regulation by private parties because of its public-serving nature and possibly more strict self-discipline. If that is the case, self-regulation might work comparatively well when absent formal government regulation in the context of e-government. These two aspects make the specific role of government regulation in protecting personal data in e-government process a question to be explored and answered.

Further, there is a general consensus that government involvement in regulating information privacy is associated with the level of privacy concern in a country (Bellman, Johnson, Kobrin, & Lohse, 2004; Bennett, 1992). This indicates that government

regulation might be a good subject to analyze in order to examine the impact of national context on the governance mechanism (including government regulation) of the issue under discussion.

Based upon the above research question and rationale, government regulation was chosen as the main subject of analysis in this study. After examining different countries' and relevant supranational organizations' response to this emerging issue from a policy perspective, namely the legislative system and related enforcement measures (legal measures, technical solutions, and other management arrangements), the overall governing mechanism of the data protection issue in e-government was analyzed and discussed. Before the legal and policy measures are examined, the theoretical framework serving as the basis of documentary research and discussions, the research questions, and the research methodology of the study are presented in this chapter.

A Theoretical Framework of Governance and Internet Governance

Theory of Governance and Internet Governance

In the past two decades, the terms governance and governance theory have been brought to the fore of many disciplines, ranging from political science, economics, business, international relations, to internet governance. Derived from the Latin word "gubernare", governance originally means steering (Schneider & Bauer, 2007). Now it is generally viewed as a cooperative mode where various state and non-state actors participate in mixed public/private networks to create the conditions for ordered rule and collective action (Mayntz, 2003; Peters & Pierre, 1998; Stoker, 1998). For instance, Benz (2004; as cited in Schneider & Bauer, 2007) defined it as the steering and coordination of interdependent actors within complex rule systems. Schneider and Bauer (2007) posited

that the essence of governance theory is that social order is generated "not only through central decision-making and top-down control but also by local interaction and horizontal coordination" (p. 31). Overall, governance theory emphasizes diffused authority and numerous influences on policy from various levels and actors.

According to Chhotray and Stoker (2009), the substantial social and economic changes in our society over the last decades, especially the developments of globalization and democratization, caused the surge of a discourse on governance in many disciplines. Globalization, or more precisely regionalization in many cases such as in North America and Europe, creates a greater sense of interconnectedness and interdependency between peoples, organizations, and nations worldwide. This interconnectedness include, for instance, diverse vertical links between many agencies of government at local, sub-national regional, national, and supranational levels and at each level a diverse range of horizontal relationships with other government agencies, private companies, non-profit organizations and interest groups (Chhotray & Stoker, 2009). At the same time, the spread of democratic idea requires various parties and stakeholders have the right to have a say in decision-making processes. This new social and economic context, together with the complexity of many newly-rising social problems, has challenged the established governmental form of governance, and created demands for new forms of governance.

The existing governance literature features a wide variety of governance modes. A majority of governance scholars look at the relationship between state intervention and societal autonomy in the societal rule making process. In this regard, for example, Treib, Bahr, and Falkner (2007) provided a general overview by organizing the different approaches that fall on the continuum between public authority and societal self-

regulation into different categories according to whether they emphasize the politics, policy, or polity dimensions of governance. For instance, a politics dimension creates two extreme poles of governance modes – governmental laws/regulations versus private self-regulation – and other alternative modes falling between these two ends. In the policy dimension, governance instruments could be classified into policy outputs with 'legal bindingness' versus non-binding 'soft laws' (such as guidelines and recommendations), and outputs with a 'rigid approach to implementation' versus 'flexible approach to implementation'.

Instead of providing a new normative theory, the value of the governance perspective lies in "its capacity to provide a framework for understanding changing processes of governing" (Stoker, 1998, p. 18). As in many established fields such as international relations and political science, governance theory provides a useful framework for understanding the new and/or changing governing processes of the internet. In the early days of the internet development, there was a strong belief among internet pioneers and early pundits that the internet should remain unregulated. Yet as the internet becomes widely accessible and a routine means of communication, various public policy issues relevant to the internet have been emerging, which include transition to next-generation numbering, intellectual property protection, privacy, cyber security, and many more that have been identified by the World Summit on the Information Society (WSIS), which cannot be effectively addressed by a mere reliance on market forces and self-regulation. In this situation, questions on how the internet can be governed have been raised and heatedly debated in the internet community. Consequently,

a new area of *Internet Governance* has emerged, which was defined by the Working Group on Internet Governance (WGIG) (2005b) as follows:

> Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet." (p. 4).

As indicated in the WGIG definition, internet governance is a multi-stakeholder coordination process. How such coordination can be achieved, however, is a very large and complex topic. The internet governance literature, built upon the general governance literature, proposes a wide range of governance modes for the internet. For example, Weber (2002) outlined four regulatory models for the internet: traditional government regulation, international agreements and cooperation, self-regulation, and code-based regulation. Arguing that the internet is 'a multi-layer adaptive socio-technical system', Bauer (2007) also presented a broad spectrum of alternative coordination mechanisms involving different levels of central planning for the internet, which range from self-organization, self- and co-regulation, multi-level governance, to government intervention and regulation. More recently, Solum (2009) proposed five internet governance models, which include spontaneous ordering of cyberspace, transnational institutions and international organizations, code and internet architecture, national government regulation and law, and market-based ordering. It could be seen that the models proposed by different authors share great similarity. Another thing worth noting is that in both the internet governance literature and the general governance literature, the role of alternative forms of regulation (including self- and co-regulation) has been increasingly emphasized.

While self-regulation refers to bottom-up non-governmental organizations' voluntary development and enforcement of rules and codes of conduct, co-regulation refers to cooperation between the public and the private actors in the rule-making process (Eijlander, 2005; Senden, 2005).

With all these governance modes being proposed, however, how the different modes (should) interplay and function in the process of governing is an open question and involves a number of debates. One of the debates focuses on the role of government in governance. Some governance scholars propose a 'governance without government' perspective, which emphasizes the role of relatively autonomous networks of non-government actors in collective decision-making (Rhodes, 1997; Sorensen & Torfing, 2007). These scholars, however, recognized that government still plays a steering or guiding role in the governing process. So 'governing without government' is used more for "rhetorical purposes" by these authors in order to emphasize the changed conditions of governing and the changed role of government (Chhotray & Stoker, 2009). The other side of the debate takes a stronger stance about government still being a powerful and dominant actor in the governing process. In the field of internet governance, for instance, Solum (2009) posited that national government regulation should be one of the top choices of policymakers for internet issues. He argued that many internet problems can be solved at the national level through regular lawmaking processes. In line with this debate on the role of government in the governance literature, one purpose of my study is to explore what role government and government regulation play in the governing process of the particular case of data protection in e-government.

Despite different stances on the specific roles of the governance modes, a majority of analysts and scholars believe that no single model provides the solution to all internet problems. Rather, a hybrid model combining different governance modes is essential to solve internet issues effectively. Recognizing that internet governance overall is a hybrid of different models, the next key question we have to ask is which or which mix of governance mechanisms to apply for different public policy issues in the field of internet governance. There are a variety of transnational institutions specifically targeted at internet governance, such as the ICANN and the Internet Engineering Task Force (IETF), which primarily govern the architecture and technical standards of the internet. As the internet develops, however, the range of internet-related policy issues has expanded, which go far beyond technical problems. Existing internet governance institutions therefore may not be sufficient to deal with these policy issues. Most of the policy issues have to do with the content on the internet rather than the channels over which the content flows, and thus the real question is: "who owns content and who can regulate it in a borderless world" (Mathiason, 2009, p.59).

In short, the novelty and the complex nature[3] of many internet policy issues leave most of these issues unresolved. Both in practice and in theoretical research, much work is to be done to help address the challenge of finding appropriate governance mechanisms for online policy problems. For the purpose of this study, the specific issue of information privacy protection in the context of e-government is to be analyzed to explore its governance mechanism and the impact of the national context on such mechanism.

---

[3] For example, many internet problems have local origination. Yet the internet's global reach are not compatible with the national reach of the traditional political system. Meanwhile, there are multiple stakeholders involved in most online issues, yet the stakeholders' interests are diverse.

Drawing on governance and internet governance theory and existing literature, the basic theoretical framework underlying this study is that internet governance in general is a **multi-layer, multi-stakeholder**, and **multi-form** coordination process. As one of the internet-related public policy issues, personal data protection in e-government is hypothesized to be governed by these same mechanisms. Specifically, the conceptual framework serving as the point of reference in the review and discussion in this study is primarily a mix of the *multi-level governance* approach and the governance modes of national government regulation, alternative regulation, and code-based regulation that are proposed in the literature (see *Figure 1*).

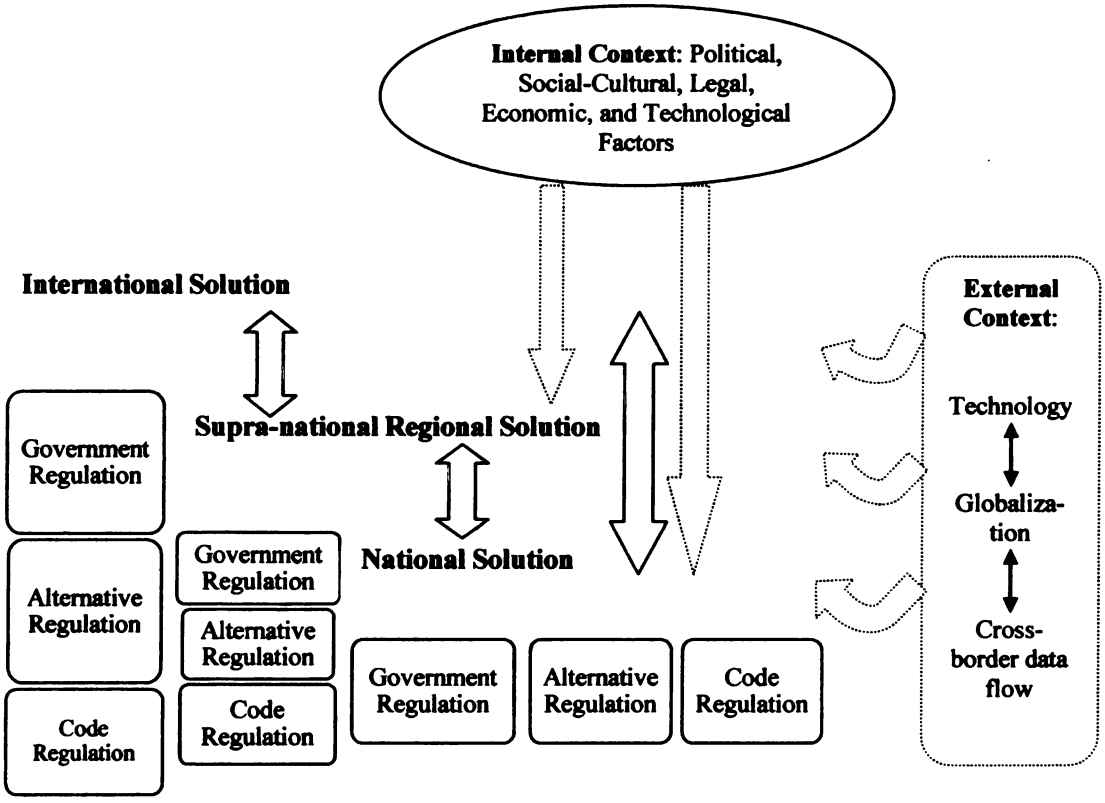

Figure 1 *Conceptual Framework for Personal Data Protection in E-government*

Regarding the *multi-level governance* mechanism, it is a hierarchical governance structure differentiating between global, regional, national, and sub-national governance arrangements, and is the outcome suggested by the theory of complex adaptive systems to assure system coherence (Bauer, 2007). The biggest question of this approach is how to assign tasks to different layers of the governance structure and how to relate these layers to each other, which is one of the questions to be answered in this case study. Due to resource constraints of the dissertation project, the multi-level component is limited to the national and supra-national (supra-national regional and international/global) levels. Data protection actions and efforts at sub-national local levels are not examined in this study. Some more detailed introduction of the governance modes in the conceptual framework and their potential application to the issue under discussion is presented below.

A Synopsis of the Components of the Conceptual Framework

This section presents an overview of the key dimensions of, or governance models in, the conceptual framework that will be used as the reference framework to examine and analyze the e-government personal data protection issue at the domestic and international level. As the major components of the conceptual framework, the alternative governance modes available for the protection of personal data involved in e-government are: *traditional national governmental regulation*, *supra-national regulation*, *alternative regulation* (*self-* and *co-regulation*) and *code-based regulation*.

National Government Regulation

The key function of government regulation/intervention is the "enforcement of laws of general applicability", or producing norms that are enforceable and in most cases

involve legislative process (Weber, 2002, p. 58). Government regulations include both legally-binding laws/regulations (legal regulation) and non-binding 'soft-laws' such as guidelines and various policy recommendations as well as administrative actions.

Although the internet is different from the physical world in many aspects, it shares many similarities with and is increasingly inseparable from the physical offline society. There is great state interest in establishing an ordered online society. Thus, despite its various weaknesses such as 'regulatory-lag' (lagging behind technological advances) (Weber, 2002) and the theoretical feasibility of decentralized governance, government regulation might still be an important tool adopted by nations to address many, if not all, public policy issues caused by the internet, including the information privacy issue in the context of e-government.

While it is hypothesized that government regulation is an important governance mode for the issue under discussion, what specific role this mode plays and how it functions in the governing process of this issue, especially in different national contexts, is still a question. It was mentioned earlier that government regulation of information privacy is found related to the level of privacy concern in a country. Yet notions of privacy and privacy concerns are influenced by many factors such as social, cultural, political, and economical factors (e.g. Bellman et al., 2004; Milberg, Smith, & Burke, 2000). One would therefore expect that governments around the globe take on different approaches towards data privacy protection in general (such as that in the private sector) and in the specific context of e-government, with the former already being proved and the latter to be examined and proved. In other words, the conditional nature of privacy makes it reasonable to hypothesize that government regulation of information privacy as well as

the overall scheme of privacy protection in the particular context of e-government is influenced by national context. An evaluation of this issue at the national level is therefore of great necessity.

Supra-national Regulation

There are different forms of international regulation. Generally speaking, there are two primary kinds of policy outputs at the supranational level: regulations that are legally binding such as treaties and conventions and non-binding 'soft laws' such as guidelines and recommendations (Non-governmental international cooperation and actions will be discussed under 'alternative regulation'). The legally binding international agreements have a contractual character since sovereign states voluntarily consent to be bound. Different from national regulation, international binding agreements and non-binding guidelines very often codify comparatively general provisions or general principles that allow for different enforcement in different state nations.

The global nature of the internet poses great "jurisdictional dilemmas and choice of law problems" (Reidenberg, 1998, p. 572). Its borderless nature makes it difficult in many cases to decide which jurisdiction certain online activity is subject to and it is also fairly easy for malicious people to circumvent certain national laws. Ideally, corresponding to such an 'international' network or structure, a global-level legal framework could be constructed to solve relevant policy issues. In reality, however, there is great difficulty in establishing such a global legal framework considering the substantial differences in political and social-cultural reality and national interests of individual state nations. In this case, whether and how well international solutions could solve online policy issues becomes an open question.

In terms of the specific case of e-government, government agencies today have increased data processing and data sharing across borders. Such practice will increase further as e-government develops around the globe. The borderless nature of the internet also enables people to access websites of foreign governments easily, which might create personal data profile of foreign citizens. This vast increase in cross-border data flow undermines the enforceability of national information privacy laws, especially when the countries involved have different levels of or approaches to privacy protection. How to best avoid possible disagreement among countries on this issue is becoming a big challenge. In this situation, a certain degree of harmonization in data protection at the international level might be desirable to facilitate resolving problems of law conflicts and necessary international data flows in the context of e-government. Further, the borderless nature of the internet makes international standards and actions key to establishing a secure digital infrastructure and to achieving the security of online personal information.

In brief, the global nature of the internet, the growing disputes between jurisdictions and the overall globalization trend during the past decades have resulted in increasing country and policy interdependence, which indicates that the global level will probably arise as a significant arena in which e-government data protection rules are negotiated. Thus the question posed for this study is whether or to which degree joint solutions at global level are possible regarding the information privacy protection in the e-government area.

Alternative Regulation – Self-regulation and Co-regulation

As defined earlier, self-regulation is a kind of bottom-up autonomous regulation. Economic actors, social players, non-governmental organizations (NGOs) and organized

groups voluntarily establish practices, common rules, codes of conduct and agreements to regulate and organize their activities (Eijlander, 2005). Co-regulation is a combination of self-regulation and government intervention. It usually operates upon certain legal basis. According to Latzer et al. (2006), in co-regulation "the possibility of stakeholder involvement is often provided for by the law on which these institutions operate" (p. 164). Private parties in practice often follow certain guidelines, frameworks, or objectives defined by the government. In legal and governance literature, these two governance modes together are often termed as 'alternative regulation'.

Although it is by no means a new phenomenon, alternative regulation is gaining more regulatory importance and recognition in both theoretical works and practice, which is especially true when it relates to the internet. Latzer et al. (2006) pointed out that alternative regulation is mainly employed when industry interests are more homogeneous, as in the case of consumer and data protection. One point to note here is that, unlike in many other cases, in e-government context it is the public sector rather than private industry that is the major party to be regulated, which means that for this case self-regulation is primarily voluntary rules or codes of conduct of government agencies. The specific application of alternative regulation in the case of personal data protection in e-government is to be explored and discussed in the last chapter.

Code-based Regulation

Apart from legal regulation and alternative regulation (self- & co-regulation), the use of 'code-based regulation' is another feature of internet governance. 'Code-based regulation', as the name indicates, refers to the governing of the internet through technical means of computer coding or computer architecture. It is one of Lawrence

Lessig's four modes of internet regulation (law, architecture, norms, and markets) (1999). In his book *Code and Other Laws of Cyberspace*, Lessig argued that code (architecture) is the most effective and most powerful (yet rarely recognized) regulator of the internet, given that computer code exerts self-executing constraints and internet architectural changes can change the nature of cyberspace. Specifically, the importance of code lies in the fact that cyberspace is built on adjustable protocols and standards, and individuals' use of the internet is a function of the code built into the internet architecture, which means that internet architecture can be configured to perform regulatory functions such as controlling access to certain information and communication services (Biegel, 2003). According to Reidenberg (1998), three advantages make technological solutions ("Lex Informatica") a particularly valuable information policy instrument: borderless nature, easy customization, and capabilities of self-enforcement and compliance-monitoring. Although code-based regulation alone cannot solve many practical problems in the online world, such an approach could be a valuable supplement to the other governance modes.

In line with code regulation theory, technological tools and mechanisms can help protect the privacy and security of electronic personal data. Various forms of privacy-enhancing technologies (PETs) exist as useful complements to existing regulatory and self-regulatory approaches in privacy protection. As possible solutions, for example, Reidenberg (1998) described several technological mechanisms that could make information anonymous, or allow users to determine the distribution of personal information. Although these technical arrangements are not a complete solution, they can improve the level of data protection. It is expected, therefore, that code-based regulation is one of the governance modes adopted.

Concluding Remarks

When we talk about governance instruments and/or mechanism of the e-government personal data protection issue as well as other internet governance issues, governance is a broad term that is carried out in different modes, which in this study is reflected in various policy outputs at both national and international levels. The combination of global and local components is one prominent cause of the complexity of the issue under discussion and of the governing of this issue. Theoretically, problems of different nature in the e-government privacy area may better be addressed at respective government levels (e.g., national level vs. international level) and by using different governance modes. Considering the nature of the problem and the macro-environment of this issue (such as globalization), therefore, we may hypothesize that a mix of different governance approaches might be needed to effectively address this issue.

E-government is a comparatively new area for the privacy issue. It is well worth exploring, by examining the relevant laws and policies at national and supranational levels, what governance mechanisms are in place for this issue and how national context shapes the specific governance framework adopted. Meanwhile, however, we should keep in mind that the privacy protection issue in the e-government area is still in the very early phase of development and further changes are undergoing.

Research Questions

As stated earlier, the non-territorial nature of the internet and the globalization trend featured by increasing country interactions, interdependence, and cross-border data flows create a need of global regulation and cooperation and might also create a trend of privacy policy convergence. But meanwhile a considerable divergence in terms of policy

instruments might also exist due to the conditional nature (e.g. social, cultural and political differences) and problem nature (e.g. local. vs. global problems) of the privacy issue in e-government. To clarify these uncertainties, a set of research questions are put forward to examine the current information privacy protection practices in the context of e-government by different national governments and to explore whether or at which degree international solutions are possible regarding this issue. Given the numerous changes affecting privacy that had occurred with the development of e-government, one of the specific aspects to look is how different governments view the sufficiency and relevance of the existing legal framework to protect personal data in e-government area. Are there modifications and revision on previous laws or are there new privacy legislations drafted taking into account this specific issue?

Research questions are also proposed to evaluate the respective role that different governance modes play in the current practices coping with this issue, therefore contributing to the open question of which governance mechanisms might be best suited to address this issue and how the national context affects the mechanisms adopted. For the latter purpose, I will profile each country with regard to the specific mix of governance instruments in the discussion part.

The specific research questions and hypotheses are posed as follows:

RQ1: How have different countries responded to the privacy issue in the context of e-government? Specifically,

RQ1a: How have different countries legally defined privacy and interpreted privacy rights?

RQ1b: Have the countries responded to the privacy concerns in e-government area by changing or updating the existing legal framework such as by modifying, revising or enforcing new privacy legislations?

RQ1c: What legal, regulatory, organizational, technological, and other arrangements have the sampled countries adopted to protect personal information privacy in the context of e-government? What are the most distinct similarities and differences in these arrangements across different countries?

RQ2: In terms of the governing mechanism, what is the mix of local and global solutions for this particular area of internet governance? Specifically,

RQ2a: As an issue with a strong local component (socially and culturally conditioned), what challenges does the protection of information privacy in e-government raise for finding appropriate solutions at an international level? How well does the existing international regulatory framework address this issue?

RQ2b: In the e-government privacy domain, to what degree is the nature of a specific problem (local problem vs. global problem) aligned with the level at which a solution is sought (local solution vs. global solution)?

RQ3: Which or which mix of governance instruments have the sampled countries adopted to address the information privacy issue in e-government? How does national context affect the specific governance mechanisms adopted? Specifically, four conjectures are proposed:

RQ3a: The existing legal system of a country impacts the form and level of protection and the choice of governance modes with respect to data privacy and security in the context of e-government in that country.

RQ3b: National differences in the attitudes toward and the social value of privacy, as reflected in existing laws and regulations, influence government regulation of data handling practices in the context of e-government.

RQ3c: National differences in the tradition of privacy protection influence the form and level of data protection in the context of e-government.

RQ3d: The level of economic and technological development and the political regime of a country affect the roles of different governance instruments used in the protection of privacy in e-government adopted by that country.

RQ4: Which set of governance instruments is the most effective to protect personal data in the particular context of e-government? Specifically,

RQ4a: What role do different governance modes (national government regulation, international regulation, alternative regulation, and code-based regulation) play in the current practice of personal data protection in the e-government context?

RQ4b: What is the available evidence about the effectiveness of the governance modes adopted to protect information privacy and security in e-government?

In brief, this dissertation (1) reviews legislative and administrative actions relevant to data protection in e-government in the selected countries and relevant international arenas, and (2) theoretically explores and discusses the governance

mechanism of the e-government information privacy issue as a case of internet governance.

Research Methodology

Use of a Qualitative Case Study Approach

This study uses a qualitative methodology. An in-depth case study approach is chosen as the primary research method. Being defined as an intensive study of a single unit aiming to generalize across a larger set of units (Gerring, 2004), case-study research methodology has been recommended by many researchers for study areas that are not yet well understood and lack formal theories (e.g. Flynn, Sakakibara, Schroeder, Bates, & Flynn, 1990; Yin, 1984), which is the case with the area of personal data protection in e-government.

Bent Flyvbjerg (2001; 2006), a renowned scholar in the field of social science philosophy, gives high credence to the in-depth case study method and argues for greater use of this approach, which has often been denigrated as producing biased and unreliable information. He examined five major criticisms of case studies and corrected them one by one based upon theoretical reasoning and factual support. These five misunderstandings are: (a) theoretical knowledge is more valuable than concrete and practical knowledge; (b) one cannot generalize based on an individual case; (c) case studies are most useful for generating hypotheses rather than hypotheses testing and theory building; (d) a case study tends to confirm the researcher's preconceived notions; and (e) it is often difficult to summarize specific case studies (Flyvbjerg, 2006). To correct these misunderstandings, for instance, he showed that case study can be used for hypothesis testing through the process of "falsification". Yin (2003) also noted that the case study method may be

involved in all three roles including exploratory and descriptive purposes, evaluation, and hypothesis testing. Barkley (2006) posited that "the complexities, contradictions, and causal relationships in a situation may be more readily revealed in case studies than alternative research methodologies" (p. 12). Although context-independent explanations and theoretical predictions drawn from large sample research (such as quantitative survey analysis) is essential to the development of social sciences, context-dependent and practical experience gained from case studies are equally important, or even more important as Flyvbjerg (2001) argued, for social sciences. To advance social sciences, case study research should complement large-sample analysis. The key is, as Flyvbjerg states, "good social science research is problem driven and not methodology driven" (2006, p. 242).

While the balance between case studies and large samples has been quite biased in favor of the latter in social science, the value of case study research should be revisited and emphasized because of the 'depth' it can add to the analysis (the advantage of large sample studies is 'breadth') (Flyvbjerg, 2001, 2006). With good research design, such as by selecting cases of different natures, the result of a case study research can provide both 'the depth and richness' necessary for enlightened public policies (Barkley, 2006). For this reason this method has been gaining increasing popularity in the public policy literature. It is thus chosen as the method for this study to further our understanding of the data protection issue in e-government, which is not yet well understood and requires rich context-dependent knowledge and practical experience to assist relevant policy-making.

Aiming to understand the current status of the personal data protection issue in e-government and its overall governance mechanism, this study examines and analyzes

relevant laws and policies in different countries and protection measures/schemes adopted at relevant (to the selected countries) international levels. To do that, relevant legal documents, policy documents, government publications, relevant international activities, and academic literature are reviewed. The goal, however, is not to provide a complete and detailed analysis and evaluation of the laws/policies content and operation but rather to identify the general scope and general pattern of relevant controls.

The unit of analysis is a country. As presented earlier, the conception of privacy is socially and culturally conditioned, which makes privacy protection a very good issue for comparative studies. Moreover, the internet's non-territorial nature, the unique nature of electronic data, and the ubiquity of privacy concerns (though with different awareness and priority levels) make the privacy, as well as e-government privacy, protection issue an essentially global policy issue, which indicates that this issue cannot be thoroughly and adequately analyzed and understood by looking at only one singly country. Due to these reasons, a multiple-case approach is adopted, through which we can see how the e-government privacy protection issue is addressed in different countries and the overall governance mechanism of this issue across countries and beyond country. A total of three countries were selected to achieve the study purpose.

Case Selection

Selection of cases is a very important aspect of building theory from case studies. While cases may be chosen randomly, random selection is not necessary for case studies (Eisenhardt, 1989). For instance, given the limited number of cases which can usually be studied, some scholars suggested that researchers choose cases of extreme situations and polar types in which the process of interest is transparently observable (Eisenhardt, 1989;

Pettigrew, 1990). In addition to random selection of cases, Flyvbjerg (2001) also suggested another category of case selection -- information-oriented selection, which includes four different strategies for case selection: extreme/deviant cases, maximum variation cases, critical cases , and paradigmatic cases (see Table 2). The various strategies of selection are not necessarily mutually exclusive.

Table 2 Strategies for the Selection of Samples and Cases

Type of Selection	**Purpose**
A. Random Selection	To avoid systematic biases in the sample. The sample's size is decisive for generalization
1. Random sample	To achieve a representative sample that allows for generalization for the entire population.
2. Stratified sample	To generalize for specially selected subgroups within the population.
B. Information - Oriented Selection	To maximize the utility of information from small samples and single cases. Cases are selected on the basis of expectations about their information content.
1. Extreme/deviant cases	To obtain information on unusual cases, which can be especially problematic or especially good in a more closely defined sense.
2. Maximum variation cases	To obtain information about the significance of various circumstances for case process and outcome (e.g., three to four cases that are very different on one dimension: size, form of organization, location, budget).
3. Critical cases	To achieve information that permits logical deductions of the type "If this is (not) valid for this case, then it applies to all (no) cases."
4. Paradigmatic cases	To develop a metaphor or establish a school for the domain that the case concerns.

Source: (Flyvbjerg, 2006)

In this study, a mixed selection strategy of maximum variation cases and paradigmatic cases is used. Specifically, legal and policy documents of three countries are scrutinized. The three countries are the US, Germany and China (excluding the

special administrative regions of Hong Kong and Macau, which have their own legal systems). These three cases were chosen because they are very different on three dimensions: distinct traditional privacy philosophies and privacy protection models, different e-government development levels, and dispersed location. These differences make it possible to obtain maximum variant information on the issue under discussion. At the same time, these three countries could be regarded as falling into three general paradigms in terms of culture, economy, law system, and traditional privacy protection. The use of such a mixed strategy is expected to provide a unique wealth of information on the issue I want to discuss.

Traditional Privacy Protection

The foremost rationale for the country selection in this study is the historical approach to the privacy issue. As is widely known, the EU and the US have historically taken different stances on the privacy issue and adopted distinct privacy protection models. Their models represent the two most dominant frameworks of privacy protection in the world. Germany is chosen randomly as a representative member country of EU that has traditionally treated privacy as citizens' fundamental human right and has quite stringent rules in protecting citizen's informational privacy, while the US treats privacy right more as a property right that could be given up and is widely known for its self-regulation privacy protection model in the private sector. Regarding China, it is one case of a developing country, many of which have historically treated citizen's privacy as a low priority issue for various reasons, including different political systems and social needs. However, privacy is starting to gain attention there in recent years. This difference in traditional privacy protection schemes could be an interesting starting point

for us to look at the governing pattern of the personal information protection in the newly-thriving area of e-government. The traditional privacy protection schemes might or might not be applied to the e-government domain.

E-government Development

Since the topic under discussion is privacy protection in the context of e-government, it is reasonable to assume that the protection measures and the overall governance structure of this issue in a country might have some connection with the e-government development level in that country. According to the 2008 UN global e-government readiness report, the overall e-government ranking of the US is No. 4, Germany No. 22, and China No. 65, which indicates that the three countries hold quite different positions on the continuum of e-government advancement. The US leads most countries and is among the pioneers of e-government adoption. Germany is a relative laggard compared to the US, yet overall is one of the countries with advanced e-government services. China lagged behind most developed countries in e-government deployment. But its substantial online government presence (as indicated by its ranking) makes China a reasonable case to represent those countries with less developed e-government services.

Location

The last criterion used to select the cases is location. The selected countries are dispersed on different continents, or in different regions, of North America, Europe, and South-East Asia, which are three major economic blocks in the world. As mentioned earlier, development in economics, more specifically the economy regionalization, has

created a governance response and space for regional governance, such as in the case of the EU (Chhotray & Stoker, 2009). Moreover, countries in the same region may very well share similar conceptions of privacy because of similar historical origins and culture elements. These two factors render the selected countries able to represent other countries in the same region to a certain degree.

Use of Expert Interviews

To complement findings from documentary search and analysis, a series of in-depth interviews were conducted with individuals who have substantial knowledge of personal data protection in general or in the specific area of e-government in the US, Germany, and China. The interviewed experts are from government agencies, non-government organizations, and scholarly fields. Detailed content analysis of the interviews is not conducted. Instead, the viewpoints and inputs gained from the experts are treated as supplementary information to support and ensure the completeness and accuracy of my documentary findings. In other words, the purpose of the interview design is to ensure a diversity of perspectives in order to reduce bias in my data.

Selection of interview participants was based on a convenience sampling approach. First, due to the short history of e-government and of the privacy protection issue in this area, there is a scarcity of scholars specializing on the exact topic under discussion. In this case, scholars knowledgeable on personal data protection in general were sought for consultation. The list of scholars comes from two main sources: literature review and peer recommendation. Background search was conducted to ensure their expertise on the topic before initial contact. Second, a few key government agencies and non-government organizations whose work are closely related to the e-government

privacy protection issue were contacted via e-mail, in which they were asked to help identify somebody in the organization who has expertise on this issue. In both cases, when there was no access or no convenient access to interested individuals and agencies/organizations, social networking resources were used. Acquaintance referring was used to contact the interested individual experts or agencies in this case. The experts involved were from the US Office of Management and Budget (OMB), the Federal Ministry of Interior of Germany (BMI), Electronic Privacy Information Center (EPIC), as well as the academic and legal field. (The list of organizations from which experts were interviewed is attached in Appendix A.)

After explicit agreement to participate in a telephone interview was obtained via e-mail and the list of experts was finalized, a structured questionnaire and consent form was e-mailed to the experts before formal interviews. A 30-60 minute telephone interview was conducted with each individual expert to systematically explore the current practice of personal data protection in e-government in each of the three countries and relevant international arena. Interview questions are customized to reflect the particular role and circumstances of each specific interviewee. A total of seven interviews were conducted (six via telephone, one via e-mail), with two interviews for the US, three for Germany, and three for China (one of the experts was expert on both Germany and China). Some of the experts were consulted with follow-up questions in the writing process via e-mail.

CHAPTER 3

THE DEVELOPMENT OF E-GOVERNMENT

As briefly introduced earlier, the three countries of the US, Germany, and China differ in e-government development levels. In this chapter a more detailed introduction of e-government development, e-government application, and e-government strategies in the three countries is provided as background information for the following overview and analysis of the data protection issue in this specific context.

E-government in the United States

With the emergence of the internet and World Wide Web technology, the US government began to deliver online information and public services from the early 1990s. In the late 1990s the term e-government began to take form for the federal government (Relyea & Hogue, 2004). In 2000, the US government launched its official web portal – FirstGov.gov, which was renamed to USA.gov in 2007. Aiming to provide "one-stop shopping" for citizens, it allows easy access to any government service from one portal, which serves as a catalyst for the growing use of e-government in the US.

The growth and development of e-government in the US was greatly advanced by the executive branch as a tool of "bureaucratic reform" (Fountain, 2009). A number of acts and policy initiatives were created to help promote e-government. During the Clinton administration, for instance, the 1998 *Government Paperwork Elimination Act* and the 1999 *Presidential Memorandum on Electronic Government* played an important role in promoting government use of the web to deliver public service. Take the latter for example, by ordering the top 500 forms used by citizens to be placed online and directing

agencies to construct a citizen-oriented and secure e-government infrastructure, the 1999 memo represents "the Clinton Administration's first concrete attempts to begin implementing e-government government-wide" (Seifert & Chung, 2009, p. 5).

Bureaucratic reform through e-government was continued by the Bush administration. Various policies and initiatives were carried out to guide, stimulate and promote e-government. For instance, in 2001 the Bush Administration issued the *President's Management Agenda (PMA)*, which included "Expanded Electronic Government" as one of its five government-wide initiatives. The PMA e-government initiative emphasized the need to break down bureaucratic agency barriers, increase cross-agency interoperability and information flows and sharing (U.S. Executive Office of the President, 2001). To achieve this vision of e-government, the PMA outlined a range of potential e-government projects such as e-procurement, e-grants, e-regulation, and e-signatures. Overall, e-government in the US has been driven by two key guiding principles: creating business-like efficiency and providing citizen-centered services, which conform to the subtitle of Vice president Al Gore's 1993 *Report on Reinventing Government* -- "building a government that works better and costs less". This bureaucratic reform goal was also echoed in the PMA by underscoring the core values of its Expanded Electronic Government initiative: improving citizen-oriented service and saving cost.

In addition to the above acts and policies, various other actions were taken in the following years by the administration to advance e-government at the federal level in the US. Some of the crucial measures are the Quicksilver cross-agency initiatives, the Federal Enterprise Architecture initiative, the Lines of Business Initiatives (Fountain,

2009; Seifert & Chung, 2009), OMB (Office of Management and Budget) e-government strategies, and the *E-Government Act of 2002*. With these strategic guiding, the U.S. federal government has made notable progress on e-government in the past decade.

Based on a comprehensive analysis of 1,537 state and federal government websites, West (2008b) found that by mid-2008 89% of state and federal websites in the US had services that were fully executable online. Meanwhile, his global survey (2008a) of e-government ranked the US No. 4 among the 198 surveyed nations. This rank coincides with the one derived from the UN's e-government readiness report (2008) despite the use of different measurement schemes. The former assessed only government websites features and the latter used an overall e-readiness index consisting of website assessment, telecommunication infrastructure and human capital resources. More specifically, the UN report found that, among the 192 countries under study, the US scored No. 1 on e-participation functions, No. 4 on transactional services, and ranked No. 3 on the overall Web Measurement Index (which measures the overall web features and functions of government websites). In sum, the US has been among the leading countries in e-government and its federal government web system is regarded by the UN as a model for e-government in other countries.

E-government in Germany

The German government is regarded as a comparatively late adopter of e-government among the industrialized countries. While e-government trials were started from the late 1990s at the local level, the German federal government launched its first e-government strategy *BundOnline 2005* in September 2000, then the largest e-government program in Europe. Presenting the e-government vision for the years 2000-2005,

BundOnline 2005 was regarded as Germany's key *'first generation'* e-government initiative. Its objective was to make available online all federal public services capable of electronic delivery by the end of 2005 and to enable citizens and industry to use government services more simply, rapidly and cost-efficiently. Emphasizing the citizen- and service-oriented concept, *BundOnline 2005* was regarded as an important tool to modernize the federal administration in Germany.

Like e-government efforts in many other countries, this federal level initiative made e-government a mandate in Germany. In March 2001, the federal service portal *Bund.de* was launched to provide a central gateway to the online services of the federal administration. From December 2001, the *BundOnline 2005 Implementation Plan* was issued annually through 2005 to guide the e-government initiative, accompanied by an annual report informing the public of the overall e-government progress. According to the BundOnline final report (Federal Ministry of the Interior, 2006a), the initiative was successfully completed with 440 federal government services available online by the end of 2005, which exceeded the number initially planned.

Following *BundOnline 2005,* the German government has implemented a range of other measures and initiatives to accelerate the development of e-government in Germany. One important *second generation* e-government initiative was *Deutschland-Online,* which was launched jointly in 2003 by the federal government, the federal states, and the municipalities to achieve an integrated e-government structure across different administration layers. More specifically, it aims to integrate portals and e-services, develop common e-government infrastructure and standards, and share e-government knowledge and experience across all levels of government in Germany. To support the

above strategic guidelines, *Deutschland Online Action Plan* was published annually from 2006 to provide concrete action guidance. Engaging different layers of government in one joint undertaking, *Deutschland Online* is viewed as an effort "to overcome the lack of coordination between the different layers that has been identified as a major obstacle to e-government in Germany" (European Commission, 2005, p. 6).

While the *BundOnline 2005* and *Deutschland-Online* initiatives provide the general policy framework and solid groundwork for e-government development, the German government has also made efforts to expand its e-government services and integrate its e-government strategy into the European e-government landscape. To comply with the objectives defined by the European Commission in the *EU i2010- A European information society for growth and employment* initiative, the Germany federal government developed and adopted the *eGovernment 2.0* programme as new strategy for 2006-2010 (Federal Ministry of the Interior, n.d.). The *eGovernment 2.0* programme identifies four fields of action to expand e-government services by 2010, which include expanding e-government with demand-oriented quality and quantity, enhancing business-government cooperation, creating a secure communication infrastructure, and securing electronic transactions by using e-Identification Cards (Federal Ministry of the Interior, 2006b).

Guided by these centrally managed e-government initiatives and a range of other action plans and policies, e-government in Germany has been advancing steadily. Though globally it does not make one of the top countries regarding e-government presence, Germany ranked quite well in various international e-government comparison studies. For instance, the West global e-government study (2008a) ranked Germany 7th on its

web government functions. The result from the UN study yielded a little different picture due to the different evaluation criteria and scope (the former study assessed both national and local e-government yet the latter only evaluated national-level services). The UN (2008) ranked Germany number 22 out of 192 countries on the composite e-Government readiness index for year 2008. For its component of Web Assessment Index that is directly related to the delivery of online government services, Germany received a lower ranking of 33 due to its relatively low score for the transactional and e-participation functions.

While the above studies show some discrepancies in the global ranking of German e-government, data from *Eurostat* concerning e-government offerings in Germany can provide some more indication of the current status of e-government in the country. Looking at the supply side, statistics published by *Eurostat* showed that in 2007 74% of government services were fully available online in Germany. From the demand side, in 2008, around 33% of citizens in Germany made general use of e-government offerings, while 31% of citizens visited government websites to gain information, 16% download forms, and 10% filed forms electronically. These numbers indicate that there is ample room for further development and popularization of e-government in Germany.

E-government in China

From the mid-1980s, informatization *(Xinxihua)* has been regarded as a driving force for modernization and economic development in China, and has been a key component of China's development policy and strategy. To keep pace with the rapid social and economic changes, the Chinese government has made efforts to reform its administrative system to overcome its inefficiency and bureaucracy. Under these

circumstances, the Chinese leadership views government informatization (e-government as the core) as good opportunity to transform administrative functions and promote economic development. In addition to improving administrative efficiency and effectiveness, the introduction of e-government is believed to be able to accelerate the process of informatization in China, both by setting a good example for private enterprises, and by making government a major consumer of computer industry products to boost the national production of hardware and software as well as e-commerce (Zhang, 2003). E-government is also regarded as a means to catch up with other countries and to build a good image for Chinese government internationally.

As a strategy to drive informatization, the Chinese government demanded in the early 1990s that all government offices move online step by step, starting with information-delivering websites and then developing more complex and comprehensive interactive services. The three "Golden" projects launched from 1993 (before China's direct full connection to the internet in 1994) became the roots of e-government in China. In 1999, China's first official e-government initiative *Government Online Project* was started, together with the trial operation of the national government's portal www.gov.cn, which was, however, not officially launched until January 2006. Dividing the e-government project into three stages, the main goal of the initiative is to build up and interconnect government websites at both national and provincial levels, and create a centrally accessible online administrative system.

In 2001 and 2002, the State Informatization Leading Group (SILG), which is in charge of setting general policies and standards for China's e-government initiatives, held its first and second meetings, when the group issued e-government framework and

specifications, and promulgated several official documents to guide Chinese e-government practice. One important document is the *Guiding Suggestions on Constructing China's E-Government*, or *Decree No. 17* (China Internet Network Information Center (CNNIC), 2006), which lists the main objectives and tasks of China's e-government initiative. It was at these meetings that the Chinese leadership officially designated government informatization as a national strategy to advance the economy and informatization of society. The promotion of e-government is at the core of government informatization and considered to be a critical strategy to drive the "information economy".

From then on, e-government development in China entered a period of overall advance. As stated in various government reports and policies, the main goals of e-government in China can be summarized as follows: to (1) reduce the cost of administration and enhance efficiency, (2) promote government accountability by increasing the transparency and fairness of government work, (3) reduce bureaucracy and corruption, and (4) improve public service. It could be seen that reforming the public administration is the key purpose of China's e-government initiative, which is expected to ultimately drive economic development.

In March 2006, to comply with China's *11th Five-Year (2006-2010) Plan for National Economic and Social Development*, the SILG issued the *General Framework of National Electronic Government* as a new five-year plan for e-government. This new strategic framework announced the starting of a new e-government development phase in China that features popularizing use of e-government. Some of the important goals by 2010 include constructing a unified national e-government system, making available

online 50% of government services, and establishing a basic legal framework for e-government.

Under the guidance and push from central government, e-government initiatives at national and local levels in China have been evolving rapidly. According to a report by the China Internet Network Information Center (CNNIC) (2009), there were 45,555 gov.cn domain names and 24,912 gov.cn websites by the end of 2008, which is more than 25 times the number in 1999. All the 31 provinces in mainland China have established government portals. By December 24, 2009, the central government portal www.gov.cn has connected more than 70% central (national-level) government agencies and all the 31 provincial portals[4]. Compared to many developed countries such as the US, however, e-government in China is still at a comparatively early stage, with more emphasis on information delivery and basic interactional and communicative features, yet very limited transactional functions. However, an increasing number of government agencies in China have been exploiting online communications tools to enhance citizen participation (Wu & Bauer, 2009). The 2008 UN global e-government report ranked China 20th on its e-participation index. The overall e-government readiness index ranked China at No.65 globally and the web measurement index ranked it at No. 47. Although the global survey shows that China still has a long way to go in e-government development, the rapid expansion of the online infrastructure and active users (with the biggest online population in the world) in China during this decade create tremendous potential for the expansion of e-government and transformation of the public sector in the country (United Nations, 2008).

---

[4] http://news.xinhuanet.com/politics/2009-12/24/content_12700015.htm

More specific data from the recent CNNIC report (2009) on e-government use shows that about 33% of internet users in China have never visited government websites, while 18% internet users reported visiting government websites multiple times a year, 16% visiting multiple times a month, and 6% visiting multiple times a week. Among the visitors, the majority of people (94%) visited government sites for information, while 16% of the visitors downloaded forms, 8% used them for online consulting, and 2% for online complaints and online suggestions to government. The numbers have remained quite stable during the past three to four years. The low number of government site visitors/users to some degree indicates that there is ample room to popularize e-government use among citizens in China while the Chinese government is striving to construct a sophisticated and integrated e-government platform.

CHAPTER 4

A COMPARATIVE ANALYSIS OF PRIMARY PERSONAL DATA PROTECTION LAWS FOR E-GOVERNMENT

The distinctive social, cultural, political contexts and regulatory legacies across countries and regions create a diversity of regulatory frameworks, including internet regulations, around the globe. Take personal data protection in the private sector for example, it is widely acknowledged and documented that the US and Europe adopt fundamentally different approaches to protect individuals' privacy -- self-regulatory approach by the US and strict legislative intervention approach by Europe (e.g. Baumer et al., 2004; Steinke, 2002; Strauss & Rogerson, 2002). Disparity might also exist with respect to personal data protection in the particular context of e-government. This chapter and Chapter 5 present a comparative overview of the national regulatory frameworks of personal data protection in the area of e-government by the US, Germany, and China. Considering the limitation of paper length, my exploration of related laws and policies in this study only focuses on federal/national laws. Local laws and policies on personal data protection are not reviewed in this study.

National Administrative and Legal Context

General Political and Legal Context

The particular political and legal contexts of the US, which include its hierarchical power division among federal and state governments, the tripartite (executive, legislative, and judicial) government system, and its common law system, determines the complexity and source disparity of legal regulation in the US (Cate, 1997). The US

federal government and the 50 states share sovereignty, which means that American citizens are affiliated to two sovereign entities (Hagen, 2004). The US constitution grants the states great power in administration and legislation (Tenth Amendment). Thus privacy protection in the US is based upon various laws and policies of different natures as well as different protection degrees at both the federal and state levels. Moreover, court interpretation and application of existing laws and legal precedent also create "a body of disparate case law" (Cate, 1997, p. 49). Examination of case law as well as state-level laws and policies are beyond the scope of this study; nevertheless, it should be noted that they are also very important to understand the whole picture of the e-government privacy protection scheme in the US.

The Federal Republic of Germany is also composed of a federal level (Bund) and a state level (Länder). The Basic Law (German Constitution) grants the states a high degree of administrative and legislative autonomy (e.g. Article 28, 70). So the Länder (a total of 16) have their own legislative and executive bodies (European Commission, 2008). Although the states are empowered to implement their own laws, a majority of federal laws are also implemented by the states (Article 83-91). Regarding data protection, in addition to the *Federal Data Protection Act* and other federal-level laws that is examined in this study, at the state level the Länder implement their own data protection laws that are largely based upon this federal act. The state-level data protection laws, however, are not examined here. With respect to legal system, Germany is a civil law country, which differs from the US common law system.

China is a historically highly-centralized country with a unitary political system. There are 31 province-level administrative units, if excluding the two special

administrative regions of Hong Kong and Macao that have separate legal traditions and systems. Despite the high concentration of power in the hands of the central government in China, provinces enjoy quite much autonomy in the area of economic and social development (Tan, 2006) and has limited legislation power on enacting local regulations that are consistent with national laws. China is largely a civil law country, with strong influence from the European, in particular German, legal system (Chen, 1999).

Constitution and Privacy Protection

The United States

The US Constitution does not explicitly mention a right to privacy. However, the amended Bill of Rights protects some specific aspects of privacy, in most cases against government actions, such as freedom of expression and religion (First Amendment), home privacy (Third Amendment), and right to be against unreasonable search and seizure (Fourth Amendment). Yet there is no Constitution provision specifically protecting individuals' information privacy.

Other than the above specific privacy elements, privacy protection in the US, including information privacy protection, is largely based upon case law and the Supreme Court's interpretations of the Constitution. Supreme Court decisions over the years have ruled that the right to privacy is generally protected by the Constitution's Ninth Amendment, which states "the enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people", and is also broadly protected by the Fourteenth Amendment's due process and liberty clause (Adams, Bocher, Gordon, & Barry-Kessler, 2005; Cate, 1997). The US legal system traditionally treats privacy as a personal property right that may be disposed at the discretion of individuals

instead of "an unassailable human right"(Long & Quek, 2002, p. 332). It is based upon this property right nature of information privacy, the Fifth Amendment was extended by the Court to be able to provide some protection for the privacy of personal information and stored data in the name of property taking (Cate, 1997). In sum, despite a lack of explicit protection of privacy right, the Constitution of the US does provide some implicit privacy protection for the public.

In the US, privacy protection is mainly achieved through privacy torts. "Public disclosure of private facts" is one of the four privacy torts in the US, while the other three privacy torts are: intrusion upon seclusion or into private affairs, publicity placing an individual in a false light, and appropriation of an individual's name or likeness. (Privacilla, 2002; Prosser, Keeton, Dobbs, Keeton, & Owen, 1984). Most states have adopted the privacy torts by common law or statute, which recognize a civil right of action for privacy invasion (Privacilla, 2002; Privacy International, 2007d).

Regarding the protection of personal data or information privacy, the US has no comprehensive law governing the collection and use of personal data by both the public and private sectors. Historically the US has been more concerned with government violations of privacy than with private sector intrusions (Schwartz & Reidenberg, 1996), which is partly shown by the constitution's provisions. Therefore the public sector is under more government regulation regarding information practices, while self-regulation is the primary approach to information privacy protection in the private sector. A second key element of the US data protection regime is its sectoral approach to information privacy protection, in which specific laws protect specific categories of personal information such as financial records, medical care records, children's personal

information, and personal information in government's hands.

Germany

The German Constitution, officially the *Basic Law for the Federal Republic of Germany*, explicitly protects communications privacy as citizen's basic right under Article 10 by declaring that privacy of correspondence, posts and telecommunications inviolable[5]. Article 13 protects home privacy. Moreover, the Federal Constitutional Court ruled in 1983 that individuals have a 'right of informational self-determination' based on Articles 1 and 2 of the Basic law, which declare human dignity and personal freedoms are inviolable (Electronic Privacy Information Center, 2007). In brief, the German Constitution treats privacy as an inviolable fundamental human right and provides explicit protection for communications privacy and home privacy. It also provides implicit protection for information privacy.

As the home country of the world's first data protection law[6], Germany is believed to have one of the strictest data protection laws in the EU as well as in the world (Privacy International, 2007c). For instance, it is found that German data protection index ranks No. 1 in Europe (Reigada, 2006). Germany has a comprehensive data protection act that governs personal data use by both the private and public sectors.

China

Similar to the German Constitution, the Constitution of the People's Republic of China mentions the right to privacy explicitly. It protects communication privacy as

---

[5] The latest official English translation of the Basic Law (2008) is available at http://www.bundestag.de/interakt/infomat/fremdsprachiges_material/downloads/ggEn_download.pdf.

[6] The world's first data protection law was passed in the German Land of Hessen in 1970.

citizens' fundamental right under Article 40. In addition to this provision, Article 37 defines the protection of personal freedom, for instance, against unlawful search and arrest. Article 39 protects the residence. Moreover, Article 38 declares that citizens' personal dignity is inviolable, which does not regulate privacy per se yet it is regarded as the foundation for privacy protection in many cases in China. The Constitution does not provide explicit protection for information privacy.

China currently has no specific privacy and data protection laws. However, with the rapid development of digital technology and pervasive use of the internet, privacy concerns have been increasingly expressed by the general public, academics, legal experts, and the government itself through various channels, which include channels as informal as netizens' online postings and as formal as official proposal by representatives on National People's Congress (e.g. the 11th National People's Congress in March 2008). Passing a major privacy and data protection law is becoming pressing in China.

Comparison Summary

Two main aspects directly relevant to personal data protection in e-government are discussed in the previous paragraphs: the constitutional protection of privacy rights and privacy protection traditions in the three countries.

First, the privacy concept and constitutional protection of privacy differ across countries. In Germany, privacy is explicitly protected by the constitution as a basic human right, which justifies considering Germany as one of the countries with the most comprehensive and strictest regulation on personal data use in both the public and private sectors in the world. According to Cate (1997), the high value placed upon privacy protection by this " fundamental human right" concept justifies "sweeping regulation"

and "considerable costs" (p. 42) imposed upon all relevant stakeholders, including government agencies, and upholds privacy regulations against challenges from other interests. In the case of the US, although privacy right is recognized as an important right to be protected, the constitution does not provide explicit privacy protection, which to certain degree reduces the value of privacy interests, especially when they are weighted against other more explicit constitutional rights (Cate, 1997). Further, instead of fundamental human right, privacy right in the US is treated more like an individual's property right that are likely to be given up by individuals. This concept of privacy to some degree limits the privacy protection scope in the US and creates a less strict privacy protection regime than Germany. With that being said, it should be noted that the constitutional emphasis against government misbehaviors lays a comparatively more solid foundation for personal data protection in the public sector (and thus for e-government) than in the private sector in the US. Regarding China, although its constitution provides explicit protection for privacy, the concept of privacy is not commonly known or realized in people's daily lives until the recent years when internet application and consequent privacy intrusion become increasingly pervasive.

Second, the general personal data protection paradigm or tradition is greatly diversified across countries. There is no single form of data protection law or uniform data protection approach around the globe. As is briefly mentioned above, Germany has one of the world's most comprehensive data protection laws, which governs both the public and the private sectors. This is consistent with Germany's civil law legal system in which statute codes are established to regulate various aspects of social life in great details. The US adopted sectoral approach to only regulate the public sector's use of

personal data as well as some specific categories of personal data, while self-regulation is the primary approach to information privacy protection in the private sector. As a civil law country, China will also adopt the German approach -- a comprehensive data protection law governing both the public and private sectors, according to a legal expert who has been actively involved in the drafting process of China's first data protection law. Yet the great insufficiency of legal measures on privacy protection for both the public and private sectors currently provides Chinese people minimum protection against personal data misuse by various parties.

Primary National Data Protection Laws Governing E-government

In this section the major laws regulating information practices of relevant parties, especially the government sector, with respect to the context of e-government in the three countries are reviewed under four subheadings: what are the major laws, data protection scope, data protection principles and requirements, and supervisory authorities.

Major Federal/National Data Protection Laws

The United States: Privacy Act of 1974 and E-government Act 2002

Although there is no single omnibus data protection law in the US for both the private and public sectors, there is a general law protecting the privacy of personal data in government's hands, which is the *Privacy Act of 1974(5 U.S.C. § 552a)*. It is "one of the first and still the most important federal statutes" protecting personal information privacy in the US (Adams et al., 2005, p. 3). The act regulates federal agencies' collection, maintenance, use, and dissemination of personally identifiable information on individuals

held in 'systems of records'. Thus it applies to personal information privacy protection in the context of e-government.

Moreover, the collection and use of citizens' personal information by federal government agencies in the specific context of e-government are also regulated by the *E-Government Act of 2002*. With the increasing use of internet technology and the development of e-government, the *E-government Act of 2002* (*Public Law 107-347, 44 U.S.C. Chapter 36*) was signed into law in the US in December, 2002. While the *Privacy Act* is a comprehensive data protection law governing the public sector's handling of personal information, the *E-government Act* is a comprehensive e-government law that establishes a broad regulatory framework for e-government in the US, which, among various issues, includes the personal data protection issue.

The *Privacy Act of 1974* and the *E-Government Act of 2002* provide the major requirements for federal agencies' protection of personal information privacy in the context of e-government in the US.

Germany: Federal Data Protection Act

Germany has a comprehensive data protection law--the *Federal Data Protection Act* (Bundesdatenschutzgesetz or BDSG)[7] --governing the collection, processing and use of personal data by public federal authorities, public state (*Länder*) authorities (if there is no state regulation) as well as private parties. It was passed in 1977, reviewed in 1990, and then amended in 1994 and 1997 (European Commission, 2008). The law was further revised and then took effect in 2002 to adapt to the *EU Data Protection Directive* (95/46/EC) by adding provisions, for example, on cross-border personal data flow and

[7] The official English version of this act is available at http://www.bdd.de/Download/bdsg_eng.pdf.

sensitive data (Privacy International, 2007c). It was then amended in 2006 and the latest amendment occurred in 2009 (some revisions came into force on September 1, 2009, others in 2010 or later). All of the sixteen Länder have their own data protection regulations covering the public sector of the Länder Administrations (Privacy International, 2007c; Reigada, 2006). There is no overall e-government law in Germany and the personal data handling in e-government is primarily governed by this act.

Although e-government is not specifically mentioned in the major part of the act, the general provisions in Part I (Sections 1-11) and the provisions on "Data Processing of Public Offices" in Part II (Sections 12-26) of the act cover the general public administration area, which includes e-government. Some of the provisions, such as the ones in the Annex part, specifically address the protection of personal data collected, processed or stored in automatic data processing systems, which makes the provisions directly applicable to personal data protection in the e-government domain.

China: Draft of the Personal Information Protection Act

China currently lacks general privacy and data protection laws. There is no comprehensive e-government law either. Privacy in China has been largely protected indirectly under scattered provisions in various relevant laws and regulations. Enacting a personal data protection law, however, is one of China's priorities to improve its legal system and establish a rule-of-law society. As early as 2003, the former Informatization Office of the State Council, now the Ministry for Industry and Information, initiated relevant legislation activities and entrusted the Institute of Law of Chinese Academy of Social Sciences (CASS) to draft a data protection law for consideration. This "experts' suggestion draft" (*Zhuanjia Jianyi Gao*) was finished and submitted to the State Council

in 2006. In this process, an EU-China Information Society Project was set up between the EU and the Chinese government in 2005 to support informatization in China. One of its tasks is helping China draft a personal data protection law (Sutton et al., 2007). Currently the drafting and discussing process is still going on. It is reported (Greenleaf, February 2008) and also confirmed by the experts I interviewed that currently there are a few (at least two) draft data protection laws circulating within the Chinese government for discussion. The specific approach or model of protection has not been decided yet. Although 2008 was the year many people initially expected to see China's national data protection law enacted, it proved to be just an unfulfilled expectation. According to one of the interviewed legal experts who participate in the drafting process, it will take some more time, maybe longer than most would expect, to have the final data protection law officially adopted in China.

Although China's national data protection law has not been enacted and not been finalized both in format and in content, to provide a very initial peek into China's data protection scheme on the public sector, I will provide in this dissertation some brief introduction of the *Personal Information Protection Act of the People's Republic of China (*the *experts' suggestion draft)*, which was drafted in 2005 by an expert team headed by Professor Zhou Hanhua, director of the Institute of Law at CASS. It is the only draft made public so far and was the version receiving the "most official acknowledgement" (Greenleaf, February 2008), although it is uncertain now whether or how much this draft will be incorporated into the final law. As the first official (government-entrusted) experts' draft of data protection law in China, this act might very well be viewed as "a harbinger" of China's future data protection legislation (Maisog &

Zhao, 2006). By briefly reviewing this act we can have a better comparative view of the personal data protection landscape in the e-government context in the three countries. Citations of this act in this paper is mainly based on the English version of the experts' suggestion draft translated by two lawyers Maisog and Zhao (2006).

Data Protection Scope

The United States: Privacy Act of 1974

The *Privacy Act of 1974* itself does not specify an explicit objective. Yet the general purpose of the act is to establish a code of "fair information practices" for US federal agencies and to balance the government's need to maintain individuals' information with individuals' rights to be protected against privacy invasions stemming from federal agencies' information practice (United States Department of Justice (USDOJ), 2004). It was amended by the *Computer Matching and Privacy Protection Act in 1988* (took effect in 1989), which adds some protection for the subjects in the records used in automated or computer matching programs.

There are three points worth noting regarding the law's protection scope. First, the *Privacy Act* applies only to a federal "agency", which is defined as "any Executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency." (5 U.S.C. § 552(e)). The act does not cover federal entities outside of the executive branch such as a federal district court and members of the White House Office[8], neither does it cover private entities, state and local government agencies (except the social security number

[8] See list of relevant cases at http://www.usdoj.gov/opcl/1974definitions.htm#agency.

usage restrictions in Section 7). In this sense the act provides somewhat limited privacy protection for citizens. Second, the "individuals" protected by the *Privacy Act* are US citizens and lawful permanent resident-aliens (5 U.S.C. § 552a(a)(2)), which means information privacy of foreign visitors and non-resident aliens in the US is not protected by the law.

Third, the law protects personal information maintained in 'systems of records'. Record refers to "any item, collection, or grouping of information about an individual that is maintained by an agency" and "contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph" (5 U.S.C. § 552a(a)(4)). The act does not differentiate the sensitivity degree or protection level among different category of personal information. 'Systems of records' is defined in the first section of the act as "any grouping of records under the control of a government agency" from which information is retrieved by **individual identifier**. The 'systems-of-records' construct was widely criticized as being "too narrowly defined" considering the fact that it does not apply to all federal collection and use of personal information (e.g. GAO, 2008b; Information Security and Privacy Advisory Board (ISPAB), 2009; Privacy Protection Study Commission (PPSC), 1977). The act's protection does not apply when agencies do not use personal identifier to retrieve information. The PPSC's report pointed out in as early as 1977 that the definition emphasizing retrieval by unique identifier reflected "a manual rather than a computer-based model of information processing" (as cited in GAO, 2008b, p. 22). As criticized by PPSC, this definition scope does not fully consider the increasing use of computer and communication technology (as in the case of e-government area) that permits 'attribute

searches' (pattern search). This limitation was confirmed by a GAO survey of 25 federal agencies in 2002, which estimated that 70 percent of the agencies' systems of records contained electronic records (this number should most likely be higher today) and that 11 percent of 730 major information systems in use that year contained personal information that was not subject to the *Privacy Act*'s protections (GAO, 2003). The most frequently reported reason was that the agency did not use a personal identifier to retrieve the personal information but rather by other non-identifying information.

In short, the systems-of-records definition greatly limits the act's protection scope of individuals' privacy, which is even more a problem when data analysis technology is becoming increasingly sophisticated and data mining practice increasingly common in the era of e-government.

The United States: E-government Act of 2002

Like the *Privacy Act*, the *E-government Act of 2002* only applies to federal agencies and protects only US citizens and lawful permanent resident aliens. Section 208 of the *E-government Act of 2002* contains specific provisions to protect information privacy in the e-government area. It requires federal agencies "to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic government" (Sec. 208. a). The act protects any information in an 'identifiable form' that permits physical or online identity of an individual by either direct or indirect means (Sec. 208. b, d). The information protected under this act is broadened compared to the 'system of records' retrievable via personal identifier in the *Privacy Act*. Although this broader definition could help in part address the narrow system-of-records concept, the requirements in this act (see next section for specific

requirements) are also criticized as too limited because the act imposes no restrictions on agency collection and use of personally identifiable information (GAO, 2008b). therefore, in addition to revising the system-of-records definition to cover all personally identifiable information handled by the federal government, recommendation is also proposed to revise the *E-Government Act*'s scope to cover federal rulemaking (GAO, 2008b; ISPAB, 2009)

In addition to privacy protection, the *Federal Information Security Management Act of 2002* (FISMA) was signed into law as TITLE III of the *E-Government Act* in 2002 and is the primary law governing information security in the US federal government. FISMA provides a comprehensive framework to protect the security of computerized information and information systems, including personally identifiable information, operated by the federal government or other entities in support of federal operations like government contractors.

Germany: Federal Data Protection Act

The German *Federal Data Protection Act*[9] presents its objective at its very beginning: "to protect the individual against his right to privacy being impaired through the handling of his personal data" (Section 1). According to the act, the public authorities regulated include all "the authorities, the bodies of the judicature and other public-law institutions of the Federation, of the Federal corporations, establishments and foundations under public law as well as of their associations irrespective of their legal structure" (Section 2). Moreover, the act applies irrespective of the nationality of the data subject.

[9] The content analysis of this act is based upon the 2006 version, unless otherwise noted, since the official English version of the 2009 amendments was not available yet by the time I wrote this dissertation.

He/she doesn't need to be a German citizen to be protected by the act. It is obvious that the objects regulated and subjects protected are more inclusive than that by the US *Privacy Act*.

The *Federal Data Protection Act* defines personal data to be protected as any "information concerning the personal or material circumstances of an identified or identifiable individual (the data subject)" (Section 3). Compared to the US "system-of-records" concept, this act's inclusion of "material circumstances" (in addition to "personal circumstances") and "identifiable" (in addition to "identified) extends the protection scope significantly. The 2001 revisions of the act provides more stringent protection to some "special categories of personal data" as particularly sensitive personal data, which include "information on a person's racial and ethnic origin, political opinions, religious or philosophical convictions, union membership, health or sex life" (Section 3 (9)). The categorization of sensitive data, to a certain degree, enhances the privacy protection of individuals.

China

As briefly introduced earlier, the mainland China lacks any systematic data privacy regime. Because of China's long-time political as well as social culture ignoring personal privacy and the overall underdevelopment of China's legal system, there is no data protection law in China, nor comprehensive e-government law. So there is no general law governing the use of personal data in the context of e-government, as well as in the overall public sector, in the country. Although the constitution offers explicit privacy right to individuals, in China's law enforcement there is no formal legal right of personal privacy. The absence of specific legislation protecting individual's privacy right

makes personal privacy, including information privacy, in China largely unguarded. The existing limited legal protection of privacy largely relies on the remedies afforded through protection of the personal reputation right in existing laws and regulations (except the latest 2009 amendments to criminal law, which provide direct protection for information privacy). This indirect privacy protection approach is surely not as effective as a formal legal right of personal privacy and the operational potential is also questionable.

Although China's data protection law is still being drafted and the specific content and timetable for enactment remains unclear, one thing with great certainty at this moment is that China will adopt a Germany-style omnibus data protection law regulating both the public and private sectors, which is the case with the CASS experts' suggestion draft of *Personal Information Protection Act.* The experts' draft proposes a purpose of "regulating the processing of personal information by government authorities or other data processors, to protect individual rights and to facilitate the orderly flow of personal information" *(Article 1).* The 'orderly flow of personal information' is a new objective component compared to those for the other two countries, which partly shows that individuals' rights is not the most or only important goal of China's data protection law. This somewhat poses an interesting contrast with the pure purpose of 'protecting personal privacy right' in the *German Federal Data Protection Act.*

The proposed act covers, other than the private sector, all government authorities at all administrative levels in China, which differs from the federal-state dual system in the US and Germany, and broader than the US definition of 'public agency'. "Personal information" is defined by the proposed act as "the information which can, in reference to

it alone or in comparison (*literally combination)* with other information, [be used to] identify a specific individual" *(Article 9)*. This definition also has broader protection than the US "system-of-record" concept and more resembles the German counterpart. Data subject is not clearly defined in the draft. The current definition of "the specific individual who can be identified by means of personal information" does not explain whether non-Chinese citizens will be protected by the act.

Data Protection Principles and Requirements

This section provides a brief overview of the major principles and requirements outlined in the primary laws protecting individuals' privacy regarding their personal data handled in the process of e-government in the three countries.

The United States

In early 1970s, the US Department of Health, Education and Welfare (HEW) conducted a study to explore the impact of computerized record keeping on individuals. This HEW study committee (1973) published a report proposing a set of Code of Fair Information Practices (FIPs), which has become the basis for privacy laws in many countries as well as international treaties, such as the *Privacy Act of 1974* and the OECD privacy guidelines (the latter introduced in Chapter 6) (ISPAB, 2009).

The Privacy Act of 1974

The *Privacy Act* establishes a "code of fair information practices" for the US federal agencies in terms of protecting personal information in their hands. Based upon the FIPs terms and the provisions in the subsections of (b), (d) and (e), the key information practices addressed by the act can be summarized as follows: (1) Use

Limitation: maintain only personal information that are relevant and necessary to accomplish a legal agency purpose; disclose and share personal information with third parties or other agencies only with written consent of the subject individual (with twelve exemptions); (2) Transparency and Openness: inform individuals about data collection and use; publish public notice in the Federal Register of the existence, characteristic, and any new or intended use of existing systems of records; (3) Data Quality: maintain records with accuracy, relevance, completeness, and timeliness; (4) Data Security: establish administrative, technical and physical safeguards to insure the security and confidentiality of records, and (5) Individual Participation: offer subject individuals rights to access and correct their personal data contained in a system of records, and request a review if correction is refused by the agency.

All the act's requirements also apply to government contractors when the operation of a system of records is contracted out to accomplish an agency function *(§552a (m) (1))*. The act prescribes both civil remedies *(§552a (g))* and criminal penalties *(§552a (i))* for agencies' violations of the law. However, there are two points worth noting. First, the act does not apply to personal data obtained by government agencies from private data-resellers (ISPAB, 2009). Second, the act only regulates intentional data disclosure or misbehavior. Yet with larger volume of electronic data collected and stored, and greater risk of personal data security breaches within government agencies, it is suggested that the act should be amended to also offer protections or remedies for "unintentional disclosure/loses" (ISPAB, 2009).

Another special note is regarding the 'no-disclosure without consent' rule. There are twelve exemptions for this provision, which, for example, allow information use for

statistical research and criminal enforcement purposes. Among these exemptions, the exemption of 'routine use' is one of the most controversial provisions in the act. It was observed that government agencies used that exemption to justify almost "any use" of data (ISPAB, 2009; Schwartz & Reidenberg, 1996). In numerous cases various types of information sharing between agencies and with organizations or individuals have been upheld as valid routine uses (USDOJ, 2004). Because of its potential breadth, it is criticized widely as significantly weakening the effectiveness of the act in protecting individual privacy (e.g. Cate, 1997; Privacy International, 2007d).

Computer Matching Act

In 1989, the *Computer Matching and Privacy Protection Act of 1988* became effective as an amendment to *the Privacy Act of 1974*. Some new provisions were added, which provide procedural requirements for agencies to follow when engaging in matching programs of electronic records and offer some more protection regarding privacy of the data subjects in such programs. In addition to the general principles of data handling presented earlier, the major requirements for federal agencies involved in computer matching programs could be summarized as: (1) negotiating written agreements on matching programs between agencies and making it available to the public upon request; (2) establishing a Data Integrity Board to approve, oversee, and coordinate matching programs; (3) Conducting cost-benefit analysis of proposed matching programs; (4) providing detailed reports about matching programs to supervising agencies such as OMB; and (5) notifying subjects about the matching program and verify match findings before adverse action are taken against subjects *(§552a (o), (p), (q), (r) (u))*.

E-government Act of 2002: Privacy Impact Assessments

To achieve the privacy protection purpose in the context of e-government, the *E-government Act of 2002* requires government agencies to conduct 'privacy impact assessments' (PIA) and post privacy policies on federal websites, which supplement the protection provided by the *Privacy Act of 1974*. Specifically, PIA is required when new information technologies is used for information handling and when personal information is collected on 10 or more people using information technology (*Sec. 208. b (1)*). This assessment is required to be provided to OMB and, where practicable, made public through agency website, publication in the Federal Register, or other means. A PIA is required to be commensurate with the size of the assessed information system, the sensitivity of identifiable information in that system, and the risk of harm from unauthorized disclosure of that information (*Sec. 208. b (2)*). The assessment should include a few components, including what information is to be collected, the collection purpose, intended use and security measures, as well as available consent opportunities (*Sec. 208. b (2)*). Requiring agencies to go through the process of answering those questions is seen as a means to strengthen the protection of individual privacy.

In addition to the PIA requirement, the act also requires the OMB Director to establish guidelines mandating the posting of privacy notices on agency websites. It provides a list of information to be included in privacy policies, which mostly resemble the content in PIA by addressing how personal information will be collected, used, secured, plus individual rights[10]. The Director is also required to provide guidelines on how to translate privacy policies into a standardized machine readable format.

---

[10] See privacy policy example at http://www.whitehouse.gov/privacy/.

Data Security: Federal Information Security Management Act of 2002

As a part of the *E-Government Act*, the FISMA provides specific protection for the security of personal information in the context of e-government. Federal agencies are required by the act to: (1) designate a Chief Information Officer to ensure compliance with the FISMA requirements, (2) develop, document, and implement an agency-wide security program, (3) report on the adequacy and effectiveness of its information security policies and practices, and on compliance with this act, (4) provide the public with timely notice and opportunities for comment on proposed information security policies and procedures when needed, (5) participate in annual independent evaluations of its information security program and practices, and (6) develop and maintain an inventory of its major information systems (*Sec. 301. § 3544-45,3505(c)).*

Specifically, to protect government's information and information systems from "unauthorized access, use, disclosure, disruption, modification, or destruction", the act underscores the importance of an agency-wide security program. This security program is required to contain some important components such as assessments of the information security risk and harm magnitude, sustaining and cost-effective security policies and procedures, personnel security awareness training, and security-incident detecting and response procedures (*Sec. 301. § 3544 b).* A central theme the act establishes is its "risk-based" and "cost-effective" security approach. Government agencies are required to implement policies and procedures "commensurate with the information security risk and harm magnitude", and to "cost effectively reduce information security risks to an acceptable level" (*Sec. 301. § 3544(a)*).

Germany: Federal Data Protection Act

The *Federal Data Protection Act* of Germany delineates a few key data protection principles that should be followed when federal government agencies deal with citizens' personal data in electronic communications, which could be summarized as: (1) Admissibility: Personal data may only be gathered, processed and used (including sharing) upon permission, either by a legal provision or the data subject (*Section 4*); (2) Data Reduction and Data Economy: The aim of data processing systems is to collect, process or use no personal data or as little as possible (*Section 3a*); (3) Necessity: Collection and use only occur when necessary and storing should be avoided whenever possible (*Section 13, 14*); (4) Use Limitation: Personal data generally can only be used for the purpose for which it was gathered; (5) Transparency: Data subjects should be informed about the collection and processing of their personal data unless otherwise stipulated (*Section 19a*); (6) Individual Participation: Data subjects have the right to access their own personal data and relevant information (with exceptions) free of charge; have the right to object to data collection, processing and use; and have the right to correct, block or delete their data in certain situations (*Section 19, 20*).

Overall, the act regulates the federal public agencies (as well as the private sector) in great detail regarding the procedures and circumstances of collection, processing, and use of personal data of the public. For instance, specific conditions are outlined for the collection, storage and use of special types of personal data (sensitive personal data as defined earlier), which center on 'necessity'. Rules are also laid out for government agencies transferring citizens' personal data to other public bodies (*Section 15*), private bodies (*Section 16*), abroad and to supranational or international bodies (*Section 4b, 4c*).

For data transfer abroad, an adequate level of data protection is required to be guaranteed. Provisions are also provided on data protection audit (*Section 9a*) and commissioned personal data collection, processing or use (*Section 11*). Both administrative offences and criminal offences are defined (*Section 43, 44*). Specifically, administrative offences are defined to be committed "whether intentionally or through negligence" (*Section 43*), which offers broader and more effective protection of today's electronic data privacy than the US approach which only punishes 'intentional' misbehavior.

Some special requirements are outlined for federal public agencies specifically dealing with automatic data collection and processing, which is directly related to e-government. Such provisions include, but are not limited to, 'prior checking' for special categories of personal data (*Section 4d*), appointing a data protection official to work towards ensuring compliance with data protection provisions (*Section 4f*), harm compensation (*Section 8*), and the need of technical and organizational measures to ensure data security and confidentiality (*Section 9, Annex*). For the latter, federal public agencies are required to provide particular control measures to ensure the privacy and security of citizens' personal data. Such measures include access control, transmission control, input control, job control, availability control (against accidental destruction or loss), and separate processing of data collected for different purposes (*Annex*). Meanwhile, the act points out that protection measures or efforts should be reasonable in relation to the desired level of protection (*Section 9*), which is similar to the US risk-based and cost-effective security approach.

The *Federal Data Protection Act* was newly amended in July 2009. According to a German law firm online newsletter (Schweinoch, Steger, Schicker, Kröger, & Bühr,

2009), the act became stricter on a few aspects[11], which include, as relevant to the e-government context, the requirement of anonymizing or pseudonymizing personal data, adding data encryption as one data security measure to warrant access and transmission control, stricter requirements regarding formal prior consent by the data subject, new duties to notify data abuse, and aggravated regulations regarding administrative fines.

China: Personal Information Protection Act (draft)

The CASS experts' suggestion draft of China's data protection law explicitly outlines the following major principles on individuals' personal data handling in Chapter I as general provisions and Chapter II as specific requirements for the public sector: (1) Principle of Lawfulness, (2) Principle of Rights Protection (rights of access, correction, and cessation), (3) Principle of Interests Balance, (4) Principle of Information Quality (purpose restriction and data accuracy, integrity and timeliness), (5) Principle of Information Security, (6) Principle of Professional duties (to keep confidential), (7) Principle of Remedy, and (8) Principle of Use Limitation. Moreover, principle of data minimization is indirectly addressed, at a lesser degree than Germany, by requiring public agencies to "decrease societal burdens, avoid duplicative collection of personal information", and delete unnecessary information (*Article 11*). These principles largely resemble the ones found in the national data protection laws for the US and Germany. Similar to the US *Privacy Act*, there is no special protection of sensitive data under this draft.

[11] Because of the lack of English version of the amendments, official version of the amendments issued by German government should better be referred to for accuracy.

Despite the above similar principles, the public sector in China is quite weakly regulated, at least much more weakly than the other two countries especially Germany, regarding personal data handling under this draft law. First, unlike the other two countries, there is no transparency principle on personal data use in this draft. Data subjects have no right to be notified regarding data collection and use. Second, there are very broad exemptions in the data use limitation provisions. According to the draft, government authorities or agencies in China are required to register data collection with the 'agencies in charge of information resources' at the same level (the latter need to make announcement of the registration to the public) (*Article 12, 13*). Yet there is a list of exemptions from this registration requirement, which include "matters involving the internal personnel administration of government agencies" and "the personal information documentation used by government to process their internal business" (*Article 12*). Personal data can also be used by government beyond its original collection purpose when, other than those internationally common situations such as for state security and crucial public interest, it is required by international law to provide the personal information to foreign governments or international organizations, or "in order to prevent damage to important rights and interests of others", and when such personal information is "processed for proper reasons and is only used for internal purposes by government agencies" (*Article 15*). Third, while the act restricts cross-border data transfer by the private sector, there is no such restriction on the public sector. The public sector is more weakly regulated regarding information practices than the private sector under this act.

One special note is that under this proposed act, data controllers might have criminal liabilities if insufficiency of security measures causes security breaches of

personal information such as disclosure, loss, or destruction (*Article 68*). Yet in the US *Privacy Act*, only *intentional* data disclosure is regulated and punished. Although under the *German Data Protection Act* administrative offences could result from negligence, insufficiency of security measures is not explicitly regulated either. Considering the increasing data security incidents nowadays, such provisions like that in the Chinese data protection draft act, could be viewed as a timely and necessary component to achieve effective data protection in the context of e-government.

Supervisory Authorities

The United States: Office of Management and Budget

There is no independent privacy supervisory authority in the US. Subsection (v) of the *Privacy Act* requires the Office of Management and Budget (OMB), among its various other responsibilities, to: (1) prescribe guidelines and regulations for the use of agencies in implementing the provisions of the *Privacy Act*, and (2) assist and oversee agencies' implementation of the Act. In 1975, OMB issued *Privacy Act Implementation Guidelines*. Since then, by providing periodic supplemental guidance related to privacy on specific subjects, OMB plays a major role in supervising and guiding the privacy protection practice by federal government agencies in the US.

Pursuant to the *E-government Act of 2002*, an Office of Electronic Government was established in OMB to oversee the implementation of e-government activities by federal agencies, which include the information privacy protection in e-government, such as the implementation of PIA requirement. Agencies are required to submit to OMB an annual E-Government Act status report. According to the most recent OMB report to the Congress (2008), in fiscal year 2008, 92 percent of applicable systems within the 25

major federal agencies in the US had publicly posted PIAs[12]. Regarding the quality of each agency's PIA process, 24 out of 25 agencies received an assessment as "satisfactory" or better, only one agency received a "failing" rating. Both PIA posting percentage and quality ratings represent an improvement over the previous years.

Meanwhile, the FISMA also charges OMB to develop and oversee the implementation of policies, standards, and guidelines on information security (*Sec. 301. § 3543)*. OMB is required to report to the Congress on agency security practices and compliance with the act, and oversee the operation of the federal information security incident center. The 2008 OMB report showed that the US federal agencies spent $6.2 billion on IT security and had continued to improve information security performance. For instance, the federal agencies reported security controls testing for 93 percent of the operational systems in fiscal year 2008, while the number was 60 percent in 2002. Agencies also reported 89 percent of employees received security awareness training.

Regarding the effectiveness of this supervisory mechanism, the US Information Security and Privacy Advisory Board (ISPAB) in its 2009 report -- *Toward A 21st Century Framework for Federal Government Privacy Policy* -- blames the lack of updating of the *Privacy Act* and the inadequacy of OMB's oversight and guidance in the past years for the deficiency of the US federal agencies' data protection practice. ISPAB recommends improving government leadership on privacy, which include, for example, establishing a Chief Privacy Officer to oversee government-wide data protection.

FISMA makes the National Institute of Standards and Technology (NIST) responsible for developing technology standards and guidelines for information and

[12] See a PIA example at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_prism.pdf

information systems used or operated by or on behalf of federal agencies, except national security systems (*Sec. 303*). Pursuant to FISMA, NIST has developed various information-security-related standards and guidelines for the federal government, which will be introduced in more detail in the next chapter.

Germany: Federal Commissioner for Data Protection and Freedom of Information

In Germany, the Federal Commissioner for Data Protection and Freedom of Information is an independent authority supervising compliance with the provisions of the *Federal Data Protection Act* and other data protection provisions by federal public bodies (*Section 22*). (At the state level, each Land has a data protection commissioner to enforce the Länder data protection acts.) The commissioner is established with the Federal Minister of the Interior. The entity's major duties include monitoring federal public bodies' compliance with data protection provisions, filing complaints against public agencies for infringements of data protection laws (including this act), investigating data protection matters in public agencies upon request, submitting biennial reports informing the Bundestag and the public of major developments in data protection, and making recommendations to the Federal Government and public agencies on how to improve data protection (*Section 24, 25, 26*). Data subjects can appeal to the Federal Commissioner for rights infringement occurring through the collection, processing or use of his personal data by public authorities of the Federation (*Section 21*).

Other than the role of monitoring, investigating, and recommending, the data protection commissioner has no power to issue legally-binding orders on data protection issues, which is why it is termed by Cate (1997) as an "advisory" supervisory authority,

as contrasted with "regulatory" authority in some other countries that has more power and obligation in regulating, such as the OMB in the US.

China: Government Information Agency

Like the US model, the experts' draft of China's data protection law does not propose the appointment of a national-level central privacy authority or supervising agency. Instead, it requires establishing a 'government agency in charge of information resources' at each above-county level of the Chinese government to supervise the implementation of this act by government agencies and private bodies. Yet considering the fact that most relevant supervising and law enforcement work as delineated in the act only applies to the private sector, the role of these information government agencies in supervising personal data handling practice by the public sector seems quite limited. One major responsibility for them is to take care of the registration of data collection activities conducted by the public sector (*Article 12*). Data subjects' complaints against public-sector bodies are required to be filed with the data processing agencies, not to those supervising agencies. These supervising information government agencies do not have the power to issue legally-binding rules and policies. Overall, the administration and enforcement of the proposed data protection act is "widely distributed among sectors and among the levels of government" (p. 11), which is most similar to the model adopted in Japan and Chinese Taiwan (Greenleaf, April 2008).

Conclusion

The comparative overview of the constitutional privacy rights and major data protection laws in the three countries shows both consistency and diversity in national

approaches to the protection of personal data handled by the public sector in the e-government context (see Table 3 for a comparison of the major laws in three countries).

Table 3 A Comparison of Major National/Federal Data Protection Laws Governing E-government

		United States	**Germany**	**China**
Constitutional privacy protection		Implicit	Explicit (Communication privacy)	Explicit (Communication privacy)
Primary law(s) protecting personal data in e-government context		Sectoral data protection Law (public sector): *Privacy Act of 1974* *E-government Act of 2002*	Omnibus data protection law (Public & private sectors): *Federal Data Protection Act*	No Draft omnibus data protection law (Public & private sectors): *Personal Information Protection Act*
Data Protection Scope	Subject under protection	Citizens & permanent residents	Everybody irrespective of nationality	Not specified in the draft
	Regulating public sector's cross-border data transfer	No	Yes	No
Key data protection principles		Use Limitation, Transparency and Openness, Data Quality, Data Security, Individual Participation	Admissibility, Data Reduction and Data Economy, Necessity, Use Limitation, Transparency, Individual Participation, Data Security	Draft law: Principle of Lawfulness, Principle of Rights Protection, Principle of Interests Balance, Principle of Information Quality, Principle of Information Security, Principle of Professional duties, Principle of Remedy, Principle of Use Limitation
Supervising authority for data protection		Non-independent: *Office of Management and Budget*	Independent: *Federal Commissioner for Data Protection and Freedom of Information*	Independent yet not centralized (draft law): *Government Information Agency at each above-county level*
Overall data protection		Modest	High	Low, barely

First, consistency lies in a basic common notion that personal data should be protected as an individual's important right. Government's handling of electronic personal data requires particular legislative attention. This point is not only proved by the existence of the US *Privacy Act* and *E-government Act*, the *German Federal Data Protection Act*, but also evidenced by China's undergoing legislative efforts on its first data protection law. Second, there is great consistency in major data protection principles across countries. The overview of the major data protection laws applicable to the public sector in the specific e-government area shows that the US and Germany share greatly consistent general data protection principles. The experts' draft of China's data protection law also adopts most of these internationally accepted data protection principles, although its lack of data transparency principle indicates that the legitimacy of data collection might not be a primary concern of China's legislation.

Meanwhile, national diversities exist in the specific concepts of privacy right, the scope and level of public sector's data protection, and the data protection supervising mechanisms. Regarding data protection level, while China is still waiting for its first data protection law to be enacted and has the weakest protection of personal data in the e-government arena, Germany has the most comprehensive and strictest data protection law of the three countries. The public sector's handling of individual's personal data is heavily regulated and quite rigidly enforced under German law. Further, from the 1990s, Germany has amended its *Federal Data Protection Act* five times to address new privacy concerns stemming from technology changes and data protection practices, though most do not concern the particular e-government area. In terms of the US, compared to the other two countries, it has an overall modest protection of individual's personal data

collected and processed by the public sector, partly exemplified by the 'system of records' requirement. The relevant US laws also lag behind Germany in keeping pace with technology changes and the current public sector's information handling practices. To be specific, the *Privacy Act* has not been amended since its enactment in 1974 except the adding of *Computer Matching Act* in late 80s. The *E-government Act of 2002* also has its own weakness and limitation as stated earlier. Overall the US laws governing the information practices of the federal agencies are regarded not sufficient to protect individuals' privacy nowadays and revisions to the *Privacy Act* and *E-Government Act* are called upon by privacy legal experts (GAO, 2006, 2008b; Information Security and Privacy Advisory Board (ISPAB), 2002, 2009).

CHAPTER 5

A COMPARATIVE OVERVIEW OF SUPPLEMENTARY E-GOVERNMENT PERSONAL DATA PROTECTION LAWS AND POLICIES

In addition to the general data protection laws that govern either the specific e-government domain (in the case of US *E-government Act of 2002*), the public sector in general (in the case of US *Privacy Act of 1974*), or both the public and private sectors (in the case of *German Data Protection Act* and China's experts' suggestion draft), some other federal/national laws, including sectoral laws, and policies in the three countries also play a role in protecting the privacy and security of personal data processed in the specific context of e-government. This section provides a brief overview of these laws and relevant policies (see Table 4 for the summary list).

Since e-government activities involve various online communications and transactions occurring on government websites, other than the government agencies providing online government services (one of the communication endpoints), other online service providers such as those provide network connection and digital communication transmission services should also play a role in protecting the security and confidentiality of individuals' personal data that are logged and exchanged through the internet in the e-government process. While it is necessary and crucial to have laws in place to regulate government's information practices to protect personal data in e-government, it is also important to implement laws that regulate online service providers and general electronic communications with respect to personal data handling. The supplementary laws are

therefore organized under two major categories in this chapter: electronic communication laws governing the particular medium of the internet and additional laws that apply.

Table 4 Supplementary Laws/Policies Protecting Personal Data in E-government

	United States	**Germany**	**China**
Government regulation with legal bindingness: laws and administrative acts	▪ *Uniform Electronic Transactions Act* (1999) ▪ *Paperwork Reduction Act (1995)* ▪ *Computer Security Act of 1987*(superseded by *FISMA*) ▪ *Electronic Communications Privacy Act of 1986* ▪ *Computer Fraud & Abuse Act* 1986 ▪ *Freedom of Information Act* (1966) ▪ Sectoral laws; OMB requirements	▪ *Telemdia Act (2007)* ▪ *Telecommunications Act* ▪ *Freedom of Information Act (2005)* ▪ *Criminal Code* ▪ *Electronic Signature Act (2001)* ▪ *Information and Communication Services Act (1997) (replaced by Telemedia Act)* ▪ More sectoral laws	▪ *Criminal Law (2009 Amendments)* ▪ *Regulation of P.R. China on Open Government Information (2007)* ▪ *Electronic Signature Law (2004)* ▪ *Regulation on Telecommunications of P.R. China (2000)* ▪ Regulations on Internet Security (multiple) ▪ More sectoral laws
Government regulation without legal bindingness	▪ *National Strategy to Secure Cyberspace (2003)* ▪ *Administration's Cyberspace Policy Review (2009)* ▪ OMB Guidelines ▪ NIST standards and guidelines	▪ *Decision on Security in E-transactions with the Federal Administration (2002)* ▪ *E-government Manual* ▪ eID Card Project & Citizen's Portals Project	▪ *State Informatization Development Strategy 2006-2020* ▪ *General Framework of National Electronic Government (2006)* ▪ *Circular on Strengthening the Risk Assessment of Information Security in E-government Project Construction (2008)*

United States

Statutory Laws

While the US federal agency use of personal information in the context of e-government is primarily governed by the *Privacy Act* and the *E-Government Act of 2002*, a few other federal laws also play a role in this regard.

Laws on the Privacy and Security of Electronic Communication

Electronic Communications Privacy Act of 1986

The *Electronic Communications Privacy Act of 1986* (ECPA) (Public Law 99-508, 100 Stat. 1848) relates to the topic of personal data protection in e-government because of its protection of electronic communication in general. The law primarily regulates the disclosure of the contents of individuals' electronic communications or relevant information (subscriber's personal record such as name or IP address) by electronic communication service providers. It is composed of two major parts: Title I of the *Wiretap Act* (*18 U.S.C. §§ 2501-2522*) and Title II of the *Stored Communications Act* (SCA) (*18 U.S.C. §§ 2701-2711*). Title II of ECPA protects the privacy and confidentiality of stored electronic communications and transaction records. In addition to delineating unlawful access and punishments, the SCA prohibits a provider of an electronic communication service from "knowingly divulging" the contents of electronically stored communications by that service to any person other than the addressee or intended recipient (*18 U.S.C. § 2511, 2702*). The ECPA was later amended by some provisions of the USA PATRIOT Act, which somewhat weakened restrictions on government access to stored communications.

Computer Fraud and Abuse Act (1986)

The *Computer Fraud and Abuse Act* (*18 U.S.C. § 1030*) is primarily a criminal statute fighting computer crimes. Amending the 1984 provisions on cyber crimes in 18 U.S.C. § 1030, the act was officially enacted by Congress in 1986 and further amended in 1988, 1989, 1990, 1994, 1996, 2001, 2002, and 2008 (by the *Identity Theft Enforcement and Restitution Act*) (United States Department of Justice (USDOJ), 2007). It

criminalizes intruders of the computers or computer networks used by the US federal government, financial institutions, or used in interstate and foreign commerce communication. The law particularly relates to the topic of data protection in e-government in that it criminalizes unlawful access and damage to electronic data in any computer used by or for the Government of the United States (*18 U.S.C. § 1030 (a)(2)(3)(5)*).

Computer Security Act of 1987

Before FISMA in the *E-government Act of 2002*, the security of personal information in the US public sector was mainly guarded by the *Computer Security Act*, which was enacted in 1987 as the first major legislative effort to improve the security and privacy of sensitive information in federal computer systems. The term 'sensitive information' includes all personally identifiable information protected by the *Privacy Act* (*Section 3*). It required NIST (at the time National Bureau of Standards) to develop security standards of minimal acceptable (cost-effective) practices for federal agencies. Moreover, it required federal agencies to establish security training programs and create security plans for computer systems with sensitive information. It also established a Computer System Security and Privacy Advisory Board within the Department of Commerce. The act was superseded by FISMA 2002.

Additional Laws Protecting Personal Data in E-government

Freedom of Information Act (1966)

The US *Freedom of Information Act* (FOIA) (*5 U.S.C. § 552*) was signed into law in 1966 and has been amended a few times in the past years. It provides "any person"

with legal rights to have access to US federal agency records, subject to nine exemptions. Two of these nine exemptions are specifically set out to protect personal privacy. For instance, according to exemption 6, federal agencies are not allowed to disclose "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy" (*5 U.S.C. § 552(b)*). The *Electronic Freedom of Information Act Amendments of 1996* makes this act more directly related to the privacy issue in e-government by applying the act to government records maintained in electronic format.

Paperwork Reduction Act of 1995

The *Paperwork Reduction Act* was enacted in 1980 and significantly revised in 1995. It is not a law targeting information protection. Yet one of the act's main requirements is to reduce the paperwork burden of information collection on the public, or in other words, limit information collection from individuals, which makes the act play an important role in protecting individuals' privacy by setting such controls (GAO, 2008b). Other than that, the act also sets various requirements and procedures for data collection on the public, such as review and approval by OMB, and notifying the public on data collections. It requires federal agencies to "ensure that the creation, collection, maintenance, use, dissemination, and disposition of information by or for the Federal Government is consistent with applicable laws" such as the *Privacy Act* (*Sec. 3501(8)*).

Uniform Electronic Transactions Act (1999)

Electronic transaction is an important component of e-government service and is becoming increasingly common as e-government matures. The US *Uniform Electronic*

Transactions Act (1999) is a national-level uniform act aiming to harmonize state e-signature laws and attempts "to facilitate and promote commerce and governmental transactions by validating and authorizing the use of electronic records and electronic signatures"(*Section 6*). The act provides indirect protection of personal information involved in e-government activities in the sense that the use of electronic signature and relevant technologies help protect the security and privacy of personal information conveyed in e-government transactions.

Additional Sectoral Laws that Apply

Apart from the laws introduced above, the US government's handling of personal data is also governed by some other laws that protect the privacy and security of agency-specific or sector-specific personal information. Following are some of the examples.

Driver's Privacy Protection Act (1994). The *Driver's Privacy Protection Act* (*Public Law 103-322*) was passed in 1994. It requires state Department of Motor Vehicles to limit the use and disclosure of personal information contained in individuals' motor vehicle records to fourteen purposes. The fourteen purposes include, for instance, use by government agencies, insurance companies, and any use with individuals' written consent (*18 U.S.C. § 2721 (b)*). While playing a positive role in protecting the privacy of personal information, the act's exemptions are fairly broad. There is barely any limit on government use of such data.

Health Insurance Portability and Accountability Act of 1996. Another sectoral law example is the *Health Insurance Portability and Accountability Act of 1996* (HIPAA, *Public Law 104-191*). Sections 261 through 264 of HIPAA, collectively known as the Administrative Simplification provisions, require the Secretary of Health and Human

Services (HHS) to establish standards for the electronic exchange, privacy, and security of personal health information. Pursuant to the act, the HHS has issued a series of rules to implement requirements regarding Administrative Simplification, which include the *Privacy Rule* (final rule issued in 2002) and *Security Rule* (final rule issued in 2003). These two rules establish national standards for the protection of individually identifiable health information held or transmitted by "covered entities", which include, among others, federal agencies concerned with health and health services such as Medicare program.

Gramm-Leach-Bliley Financial Modernization Act of 1999. The *Gramm-Leach-Bliley Act* (GLBA) (also known as *Financial Modernization Act of 1999*) (*Public Law 106-102*) includes provisions protecting the privacy and security of personal financial information held by financial institutions, which, although mainly refer to the private sector, also include government entities that provide financial products such as student loans or other financial services such as processing taxpayer data. The data protection requirements consist of, among other rules, the *Financial Privacy Rule* that regulates the collection and disclosure of personal financial information (such as the requirement of providing privacy notice), and the *Safeguards Rule* that requires financial institutions to design, implement and maintain a security plan to ensure the security and confidentiality of personal financial information. The act, however, is criticized by the Electronic Privacy Information Center (EPIC), a non-profit privacy research group, as too limited to protect individuals' personal financial information.

There are other specific restrictions on government's use of personal information at the federal level. For instance, as the first data breach notification law at the federal level, the *Veterans Benefits, Health Care, and Information Technology Act of 2006* (*38*

U.S.C. § 101, Public Law 109-461) applies specifically to the Department of Veterans Affairs[13], setting out information security requirements for personal information. Other examples include, but are not limited to, federal laws prohibiting unauthorized inspection and disclosure of individuals' tax return information by government employees (*26 U.S.C. § 6103, 7431*) and the law prohibiting non-statistical use of census data by Census Bureau and relevant agencies (*13 U.S.C. § 9*).

Federal Policies Protecting Personal Data in E-government

In addition to the above federal/national level statuary laws, there are also various federal strategies, policies, standards, and guidelines that address the protection of personal information in the hands of the US government as well as in the particular context of e-government.

National Strategy to Secure Cyberspace (2003)

The *National Strategy to Secure Cyberspace* was released in 2003 as a component of the US *National Strategy for Homeland Security*. It offers suggestions, not mandates, to government agencies, business, and individual users of cyberspace to secure computer networks and systems. Although its main objective is to prevent cyber attacks against the nation's critical infrastructures and reduce damage from cyber attacks in general rather than to protect the security of electronic personal data in specific, protection of electronic personal data is a natural consequence of the macro-level protection. The Strategy is briefly reviewed as it relates to the topic under discussion.

---

[13] According to GAO's report (2008a), there were nine data breach incidents occurring in the Department of VA from November 2004 through January 2007 alone.

The Strategy outlines five national priorities to protect US cyberspace security. One of these priorities is to secure governments' cyberspace and information systems. To achieve this purpose, it identifies a few major initiatives for government agencies, which include: (1) continuously assess threats and vulnerabilities to federal cyber systems; (2) authenticate and maintain authorized users of federal cyber systems; (3) secure federal wireless local area networks; (4) improve security in government outsourcing and procurement; and (5) encourage state and local governments to consider establishing information technology security programs and participate in information sharing and analysis centers (The White House, 2003). The Strategy also underscores the principle of protecting privacy in cyber security programs and requires federal agencies to lead by example in implementing strong privacy policies and practices.

Moreover, the Strategy emphasizes the priority of establishing a system of international cooperation to facilitate information sharing and improve the international management of and response to cyber attacks. Recommended actions include, for example, promoting a global "culture of security" by facilitating dialogue and partnerships among international public (as well as private) sector on protecting information infrastructures, establishing international watch-and-warning networks to detect and prevent cyber attacks, and encouraging other nations to accede to the *Council of Europe Convention on Cybercrime.*

Administration's Cyberspace Policy Review (2009)

In 2009, the US President Obama released the Administration's *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.* Existing problems on cybersecurity are reviewed and initial areas of action are outlined to help the US government guard the security of the nation's digital

infrastructure. Among the actions proposed, the report particularly underscores the necessity and urgency to establish a public-private partnership as well as international cooperation and norms to achieve a secure cyberspace (The White House, 2009). Other actions include, for example, the need to aggressively research and develop new cybersecurity-enhancing technologies and raise public awareness of cybersecurity. A cybersecurity policy official is to be established at the White House to coordinate all cybersecurity-related policies and activities. Recognizing that privacy and security are complementary values, the report stressed privacy protection in virtually every aspect of the Administration's new cybersecurity strategy, which includes the plan to designate a privacy and civil liberties officer.

OMB Guidelines

Under the *Privacy Act* and the *E-government Act*, OMB is responsible for establishing polices, prescribing guidelines, and providing continuing assistance to and oversight of federal agencies' implementation of the acts, or in other words, oversees the implementation of the federal government's information security and privacy protection. From the 1970s, OMB has issued various policies, or 'both recommended steps and required actions' (GAO, 2008a), to the federal government regarding information protection, which are either directly or indirectly applicable to the e-government area. Following are some of the most relevant examples in chronological order.

For example, in February 1996, OMB revised *Appendix III* of *Circular A-130* (*Management of Federal Information Resources*) --- *Security of Federal Automated Information Resources* to respond to the rapidly changing technological environment. Requiring federal agencies to adopt a risk-based policy for cost-effective security, which

was established by the *Computer Security Act* and later the central theme of FISMA, the Appendix established government-wide responsibilities for federal computer security. Government agencies were required to establish four management security controls in all government general interconnected support systems and major applications: assigning security responsibility, security planning, periodic review of security controls, and management authorization. Overall, the Appendix provided some of the earliest guidance to agencies on how to secure information as governments increasingly conduct business via open and interconnected electronic networks.

Realizing that the full potential of the web, or e-government, cannot be realized until people are confident that their privacy on the government website is protected, OMB issued memorandum M-99-18, *Privacy Policies on Federal Web Sites*, and M-00-13, *Privacy Policies and Data Collection on Federal Web Sites*, directing federal agencies to adopt privacy policies and forbade agencies to use cookies except in certain limited circumstances. To be specific, M-99-18 required government departments and agencies to post clear privacy policies on agency principle websites, any other major site entry points, and any web page where substantial personal information is collected from the public. Each policy must inform site visitors what information is being collected, why it is being collected, and how the information will be used. With regard to the memorandum M-00-13, its purposes were reminding agencies and agency contractors to post privacy policies on their websites and to comply with those stated policies, and directing agencies to only use "cookies" or other automatic means of collecting information unless certain conditions are met. The "cookies" conditions are (1) a

compelling need to gather the data on the site, (2) appropriate and publicly disclosed privacy safeguards for information handling, (3) personal approval by the agency head.

As governments moved to electronic collection and dissemination of data, opportunities to share them among agencies expanded. In this situation, OMB issued memorandum M-01-05, *Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy*. According to the memo, data sharing should only be pursued when the benefits outweigh the costs (mainly privacy costs). Eight key privacy principles in conducting inter-agency data sharing were delineated in the document: (1) notice of proposed data match, (2) consent from individuals as appropriate, (3) re-disclosure limitations, (4) accuracy, (5) security controls, (6) minimization of information shared, (7) accountability, and (8) privacy impact assessments which later became the privacy focus of the *E-government Act of 2002*.

Following a number of highly publicized data breaches at government agencies, in May of 2006, OMB issued guidance (M-06-15) instructing senior agency privacy officials to "conduct a review of policies and processes and take corrective action as appropriate to ensure adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to personally identifiable information." In June of the same year, OMB through memorandum M-06-16, *Protection of Sensitive Agency Information*, required departments and agencies to establish safeguards for sensitive personal information that is either accessed remotely or physically transported outside of an agency's physical perimeter. Specific recommendations are outlined, which include, for example, data encryption and authentication. Government units were also recommended to apply a multiple-step NIST checklist to protect remote sensitive information.

In May 2007, OMB required agencies to review and reduce "current holding of all personally identifiable information" to the minimum necessary (M-07-16, *Safeguarding against and Responding to the Breach of Personally Identifiable Information*). The memo stressed its application to all federal information and information systems, which means that OMB realized information protected should not be limited to that is "retrieved by identifier". Specific requirements include, for instance, eliminating unnecessary collection and use of SSNs in agency programs and implementing a breach notification plan. The memo also emphasized a few additional steps to reduce the risks of data breach, such as reducing information volume, limiting data access, and using security controls such as encryption and authentication. According to the OMB's 2008 report, federal agencies demonstrated progress in establishing breach notification plans since the issuance of M-07-16. Most agencies were able to provide formal and comprehensive breach notification polices.

To facilitate the reduction of SSN use, in November of 2008, the White House issued the Executive Order 13478, which removed a requirement for agencies to use SSNs as individuals' unique identifiers. This serves a significant role in terms of government's efforts to protect individuals' privacy.

All the above and other OMB memorandums that are relevant to the protection of personal information in e-government are listed in Appendix B.

NIST Standards and Guidelines

As introduced earlier, FISMA (Title III of the *E-government Act*) requires the NIST responsible for developing technology standards and guidelines to protect the security of the information and information systems that support the operations of the US

federal government. In the past years, NIST has issued various computer security standards and numerous guidelines to help the federal government implement the provisions of FISMA and protect the sensitive information (including individuals' personal data) that are electronically used or maintained by or for the federal departments and agencies. NIST issues two forms of publications to federal government agencies (which are also available references to the general computer security community): mandatory Federal Information Processing Standards (FIPS) that do not allow for waiver and non-mandatory Special Publications (SP) guidelines in the 800 series.

For instance, pursuant to FISAM, NIST developed two mandatory security standards that are key to the protection of electronic information and information systems in the federal government, which are briefly introduced here.

(1) FIPS 199: *Standards for Security Categorization of Federal Information and Information Systems* (2004a). To cost-effectively secure information and information systems collected or maintained by or on behalf of federal agencies, NIST developed security categorization standards to enable agencies to provide appropriate levels of information security according to different risk levels (low, moderate, high). Risk levels are classified based upon potential impacts of security incidents. Special Publication 800-60 *Guide for Mapping Types of Information and Information Systems to Security Categories* (NIST, 2004b), which was revised in 2008, provides complementary guidance on how to implement FIPS 199. During fiscal year 2008, the US federal agencies reported a total of 10,679 systems, which are categorized by a risk impact level of high (11%), moderate (38%), low (44%), and not categorized (7%) respectively (OMB, 2008).

(2) FIPS 200: *Minimum Security Requirements for Federal Information and Information Systems (2006)*. This standard provides minimum information security requirements for federal information and information systems in seventeen security-related areas, such as the area of awareness and training, and area of identification and authentication. To meet the requirements in this standard, NIST Special Publication 800-53 (*Recommended Security Controls for Federal Information Systems)* provides guidelines on how to select appropriate security controls for federal information systems based on the systems' security categorization in accordance with FIPS 199.

Apart from the above security standards and corresponding guidance, NIST has provided various other guidelines, standards, and technologies to help the federal government protect electronic information against threats to the confidentiality, integrity, and availability, which cover cryptographic standards and technologies, digital signature standards, secure virtual private network (VPN) technology, and biometric information standards, to name a few. All these NIST efforts help the federal government establish and improve its information security and privacy mechanisms. For further reference, the NIST FIPS standards and SP guidelines (public draft not included) that are directly related or applicable to the protection of personal data in e-government are listed in Appendix B. Due to the large number of SP publications, only those issued in or after 2002, when FISMA was adopted, are included in the Appendix.

Concluding Remarks

While the US *Privacy Act* is criticized not to be adapting to technology advances and consequent new information practices in the public sector, and *E-government Act* is limited in its scope to protect individuals' personal information, the OMB and NIST have

played valuable supplementary role in this regard by providing updated requirements, technologies, and guidance on how the federal government should protect the privacy and security of individuals' personal information in the digital age as well as in the particular context of e-government.

Germany

In addition to the omnibus *Federal Data Protection Act*, which provides the basic principles for data protection, there are other laws, especially specific data protection laws for different areas, and policies in Germany that either directly address the privacy and security issue in e-government or do not specifically aim at e-government yet are applicable or related to the issue under discussion.

Statutory Laws

Laws on the Privacy and Security of Electronic Communication

Information and Communication Services Act (1997) and Telemdia Act (2007)

The federal *Information and Communication Services Act* (better known as *Multi-media Law*) was passed in 1997 to create a legal framework for the development of electronic information and communication services in Germany. The act contains three major parts: *Teleservices Act* (*Article 1*), *Teleservices Data Protection Act* (*Article 2*), and *Digital Signature Act* (*Article 3*). The *Teleservices Data Protection Act* set legal provisions for the protection of personal data used in 'teleservices', which include online electronic communication. It mandated how private data could be collected, should be stored and disclosed. The data protection principles outlined were quite consistent with the ones in the *Federal Data Protection Act*, including for instance data minimization

principle, transparency principle and admissibility principle. Data could only be collected and used for service utilization and accounting purposes.

In February 2007 the German *Telemedia Act*[14] was passed. It replaces the *Teleservices Data Protection Act* and the *Teleservices Act* and becomes a major law regulating internet services in Germany. It governs all electronic information and communication services, yet excluding telecommunication and broadcasting services. The act contains provisions on service providers' responsibilities and liabilities with respect to data protection (*Section 13*), which are applicable to e-government services that are offered via the internet. Specifically, teleservice providers are required to inform users in detail about the "nature, extent and purpose" of the collection and processing of user-related data. At the same time, service providers have to make user data, such as user names or addresses, available to investigating authorities for crime prevention purposes and for the enforcement of intellectual property rights (*Section 14*). The latter IP provision raises serious data protection concern and causes severe criticism from data protection proponents in Germany. One point to note is that the *Telemedia Act* is only applicable to the processing of users' data in relation to using the internet service (such as IP addresses, time and duration of uses). The content data of the e-government service is governed by the general *Federal (or state) Data Protection Act.*

Telecommunications Act

In 2002, the EU adopted the *Directive on Privacy and Electronic Communications (2002/58/EC)*, which sets out EU standards and basic obligations

[14] To the author's knowledge, no English version of this act is available by October 2009. A German version is available at http://bundesrecht.juris.de/tmg/index.html. The summary was presented by a German native speaker and proof-read by an expert from the German Federal Commissioner of Data Protection and Freedom of Information.

protecting the contents of and personal data related to electronic communications (see Chapter 6 for more detail on this directive). Germany transposed this directive mainly through the *Telecommunications Act* of 2004 (European Commission, 2008).

Under the *Telecommunications Act*, telecommunication service providers are required to take technical and organizational measures to maintain telecommunications privacy and protect users' personal data (*Part 7*). The collection and use of customer data, traffic data, and location data are strictly limited. Specifically, they are limited to the purposes of charging and billing, marketing provider's services, providing value-added services, detecting and remedying telecommunications system malfunctions and service fraud, and with the consent of the data subject (*Sections 96, 97, 98, 100*). In the sense that telecommunication service providers also provide internet service, this act might also apply to the issue under discussion in cases where individuals have online communications with government entities via services provided by telecommunication service providers.

Data Retention Law (2007). After years of debating, in November 2007, Germany adopted a data retention law, which amends the *Telecommunications Act* by transposing the EU data retention directive (Directive 2006/24/EC). The law requires telecommunications providers to retain all customer communication data, including telephone services, internet access services and e-mail services (e-mail addresses, time stamps, and IP addresses) for a period of six months. These retained data should be accessible to the law enforcement authorities under the condition of a court order and to the intelligent services without any restriction. The adoption of the law causes great privacy concern and strong opposition from the civil society and data protection activists

as well as the Federal Commissioner for Data Protection. The German Working Group on Data Retention challenged the law at the Federal German Constitutional Court and currently the case is still pending[15]. In January 2009 the Administrative Court of Wiesbaden claimed the law "invalid" and that "data retention violates the fundamental right to privacy (European Digital Rights, 2009).

Additional Laws Protecting Personal Data in E-government

Criminal Code

The German *Criminal Code* contains provisions on personal privacy violations. Specifically, the law prohibits and punishes unauthorized access to electronic data, including personal data (*Section 202a*), and explicitly prohibits unauthorized disclosure of personal privacy by general public officials or staff in public agencies as well as data protection officers (*Section 203*). These provisions provide direct protection of the privacy and security of personal data in e-government. The latest 2008 amendments to the Code provide new provisions on phishing, which rule that unlawful interception of data by technical means are crimes liable to imprisonment or fines, so are the acts that prepare the offences of data espionage and phishing (*section 202c*).

Electronic Signature Act (2001)

Germany is the first member state of EU to pass legislation regarding digital signatures. It is also the first country in the world that issued a national digital signature

---

[15] The request for a temporary injunction of the data retention law has been partly successful in that the Federal Constitutional Court did not suspend the obligation to retain the data itself but permitted the communication and use of these retained data only for the purpose of investigating serious criminal offences. Details could be found in the court press release available at http://www.bverfg.de/pressemitteilungen/bvg08-037en.html and http://www.bverfg.de/pressemitteilungen/bvg08-092en.html.

law. The first *German Digital Signature Act* came into force in 1997. In 2001, a new *German Electronic Signature Act* was drafted and took effect to transpose the EU directive on electronic signature (1999/93/EC). Setting out the overall rules governing the use of electronic signatures, such as standard requirements and certification authorities' responsibilities, the central theme of the act and the accompanying *Ordinance on Electronic Signatures* is to establish a secure infrastructure for the use of electronic signatures in electronic communications and transactions, and thus to establish a framework for trust and security for data exchange occurring both in the private and public sectors. In brief, electronic signatures can protect the integrity and authenticity of electronic data transfer in e-government interactions and transactions.

Freedom of Information Act (2005)

After years of debating, the German federal government passed the *Freedom of Information Act* in 2005 (entered into force in January 2006) (Privacy International, 2007c). The law grants the public a general right to access official federal government information, yet with quite broad exceptions, which cover for instance public safety, national security, and trade secrets (*Section 3*). In the case of personal data, government authorities generally need to weigh which interests are more significant – those of the applicants or of the data subjects – in determining whether to release the record (*Section 5*). While special types of personal data (as defined in the *Federal Data Protection Act*) such as health information may only be transferred with the express consent of the data subject (*Section 5 (1)*), the applicant's interest in obtaining personal data should generally outweigh the privacy interests of the data subject and such personal information is limited to individuals' names, titles, university degrees, designations of professions and functions,

official addresses and telecommunications number (*Section 5 (3) (4)*). Complaints or violations are required to be filed with the Federal Commissioner for Data Protection and Freedom of Information (*Section 12*).

Additional Sectoral Laws that Apply

Apart from the sector-specific laws introduced above, there are also some other specific laws or law provisions regulating the German public sector with respect to personal data handling. For instance, the *German Social Code* provides protection for highly-sensitive personal social security data such as health insurance data. Under its data protection provisions, social welfare agencies are not allowed to collect, process and use individuals' social security data without authorization.

Other specific law examples include, for example, the *Federal Administrative Procedure Act*, which requires government authorities not to reveal matters of a confidential nature such as data relating to individuals' private lives, the draft law on electronic ID card and draft law on de-mail (both signed by the cabinet but not officially issued yet) that aims to secure online communication as well as transactions in e-government, and the latest *Law Improving the Security of the Federal Government's IT* (European Commission, 2009c).

Federal Policies Protecting Personal Data in E-government

As that in the US, in addition to federal-level statuary laws, there are also various federal policy guidelines, strategies, projects, and standards that are relevant to the protection of personal data in the particular context of e-government. Following are some key examples.

Decision on Security in E-transactions with the Federal Administration (2002)

Being aware that security measures are an important prerequisite for implementing a successful e-government program, after the enactment of the *Electronic Signature Act* in 2001, the German federal government in January 2002 issued a policy paper *Decision on Security in Electronic Legal and Business Transactions Involving the Federal Administration*, which establishes a framework for the introduction of electronic signatures as well as for the authentication and encryption of government online communications. The particular intention is to promote legally binding and secure e-government transactions between the federal administration and its partners as citizens, businesses, as well as government administrations. The decision paper explicitly requires security measures of digital signatures, authentication and encryption to be integrated into numerous e-government applications and systems to safeguard the confidentiality, integrity, authenticity and availability of government electronic communications. In addition to the technical security applications, government agencies should also incorporate organizational processes such as necessary training.

E-government Security Policies and Measures by the Federal Office for Information Security (BSI) as a Result of BundOnline 2005 (2001-2005)

As the central IT security service provider for the German government, the Federal Office for Information Security (BSI) in Bonn plays a key role in protecting the security of personal data in German e-government. The launch of *BundOnline 2005*, the German e-government strategy for the year 2001-2005, brought about new challenges of data protection to the German government. In this context, the *Implementation Plan for the BundOnline 2005*, which was issued in 2001, developed "data security" as a basic

component of the e-government initiative and assigned the data security responsibility to BSI. The implementation plan also charged the BSI with the task of setting up the Data Security Competence Center. In regard to supporting German secure e-government, BSI has three main tasks: providing consulting services towards IT security, publishing E-government Manual of the Federal Administration, and developing also improving the Virtual Post Office concept.

E-government Manual

To support the *BundOnline 2005* initiative, BSI published in 2001an *E-government Manual* to provide policy guidance and authoritative recommendations on all aspects of e-government development. The manual has six chapters with different themes that are constantly expanded. Under each chapter important issues are explored in detail in separate modules. Among the various topics of e-government development, there is specific guidance on data protection in e-government (a module in chapter II)[16], which provides data protection information with regard to frames of reference, challenges and recommended actions.

Chapter IV of the Manual attempts to address issues covering all aspects of e-government security, including personal data security, and to present pragmatic solutions. The modules in this chapter include topics such as *Secure Internet Presence in E-Government* (2002), *Secure Payment Methods for E-Government* (2005), *Secure Communication in E-Government* (2004), *Authentication in E-Government* (2004), and *Secure Client-Server Architectures for E-Government* (2006), to name a few. These issues are all related to personal data protection and data security in e-government.

[16] English version is not available for this module.

In chapter V of the Manual, *SAGA--Standards and Architectures for E-government Applications (version 2.0)* (2003) also provides standards and recommendations for data security in e-government services. According to the potential damage caused by security impairment, SAGA breaks protection requirements for each e-government IT application into four categories: none, low-medium (moderate), high, very high. It also classifies three interaction scenarios for e-government services: information, communication, and transaction. Though SAGA does not provide specific data protection measures, it postulates that security standards should be customized based on specific protection needs and interaction scenarios.

Virtual Post Office

The design and implementation of the Virtual Post Office (*VPS*) was treated as the basis for secure e-government communication and the central element of data security in Germany. It makes electronic communication with public agencies easier and more secure. Briefly speaking, VPS acts as a central security gateway allowing public agencies to use available security mechanisms such as encryption and decryption, electronic signature creation and verification, and authentication check when they interact with the public with electronic data traffic[17]. In this way, it can help safeguard the confidentiality, integrity, and privacy of sensitive data. It can also provide protection against malicious software with its anti-virus scanning interface. By simplifying secure electronic communications with the public agencies, the Virtual Post Office was regarded as a pioneering solution developed by BSI to the security issue which became more acute with the introduction of e-government. The Virtual Post Office is available in Version 2.0

[17] Source for the introduction of VPS: https://www.bsi.bund.de.

with full functionality since the end of 2004. According to BSI's 2006-2007 annual report, the e-mail component VPS-Mail was being used in 61 public authorities.

According to a government official from the German Federal Ministry of the Interior that I interviewed, another relevant but different security technology used commonly in practice is OSCI, which is a two-layered protocol for the secure exchange of messages in the e-government context. It is based on international standards and becomes an important part of the German e-government infrastructure (Steimke & Hagen, 2003)[18]. In the past few years a few other federal projects related to e-government security have been initiated, two of which are introduced as follows.

E-government Security Policies and Measures by BSI as a Result of eGovernment 2.0 (2006-2010)

In 2006, the German federal government adopted a comprehensive development strategy -- *Focused on the Future: Innovations for Administration*, which aims at modernizing the federal administration and improving the efficiency, quality and citizen-orientation of public sector services (European Commission, 2009a). An integral part of this strategy is the *eGovernment 2.0* program, which identifies four fields of action to expand e-government services by 2010, two of which relates to the protection of personal data: developing an electronic identity card (eID Card) to secure electronic transactions and creating a secure communication infrastructure for business, citizens, and the public administration (Federal Ministry of the Interior, 2006b). To achieve these goals, the German federal government has conducted two core projects: the eID Card Project and the Citizen's Portals Project. Both projects have the potential to contribute significantly

[18] More detailed introduction on OSCI could refer to (Steimke & Hagen, 2003).

to the cyber-security culture in Germany (Helmbrecht, 2008), thus are expected to play an important role in protecting personal data in e-government.

Electronic Identity Card and eCard Strategy

The German electronic ID card is planned to be officially introduced in November 2010. The eID card has three functions: the enhanced identification function for identity checks by providing biometric identifiers (used as e-passport), the electronic authentication function to secure online communication and transactions with government as well as business parties by digitally storing personal data on RFID chip, and the optional function as qualified electronic signature to facilitate some e-government and e-business applications (Langer, Schmidt, & Wiesmaier, 2009). The eID card also provides enhanced password protection and the misuse of data associated with the eID is prevented by a PKI-based (PublicKey Infrastructure) access management system. Pilot projects on eID card have already been conducted in universities in Germany.

The eID card project is only one component of Germany's eCard strategy. In March 2005, the German federal government approved the outlines of a common eCard strategy, which includes electronic passport (ePass), electronic identity card (eID), electronic health card (eGK), electronic income statement (ELENA) and electronic tax return (ELSTER) (Federal Office for Information Security, 2008). This eCard strategy has great potential to contribute to data security in e-government in Germany.

Citizens' Portals (De-Mail)

The Citizens' Portals Project aims at providing a secure communication infrastructure for business, citizens, and the public administration (Federal Office for

Information Security, 2008). As is introduced by Udo Helmbrecht (2008), the current president of BSI, the core of the Citizens' Portals initiative is establishing a new form of trusted email infrastructure to make online electronic communication as "secure, authentic, confidential and binding" as paper mail. This is achieved by establishing a network of government certified and privately operated Citizens' Portals, on which every citizen is entitled to a free so-called De-Mail (Deutschland Mail) address to send important e-mails and electronic documents in encrypted form for e-business and e-government purposes. Such portals will offer delivery evidence -- qualified, signed confirmations of electronic transmissions and receipt of e-mails. Security targets of confidentiality, authenticity, integrity and reliability are required to be guaranteed on such portals (BSI, 2008). In addition to email service, Citizens' Portals will also provide an identification service and a document safe for long-term documents deposit (Helmbrecht, 2008). The eID Card is expected to be the key authentication instrument for the Citizens' Portals. The De-Mail testing phase has already started and it is planned to be officially delivered in 2010 (European Commission, 2009b).

Strategies Protecting Information Infrastructure in Germany

In July 2005, the German federal government adopted the *National Plan for Information Infrastructure Protection* (NPSI) as an overarching national IT security strategy. In 2007, the *Implementation Plan for the Federal Administration* (UP Bund) was adopted to implement the NPSI in the Federal Administration. As the first uniform IT security guideline for the federal government, the UP Bund defines "technical, organizational, and process-related standards" for all government branches (Federal

Office for Information Security, 2009), which surely affects how federal government entities' take measures to protect data security in e-government activities.

Concluding Remarks

The national security projects and guidelines show that Germany has put much effort on technological security measures for e-government purposes, especially in the area of authentication and encryption. Just as stated in the BSI 2009 IT security report, "The fundamental awareness that IT security must not be neglected has indeed taken hold over the past years" (p. 11). Despite this, the BSI pointed out that there was still an insufficiency of the IT security awareness among public administration decision makers and of the financial resources, as well as a lack of qualified IT security personnel.

China

As introduced earlier, there is neither general data protection law nor e-government law regulating the collection, use and processing of personal data in e-government in China. Individual's privacy right and personal data security are protected by a patchwork of laws and law provisions in both direct and indirect means. Relevant laws, rules, and policies are briefly introduced in this section as they relate to personal data protection in the context of e-government in China.

Statutory Laws and Administrative Regulations

Regulations on the Privacy and Security of Electronic Communication

There are no statutory laws on electronic communications and telecommunications in China so far. Yet there are some administrative regulations and

regulation provisions addressing the protection of personal data, especially data security on the internet in general, which are applicable to the e-government context.

Regulation on Telecommunications of the People's Republic of China (2000)

The *Regulation on Telecommunications of the People's Republic of China* was passed in 2000. Article 58 of the regulation prohibits activities that endanger the security of telecommunication networks and information transmitted on these networks, which include, for instance, the acts of illegally accessing, stealing, modifying, damaging personal data that are stored, processed, transmitted over telecommunication networks or in related services, and the act of deliberately producing and spreading computer viruses to attack telecommunications network. It also prescribes that telecommunication subscribers' communication confidentiality is protected by law. Communication contents should only be accessible to relevant authorities for crime investigation and state security (*Article 66*). As specified by the regulation, internet connection and various internet services such as e-mail and online data processing and transmission are sub-categories of telecommunication services and thus within the protection scope of the law.

Regulations on Internet Security

Management Measures for Security Protection of the International Networking of Computer Information Systems (1997). This law was adopted in 1997 as the first regulation on computer network security in China. It dictated the agency of computer administration and supervision under the Ministry of Public Security be responsible for internet security, or in its original words, "for the public security of the international networking of computer information networks and safeguard the legitimate rights and

interests of units and individuals engaging in international networking businesses and public interest" (*Article 3*). The protection of personal data is implicit in the provision of no infringement on citizens' rights/interests and illegal criminal activities (*Article 4*); and explicit in the provision that prohibits online data modification (*Article 6*) and the provision on online communication privacy (*Article 7*). Article 10 requires all parties using the internet, including government agencies, to fulfill security protection responsibilities of both technical security measures and organizational security measures such as security training/education.

Regulation on Internet Information Service of the People's Republic of China (2000). The State Council passed this regulation in 2000. It requires internet information service providers to provide adequate measures to ensure network and information security, which include security measures for the web site, management measures for information security and confidentiality, and management measures for the security of user information (*Article 6*). Article 14 requires internet network connection service providers to retain customers' data such as telephone services, internet connection time, account numbers, IP addresses or domain names for a period of sixty days. These data should be accessible to relevant law enforcement authorities.

Decisions of the National People's Congress Standing Committee on Safeguarding Internet Security (2000). Article 4 of the above titled regulation prescribes that illegally intercepting, tampering with and deleting e-mail or other data materials of others constitute an infringement of freedom and privacy of correspondence and thus should be prosecuted for criminal liability. One point to note is that although the law urges "relative" government agencies to take active measures to protect the internet

security, such as developing internet security technologies and providing necessary training on data and information security, these government agencies are mostly the security supervising agencies, instead of government agencies in general.

Provisions on the Technical Measures for the Protection of the Security of the Internet (2005). Based upon the aforementioned 1997 regulation on internet security, the Ministry of Public Security issued an order on intensifying and regulating the technical measures of internet security in 2005. The order dictated specific technical measures and requirements to protect internet security on the part of internet service providers and internet entity users, the latter including government entities that use the internet to deliver e-government services. Article 4 requires internet service providers and entity users of the network not to disclose user information without user approval, unless it is required by law. Users' confidentiality of online communication is also emphasized. Specific technical measures are required, such as necessary measures to prevent computer viruses, invasions and attacks, and measures to back up key database (*Article 7*). Internet service providers are also required to retain users' personal data, record and if necessary audit individuals' net operations (*Articles 8-14*), which indicates that personal privacy gives way to internet security when they contradict. Although similar requirements exist in laws of other countries such as Germany, the degree of imbalance between individuals' right to privacy and internet security is more severe in China.

Additional Laws/Regulations Protecting Personal Data in E-government

Civil Law

Because of the absence of special legislation protecting individual privacy, the legal protection of personal privacy, including information privacy, in China has largely

relied on the protection of individuals' dignity and the personal right to reputation in existing laws and regulations. For instance, according to the *General Principles of the Civil Law of the People's Republic of China*, inappropriate uses of an individual's name and portrait, which are part of personally identifiable information under discussion, are prohibited. Remedies are prescribed when misuse of personal data harms an individual's reputation. This kind of indirect protection of personal data, however, is quite limited in scope and very often ambiguous in application, and thus might not be effective enough compared to a formal legal right of personal privacy.

To add to that, in the finished draft of the *Civil Law Code of People's Republic of China*, which is expected to be issued in the near future, a personal privacy right is stipulated as an independent formal legal right. It prescribes that every individual is entitled to the right of privacy and prohibits disclosure of personal data without consent. The provisions protecting the personal privacy right in the Civil Code will make the legal protection of personal data more direct and effective in China.

Criminal Law and the Seventh Amendment

The *Criminal Law of the People's Republic of China* was amended for the seventh time in February 2009. One major highlight of this amendment is that it criminalizes the infringement of personal information privacy. It is the first time that personal information has come under the protection scope of criminal law in the PRC.

With the new amendments, specific provisions were added to punish unlawful disclosure of citizens' personal information by government agencies, as well as telecommunications, transportation, financial, educational, and medical care entities. According to Article 253, staff members in government agencies as well other entities are

subject to criminal liability when they sell or illegally disclose citizens' personal information obtained in the process of performing official duties or providing services and where such behavior causes severe consequences or the 'circumstances are severe'. There is also criminal liability for stealing or other means of unlawful access to citizens' personal data under the same "severe consequence" condition. The amended Article 285 addresses the online security issue. The provisions state that any unlawful control of or access to computer data system, and any interception of or access to the data stored or processed in such systems are crimes liable to fines or imprisonment for up to seven years if the consequences or circumstances are severe, so are the acts that prepare the above crimes by producing or providing necessary tools.

Although some legal experts criticize the amendments for the ambiguity and limitation of the "severe consequences" condition, the amended *Criminal Law* extends the protection of personal information in China. It is so far the only statutory law with explicit and specific provisions protecting personal information in the government's hand in China. Other relevant laws usually mention the need to protect individuals' privacy in very general terms and in passing (in one phrase or in one sentence), or target at specific categories of data. The latest amendments show that legal liabilities in personal information misuse are becoming more stringent in China. It might also represent a beginning that Chinese laws and regulations are paying more attention to individual's interests and rights in the process of personal information handling. Although how the amendments are applied in practice remains to be tested in court, the seventh amendment to the *Criminal Law* is an important step towards directive and more effective protection

of personal information in China. These amended provisions are directly applicable to the protection of personal data in the context of e-government in China.

Electronic Signature Law (2004)

In China, the *Electronic Signature Law* was passed in 2004 and took effect in 2005. It was regarded as a landmark statutory law as the first national informatization-legislation in China. The law stipulates specific provisions on proper procedures, supervision agencies, security requirements, and legal liabilities of e-signature. By establishing the legal effect of electronic signature, it has the potential to facilitate the development of e-commerce as well as e-government in China. The current *Electronic Signature Law* is primarily intended to regulate e-commerce in the private sector. Article 35 in the Annex of the law, however, stipulates that the State Council or government departments specified by the State Council may frame specific rules on the use of electronic signature in government administrative affairs and other public activities pursuant to this law. Despite the lack of direct application and more specific provisions on e-signature use in the public sector, this law offers a legal base as well as a basic guide for using e-signature and e-authentication to secure electronic communication and transactions in e-government in China. Some Chinese provinces have already started to experiment relevant e-authentication mechanism in e-government practices.

Regulation of the People's Republic of China on Open Government Information (2007)

The above-titled regulation was passed in 2007 and enacted in 2008. The law prohibits administrative agencies from disclosing government information involving citizen's privacy without consent of the right-holder unless administrative agencies

believe that non-disclosure might cause great impact on the public interest (*Article 14*). Article 25 requires citizens to provide valid identification certificates or relevant documents when requesting personal data from government agencies. Moreover, it offers citizens the right to correct personal information.

Additional Sectoral Laws that Apply

In addition to the laws and regulations introduced above, a few other laws also contain brief provisions requiring the protection of specific types of personal data. These sectoral laws cover the protection of passport-related personal information (*Passport Law*), identity card relevant personal information (*Law on the Identity Card of Residents*), women's personal information (*Law on the Protection of Women's Rights and Interests*), and minors' personal information (*Law on the Protection of Minors*). Yet data protection provisions in these laws are usually very general and brief (with no specific requirements).

National Policies Protecting Personal Data in E-government

In addition to the above national laws and regulations, a few national administrative policies and guidelines are also relevant to personal information protection in e-government in China directly or indirectly.

State Informatization Development Strategy 2006-2020

The State Council of China issued the *State Informatization Development Strategy 2006-2020* in 2006. Establishing a legal system for informatization was listed as one of China's informatization development goals for the following 15 years. Enacting and improving laws and regulations on personal data protection and network information

security is one key component of this goal. The Strategy also emphasizes the importance to actively participate in the researching and formulating of relevant international rules. As one of the few national administrative directives addressing the personal information protection issue directly, this Strategy indicates that the Chinese government has realized the necessity of personal data protection in the digital age and has put this issue on immediate legislative agenda.

General Framework of National Electronic Government (2006-2010)

In 2006, the SILG issued the *General Framework of National Electronic Government* as the next five-year (2006-2010) plan for e-government development in China. The Framework provides strategic guidance on information practices in e-government. It puts forward the principle of 'one data, one source' for basic information needed in the routine work of government agencies, which include citizens' basic personal information. The guidance points out the necessity to avoid duplicated data collection, to guarantee data accuracy, completeness, and timely updating, and to centrally manage basic information systems. Although some basic international data protection principles are addressed, more stringent privacy protection principles such as the necessity of data collection and user notification are absent in the Framework. While data-sharing is greatly encouraged across agencies to achieve economic efficiency, the consequent personal privacy concern is ignored by the guidance and no limit is placed on agencies' data sharing.

Regarding information security infrastructure, the Framework emphasizes the importance of building and standardizing an e-government trust system, which includes establishing effective authentication, certification, and liability mechanism, constructing

information security monitoring system, perfecting precautionary measures against cyber attacks and measures for timely identification of security breaches. It also requires security plans in place for e-government incident response, data backup and disaster recovery. Government agencies in the process of adopting e-government are required to combine the construction of information security infrastructure with the improvement of information security management mechanism. Similar to the information security strategy in the US and Germany, the framework also points out that security standards need to be customized based on risk levels and protection needs.

Circular on Strengthening the Risk Assessment of Information Security in E-government Project Construction (2008)

In 2003, the SILG issued the No. 27 policy paper of *Opinion on Strengthening Information Security Protection*. Nine specific tasks were listed towards protecting information security, which, for example, include establishing an information security responsibility mechanism, classifying information security levels, and increasing public awareness of information security. This policy paper became the ground work of information security protection in China.

Guided by this order, in 2008 the National Development and Reform Commission, together with two other government agencies, issued the *Circular on Strengthening the Risk Assessment of Information Security in E-government Project Construction*. The Circular requires all e-government projects, including e-government website, basic database, and other supporting systems, to conduct information security risk assessment. It specifies items to be assessed, among which the importance levels of information data, security threats, system fragility, and existing security measures are the primary items for

the assessment. Though personal data is not specifically mentioned, it is one crucial component of the government's electronic information system. This circular indicates an awareness of the importance of information security in e-government by the Chinese government.

Concluding Remarks

Overall, personal data protection in China is fairly inadequate. There is not only a lack of general data protection law, but also a scarcity of specific data protection legislation, administrative guidelines, and technologic measures applicable to data protection in the public sector or e-government area. Although more rules and regulations in recent years begin to use the concept of "personal information" and the legislation protecting personal information is being improved and strengthened, the overall legal system for personal data protection, especially data privacy protection, in China is fairly weak, not to mention the legislation protecting personal data in the specific domain of e-government. In the laws, regulations, and policies relevant to the topic under discussion, electronic data security is much more emphasized than information privacy. In the few cases where personal data privacy is stipulated, the protection requirement is often very general and ambiguous. The real practice of the protection is a big question. In brief, because of the lack of data protection legislation and administrative guidelines, Chinese government agencies have to largely rely on self-established code of conduct in handling individuals' personal data (more discussion in the last chapter), which is confirmed by a Chinese legal expert that I interviewed. It is imperative to speed up the legislation on personal data protection in general and also for e-government in China.

CHAPTER 6

THE INTERNATIONAL LANDSCAPE

The data protection issue in e-government is global both in the nature and the scope of the problem. First, the global nature of the internet infrastructure blurs the traditional clear-cut borderline between countries and creates the global challenge of securing cyberspace, where e-government activities are conducted and electronic communication between government and citizens occur. This global cyber security challenge might not be effectively addressed by measures at the national level alone. Adequate protection of the information infrastructure is hard to be achieved by individual countries. Rather, international norms, standards, and actions are greatly desirable to establish a secure digital infrastructure, thus to achieving the security of personal information that is digitally collected and processed.

Second, the electronic form of data and the use of internet in e-government enable much faster and easier ways to share and exchange personal data and thus tremendously increase data flows across governments of different countries. Many countries see a common interest in protecting personal data and establishing a consensus on data protection fundamental principles at regional and/or international level, which could facilitate resolving problems of law conflicts and prevent circumvention of national regulations on data processing (OECD, 1980).

For these reasons the issue of protecting individuals' personal data in the context of e-government might not be analyzed and solved exclusively at the national level. Although data protection is often thought of nationally, it needs to be seen in a global

context. In addition to the efforts at national level that are examined in the previous chapters, there are also supra-national principles, agreements, and actions impacting personal data protection in e-government in the three countries. To better understand the multi-level and multi-mode governing system of this issue, international efforts are reviewed at two levels in this chapter: global level and regional level.

Global Treaties, Principles, and Standards

Privacy Right: the International Bill of Human Rights

In 1948, the General Assembly of the UN adopted and proclaimed the *Universal Declaration of Human Rights* (UDHR). Article 12 of the Declaration states that everybody has the right to law protection against arbitrary privacy interference, through which privacy is internationally recognized as an important human right. This article has been elaborated in subsequent international treaties, regional privacy guidelines, and national constitutions and laws. Yet in practice, the UN member states, including the three countries under discussion, may define privacy in different means and implement the privacy protection provision at different levels.

To impose concrete binding obligations on human rights on its member states, based upon the UDHR, the UN created the *International Covenant on Civil and Political Rights* (ICCPR) in 1966, which took effect in 1976. Article 17 of the Covenant declares the human right to privacy protection, which in principle makes privacy a legally enforceable right. Though all the three countries signed the treaty, the US, Germany, and China are distinct in national implementations of the Covenant. Specifically, Germany

signed and ratified ICCPR in 1973[19] with no reservations and declarations relevant to the privacy right. China signed the Covenant in 1998 yet has not ratified so far. The US case is a little more complicated. The US ratified ICCPR in 1992 with certain reservations and declarations. In declarations, the US declares the provisions of articles 1 - 27 of the Covenant, which include the privacy article, not self-executing. This means that, where the US Congress does not implement the agreement with national legislation, the treaty itself is nonbinding or ineffective. In this sense, the ratification of the Covenant as an international law by the US has very limited meaning to its practice of protecting the public's privacy right, which was also realized and criticized by the UN as 'material non-compliance'.

Fair Information Practices

Fair Information Practices (FIPs) are a set of internationally recognized principles on responsible handling of personal data, which has been developed to protect the privacy and security of personal information in computerized information systems and are enshrined in many key privacy rights instruments around the globe.

FIPs were first proposed in 1973 by a US government advisory committee (GAO, 2008b). Aiming to balance the benefits of computerization and the protection of personal data privacy, the earliest FIPs consist of five key principles of privacy protection, based upon which the Organization for Economic Cooperation and Development (OECD) created eight core FIPs and codified them into its 1980 Privacy Guideline. These FIPs form the foundation of various supra-national regional data protection frameworks, such

[19] A country list of declarations and reservations made upon ratification is available at http://www.unhchr.ch/html/menu3/b/treaty5_asp.htm.

as the EU *Data Protection Directive* and the *APEC Privacy Framework*, and many national privacy laws, including the US *Privacy Act* and the *German Federal Data Protection Act*.

Varying in wording or terminology, the core principles for fair information practices can be summarized as follows (GAO, 2008b; OECD, 1980):

- *Collection Limitation Principle*: The collection of personal data should be limited and should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the data subject.
- *Data Quality Principle*: Personal data should be relevant to the purposes for which they are to be used, and should be accurate, complete and updated.
- *Purpose Specification Principle*: The personal data collection purposes should be specified before data collection and whenever change occurs, and any subsequent use should be limited to those purposes or other compatible purposes.
- *Use Limitation Principle*: Personal data should not be disclosed or used for non-specified purposes without the consent of the data subject or legal authority.
- *Security Safeguards Principle*: Personal data should be protected by reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification or data disclosure.
- *Openness Principle*: Personal data developments, practices and policies should be made public, as well as the main purposes of their use and the basic information about the data controller.
- *Individual Participation Principle*: A data subject should have the right: to obtain his data, to know about the collection of his data, to know the reasons for request

denial and challenge such denial, to challenge data relating to him and to have the data erased, rectified, completed or amended if the challenge is successful.

- *Accountability Principle*: A data controller should be accountable for taking measures to implement the above principles.

Based upon the above principles, a growing number of countries have adopted national data protection laws and policies to protect personal data collected by the public and private sectors. Regarding the data protection issue in e-government, as is demonstrated by relevant legislations and policies in the US and Germany, the FIPs provide a framework of principles for balancing the need for individuals' information privacy with the benefits brought about by e-government such as administrative efficiency. Yet compared to the US, Germany shows more stringency in national implementation of these data protection principles. For instance, Germany emphasizes the data reduction and economy principle, yet the US does not have such explicit requirement. In the case of China, although most of the FIP principles are imbedded in its data protection draft law, the openness principle is missing and there is much weaker implementation of some other principles. For example, there is no requirement of informing data subject about government's collection of their personal data and of requesting data subject's consent on such collection. Further, there are very broad exemptions to the lawful principles. These will make the actual implementation of the principles much more limited and data protection much weaker in China.

UN Guidelines Concerning Computerized Personal Data (1990)

In 1990, the UN issued *Guidelines Concerning Computerized Personal Data* (A/RES/45/95), which was applied worldwide without being legally binding. A total of

nine principles are listed for member states to consider as the minimum guarantee in national legislations to protect computerized files in both public and private sectors, which are lawfulness and fairness, accuracy, purpose specification, data subject access, prohibition of discrimination, power to make exceptions, security, supervision and sanctions, and trans-border data flows. The principles include all the basic components of the FIPs as well as offering guidance on electronic trans-border data flows. Although these are non-legally binding principles, the UN requests all governments to respect and take into account these guidelines in their legislation and administrative regulations.

UN Information Security Guidelines

The UN has also developed various cyber security policies relevant to personal data protection. For instance, in 2000 and 2002, it adopted Resolutions 55/63 and 56/121 on *Combating the Criminal Misuse of Information Technologies*. Resolution 55/63 recommends ten measures to combat misuse of information technology, such as international cooperation in law enforcement, law enforcement personnel training, and increasing public awareness. The resolution specifically emphasizes the importance to establish legal systems to protect the confidentiality, integrity and availability of data and computer systems. Meanwhile, it provides that states should balance the need to protect individual privacy and to ensure governments' capacity to combat criminal misuse. Resolutions 56/121 re-emphasizes the ten measures outlined in resolutions 55/63 and invites member states to consider those measures in their efforts to combat cyber crimes. It also invites member states to take into account the related work by other regional and international organizations, such as the Council of Europe's *Convention on Cybercrime*.

In addition to the above two resolutions, there are more UN resolutions of the same category, which, for example, include Resolution 58/199 *Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures*. These resolutions are indirectly relevant to personal data protection in e-government in the context of guiding the international and national protection of cyber security.

Data Protection Efforts by the International Standardization Organization

As data protection and privacy laws proliferate around the world, more countries see a common interest in having an international standard for personal data protection. As the world's largest international standard body, the International Organization for Standardization (ISO) is involved with attempts to develop an information privacy protection standard (Bennett & Bayley, 2007). Although so far such an international standard has not been established, various other standards have been built or being built in the field of IT security by a joint committee of ISO and the International Electro-Technical Commission. These technical and management standards protecting the security of digital information have key privacy components and are directly relevant to personal data protection in the context of e-government. These standards cover various aspects of digital information security, which include cryptography topics such as digital signature and message/entity authentication, identity management, biometrics, and many other relevant aspects. A Privacy Framework (ISO/IEC 29100), primarily driven by the need to cope with online privacy risks, is currently also under development and expected to be published in November of 2010 by ISO.

Though the issue of personal data protection in e-government is not specifically dealt with by ISO, most of the ISO technical and management standards on IT security

and personal data protection are applicable to the e-government area. Since the US, Germany, and China are all member countries of ISO, these standards may have un-negligible influence on the countries' national approach to data protection, particularly on the protection of data security. Although regulations differ across countries, such "consensus based standards could help provide a global base of protection" (Bennett & Bayley, 2007, p. 19).

Supra-national Regional Conventions and Guidelines

While international principles and treaties lay down foundations that national legislation could build on and obligations that party states are bound to respect, data protection instruments are also established at supra-national regional level, which reflect the particular privacy concerns of the region and provide more specific guidelines for national implementation of data protection. The primary regional treaties and guidelines relating to personal data protection in e-government, which the US, Germany, and China are member of or accede to, are briefly introduced as follows.

OECD Guidelines

As an intergovernmental forum, the OECD Working Party on Information Security and Privacy is responsible for developing policy guidance on information security and privacy in the global networked society for OECD member states, including the US and Germany, as well as non-member states. Following is a brief introduction of its work on information privacy and security that are applicable or relevant to the context of e-government.

Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data (1980)

Faced with new privacy challenges brought about by automatic data processing and increasing trans-border flows of personal data, the OECD saw a need to develop compatible rules and practices among its member countries. In 1980, it issued *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data,* aiming to harmonize national privacy legislation and meanwhile prevent interruptions in international flows of data (OECD, 1980). The Privacy Guidelines set out specific rules governing the handling of electronic, as well as offline, personal data by both public and private sectors. In addition to eight principles on personal data collection and processing, the Guidelines also propose the general principle of 'free flow and legitimate restrictions' for cross-border data flows. As one of the first and most influential regional agreements on personal data protection, the principles published by OECD become the core elements of the FIPs, which represent international consensus on general guidance regarding the collection and management of personal data, including personal data in e-government. These principles form the basis of many international privacy agreements and national legislation. As member countries, the US and Germany both agreed upon and endorsed the principles in the Guidelines. The OECD Guidelines, however, are not legally binding.

OECD Guidelines for Security of Information Systems and Networks: Towards a Culture of Security (2002)

In 1992 OECD issued the *Guidelines for the Security of Information Systems.* To adapt to the rapidly changing environment of new information technology, in 2002 OECD released the *Guidelines for the Security of Information Systems and Networks:*

Towards a Culture of Security as updated recommendation to its member, and non-member, countries on cyber security. Applying to all participants in the new information society, the Guidelines provide nine principles to guide practices for a "culture of security", which include, for instance, security awareness, timely and cooperative response, risk assessment, security design and implementation, comprehensive security management, and periodic security reassessment. The Guidelines also recommend member countries to strengthen international cooperation on information systems/networks security issues and to 'consult, co-ordinate and co-operate' at both national and international levels to implement the Guidelines. Like the Guidelines on privacy protection, the Guidelines on information security are voluntary and nonbinding.

Additional OECD Guidelines Relevant to Data Protection in E-government

In addition to the above two general guidelines, OECD has developed various other recommendations that are also relevant to electronic personal data protection in the public sector. For example, in 1997 OECD issued the *Guidelines for Cryptography Policy*, which outlines eight interdependent principles as key policy recommendations to governments (as well as businesses) to promote the use of cryptography as a valuable tool for the protection of data privacy and security in national and global information networks and systems. Public-private and international co-operations are emphasized for the development and implementation of national and international cryptography policies and practices. OECD has also been working on policies for some other information security areas such as electronic authentication and digital identity management.

Additional important OECD policy measures related to privacy protection in e-government include the *Ministerial Declaration on the Protection of Privacy on Global*

Networks (1998), *Privacy Online: OECD Guidance on Policy and Practice* (2002), and *Making Privacy Notices Simple: an OECD Report and Recommendations* (June 2006). In 2007, OECD adopted the *Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, which recommends both the public and private sectors in the member countries take appropriate steps at domestic and international levels to co-operate across borders in the enforcement of laws protecting the privacy of personal data. All these guidelines are non-binding for the member states.

European Treaties and Guidelines

Germany is a member state of the Council of Europe (CoE) and the EU, which are two different European organizations. This part reviews the primary data protection treaties and guidelines developed by these two entities. While CoE Conventions are binding for its member states upon their signature and ratification, the EU data protection directives are automatically legally binding and have to be transposed into national laws of its member states, including Germany.

Council of Europe Conventions

European Convention of Human Rights (1950)

The *European Convention of Human Rights (the European Convention for the Protection of Human Rights and Fundamental Freedoms*) was adopted by the CoE in 1950. All its member states including Germany are party to the Convention. The Convention reaffirms individuals' rights of privacy in Article 8 and rights of expression freedom (to receive and impart information without interference) in Article 10, with certain restrictions such as for the interests of national security, public safety, or crime

prevention. The Convention establishes a European Court of Human Rights, which may receive applications from any individual, non-governmental organization, and government unit claiming to be the victim of a violation of the rights set forth in the Convention, including the privacy right (*Article 34*). This Convention is the only international human rights agreement providing individual privacy protection as high as at the international level.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981)

Aiming to strengthen legal protection of individuals with regard to computer processing of their personal information, the CoE's 1981 *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, known as *Convention 108*, sets out specific rules for the handling of personal data by both public and private sectors based upon the FIPs principles and thus shares great similarity with OECD's 1980 privacy protection guidelines. For instance, the Convention stipulates rules of data quality, data security, purpose limitation, and data subject participation. It also provides general guidance on cross-border personal data flows and emphasizes the importance of international cooperation.

Compared to the OECD Guidelines, however, the Convention provides some more rigorous protection of personal data in the sense that it offers extra protection for 'special categories of data' that reveals individuals' racial origin, health or sexual life, political opinions, and religious or other beliefs (*Article 6*). Different from OECD privacy guidelines, the CoE Convention is binding for its member states upon their signature and

ratification. Out of its 47 member states, 41 have ratified the Convention so far. Germany signed the Convention in 1981 and ratified it in 1985.

Like the OECD privacy protection guidelines, this agreement also has profound effect on global privacy laws, rules, and policies. There are campaigns undergoing to request non-member governments to support the CoE Privacy Convention and adopt comprehensive privacy legislation of that standard. The Convention formally opened up for signature by non-member States from 2008, which makes it "the only binding international legal instrument with a worldwide scope of application in the field of data privacy" (EPIC, n.d.).

Convention on Cybercrime (2001)

The CoE officially released the *Convention on Cybercrime* in 2001. Its objective is to "pursue a common criminal policy aimed at the protection of society against cybercrime". The Convention addresses the security issue of computerized personal data in the hands of public, as well as private, entities by criminalizing activities of illegal access, illegal interception, data interference, system interference, computer-related forgery, and computer-related fraud. It also offers general guidance on international cooperation in investigating those crimes.

The Convention is regarded by many to be 'fundamentally imbalanced' regarding the protection of cyber security and the privacy of individuals' personal information, and has received significant opposition and criticism from various parties such as independent legal experts and human rights activists. The Convention provides very "detailed and sweeping powers" of computer data search and seizure and government surveillance of electronic data communication in virtually all areas of online activities at both the

domestic and international levels (Taylor, n.d.). It is thus heavily criticized for its one-sided emphasis on increasing government surveillance yet failing to ensure minimum standards of privacy protection.

Despite controversial argument about the Convention, Germany signed this treaty in 2001 but ratified it much later, in 2009. As a non-member state yet an observer of the CoE and an active participant from its drafting stage, the US signed the Convention in 2001 and ratified it in 2006, with strong opposition from domestic privacy advocates.

There are some other non-binding CoE recommendations that are also relevant to the issue under discussion, which include, for instance, the *Committee of Ministers Recommendation No. R (99) 5 on the protection of privacy on the Internet* and the *Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting*. The latter addresses the security and privacy issue of personal data involved in a specific e-government area of e-voting.

European Union Data Protection Directives and Initiatives

The protection of human rights, privacy right in particular, in EU is mainly rooted in the CoE's *European Convention of Human Rights* (*Article 8*), which is re-confirmed by the Article 6 of *Treaty on the European Union* and reiterated by the 2002 *Charter of Fundamental Rights of the European Union* in Article 7 (privacy right protection) and Article 8 (protection of personal data). Following are the relevant EU data protection directives that the EU member states including Germany are required to transpose into domestic data protection laws and some initiatives in this regard.

Directive 95/46/EC on the Protection of Individuals With Regard to the Processing of Personal Data (1995)

Following the OECD and CoE, the EU enacted the *Data Protection Directive*, officially *Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data*, in 1995. By harmonizing data protection regulation in the EU member states, the Directive aims to establish a high level of protection for individuals' personal data and meanwhile promote inter-member free flows of personal data without being restricted by data protection reasons. In Germany this Directive is transposed into the *Federal Data Protection Act.*

The Directive regulates primarily, yet not limited to, automated processing of personal data. Government agency is one of the regulated parties. The Directive establishes explicit rules that govern governments' (and other parties') processing of individual's personal data, which include data quality rules such as fair and lawful processing of personal data, purpose specification, data adequacy and relevancy, data non-excessiveness and data accuracy. Other rules include the legitimacy, confidentiality, and security of data processing, notification, data subject rights, and strengthened protection over sensitive personal data. Regarding cross-border data flow, the key principle and standard is to ensure an adequate level of protection. The third country involved in trans-border data flow is required to provide a similar level of data protection.

Every EU country is required to set up an independent supervisory authority to monitor and consult on the enforcement of these protection rules regarding personal data processing. At the EU level, a Working Party on the Protection of Individuals with regard

to the Processing of Personal Data is set up as an independent advisory as well as acting unit regarding personal data protection.

Data Protection in the Electronic Communications Sector

In 1997, the EU adopted *Directive 97/66/EC of the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector*. To adapt to technology advances and markets developments, the 1997 Directive was replaced in 2002 by *Directive 2002/58/EC on Privacy and Electronic Communications*, which is required to work in combination with the *Data Protection Directive* 95/46/EC. Germany transposes this Directive mainly through its *Telecommunications Act*.

Directive 2002/58/EC sets out EU standards and obligations regarding the protection of personal data and privacy in the electronic communications sector, thus is crucial to ensure users that the services and technologies used for their electronic communications, such as e-government services, can be trusted. It stipulates rules to ensure the security and confidentiality of all electronic communications, including both the content and any personal data related to such communications. It also defines specific rules regarding the use of cookies or similar devices on users' personal computers (users should be informed of the purposes of cookies and have opportunities to refuse cookie use on their computers); the retention of users' traffic and location data (only with consent for marketing purposes and valued-added services provision); and the inclusion of individuals' personal data in public directories (with prior consent).

In 2006, the European Parliament and the Council adopted *Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications*

networks and amending Directive 2002/58/EC. The objective of this Directive is to harmonize the EU obligations of electronic communication service or networks providers with respect to the retention of users' traffic and location (not content) data to ensure that such data are available to competent national authorities for the purpose of the investigation, detection and prosecution of serious crime (*Article 1*). In particular, the Directive defines the data categories to be retained, the retention period, the storage requirements for retained data, and the rules for data protection and data security. With respect to internet services like in e-government, users' traffic and location data such as the user ID, IP address, internet service log-in and log-off time, and the Internet service type should be retained for six to twenty-four months (depending on national laws).

Additional EU Data Protection Regulations that Apply

Two other EU regulations that might also impact Germany's personal data protection in e-government are *Regulation 45/2001/EC on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data*, which aims to protect personal data processed by the EU Community institutions and bodies, and the *Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.*

Information Security Initiatives

In addition to the above data protection directives, there are also various EU initiatives and guidelines on network and information security. For instance, the 2003 *EU Council Resolution on a European Approach towards a Culture of Network and*

Information Security urges EU member states to take adequate measures to prevent and respond to network and information security incidents. It suggests the OECD information security guidelines as a valuable model for developing network and information security policies. To achieve 'a culture of security', the guidance emphasizes the key role of personal data privacy protection, the public-private sector cooperation, and the multi-level (national level, EU level, and international level) interaction and cooperation.

Another example is the 2005 *Council Framework Decision on Attacks against Information Systems*, which aims to harmonize rules on criminal law in the EU member states in the area of information systems attacks such as illegal access to information systems, illegal system interference and illegal data interference. It encourages judicial cooperation between member states regarding such attacks.

APEC Data Protection Framework

The Asia-Pacific Economic Cooperation (APEC) has 21 member states in the Asia-Pacific region, including the US and China. There are wide differences in economies, cultures, social systems and implementation of data protections between the member states. APEC operates on the basis of non-binding and voluntary commitments.

APEC Privacy Framework

In 2004 APEC Ministers endorsed the APEC Privacy Framework. Both the US and China agreed to the development of this framework. Aiming at developing appropriate information privacy protections and ensuring the free flow of information in the Asia Pacific region, the Framework applies to persons or organizations in both the public and private sectors that control the collection, processing, and use of personal

information. The Framework outlines nine principles on information privacy protection, which are largely based upon the OECD's 1980 Privacy Guidelines. Yet they are believed to be "weaker in significant respects" than the 30-year-old OECD Guidelines both in its principles and in its implementation requirements (Greenleaf, 2009, p 31), not to mention improvements on the Guidelines to address new challenges brought about by technologies advances and the consequent new situations. Overall, the principles are criticized as being weaker than the European data protection regime and most existing data protection laws in the Asia Pacific region (e.g. Greenleaf, 2009; Privacy International, 2007a). As Greenleaf (2009) argued, instead of representing objective 'consensus' of existing regional privacy laws, the principles only represent the lowest common denominator of the privacy principles in the region.

The Framework provides general rules on domestic and international implementation of privacy standards for APEC members and emphasizes the necessity of flexibility in implementation due to the disparity in data protection practices and social contexts of the member states. It also recommends information sharing and cooperation across agencies/authorities to enable cross-border transfers of personal data. Yet overall its implementation scheme is considered to be too general and significantly weaker than any other international privacy instrument.

In 2006, APEC endorsed the e-commerce-focused Pathfinder initiative to facilitate the implementation of the APEC Privacy Framework. Yet use of cross-border privacy rules by the public sector has not been covered by the initiative so far. Despite its significant weaknesses, one positive side of the APEC Privacy Framework is that it has

the potential to encourage the development of privacy laws in those APEC economies that at present have no privacy or personal data protection legislation.

APEC Information Security Strategies

The importance to secure information and information systems from cyber attacks has also been recognized by the APEC. In 2002, the Fifth APEC Ministerial Meeting on Telecommunications and Information Industry issued a *Statement on the Security of Information and Communications Infrastructures*. The statement agreed to support domestic implementation of the ten measures included in UN Resolution 55/63 *Combating the Criminal Misuse of Information*. It also noted the work of other international organizations in this area, in particular the CoE's *Cyber Crime Convention* and the *OECD Guidelines for the Security of Information Systems*. Beyond that, the statement highlighted some key aspects in developing domestic and regional strategies to secure the interconnected information and communication infrastructures within the APEC region, which include, for example, establishing a legal basis and law enforcement cooperation to address the criminal misuse of information technologies, developing government-private sector partnerships, establishing computer emergency response teams , increasing security awareness, and noting the importance of certification, encryptions, authentication as well as IT security standards.

Other relevant, yet non-exhaustive, guidance and strategies include APEC *Cybersecurity Strategy* (2002), *APEC Strategy to Ensure Trusted, Secure and Sustainable Online Environment* (2005), and the *Guiding Principles for PKI-based Approaches to Electronic Authentication* (2005), which all recommend similar principles such as

private-public partnership, regional and international cooperation, incident response and recovery capabilities, awareness and training, and so on.

Concluding Remarks

The above supra-national standards and guidelines on personal data protection are the most influential, yet non-exhaustive, of those developed by the UN and the prominent supra-national regional organizations of the OECD, the CoE, the EU, and the APEC, of which the three countries are member states. Although the overview of international legal and policy landscape on personal data protection indicates an overall lack of data protection instruments targeted at the specific e-government context at the international level, the aforementioned general or sectoral international agreements and guiding principles not only have, or might have, impact on the protection of the privacy and security of personal data in e-government context at the international level but also shape individual countries' national approaches to this issue.

However, the influence of these agreements and guidance on individual countries varies. While the EU directives are legally binding for Germany and must be transposed into its national laws, the UN, OECD, and APEC guidelines on the protection of computerized personal data are not legally binding and implemented voluntarily. Meanwhile, even the CoE Convention and EU directive are both implemented in Germany, the general principles might be enacted in different ways. At the same time, we should not ignore the fact that international guidelines carry great influence from some dominant international groups like the EU and powerful sovereign states like the US. Different international organizations also learn from each other in developing policies.

These help explain the considerable connection and consistency in international and national general data protection principles.

Additional Multilateral and Multi-stakeholder Efforts on Data Protection

Apart from international governmental organizations introduced above, there are also various less formal, non-governmental, or partial-governmental international forums (without an enforcement focus) where the personal data protection issue associated with technological advances, particularly the internet, is discussed and explored by multiple stakeholders. Such international forums include, but are not limited to, the UN organized independent forums for internet governance, the annual International Conference of Data Protection and Privacy Commissioners, the World Bank, and various privacy advocacy associations such as Privacy International.

A brief overview of the policies, reports, or conference programs of some of these non-governmental organizations/associations demonstrates that the growing concern of data protection in the globally connected information society has been increasingly recognized and addressed by various stakeholders, yet so far there is a lack of international actions and policy recommendations on privacy protection in the specific area of e-government.

The first example is the internet governance forums. The two phases WSIS in 2003 and 2005 created two multi-stakeholder internet governance bodies -- the Working Group on Internet Governance (WGIG) and the Internet Governance Forum (IGF), which identified data protection and privacy as one of the internet-related public policy issues. Specifically, the WGIG recognized a "lack of national legislation and enforceable global standards" for the privacy protection of online personal data and, among other things,

suggested the development of open technical proposals for global electronic authentication systems to meet privacy requirements (WGIG, 2005b). The 2006 Inaugural Meeting of the IGF created the Dynamic Coalition on Privacy (DCP), which originally only worked on three issues (digital identities, the link between privacy and development, and the importance of privacy and anonymity for freedom of expression) but later expanded their work to some new issues such as privacy and surveillance (Dynamic Coalition on Privacy, 2008). Although digital identities are relevant to data protection in e-government, the Coalition's work does not look at the specific area of e-government. The second IGF meeting originally even did not include privacy as a topic. The efforts of the DCP enabled privacy to be placed under the "security" subject heading (Privacy International, 2007b). It is obvious that although electronic privacy has been recognized as an issue in the internet governance arena, it is not on the priority list yet. Most relevant discussions and guidance in this area address the general topic of online privacy protection. In cases where sub-areas of privacy are specified and discussed, they mainly focus on international data flows, information security, and privacy-enhancing technologies. These privacy sub-issues apply to both the private and public sectors, thus are relevant to some aspects of data protection in e-government.

Similar conclusions could be drawn from other forums. The annual International Conference of Data Protection and Privacy Commissioners is another cooperative venue where a broad range of privacy issues are discussed by the data protection community. A review of the conference programs and reports in the recent three years (2007, 2008, and 2009) shows that the topic addressed by this Conference in terms of the new privacy risks posed by government use of personal information is largely confined to government

surveillance. Among the sub-issues of privacy protection that bare relevance to the e-government context, information security and cross-border data flows, together with the consequent global privacy regulation challenges, are the dominant topics. Other than that, the specific topics of data mining and Privacy Impact Assessment addressed by the Conference are also applicable to the public sector. But overall the particular challenges to data privacy posed by e-government have not received enough attention to be treated as a distinct topic yet.

In short, although the privacy protection issue in the digital age has attracted growing attention and discussion at various multilateral and multi-stakeholder public policy forums and the protection of personal data with respect to e-government has been addressed to certain degree through some privacy sub-areas such as cross-national data flows and data security, there is barely any formal discussion, working report, or international/regional guidelines and recommendations found on the protection of personal data in the specific context of e-government. Among the reports, policy guidance, and working agendas of the non-governmental associations I reviewed, the only working paper found directly addressing data protection in e-government area was about the privacy protection in online voting in governmental elections (The International Working Group on Data Protection in Telecommunications, 2005). Overall, more relevant work and policy recommendations are found on information security, especially on privacy-enhancing technologies such as cryptography technologies and techniques.

Table 5 presents a summary list of all the relevant governance instruments employed at the supra-national level that are introduced in this chapter.

Table 5 International Governance Instruments

		United States	**Germany**	**China**
Supra-national regional solution	Legally-binding rules	▪ *CoE Convention on Cybercrime (2001)*		N/A
		N/A	▪ *European Convention of Human Rights (1950)* ▪ *CoE Convention for the Protection of Personal Data (1981)*	
		N/A	▪ *EU Data Protection Directive (1995)* ▪ *EU Directive on Privacy and Electronic Communications (2002)*	N/A
	Non-binding guidance	▪ *OECD Guidelines for Privacy (1980)* ▪ *OECD Guidelines for Security (2002)*		N/A
		▪ *APEC Privacy Framework 2004* ▪ APEC cyber security strategies	N/A	▪ *APEC Privacy Framework 2004* ▪ APEC cyber security strategies
Global solution	Legally-binding rules	▪ *ICCPR (1966)* (signed and ratified with 'material non-compliance')	▪ *ICCPR (1966)* (signed and ratified)	▪ *ICCPR (1966)* (signed but not ratified)
	Non-binding guidance	▪ *Universal Declaration of Human Rights(1948)* ▪ *UN Guidelines Concerning Computerized Personal Data (1990)*		
Alternative regulation (both regional and global)		Example : WGIG, IGF, International Conference of Data Protection and Privacy Commissioners; limited role		
Code-based regulation (both regional and global)		Example: technical standards and techniques on information security developed by ISO		

CHAPTER 7

ANALYSIS, DISCUSSION AND CONCLUSION

This study provides a comparative analysis of the national laws and policies protecting personal data collected and processed in the context of e-government in the US, Germany, and China. It also contributes a brief examination of the international legal and regulatory landscape with respect to the issue under discussion. While traditional national government regulation and international regulation are the two governance modes examined in detail in this study, the other two governance modes presented in the conceptual framework – alternative regulation and code-based regulation -- are also identified based upon evidence gained from the national and international policy instruments. The major findings are therefore organized under the four governance modes distinguished in the conceptual framework in Chapter 2. Further discussion and implications on how the governance modes function with respect to the national context and their effectiveness in the particular context of e-government and for the internet in general are presented after the observations.

National Government Regulation

The study shows that national government regulation plays an important role in the current protection of personal data involved in e-government, especially in the economically and legally more advanced countries – the US and Germany. Overall, the examination of relevant government regulation in the three countries reveals three major points: (1) the existence of some commonalities in national approaches; (2) unbalanced

data protection across countries; and (3) room for improvement in the existing national regulatory frameworks to protect information privacy in the e-government area.

Commonality in National Approaches

The review and discussions in Chapters 4 and 5 indicate that some commonalities exist between the national approaches to the protection of privacy and information security in e-government.

First, although with different priority levels in the three countries, there is a basic common notion that government's handling of electronic personal data requires particular legislative attention. This is demonstrated by the existence of the US *Privacy Act* and *E-government Act* and the *German Federal Data Protection Act*. It is also evidenced by China's undergoing legislative efforts on its first data protection law and the recent amendment to its criminal law that for the first time criminalizes government's infringement of personal information privacy. Although specific content varies across countries, certain kinds of laws and regulations that are relevant to the issue under discussion exist in all the three countries, for example, laws that regulate electronic signature, freedom of information (or open government information), and electronic information security.

One point worth noting is that, although there is no integrated federal law of privacy in the US, there are privacy laws, regulations, and various OMB-issued rules regulating the public sector's information practices. These regulations either apply to the public sector in general or to the e-government context specifically. Thus the traditional wide gap in privacy protection between Germany and the US is greatly reduced when it comes to the public sector and to the specific context of e-government.

Second, the review of American, German, and Chinese data protection legislation applicable to the e-government context demonstrates great commonality in general data protection principles, despite the fact that the implementation of these principles are quite distinct across countries (more discussion on this variation will be provided later). The general principles found in the national laws are all largely based upon the FIPs principles introduced earlier (see Chapter 6). Specifically, the US and Germany have adopted nearly identical data protection principles for the public sector. For example, they both adopted the use limitation principle, data quality principle, transparency principle, data security principle, and data subject's participation principle. The experts' suggestion draft of China's data protection law also adopts most of these internationally accepted data protection principles, although its lack of data transparency (notification) principle indicates that the legitimacy of data collection is not a primary concern of China's legislation (or at least of this draft version).

Third, despite the diversity of specific privacy protection requirements and protection levels, all the three countries have considered data security as a priority in online administrative procedures. This is not only reflected in the data security principle underscored in national data protection laws (or law draft) and various national regulatory measures, such as the electronic signature laws and various internet security laws/regulations, but is also emphasized in general policy frameworks and through the development of specific authentication and encryption measures in the three countries. For the particular context of e-government, relevant legal and policy instruments demonstrate that, compared to information privacy, the protection of information security have attracted more government attention and action in all three countries.

Moreover, both the US and German laws and policies on information security protection explicitly point out that protection measures and efforts should be reasonable in relation to the desired level of protection, which is also echoed in some Chinese policy documents. This indicates that governments recognize that information security protection (as well as privacy protection although it is not as equally explicitly emphasized) incurs costs, such as direct financial cost, effects on work efficiency and convenience. The governments want to balance these costs with the competing interests gained from the protection of information privacy and security such as the increase of public trust in e-government services. Consequently the governments all express the view that a 'risk-based' and 'cost-effective' approach should be adopted with respect to the protection of personal data.

Divergent and Unbalanced Data Protection across Countries

Despite the above commonalities, the comparative overview finds a large degree of heterogeneity in national approaches to the protection of personal data in the context of e-government. Overall, although the general data protection principles are largely identical, the way how these principles are carried out to implement the protection differs considerably from one country to another (refer back to Table 3 for the comparison). This finding supports my conceptual model of governance: different national context results in different governance approach. More detailed discussion on the different governance approaches and relevant effectiveness will be provided later in this chapter.

A first difference in the implementation of these principles is the form of data protection law (omnibus law versus sector-specific law), which is greatly associated with the traditional legal systems of the countries as discussed in Chapter 4, and the specific content of these laws such as the definitions in the laws, the scope of law protection, and

the data protection supervising mechanism. For instance, while the US only protects its citizens' and permanent residents' privacy right, Germany protects individuals' personal data irrespective of the nationality (an EU obligation). Cross-border data transfer conducted by the public sector is only explicitly regulated in Germany but not in the US and China. The structure and function of the data protection supervising authority also differs across countries. In brief, there is considerable divergence in the form and specific content of privacy laws among countries.

Second, the study of existing laws reveals that, due to the fundamental different views toward privacy and the necessary legal protections to be provided to citizens, the level (or strength) of protection is quite unequal in the three countries. Overall, of the three countries and with respect to the particular context of e-government, Germany provides the highest level of data protection, the US offers modest protection, and China protects personal data only minimally by law. Treating an individual's privacy as a fundamental human right, Germany regulates the public sector's handling of individual's personal data quite heavily and enforces the data protection law rigidly. Moreover, electronic communication (named 'telemedia' in Germany) and telecommunications laws also stipulate strict rules to protect relevant kinds of personal data involved in e-government process. The US has an overall modest protection of an individual's personal data processed by the public sector, which is partly exemplified by the limitation imposed by the 'system of records' requirement. There are also electronic communications law and other sectoral laws in the US protecting the privacy and confidentiality of relevant electronic personal data. Compared to German laws, however, they carry more exceptions and the provisions are generally more lenient regarding restrictions on the

public sector's information practices. Moreover, the US *Privacy Act* is in great need of amendment to keep pace with technology changes and the current public sector's information handling practices. China is still waiting for its first data protection law to be issued. There are no electronic communications and telecommunications laws (only an administrative regulation on telecommunication). Thus China has the weakest legal protection of personal data in general as well as for the particular e-government context.

In addition to legal and regulatory measures, the subject is also dealt diversely across countries in the policy arena. For instance, in Germany, national projects have been conducted on national e-ID cards and various other initiatives on secure electronic communication infrastructure such as the Citizens' Portals. In the US, the implementation of data protection efforts in the public sector are mainly reflected in various OMB policy guidelines and NIST technological security standards. In China, there is only very initial and brief general agenda of data security protection for e-government development. Personal data privacy is so far not a priority in the promotion of e-government in China.

Room for Improvement in the Existing Regulatory Frameworks

The widespread adoption and development of e-government in the past years raises the question of whether the existing national (as well as global) regulations have kept pace with the changes/advances in information technology and information handling practices. Although some governments have come to realize that the existing legal and policy framework for privacy protection may need to be updated in the current situation, there is an overall lack of response to this issue.

Take the US for example: as early as in 2002, the Computer System Security and Privacy Advisory Board issued a report calling for "immediate and serious attention to

Federal government's data privacy policies and operational controls" (p. 2) due to the privacy management challenges arising from expanded e-government services. Similar recommendations on updating relevant laws have been proposed multiple times by the same agency and various other government agencies as well as think tanks in the last few years. The US data protection law for the public sector – the *Privacy Act of 1974*, however, has not been amended in the past two decades. Although the 1988 amendment of *Computer Matching Act* provides some protection for computerized data, those protection requirements are quite general and brief. The *Privacy Act* fails to address many new data protection issues arising from new information practices in the e-government era. Apart from the outdated individual-identifier-retrieving system-of-records requirement, such new information practices include, for instance, increasing data-mining practices and other increasingly sophisticated means of data collection, data processing, and data use. Although there is a comprehensive *E-government Act*, its data protection provisions do not impose limitations on agency collection and use of personal data in the e-government context (GAO, 2008b). Overall US laws are regarded inadequate to protect individuals' privacy in the e-government context and revisions to existing laws are deemed necessary.

In Germany, although the *German Federal Data Protection Act* has been amended quite a few times since the 1990s, most of these amendments do not concern the particular e-government area. There are very limited provisions in the act that are specifically targeted at electronic data. The existing e-government-centric provisions mainly focus on security measures, which include, for example, the latest 2009 amended data security requirements on data breach notification and encryption. Although the

general principles outlined for the public sector in the act are applicable to the e-government context, there is a lack of responses to the unique challenges and problems arising from the e-government environment. More specific law provisions on e-government or a specific law, such as e-government law, regulating government agencies as well as relevant parties regarding relevant new information practices could be considered to achieve more effective data protection in this area.

China does neither have an e-government law nor a personal data protection law. Although the first data protection law is being drafted and under review, existing legal, regulatory, and policy efforts that protect personal data in the e-government context in China are extremely limited. Further, the existing regulatory measures and national guidance on this issue mainly focus on data security; data privacy is barely mentioned.

Concluding Remarks

In short, the study found that government regulation, taking multiple forms ranging from legislative laws, administrative regulations and actions, to strategic guidelines, plays a key role in protecting individuals' information privacy in the context of e-government at the national level. National governmental regulatory arrangements have direct impact on how the public sector (as well as private parties) handles personal data in e-government processes[20]. Despite the existence of commonalities, the differences in national government regulation lead to divergent and unbalanced data protection across countries for the particular e-government area. This gap, however, is somewhat narrower than the national gap traditionally existing with the privacy protection regimes

[20] See the example introduced in Chapter 4: the US federal agencies widely use personal information in a 'non-identifier-retrieving' way, so that they can get around the privacy law requirement which protects personal data retrieved by using personal identifier.

for the private sector. In terms of the adequacy of government regulation on this issue, the current protection of personal data involved in e-government is largely embedded in the traditional legislative and regulatory framework. Although special efforts have been made to address the issue at the national level, such as codifying e-government law, conducting special data protection projects and issuing relevant guidelines, we might conclude that the overall legal and regulatory protection of personal data in the particular e-government area is not sufficient and there is room for further improvement.

International Regulation

In addition to emerging as an important regulatory issue in more and more countries, the issue under discussion also creates a new policy area for international regulation. There are a few important international bodies with their own privacy protection arrangements, which include the CoE and the EU, the OECD, and the APEC. These organizations and their arrangements are regional rather than global in scope. Two kinds of regulatory measures exist in these regimes: legally-binding agreements such as treaties and non-binding international guidelines. Most non-EU data protection instruments are non-binding guidance. Germany is legally bound by the EU and the CoE data protection directive/convention and is part of the soft-law data protection regime of the OECD[21]. The US is under the regime of the OECD and APEC, which have both issued non-binding data protection guidelines. China is under the regime of the APEC.

Among the major privacy or data protection instruments issued by these regional organizations, the OECD *Guidelines for Privacy* (1980) and the CoE *Convention for the*

[21] The so-named 'soft-law' here is only based on the nature of the major data protection instruments issued by OECD. Other than the non-binding data protection guidelines analyzed in this study, legally-binding instruments might exist elsewhere in OECD.

Protection of Personal Data (1981) have especially profound effects on worldwide privacy regulations by first establishing the general principles of fair information practices, which was introduced earlier. These principles form the basis of many later international privacy agreements (as well as national regulations), including the EU *Data Protection Directive* (1995) and the APEC *Privacy Framework*, although the latter is weaker in some principles and implementation requirements. The same FIPs principles are also found the basis of the non-binding UN *Guidelines Concerning Computerized Personal data* (1990). In short, first established by regional agreements and later adopted globally, the FIPs represent international consensus on fundamental principles regarding the processing of personal data and establish some general guidance for worldwide data protection at various levels and in various fields, including in the field of e-government.

Despite great similarity in the core principles of the international data protection instruments, these international agreements/guidelines primarily aim at providing general guidance instead of specific directions on data protection. Further, most of the non-EU instruments are non-binding guidelines and recommendations, which individual countries have no obligation to follow. For example, although both the US and China are under the regime of the APEC, other than the basic notion of FIPs, these two countries have adopted or plan to adopt data protection laws that bear little direct relevance to the *APEC Privacy Framework*. Rather, in the case of China, according to the experts interviewed, the European model or a mixed model might very likely be adopted. In short, the existing international regulations can only serve as basis or a basic common standard for data protection. The specific implementation of such guidelines in individual countries might

vary substantially, which meanwhile indicates the difficulty in having a highly harmonizing global instrument on this issue.

The international landscape of personal data protection indicates an overall lack of regulatory response to this issue with respect to the particular context e-government. Although all the major existing international data protection instruments are applicable to the e-government area, these instruments are quite 'old' considering most of them date about 20-30 years back. Although the APEC *Privacy Framework* was established more recently in 2004, it largely follows the 30-year-old OECD guidelines and is the weakest international privacy framework of all. In this case, the question emerges of whether new international data protection rules are needed to address new challenges such as the e-government privacy problem.

With the above being said, one slightly different regional privacy regime is the EU, whose directives need to be transposed into member states' national legislation and where there is a coherent system to implement data protection at the EU community level. Although so far the data protection directive has not been updated, the EU Data Protection Working Party has paid some particular attention to the application of the EU Data Protection Directive in the context of e-government in the member countries and the EU community. There are also some updated regulations on relevant fields such as on the privacy protection in electronic communications.

In addition to these specific privacy or data protection instruments, there is also a set of internet security agreements/guidelines at the international level, which are to some degree relevant to personal data protection in e-government. One of the goals is to promote a global 'culture of cyber-security' and call for international cooperation to

ensure cyber security and online information security. Compared to information privacy, the international organizations seem to have responded to the issue of information security more proactively, which is similar to what national governments have done as discussed earlier. While cyber security and electronic data security have been placed on the priority list in all the three countries and all major international organizations in recent years, the position of electronic information privacy is obviously lower or not actively pursued on the agenda of many countries and international organizations.

Alternative Regulation

According to Latzer et al. (2006), alternative regulation is mainly employed when industry interests are more homogeneous. In the specific case of data protection in e-government, data security seems to be an area where interests are more homogeneous than data privacy. Consequently, self-regulatory and co-regulatory efforts and actions are found more active in protecting information security.

Based upon the analysis of the existing national and international regulatory instruments, four major modes of alternative regulation are identified as in practice protecting personal data in e-government domain: self-regulation in the public sector, self-regulation in the private sector, self-regulation of individual users, and co-regulation by multiple stakeholders at both the national and international level.

Self-regulation in the Public Sector

In many countries, such as Germany and the US, there is specific data protection law or privacy law in place regulating information practices of the public sector. Meanwhile, however, there is no data protection law in some other counties, which is the

case with China, where government's handling of personal information is under very limited or no legislative control. Yet even in such countries, the public sector's data collection, data processing, data use, and data distribution is not likely to be completely unrestricted. Government today has the political and social responsibility to maintain social order by guaranteeing a basic level of citizen's privacy right. Absent legislative rules on information handling, government agencies need voluntarily establish rules of conduct and relevant control and monitoring mechanism to protect citizens' personal data and privacy. Take China for example: the public sector's use and processing of individuals' personal data, such as in the e-government context, is largely restricted by agencies' self-established codes of conduct. Before the data protection law is officially passed, this form of self-regulatory approach will continue to be the most common means to guarantee the public's basic privacy right.

Self-regulation in the Private Sector

In addition to government agencies as data collector and controller, the process of e-government also involves private parties for various reasons. First, the use of online portal websites for e-government purpose makes the provider of telecommunications and general electronic communication have access to users' personal data processed and exchanged on the portals and also possibly retain such data. Second, in some cases, the public sector might outsource the e-government portal construction and maintenance to private companies. Online administrative procedures might also be provided by private companies. Further, private industry has been working with the public sector on many data-security projects or technological products that might be used in e-government or

particularly for e-government purposes. In all these cases, how can the private companies ensure equality of treatment of users' personal data involved in relevant procedures?

Although Germany has an omnibus data protection law for both the private and public sector, not all countries provide equal protection across different sectors. In the US, because of the lack of privacy law regulating private companies' information practice, the business sector mainly adopts a self-regulatory approach to protect consumers' privacy. Although some sector-specific laws such as telecommunications law or electronic communications law might play a role in regulating relevant companies' information practice, it cannot cover all the areas discussed above. In the case of China, there is no data protection law at all. Thus, in countries where the private sector is not regulated or not regulated adequately, the private sector's handling of personal data involved in e-government process have to rely on self-regulatory approach. Such self-regulation can be based on, for instance, business contracts, necessary certification schemes, voluntarily codes of conduct, and additional self-control procedures.

Self-regulation of Individual Users

Individual users of online administrative procedure are key stakeholders in e-government. While it is crucial to regulate the public sector as well as relevant private parties' data handling practices, individual users themselves also have very important responsibility to protect their own information privacy and security. To a certain extent, this kind of self-help schemes could also be considered as a form of self-regulation.

First, the protection of individuals' personal data that are involved in on-line administrative procedures should start with information measures by citizens on the rights that are granted to them according to data protection legislations. Individuals'

acceptance of the responsibility to know and insist on their own legal rights might be an effective step toward discovering and correcting inaccurate or misuse of personal information (Cate, 1997). There are also various other self-help schemes. For example, when using e-government services, individual users should have data protection awareness and basic knowledge about possible privacy and security threats on the internet, which in some instances might need special awareness education and training. Individuals might also use certain technological forms of self-help to protect their own data when engaging in online e-government activities. This kind of self-protection might be an effective restraint to third parties' infringement of a person's privacy right. Apart from individual actions, there are also collective actions organized by the civil society, such as those privacy advocacy groups. Such user interest groups seek collectively to create certain norms on personal data protection and exert pressure on relevant parties such as the public sector for action, which might also be grouped as a form of co-regulation.

Co-regulation by Multiple Stakeholders

Co-regulation is gaining widespread acceptance in the field of internet governance as a middle ground between pure government regulation and pure self-regulation. While this form of regulation is not examined in detail at the national level in this study, the co-regulation governance mode is well represented at the international level, where there are various forms of international co-regulatory organizations and arrangements dealing with internet policy issues including the issue of privacy and personal data protection. A core component of these co-regulation arrangements is direct involvement of a wider spectrum

of stakeholders, which include representatives from national governments, international organizations, the private sector, academic, technical field, and civil society.

With regard to co-regulation mechanisms on privacy and data protection, as introduced in Chapter 6, there are a number of important multi-stakeholder internet governance forums, such as the IGF, and various cooperative arrangements on the specific topic of data protection, such as the International Conference of Data Protection and Privacy Commissioners. Norms and rules of conduct on data protection are negotiated and balanced among participants through open discussion in these forums. Yet although these co-regulation instruments play quite an active role in addressing the general online data protection issue, the protection of personal data in e-government context has barely been officially discussed in these forums. Thus the co-regulation instrument is so far not found an important approach to the protection of personal data in the particular context of e-government, except on the general topic of cross-national data flows and data security.

Code-based regulation

According to code regulation theory, technological tools and mechanisms can act as a unique policy instrument to help establish network-based rules in the information society. With respect to privacy and data security in e-government, various privacy-enhancing technologies have been developed and increasingly used in practice. And more such 'policy technologies' (Reidenberg, 1998) are under development.

Privacy-enhancing technologies is defined as "a system of ICT measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the

functionality of the information system" (van Blarkom, Borking, & Olk, 2003, p. 33). Public key cryptography is a classic and fundamental example of such technology. It includes two primary branches of technological applications: public key encryption for confidentiality purpose and digital signature for authentication purpose (van Blarkom et al., 2003). As shown in the publications of guideline and standards by NIST in the US (see Appendix B), a large variety of encryption, authentication, digital signature, key agreement, and relevant techniques have been developed in the field of public-key cryptography to secure information content against unauthorized access. Germany's policy guidance also grants substantial attention to the issue of authentication and encryption in the specific e-government area. Although lacking more detailed technology development reports and relevant guidance, China's *E-government Framework* also emphasizes the need to establish effective authentication and certification systems as an important component of building an e-government trust system. Similarly, ISO has developed various cryptographic standards and techniques, such as on digital signature and message/entity authentication, as references for countries around the globe.

In addition to public key cryptography, there are other forms of cryptographic technologies and privacy enhancing technologies. For instance, technologies of anonymity can help protect information privacy during message transmission, electronic transactions, and Internet web surfing (Reidenberg, 1998). Based upon these technologies, various technical measures or schemes have been adopted or are being developed worldwide to protect (or with the potential to protect) personal information involved in e-government process. Examples include the secure virtual private network (VPN) technology developed by NIST in the US, the Virtual Post Office concept and the

Citizen's Portals Project in Germany, and the various information privacy protection standards developed by the ISO at the international level.

Discussion and Implications

The governance of data protection in e-government involves multiple parties, namely (1) government entities as the major party handling personal data in the e-government process, (2) internet service providers that provide online communications and transactions services and other private parties cooperating with government entities in delivering e-government services or products, (3) individual users of e-government services as data subjects and non-governmental organizations and social forces that seek to defend individuals' privacy right, and (4) international organizations confronted with new regulatory needs on this issue. To achieve effective protection of personal data in the context of e-government, these multiple stakeholders need to be adequately managed and coordinated. However, how such management and coordination could be achieved is a complex question. Theoretically, a mix of different governance approaches might be needed to address this issue. The study of the existing governance instruments of this issue at both the national and international levels revealed the existence of a multi-mode governance mechanism, which is consistent with the theoretical expectation. Yet how these governance modes function and interplay and how effective these modes are in different national contexts deserves more discussion in this section.

National Context and the Roles of Governance Modes

As summarized and analyzed earlier in this chapter, the three countries differ considerably in the form and level of information privacy protection granted to

individuals with respect to the context of e-government. These differences are closely associated with differences in national context, specifically, the traditional legal systems (e.g., the civil law system justifies comprehensive data protection law), the social value or conception of privacy, the constitutional protection of privacy rights, and the privacy protection traditions in the three countries (see Chapter 4 for the comparison of national contexts). In terms of governance mechanism, the different governance modes identified earlier in this chapter are found to play different roles and have different importance in the overall governance scheme of this issue and also in different countries. The latter could also be seen as an outcome of different national context.

First, the role of government regulation differs across countries. Although e-government communications and transactions are internet-based activities, traditional government regulation is found to play a very important role in protecting personal data in e-government area in Germany and the US. The key role of traditional government regulation on this issue counters the 'governance without government' argument for internet governance. Information practices of government agencies and relevant private parties such as internet service providers are regulated through domestic legally-binding laws/rules and non-binding soft laws such as recommendations and strategic guidelines. The various rights of data subjects with respect to their personal data are also outlined in relevant laws. In this sense, government regulation could be regarded as one major mode governing the issue under discussion in the US and Germany. Where applicable laws are absent, however, as is the case in China, self-regulation becomes one major approach to protecting the privacy and security of relevant personal information. Government

regulation on information privacy protection is too limited to play a major role in real practice in China currently.

The above national difference in the role of government regulation can be seen as an outcome of differences in national context. As discussed earlier, Germany has historically placed a high value on privacy rights, which, together with its civil law system, justifies its strict and sweeping government privacy regulation imposed upon both the public and private sectors. In the US, privacy is also recognized as an important value and right to be protected, so government policies and regulations are in place regulating the public sector's information practice. Significant protections for privacy are also contained in tort law, case law, and in state statutes. Yet the social and legal perception of privacy interests in the US to certain degree differs from that in the German or European social conception and legal system (Long & Quek, 2002). This, combining with the US common law system, helps explain its less sweeping federal statutory regulation regarding government's handling of individual's electronic personal data than in Germany both in degree and scope (e.g. the *Privacy Act* only applies to the public sector).

In China, both the social-cultural conception and legal system have treated privacy as a very low-priority issue. Its historical backwardness in economical development also results in the imperfection of its legal system, which makes its government law regulation of and policy guidance on the privacy issue lag far behind the other two countries. The Chinese public sector and other relevant stakeholders thus have no choice but to primarily rely on self-regulation to protect personal data in the context of e-government at the current stage.

The study also found that code-based regulation is an important governance mode in all the three countries and at the international level. Technological means and tools are actively used and/or promoted to secure electronic communications with public agencies and protect information privacy. Virtually all existing national and international legislative and policy documents, plus various non-governmental recommendations, require technical measures in place to protect information privacy and security.

Based upon the available evidence, however, national discrepancies also exist with the application and exploration of technological codes and tools as a means to protect personal information in e-government. Although technology itself is neutral, the adoption and application of technology in data protection might be influenced by the political regime in which it is embedded (political needs). It might also be impacted by economic resources available and the development of technology in a certain country. Specifically, for example, China has spent much less effort and resources in data protection technologies or technical projects compared to the other two countries, which might be partly because of the constraints of economic resources and its comparative lagging in technological development. Meanwhile, however, one more important factor that we should not ignore is the low general awareness of and political priority on this issue, which is more evident when we consider the fact that China has adopted sophisticated technological means for online surveillance and internet censorship, which is beyond the discussion scope of this study.

National Context and the Effectiveness of Governance Mechanisms

As my study revealed, national context shapes specific governance mechanisms adopted and impacts the respective roles of the governance modes. So which or which

mix of governance instruments is the most effective in protecting personal data involved in e-government? The data indicate that government regulation is widely seen as an effective mode to protect personal data in e-government, which is evidenced by the regulation measures or undergoing legislative measures (such as in China) adopted by governments at both the national and international levels. Although more data is needed to obtain a complete picture, some preliminary facts as follows might also be able to provide some first glimpse, or partial evidence, of the effectiveness of the different governance mechanisms currently adopted by the countries, especially the effectiveness of government regulation.

In the US, during November 2004 and January 2007, US federal government agencies alone reported 26 significant data breach incidents with the loss of personally identifiable information (GAO, 2008a). The privacy laws in the US are perceived by many experts as outdated and inadequate, which consequently give rise to many privacy concerns. For example, as introduced in Chapter 4, 11 percent of 730 major information systems in use by the US federal agencies in 2002 contained personal information that was not subject to the *Privacy Act*'s protections (GAO, 2003). The major reported reason was that the agency did not use a personal identifier to retrieve the personal information but rather by other non-identifying information. The individual-identifier-retrieving requirement in the *Privacy Act* greatly reduces the adequacy of data protection and thus puts individual's information privacy at risk. These two reports to some degree indicate a lack of effectiveness of the governance mechanism currently adopted by the US.

There are no similar reports of data breaches and privacy invasion in government's databases available for Germany. It might be possible that the situation in

Germany is better than the US and the governance modes such as government laws and rules are more effective. In the case of China, according to a presentation made in Europe by a Chinese data protection study tour delegation[22] (March 2009), a survey on public awareness of personal information protection in China showed that 99 percent of the respondents believed personal information handling institutions (not specified in the report whether it includes both the public and private sectors, but assume so) do not have sound data protection mechanism, and 98 percent of the respondents were worried about the inability of information handling institutions to protect their personal information. These figures partly indicate the lack of privacy and data protection in China, including in the e-government area. It might be concluded that due to the lack of government regulation, mere reliance on self-regulation is far from enough to protect personal data in e-government and build public trust in e-government services.

In short, the conceptual discussion and preliminary evidence presented above show that government regulation might be one of the most effective means to protect personal data in e-government. Available evidence seems to indicate that Germany have so far provided the most effective protection of data privacy and security in the context of e-government, which might be because of its comprehensive and stringent legal protection. Yet the effectiveness of this particular governance mode might still vary across countries, like that in Germany and the US. The effectiveness is largely decided by the specific content of the laws, which is influenced by national context as examined and discussed earlier.

---

[22] The material was provided by a regulatory expert on the EU-China Information Society Project who participated in the telephone interview.

One point to note, however, is that my observation and conclusion on the governance modes in this study is primarily based upon my findings within the legal and policy framework at the national and supra-national levels. More systematic and complete data (beyond the legal and policy framework and below the national level) on alternative regulation (self-regulation and co-regulation) and code-based regulation, especially the former, could be collected and examined to get a full picture of the functioning of these modes and their specific roles. Future research could be conducted to complement the findings in this study from the above aspects. Further, the short history of e-government and the associated data protection issue makes a well-informed evaluation of the effectiveness of the governance modes premature at this moment. A more thorough empirical analysis of the effectiveness of different governance modes will only be possible when more data is available and more evidence and experience accumulate. In terms of the effectiveness of the governance modes, however, the basic point is that: the existence of certain governance modes alone cannot guarantee the same effect across different contexts (including national context). An adequate protection of personal data in the context of e-government should not only consider using appropriate governance modes but also grant enough attention to the substance or content of each specific governance mode.

International Solutions: Challenges, Feasibility, and Prospects

Despite the critical role of government regulation for information privacy protection, geographical and other inherent limits restrict its application in the online world. For various reasons discussed earlier, the problems of developing safeguards for individuals' personal data in respect of the e-government context might not be solved

exclusively at the national level. Theoretically, an international-level response to this issue can help resolve problems of law conflicts that result from the borderless nature of the internet and the increasing international data flows in the context of e-government. In reality, however, relevant international solutions are found mainly imbedded in the existing guidelines and conventions that protect personal data or computerized data in general. Regulatory attention to the particular context of e-government at the international level is extremely limited. The limited existing regulatory attention (including co-regulation) relevant to the context of e-government is mostly on information security rather than information privacy.

There are a few possible reasons for the limited international response to the issue under discussion. First, there is the phenomenon of 'regulatory-lag' because of the relative short history of e-government and the novelty of the information privacy issue in this context. Second, the strong local component embedded in this issue make it difficult for national governments (or other stakeholders) to agree on common standards across borders on data protection, especially data privacy protection, in e-government. Other than the widely acknowledged culturally- and socially-conditioned nature of privacy, the e-government context itself might indicate more national interest (including political interest since it mainly involves the public sector) than privacy in other contexts such as in the private sector. Comparatively speaking, the protection of data security is more of common interest to all countries and it is thus easier to establish cooperative mechanisms. Third, the international community in general sees no need to adopt new regulatory instruments to address the problem under discussion.

In terms of the third point, there are opposing viewpoints regarding the 'old' international rule phenomenon. Some scholars and legal experts believe that new international rules on data protection are needed to address the various new problems and challenges created by new information technologies and new information practices. The opposite viewpoint is that no new data protection rules are necessary since the primary goal of an international rule is to provide fundamental principles on data handling and the core principles provided by the existing international regulations are still valid today. It is hard to judge at this moment which of the opposing views is correct. The distinct national regulatory mechanisms across countries make a worldwide harmonization of legal standards on this issue very difficult. Yet how feasible a worldwide harmonization is largely depends on the degree of harmonization that is required. The "contextuality of information privacy" (Cate, 1997) and different national approaches to this issue does not mean that it is impossible to identify fundamental principles of privacy protection. Instead, the discrepancy in national approaches makes international consensus on basic principles for information privacy protection even more important in order to effectively protect personal data handled in the e-government process and to enable smooth data flows between governments across borders. Common standards do not require identical laws but rather legal regimes that are based on shared basic principles yet still reflect individual national context (Cate, 1997). Although a global privacy framework has not been established so far, there is in reality a certain degree of international consensus on basic privacy protection principles that are applicable to the e-government domain, which are the FIPs principles. In this sense, the existing international data protection agreements might suffice for the context of e-government. Yet it is also possible that new data

protection principles or other new worldwide standards will be needed to address new problems arising in this particular area as time goes on.

Some have argued that ideally a global-level regulatory framework would be helpful to solve internet policy issues. In reality, it might be easier to establish regulation on a smaller scale at the supra-national regional level, such as in Europe and in Asia as is found in this study. Because of similar political system, shared culture and value heritage, or geographic adjacency, a group of countries might adopt similar privacy protection mechanisms more easily.

Practical Implications

Some scholars, mainly the original promoters of the internet, perceive the internet as a radically different space from the physical world and thus regard it impossible to apply the existing legal framework to the online world (e.g. Johnson & Post, 1996). The online-offline differences, however, might not be substantial enough to justify totally new regulatory approaches or a new legal framework for many internet policy issues, including the issue of online privacy protection. The problems occurring might mostly be overcome by working on the existing legal framework.

With regard to the personal data protection issue in the context of e-government, government data protection legislation needs to adapt to technology changes and consequent new information practices. In the case of the US, although it was one of the first movers in addressing the privacy protection issue by first proposing the FIPs principles in the 1970s, its legislative system has not fully adapted to the major technology advances of the past decades. This might be an example of legal path dependency: the early move by the US resulted in a somewhat outdated legal framework

in the new technological environment. Nations that adopted privacy protection measures later could already take newer technologies into account. Yet to adequately protect individuals' information privacy rights and ensure further development of e-government because of the increasing public trust gained from this protection (a win-win situation), first-mover governments also need to update existing data protection legislation and in the long run might consider adopting further legislation to delineate data subject's rights and various data-handling parties' responsibilities and liabilities on the many specific issues occurring in the particular context of e-government. Countries with e-government initiatives yet lacking data protection laws need to establish data protection legislative frameworks to enhance the development of e-government. Citizens will not use internet-enabled government services that do not handle their personal data responsibly.

At the international level, international regulation and cooperation (including co-regulation) should be further encouraged and strengthened to achieve an effective protection of personal data in e-government and to avoid unnecessary restrictions on the trans-border data flow. Yet the primary involvement of government activities makes the e-government domain an area subject to more influence of national context, especially political context, and thus international regulation might play a smaller role for the protection of personal data in the e-government area than in many other privacy areas such as commercial areas and other general areas of social activity on the internet.

In terms of alternative regulation, although it has various weaknesses such as the lack of enforcement procedures, it has its own unique advantages. For example, alternative regulation is more strongly motivated by private incentives and is thus more a "need-driven rule-setting process" (Weber, 2002, p. 80). It might also be more efficient

than government regulation in some cases because it responds to changing technologies in a more flexible and faster way. Therefore, it should not be underestimated as a regulatory model for the protection of privacy in the specific field of e-government. Government self-regulation, individual and collective non-governmental actions, and public-private co-actions (in the case of co-regulation) are critical to protecting information privacy in e-government area and thus should be encouraged at both the domestic and international levels.

Compared to other forms of norms and standards, technological norms are an area where international cooperation and public-private coalition are especially stressed and where international agreement is comparatively easier to be reached. So code-based resolutions have been actively pursued and could be further promoted and developed to help address the data protection issue in e-government. In this process, however, we should not ignore the fact that although code-based technological rules can avoid many significant difficulties inherent in legal solutions, such as conflict and uncertainty (Reidenberg, 1998), government laws and policies play a key role in technological rules. It is the government that decides and controls the code structure (Lessig, 1999). It is also through laws and policies that technical rules could be more effectively implemented. Take data protection in e-government for example, government could make explicit decisions to build privacy and security into e-government applications, such as the public-key infrastructures. So while it is important to acknowledge the key role of technical solutions in safeguarding electronic personal data, technology alone without policies cannot succeed as a governance mode for this issue.

Conclusions

Originating from the 1990s, e-government has a quite short history and is still in an experimentation phase in many countries. Considering the fact that e-government is a new form of public administration occurring on a new communication platform, there are many new issues to deal with. The information privacy issue is one of them. An adequate protection of personal data is essential to guarantee individuals' right to information privacy and meanwhile crucial to the success of e-government in that it can build public trust in online government. By analyzing and discussing the current status and the governing mechanism of the information privacy protection issue with respect to the context of e-government in the three sampled countries and relevant international arenas, this study means to contribute to the reflection on this topic worldwide. Considering the continuous evolution of electronic administration services and of conclusions reached from the practice in this area, this study also aims to provide practical guidance on the governance of this issue.

With the adoption of computer technology in the public administration and the development of e-government, concerns for information privacy and security, namely personal data protection, has become a serious issue. My study found that this specific issue has been addressed in the studied national contexts, but these national responses in general are found not adequate enough to solve the problem, which is especially true with the US and China. Meanwhile, this particular issue has not attracted enough attention and has not been adequately addressed at the international level either. Overall, the study found that the national and international governance frameworks do not keep pace with technology changes and the current information practice of the public sector as well as

relevant private parties. Protecting individuals' information privacy is becoming a value shared by an increasing number of cultures. However, information privacy protection in the particular e-government context lags behind that in many other privacy fields. To solve the problems, new laws or revisions of the existing data protection laws and enforceable global standards for information privacy rights over the internet are desired.

Internet governance is a complex task requiring a complex set of governance mechanisms (Mathiason, 2009). Each problem of internet governance should be understood contextually and might require a unique set of governance approaches. For example, internet architectural issues such as domain names might be better resolved through international institutions, co-regulation, and code-based regulation. The personal data protection issue, however, requires a mix of governance modes of national government regulation, international agreements, alternative regulation, and code-based regulation, which differ in respective roles. In brief, the problem needs to be effectively addressed by a multi-level, multi-stakeholder, and multi-form governance mechanism. The available data indicates national government regulation might be one of the most effective means to achieve meaningful protection of personal data in the context of e-government, which yet has to be accompanied by other governance modes as mentioned above to be a complete success.

Based on the existing evidence, however, what is the most effective governance mechanism for this issue is still a question. For example, it is too early to decide whether the current overall inadequacy of data protection in e-government area is due to the inadequacy of international response, the insufficiency of national effort to improve and invent government regulation, or both. The whole picture of this issue and the working

system of the governance modes are still quite vague. More time, experience and research are needed to draw conclusion on the 'best' governance mechanism for this issue.

In sum, the protection of personal data in the context of e-government, as one policy area of internet governance, involves a wide range of regulatory instruments and governance strategies. How national and international regimes, technical management and regulatory control, government regulation and alternative regulation interact is and remains to be a key task to be tackled in order to effectively and adequately respond to this increasingly pressing and inherently transnational policy problem.

Appendix A: Experts List for Interview

United States:

- IT Policy Analyst, E-Gov and Information Technology, Office of Management and Budget (OMB)
- Electronic Privacy Information Center (EPIC)

Germany:

- Head of Division "Passports and Identity Documents, Identification Systems Federal Civil Registry", Federal Ministry of Interior of Germany (BMI)
- Office of the Federal Commissioner for Data Protection and Freedom of Information
- Regulatory expert, EU-China Information Society Project (German, located in Beijing)

China:

- Law professor, Chongqing University, EU-China Information Society Project
- Professor, Fudan University (e-mail interview)
- Regulatory expert, EU-China Information Society Project (German, located in Beijing)

Appendix B: OMB Policies/Memorandums and NIST Standards and Guidelines that are directly Applicable to Federal Personal Information Protection in E-government in the US

OMB Policy/Memorandums		
Policy/Memo	**Date**	**Title**
Appendix III of Circular A-130	Feb 1996	Security of Federal Automated Information Resources.
M-99-05	Jan 1999	Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records
M-99-18	Jun 1999	Privacy Policies on Federal Web Sites
M-99-20	Jun 1999	Security of Federal Automated Information Resources
M-00-07	Feb 2000	Incorporating and Funding Security in Information Systems Investments
M-00-13	Jun 2000	Privacy Policies and Data Collection on Federal Web Sites
M-01-05	Dec 2000	Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy
M-03-19	Aug 2003	Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting
M-03-22	Sep 2003	OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
M-04-04	Dec 2003	E-Authentication Guidance
M-04-25	Aug 2004	FY 2004 Reporting Instructions for the Federal Information Security Management Act
M-05-08	Feb 2005	Designation of Senior Agency Officials for Privacy
M-05-15	Jun 2005	FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
M-06-15	May 2006	Safeguarding Personally Identifiable Information
M-06-16	Jun 2006	Protection of Sensitive Agency Information
M-06-19	Jul 2006	Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments

M-06-20	Jul 2006	FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
	Sep2006	Recommendations for Identity Theft Related Data Breach Notification
M-07-16	May 2007	Safeguarding Against and Responding to the Breach of Personally Identifiable Information
M-07-19	Jul 2007	FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
M-08-09	Jan 2008	New FISMA Privacy Reporting Requirements for FY 2008
M-08-21	Aug 2008	FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
NIST Standards (FIPS) and Guidelines (SP) (the latter only list those issued in or after 2002, the year FISMA was adopted)		
Number	**Date**	**Title**
FIPS 185	Feb 1994	Escrowed Encryption Standard
FIPS 190	Sep 1994	Guideline for the Use of Advanced Authentication Technology Alternatives
FIPS 188	Sep 1994	Standard Security Label for Information Transfer
FIPS 140--1 FIPS 140--2	Jan 1994 May 2001	Security Requirements for Cryptographic Modules
FIPS 196	Feb 1997	Entity Authentication Using Public Key Cryptography
FIPS 197	Nov 2001	Advanced Encryption Standard
FIPS 199	Feb 2004	Standards for Security Categorization of Federal Information and Information Systems
FIPS 200	Mar 2006	Minimum Security Requirements for Federal Information and Information Systems
FIPS 198--1	Jul 2008	The Keyed-Hash Message Authentication Code (HMAC)
FIPS 180--3	Oct 2008	Secure Hash Standard (SHS)
FIPS 186--3	Jun 2009	Digital Signature Standard (DSS)
SP 800-30	Jul 2002	Risk Management Guide for Information Technology Systems

SP 800-47	Aug 2002	Security Guide for Interconnecting Information Technology Systems
SP 800-49	Nov 2002	Federal S/MIME V3 Client Profile
SP 800-50	Oct 2003	Building an Information Technology Security Awareness and Training Program
SP 800-36	Oct 2003	Guide to Selecting Information Technology Security Products
SP 800-35	Oct 2003	Guide to Information Technology Security Services
SP 800-37	May 2004	Guide for the Security Certification and Accreditation of Federal Information Systems
SP 800-27 Rev. A	Jun 2004	Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
SP 800-52	Jun 2005	Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations
SP 800-83	Nov 2005	Guide to Malware Incident Prevention and Handling
SP 800-40 Version 2.0	Nov 2005	Creating a Patch and Vulnerability Management Program
SP 800-77	Dec 2005	Guide to IPsec VPNs
SP 800-21 2nd edition	Dec 2005	Guideline for Implementing Cryptography in the Federal Government
SP 800-18 Rev.1	Feb 2006	Guide for Developing Security Plans for Federal Information Systems
SP 800-63 Version 1.0.2	Apr 2006	Electronic Authentication Guideline
SP 800-86	Aug 2006	Guide to Integrating Forensic Techniques into Incident Response
SP 800-92	Sep 2006	Guide to Computer Security Log Management
SP 800-100	Oct 2006	Information Security Handbook: A Guide for Managers
SP 800-89	Nov 2006	Recommendation for Obtaining Assurances for Digital Signature Applications
SP 800-94	Feb 2007	Guide to Intrusion Detection and Prevention Systems (IDPS)
SP 800-45 Version 2	Feb 2007	Guidelines on Electronic Mail Security
SP 800-90	Mar 2007	Recommendation for Random Number Generation

		Using Deterministic Random Bit Generators
SP 800-57	Mar 2007	Recommendation for Key Management
SP 800-56 A	Mar 2007	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
SP 800-54	Jul 2007	Border Gateway Protocol Security
SP 800-95	Aug 2007	Guide to Secure Web Services
SP 800-44 Version 2	Sep 2007	Guidelines on Securing Public Web Servers
SP 800-111	Nov 2007	Guide to Storage Encryption Technologies for End User Devices
SP 800-114	Nov 2007	User's Guide to Securing External Devices for Telework and Remote Access
SP 800-53 Rev. 2	Dec 2007	Recommended Security Controls for Federal Information Systems
SP 800-61 Rev. 1	Mar 2008	Computer Security Incident Handling Guide
SP 800-67 1.1	May 2008	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
SP 800-53A	Jul 2008	Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans
SP 800-113	Jul 2008	Guide to SSL VPNs
SP 800-55 Rev. 1	Jul 2008	Performance Measurement Guide for Information Security
SP 800-123	Jul 2008	Guide to General Server Security
SP 800-60 Rev. 1	Aug 2008	Guide for Mapping Types of Information and Information Systems to Security Categories
SP 800-22 Rev. 1	Aug 2008	A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
SP 800-115	Sep 2008	Technical Guide to Information Security Testing and Assessment
SP 800-64 Rev. 2	Oct 2008	Security Considerations in the System Development Life Cycle
SP 800-107	Feb. 2009	Recommendation for Applications Using Approved Hash Algorithms
SP 800-106	Feb. 2009	Randomized Hashing for Digital Signatures

SP 800-38 B-E	2005-2009	guidance and recommendations on Block Cipher Modes of Operation
SP 800-56 B	Aug. 2009	Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography
SP 800-53 Rev. 3	Aug 2009	Recommended Security Controls for Federal Information Systems and Organizations
SP 800-53 Rev. 3 (revision 2 in 2007)	Aug 2009	Recommended Security Controls for Federal Information Systems and Organizations
SP 800-41 Rev. 1	Sep 2009	Guidelines on Firewalls and Firewall Policy
SP 800-102	Sep 2009	Recommendation for Digital Signature Timeliness
SP 800-108	Oct 2009	Recommendation for Key Derivation Using Pseudorandom Functions

Source: http://www.whitehouse.gov/omb/; http://csrc.nist.gov/

References

Adams, H. R., Bocher, R. F., Gordon, C. A., & Barry-Kessler, E. (2005). *Privacy in the 21st century: issues for public, school, and academic libraries*. Westport: Libraries Unlimited.

As-saber, S., Hossain, K., & Srivastava, A. (2007). Technology, society and e-government: in search of an eclectic framework. *Electronic Government, An International Journal, 4*(2), 156-178.

Banisar, D., & Davies, S. (n.d.). *Privacy and human rights--An international survey of privacy laws and practice*, from http://www.gilc.org/privacy/survey/

Barkley, D. L. (2006). *The value of case study research on rural entrepreneurship: Useful method?* Paper presented at the ERS-RUPRI conference, Exploring Rural Entrepreneurship: Imperatives and Opportunities for Research, Washington, D.C.

Barlow, J. P. (1996). *A declaration of the independence of cyberspace*. Retrieved March 1, 2010, from http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration

Bauer, J. M. (2007). Internet governance: theory and first principles. In R. K. J. Bandamutha (Ed.), *Internet governance: an introduction* (pp. 40-59). Hyderabad, India: The Icfai University.

Baumer, D. L., Earp, J. B., & Poindexter, J. C. (2004). Internet privacy law: a comparison between the United States and the European Union. *Computers & Security, 23*(5), 400-412.

Becker, S. A. (2005). Potential trust barriers in US state e-government privacy policies. *Electronic Government, 2*(3), 334-352.

Bekkers, V., & Homburg, V. (2007). The Myths of E-Government: Looking Beyond the Assumptions of a New and Better Government. *The Information Society, 23*(5), 373-382.

Belanger, F., & Hiller, J. S. (2006). A framework for e-government: privacy implications. *Business Process Management Journal, 12*(1), 48-60.

Bellman, S., Johnson, E., Kobrin, S., & Lohse, G. (2004). International Differences in Information Privacy Concerns: A Global Survey of Consumers. *Information Society, 20*(5), 313-324.

Bennett, C. J. (1992). *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca: Cornell University Press.

Bennett, C. J. (2002). Information Policy and Information Privacy: International Arenas of Governance. *Journal of Law, Technology and Policy*(2), 385-406.

Bennett, C. J., & Bayley, R. (2007). *"Saying what you do and doing what you say": Arguments and prospects for an International Privacy Standard.* Paper presented at the 29th International Conference of Data Protection and Privacy Commissioners, Montreal, Canada.

Benz, v. A. (Ed.). (2004). *Governance - Regieren in komplexen Regelsystemen: Eine Einführung*. Wiesbaden: VS Verlag für Sozialwissenschaft.

Biegel, S. (2003). *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace*. Cambridge, MA: The MIT Press.

Braman, S. (2006). *Change of State---Information, Policy, and Power*. Cambridge, Massachusetts: The MIT Press.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology, 58*(2), 157-165.

Burgoon, J. K., Parrott, R., Poire, B. A. L., Kelley, D. L., Walther, J. B., & Perry, D. (1989). Maintaining and restoring privacy through communication in different types of relationship. *Journal of Social and Personal Relationships, 6*(2), 131-158.

Bygrave, L. A., & Bing, J. (Eds.). (2009). *Internet governance: infrastructure and institutions*. Oxford: Oxford University Press.

Carter, L., & Belanger, F. (2005). The utilization of e-government services: citizen trust, innovation and acceptance factors. *Information Systems Journal, 15*(1), 5-25.

Cate, F. H. (1997). *Privacy in the information age*. Washington, D. C.: Brookings Institution Press.

Chen, J. (1999). *Chinese Law:Towards an Understanding of Chinese Law, Its Nature, and Development*. The Hague, The Netherlands: Kluwer Law International.

Chhotray, V., & Stoker, G. (2009). *Governance theory and practice: a cross-disciplinary approach*. Basingstoke and New York: Palgrave Macmillan.

China Internet Network Information Center (CNNIC). (2006). *The Internet timeline of China*. Retrieved November 12, 2008, from http://www.cnnic.net.cn/index/0O/06/index.htm

CNNIC. (2009). *Statistics report on China's Internet development status (Zhongguo Hulianwangluo Fazhan Zhuangkuang Tongji Baogao)*. Beijing.

Computer System Security and Privacy Advisory Board. (2002). *Findings and Recommendations on Government Privacy Policy Setting and Management*

Das, J., DiRienzo, C., & Burbridge, J. J. (2009). Global E-Government and the Role of Trust: A Cross Country Analysis. *International Journal of Electronic Government Research, 5*(1), 1-17.

Data Protection Study Tour Delegation. (March 2009). China's s personal information protection and legislation outlook.

DeCew, J. W. (1997). *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology.* Ithaca, N.Y. : Cornell University Press.

Dias, G. P., & Rafael, J. A. (2007). A simple model and a distributed architecture for realizing one-stop e-government. *Electronic Commerce Research and Applications 6*(1), 81-90.

Dynamic Coalition on Privacy. (2008). *Fifth progress report.* Retrieved November 30, 2009, from http://userpage.fu-berlin.de/~bendrath/privacy-coalition/Dynamic-Coalition-on-Privacy-PR5.pdf

Eijlander, P. (2005). Possibilities and Constraints in the Use of Self-Regulation and Co-Regulation in Legislative Policy: Experiences in the Netherlands - Lessons to Be Learned for the EU? *Electronic Journal of Comparative Law, 9*(1).

Eisenhardt, K. M. (1989). Building Theories From Case Study Research. *The Academy of Management Review, 14*(4), 532-550.

Electronic Privacy Information Center. (2007). *Privacy and Human Rights Report 2006: An International Survey of Privacy Laws and Developments.*

Electronic Privacy Information Center. (n.d.). *The census and privacy.* Retrieved March 4, 2010, from http://epic.org/privacy/census/

EPIC. (n.d.). *Council of Europe Privacy Convention.* Retrieved June 2, 2009, from http://epic.org/privacy/intl/coeconvention/default.html

European Commission. (2005). *eGovernment in Germany.* Retrieved March 20, 2009, from http://www.epractice.eu/files/media/media_775.pdf

European Commission. (2008). *E-government factsheets: e-government in Germany.* Retrieved October 10, 2008, from http://ec.europa.eu/idabc/servlets/Doc?id=30818

European Commission. (2009a). *eGovernment Factsheet - Germany - History.* Retrieved October 13, 2009, from http://www.epractice.eu/en/document/288241

European Commission. (2009b). *eGovernment Factsheet - Germany - Strategy.* Retrieved October 11, 2009, from http://www.epractice.eu/en/document/288242

European Commission. (2009c, July 2009). *eGovernment Factsheets: eGovernment in Germany*. Retrieved November 10, 2009, from http://www.epractice.eu/files/eGovernment%20in%20DE%20-%20July%202009-12.0.pdf

European Digital Rights. (2009). Germany: Data retention is disproportionate. *EDRI-gram, 7*(6).

European Union. (2003). *Working Document on E-Government*. Retrieved October 22, 2009, from http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/e-government_en.pdf

Farrell, H. (2003). Privacy in the Digital Age: States, Private Actors and Hybrid Arrangements.

Federal Ministry of the Interior. (2006a). *BundOnline 2005: Final Report --- Current Status and Outlook*. Berlin.

Federal Ministry of the Interior. (2006b). *eGovernment 2.0: The Programme of the Federal Government*. Retrieved September 9, 2008, from www.verwaltung-innovativ.de

Federal Ministry of the Interior. (n.d.). *eGovernment 2.0: The Programme of the Federal Government*. Retrieved September 23, 2009, from http://www.verwaltung-innovativ.de

Federal Office for Information Security. (2008). *Annual Report 2006-2007: Secure InformationTechnology for our Society*. Bonn, Germany.

Federal Office for Information Security. (2009). *The IT Security Situation in Germany in 2009*. Retrieved October 15, 2009, from https://www.bsi.bund.de/cae/servlet/contentblob/517474/publicationFile/28002/bsi_lagebericht09_pdf.pdf

Federal Office for Information Security (BSI). (2008). *Annual Report 2006-2007: Secure InformationTechnology for our Society*. Bonn, Germany.

Flynn, B. B., Sakakibara, S., Schroeder, R. G., Bates, K. A., & Flynn, E. J. (1990). Empirical research methods in operations management. *Journal of Operations Management, 9*(2), 250-284.

Flyvbjerg, B. (2001). *Making social science matter: Why social inquiry fails and how it can succeed again* (S. Sampson, Trans.). Cambridge, UK: Cambridge University Press.

Flyvbjerg, B. (2006). Five misunderstandings about case-study research. *Qualitative Inquiry 12*(2), 219-245.

Fountain, J. E. (2009). Bureaucratic Reform and E-Government in the United States: An Institutional Perspective. In A. Chadwick & P. N. Howard (Eds.), *Routledge Handbook of Internet Politics*. New York: Routledge.

Gant, J. P. (2008). *Electronic Government for Developing Countries*: ITU Telecommunication Development Sector.

GAO. (2003). *Privacy Act: OMB Leadership Needed to Improve Agency Compliance* (No. GAO-03-304). Washington, D.C.: United States Government Accountability Office.

GAO. (2005). *Data mining: Agencies have taken key steps to protect privacy in selected efforts, but significant compliance issues remain* (No. GAO-05-866). Washington, D.C.: United States Government Accountability Office.

GAO. (2006). *Privacy -- Key Challenges Facing Federal Agencies* (No. GAO-06-777T). Washington, D. C.: United States Government Accountability Office.

GAO. (2008a). *Information Security: Protecting Personally Identifiable Information* (No. GAO-08-343). Washington, D. C.: United States Government Accountability Office.

GAO. (2008b). *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information* (No. GAO-08-536). Washington, D.C.: United States Government Accountability Office.

Gerring, J. (2004). What Is a Case Study and What Is It Good for? *American Political Science Review, 98*(2), 341-354.

Greenleaf, G. (2009). Five years of the APEC Privacy Framework: Failure or promise? *Computer Law & Security Report, 25*(1), 28-43.

Greenleaf, G. (April 2008). Enforcement aspects of China's proposed Personal Information Protection Act (Part II). *Privacy Laws & Business International Newsletter,* 11-14.

Greenleaf, G. (February 2008). China proposes Personal Information Protection Act (Part I). *Privacy Laws & Business International Newsletter,* 1-6.

Hagen, M. (2004). Electronic government in the United States. In M. Eifert & J. O. Puschel (Eds.), *National Electronic Government: Comparing Governance Structures In Multi-layer Administrations*. London and New York: Routledge.

Hart-Teeter. (2003). *The new e-government equation: ease, engagement, privacy & protection*: The Council for Excellence in Government.

Heeks, R. (2006). *Implementing and Managing eGovernment: An International Text*. London: Sage Publications.

Helmbrecht, U. (2008). Electronic identity cards and citizens' portals, *Baltic IT&T Review: A Business Journal for the Information Society* (Vol. 3).

Hiller, J. S., & Bélanger, F. (2001). Privacy strategies for electronic government. In M. A. Abramson & G. E. Means (Eds.), *E-government 2001* (pp. 162 -198): Lanham, MD: Rowman & Littlefield.

Hu, P. J.-H., Brown, S. A., Thong, J. Y. L., Chan, F. K. Y., & Tam, K. Y. (2009). Determinants of service quality and continuance intention of online services: The case of eTax. *Journal of the American Society for Information Science and Technology, 60*(2), 292-306.

Information Security and Privacy Advisory Board (ISPAB). (2002). *Findings and Recommendations on Government Privacy Policy Setting and Management.* Retrieved May 2, 2009, from http://csrc.nist.gov/groups/SMA/ispab/documents/CSSPAB-Privacy-Report-2002-09.pdf

Information Security and Privacy Advisory Board (ISPAB). (2009). *Toward A 21st Century Framework for Federal Government Privacy Policy.* Retrieved September 4, 2009, from http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/ispab-report-may2009.pdf

Johnson, D. R., & Post, D. G. (1996). Law and borders - the rise of law in cyberspace. *Stanford Law Review, 48*, 1367.

Koh, C. E., Ryan, S., & Prybutok, V. R. (2005). Creating value through managing knowledge in an e-government to constituency (G2C) environment. *The Journal of Computer Information Systems, 45*(4), 32-41.

Kudo, H. (2008). Does e-government guarantee accountability in public sector? Experiences in Italy and Japan. *Public Administration Quarterly, 32*(1), 93-120.

Langer, L., Schmidt, A., & Wiesmaier, A. (2009). *From Student Smartcard Applications to the German Electronic Identity Card.* Retrieved October 13, 2009, from http://www.cdc.informatik.tu-darmstadt.de/reports/reports/ECEG09.pdf

Latzer, M., Just, N., Saurwein, F., & Slominski, P. (2006). Institutional variety in communications regulation. Classification scheme and empirical evidence from Austria. *Telecommunications Policy, 30*(3-4), 152-170.

Lessig, L. (1999). *Code and other laws of cyberspace.* New York, NY: Basic Books.

Long, W. J., & Quek, M. P. (2002). Personal data privacy protection in an age of globalization: The US-EU Safe Harbor compromise. *Journal of European Public Policy 9*(3), 325-344.

Maisog, M. E., & Zhao, A. (2006). *English translation of Zhou, Hanhua et al's Personal Information Protection Act of the People's Republic of China (Experts' Suggestion).*Unpublished manuscript, Hunton & Williams LLP, Beijing, China.

Mathiason, J. (2009). *Internet governance: the new frontier of global institutions*. London and New York: Routledge.

Mayntz, R. (2003). New Challenges to Governance Theory. In H. P. Bang (Ed.), *Governance as Social and Political Communication*. Manchester and New York: Manchester University Press.

McDonagh, M. (2002). E-Government in Australia: the Challenge to Privacy of Personal Information. *International Journal of Law and Information Technology, 10*(3), 327.

Milberg, S. J., Smith, J. H., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science 11*(1), 35-57.

Moon, M. J. (2002). The evolution of e-government among municipalities: Rhetoric or reality. *Public Administration Review, 62*(4), 424-433.

National Institute of Standards and Technology (NIST). (2004a). *Standards for Security Categorization of Federal Information and Information Systems.* (No. FIPS Publication 199). Washington, D.C.

National Institute of Standards and Technology (NIST). (2004b). *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories* (No. Special Publication 800-60). Washington, D.C.

National Institute of Standards and Technology (NIST). (2006). *Minimum Security Requirements for Federal Information and Information Systems* (No. FIPS 200). Washington, D.C.

National Research Council of the National Academies. (2007). *Engaging Privacy and Information Technology in a Digital Age*. Washington, D.C.

OECD. (1980). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Retrieved April 2, 2009, from http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

OECD. (2003a). The case for e-government: Excerpts from the OECD Report "The e-government imperative". *OECD Journal on Budgeting, 3*(1), 62-96.

OMB. (2008). *Fiscal Year 2008 Report to Congress on Implementation of The Federal Information Security Management Act of 2002*. Washington, D. C.

Otjacques, B., Hitzelberger, P., & Feltz, F. (2007). Interoperability of E-Government Information Systems: Issues of Identification and Data Sharing. *Journal of Management Information Systems, 23*(4), 29-51.

Palanisamy, R. (2004). Issues and challenges in e-governance planning. *Electronic Government, 1*(3).

Peters, B. G., & Pierre, J. (1998). Governance Without Government? Rethinking Public Administration. *Journal of Public Administration Research and Theory, 8*(2), 223-243.

Pettigrew, A. M. (1990). Longitudinal field research on change: Theory and practice. *Organization Science, 1*(3), 267-292.

Privacilla. (2002). *The Privacy Torts: How U.S. State Law Quietly Leads the Way in Privacy Protection.* Retrieved June 10, 2009, from http://www.privacilla.org/releases/Torts_Report.html

Privacy International. (2007a). *Overview of Privacy.* Retrieved June 4, 2009, from http://www.privacyinternational.org

Privacy International. (2007b). *PHR2006 - Privacy Topics - UN Internet Governance Forum.* Retrieved November 30, 2009, from http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559087

Privacy International. (2007c). *Privacy and Human Rights 2006 - Federal Republic of Germany.* Retrieved April 12, 2009, from http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559535

Privacy International. (2007d). *Privacy and Human Rights 2006 - United States of America.* Retrieved April 13, 2009, from http://www.privacyinternational.org/article.shtml?cmd%5b347%5d=x-347-559478

Privacy Protection Study Commission (PPSC). (1977). *Personal Privacy in an Information Society.* Washington, D.C.

Prosser, W. L., Keeton, W. P., Dobbs, D. B., Keeton, R. E., & Owen, D. G. (Eds.). (1984). *Prosser and Keeton on Torts* (5th ed.). Los Angeles: West Group

Reidenberg, J. R. (1998). Lex Informatica: the formulation of information policy rules through technology. *Texas Law Review, 76*(3), 553-584.

Reigada, A. T. (2006). *Assessment on Data Protection and e-Government in European Regions and Cities* (e-PRODAT Project). Madrid: Data Protection Agency of the Community of Madrid.

Relyea, H. C., & Hogue, H. B. (2004). A brief history of the emergence of digital government in the United States. In A. Pavlichev & G. D. Garson (Eds.), *Digital government: Principles and best practices* (pp. 16-33). Hershey, PA: IGI Publishing.

Rhodes, R. A. W. (1997). *Understanding governance: policy networks, governance, reflexivity and accountability*. Buckingham: Open University Press.

Schneider, V., & Bauer, J. M. (2007). *Governance: Prospects of Complexity Theory in Revisiting System Theory.* Paper presented at the annual meeting of the Midwest Political Science Association, Chicago, Illinois.

Schwartz, P. M., & Reidenberg, J. R. (1996). *Data Privacy Law: A Study of United States Data Protection*. Charlottesville, Virginia: Michie.

Schweinoch, M., Steger, U., Schicker, S. C., Kröger, S., & Bühr, O. (2009). *Amendments to the German Federal Data Protection Act.* Retrieved September 11, 2009, from http://www.skwschwarz.de/436-1-Amendments-to-the-German-Federal-Data-Protection-Act.html

Seifert, J. W., & Chung, J. (2009). Using E-Government to Reinforce Government-Citizen Relationships: Comparing Government Reform in the United States and China. *Social Science Computer Review, 27*(1), 3-23.

Senden, L. (2005). Soft law, self-regulation and co-regulation in European Law: where do they meet? *Electronic Journal of Comparative Law, 9*(1).

Siau, K., & Long, Y. (2005). Synthesizing e-government stage models – a meta-synthesis based on meta-ethnography approach. *Industrial Management & Data Systems, 105*(4), 443-458

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20*(2), 167-196.

Solum, L. B. (2009). Models of internet governance. In L. A. Bygrave & J. Bing (Eds.), *Internet governance: infrastructure and institutions*. Oxford: Oxford University Press.

Sorensen, E., & Torfing, J. (Eds.). (2007). *Theories of democratic network governance*. Basingstoke: Palgrave Macmillan.

Steimke, F., & Hagen, M. (2003). OSCI: A Common Communications Standard for E-Government. In R. Traunmuller (Ed.), *Lecture Notes in Computer Science* (Vol. 2739, pp. 250-255). Berlin: Springer.

Steinke, G. (2002). Data privacy approaches from US and EU perspectives. *Telematics and Informatics, 19*(2), 193-200.

Stoker, G. (1998). Governance as theory: five propositions. *International Social Science Journal 50*(1), 17-28.

Strauss, J., & Rogerson, K. S. (2002). Policies for online privacy in the United States and the European Union. *Telematics and Informatics, 19*(2), 173-192.

Sutton, G., Zhang, X., & Hart, T. (2007). *Personal Data Protection in Europe and China: What Lessons to be Learned?* Beijing: EU-China Information Society Project.

Tan, Q. (2006). *China's provincial party secretarties: roles, powers and constraints.* Retrieved August 15, 2009, from http://www.nottingham.ac.uk/shared/shared_cpi/documents/discussion_papers/Discussion_Paper_7_Provincial_Party_Secretaries.pdf

Taylor, G. (n.d.). *The Council of Europe Cybercrime Convention: A civil liberties perspective.* Retrieved June 2, 2009, from http://www.efa.org.au/Publish/coe_paper.html

The International Working Group on Data Protection in Telecommunications. (2005). *Working Paper on Data Protection and Online Voting in Parliamentary and other Governmental Elections.* Retrieved November 15, 2009, from http://www.datenschutz-berlin.de/attachments/226/evoting_2_en.pdf?1201707256

The White House. (2003). *The National Strategy to Secure Cyberspace.* Retrieved May 29, 2009, from http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

The White House. (2009). *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.* Retrieved September 25, 2009, from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Torres, L., Pina, V., & Royo, S. (2005). E-government and the transformation of public administrations in EU countries. Beyond NPM or just a second wave of reforms? *Online Information Review, 29*(5), 531-553.

Treib, O., Bahr, H., & Falkner, G. (2007). Modes of governance: towards a conceptual clarification. *Journal of European Public Policy, 14*(1), 1-20.

U.S. Department of Health Education and Welfare. (1973). *Records, computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems.* Retrieved September 12, 2009, from http://aspe.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm

U.S. Executive Office of the President. (2001). *The President's management agenda.* Retrieved March 20, 2009, from http://www.whitehouse.gov/omb/budget/fy2002/mgmt.pdf

UMR Research. (2008). *Individual Privacy & Personal Information.* Wellington, Auckland, Sydney: Privacy Commissioner of New Zealand.

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

United Nations. (2005). *UN global e-government readiness report 2005---from e-government to e-inclusion.* New York: United Nations.

United Nations. (2008). *United Nations e-government survey 2008: From e-government to connected governance.* New York: United Nations.

United States Department of Justice (USDOJ). (2004). *Overview of the Privacy Act of 1974.* Retrieved April 15, 2009, from http://www.usdoj.gov/opcl/1974privacyact-overview.htm

United States Department of Justice (USDOJ). (2007). *Chapter 1: Computer Fraud and Abuse Act.* Retrieved September 23, 2009, from http://www.cybercrime.gov/ccmanual/01ccma.pdf

USDOJ. (2004). *Overview of the Privacy Act of 1974.* Retrieved April 15, 2009, from http://www.usdoj.gov/opcl/1974privacyact-overview.htm

van Blarkom, G. W., Borking, J. J., & Olk, J. G. E. (Eds.). (2003). *Handbook of Privacy and Privacy-Enhancing Technologies: The case of Intelligent Software Agents.* The Hague, The Netherlands: College bescherming persoonsgegevens.

Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review, 4,* 193-220.

Weber, R. H. (2002). *Regulatory models for the online world.* Zurich, Switzerland: Schulthess Juristische Medien AG.

West, D. M. (2008a). *Improving Technology Utilization in Electronic Government around the World, 2008.* Retrieved December 1, 2008, from http://www.brookings.edu/reports/2008/0817_egovernment_west.aspx

West, D. M. (2008b). *State and Federal Electronic Government in the United States.* Retrieved December 1, 2008, from http://www.brookings.edu/reports/2008/0826_egovernment_west.aspx

Westin, A. F. (1967). *Privacy and Freedom.* New York: Atheneum Press.

WGIG. (2005a). *Background Report to the Report of the Working Group on Internet Governance.* Geneva: The Working Group on Internet Governance.

WGIG. (2005b). *Report of the Working Group on Internet Governance.* Château de Bossey, Switzerland: Working Group on Internet Governance.

Wong, J. K. Y. (2005). Electronic government and its implication for data privacy in Hong Kong: Can Personal Data (Privacy) Ordinance protect the privacy of personal information in cyberspace? *International Review of Law, Computers & Technology, 19*(2), 143.

Wu, Y., & Bauer, J. M. (2009). *E-Government and citizen participation in developing countries: the case of China.* Paper presented at the 59th annual convention of International Communication Association, Chicago, IL.

Yin, R. K. (1984). *Case Study Research: Design and Methods*. Newbury Park, CA: Sage Publications.

Yin, R. K. (2003). *Case study research: Design and methods*. Thousand Oaks, California: Sage Publications.

Zhang, J. (2003). Good governance through e-governance? ---Assessing China's e-government strategy, *A Global Interdisciplinary Conference---China & the Internet: Technology, Economy, & Society in Transition*. Los Angeles.

Zwick, D. (1999). *Models of privacy in the digital age: Implications for marketing and e-commerce*. Retrieved May 26, 2009, from http://ritim.cba.uri.edu/Working%20Papers/Privacy-Models-Paper%5B1%5D.pdf