Government Information Quarterly 31 (2014) 150–159

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

Protecting personal data in E-government: A cross-country study

Yuehua Wu

School of Media and Design, Shanghai Jiao Tong University, 800 Dongchuan Road, Shanghai 200240, China

ARTICLE INFO

Available online 3 January 2014

Keywords:
Personal data protection
E-government
Government regulation
Self-regulation
Code-based regulation
Internet governance

ABSTRACT

This paper presents the findings of a comparative study of laws and policies employed to protect personal data processed in the context of e-government in three countries (the United States, Germany, and China) with rather different approaches. Drawing on governance theory, the paper seeks to document the mechanisms utilized and to understand the factors that shape the governance modes adopted. The cases reveal that national government regulations have not kept pace with technological change and with the current information practices of the public sector. Nonetheless, traditional government regulation remains the major governance mode for the issue under discussion. Self-regulation and code-based regulation serve supplementary roles to traditional government regulation. National context is found to impact the form and level of data protection and the choice of governance modes.

1. Introduction

Personal computers and the internet substantially increased the number of participants generating and using personal information in a way that was unimaginable decades ago (Reidenberg, 2000). This trend has been further accelerated in recent years by the emergence of new information and communication technologies (ICTs) and applications, Web 2.0 technologies in particular, which involve processing of massive amounts of personal data at a global scale. Creating a 'hyper-sharing culture' (Kumar, 2010), Web 2.0 and internet social media facilitate efficient collection and sharing of personal information, which transforms how we define the personal/private and magnifies the privacy issue. While the internet technology and people's conception of privacy are in a state of flux, the information privacy issue is gaining greater importance and will become more pressing as time goes on. Despite the increasing prominence of protecting online information privacy, how such protection could be appropriately, enforceably and effectively achieved in the borderless virtual world of the internet with the shifting landscape is a big challenge. Whether and how the changing landscape has resulted or will result in societal and regulatory changes in the protection of information privacy is largely an open question. To answer the question and best address the problem, it is crucial to first examine the current state of the privacy protection framework.

This paper looks at the information privacy protection issue in one specific domain— e-government. This realm is chosen for two main reasons. First, the unique features pertaining to data processing by the public sector make government's handling of personal data an equally significant, if not more important, research topic as that for the private sector. Compared to the commercial sector's often costly and profit-oriented data acquisition, governments acquire information from citizens because of their governing functions, which often shifts the cost of submission to the citizen. Government thus may lack the incentive to value citizen's information appropriately and is not constrained by a market incentive to limit its data collection (Privacilla, 2001). Further, personal information in government's hand is often very sensitive. Anonymity or pseudonymity is often impossible or even illegal when dealing with government. Analysis of these data thus can be highly invasive, particularly when data is combined and aggregated. As government is maintaining ever larger depositories of personal information and possessing "greater information power" (Mayer-Schonberger & Lazer, 2007a, p. 286), the risk of privacy invasion by governments is increasing.

In June 2013, the United Nations (UN) released a report calling for global attention and closer scrutiny of the widespread use of electronic surveillance by States (La Rue, 2013). Following hard on its heels came the whistleblowing of the digital surveillance and mass data-gathering program of PRISM by the United States (US) government (see Greenwald & MacAskill, 2013). The escalating public attention to electronic surveillance and data collection underlines the huge privacy implications of and increasing public concerns on government's handling of personal data in the digital age. It also underlines an urgent need to review relevant national laws/policies to advance international understanding of the protection of privacy right in light of technological advancements.

Secondly, the information privacy issue in the specific context of e-government requires research and policy attention for good reasons. As information technologies advance, initiatives of e-government, government utilizing ICTs and the internet to deliver public services (West, 2004), have been carried out at all levels of government across the globe because of its potential benefits to society, such as enhancing public

Tel.: +86 21 34205808.
E-mail address: yhwu22@sjtu.edu.cn.

0740-624X/$ – see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.giq.2013.07.003

service efficiency, effectiveness, transparency, quality (Ho, 2002; McNeal, Hale, & Dotterweich, 2008), and e-democracy (Chadwick, 2003; Jaeger & Thompson, 2004). Like many other internet applications, however, e-government substantially increases the volume of records, the storage (usually in linkable databases) and processing of personally identifiable information by the government, which poses great risk to individuals' information privacy. Balancing the development of e-government and the need to guarantee individuals' right to information privacy emerges as a pressing issue. At the same time, adequate personal data protection is essential to boost public trust in online government and thus crucial to the success of e-government itself (Beldad, Geest, Jong, & Steehouder, 2012). Empirical studies found that a lack of trust decreases e-government adoption and diffusion (Carter & Belanger, 2005; Das, DiRienzo, & Burbridge, 2009). To fully unleash the true potential and value of e-government, government needs to address and reassure citizens of the privacy and security of their personal information online.

Although scholars, policy-makers and privacy advocates have called for attention to this issue, systematic studies on this subject are very limited. E-government is regarded as one of the greatest innovations in the public sector (Potnis, 2010). The innovative services enabled by information technology not only offer the potential to improve administrative performance, but also significantly transform institutional and organizational structures and processes (Fountain, 2001, 2008), or "the inner workings of government" (Mayer-Schonberger & Lazer, 2007b, p. 4). For instance, technological advances create a greater sense of interconnectedness and interdependency within government as well as between government and private companies, non-profit organizations, and citizens (Chhotray & Stoker, 2009; Potnis, 2010). These changes in structures and processes, which might be fundamentally seen as changes in information flows (Mayer-Schonberger & Lazer, 2007b), have challenged the established government-centric forms of governance and created demands for new approaches (Chhotray & Stoker, 2009; Hale & McNeal, 2011), such as *networked governance*, which involves moving functions away from government hierarchy to more decentralized networked systems (Chadwick, 2003; Lazer & Binz-Scharf, 2007; Mayer-Schonberger & Lazer, 2007b; Mueller, 2010). Mayer-Schonberger and Lazer (2007b) argued that the significant changes of governing and governance facilitated by new technologies could be better comprehended if e-government is understood as "information government", the flows of information within and between government and citizens. The issue of personal information protection poses core governance challenges as ICT use and concurrent structural changes in government, namely e-government, continues to develop (Fountain, 2008). A governance perspective on this subject therefore should be of great value and could contribute to both e-government literature and the literature on the relationship between technology and governance practices.

E-government is an internet-based application. So the data protection issue in e-government can be regarded as an important internet policy issue. For this reason, this study is primarily grounded in an internet governance framework.[1] Over the past years, the rapid growth of the internet has caused heated discussion and debate 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 (Barlow, 1996). Yet as the internet became 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. While a broad spectrum of governance mechanisms is available for the internet, such as government intervention and regulation, self-regulation and co-regulation (cooperation between the public and the private actors in the rule-making process) (Eijlander, 2005; Senden, 2005), and market decisions (Bauer, 2007), the key problem is which or which mix of governance mechanisms to apply for the internet policy issues. The existing internet governance literature largely focuses discussions on domain names, internet infrastructure, and relevant institutional arrangements (e.g. Bygrave & Bing, 2009; Mathiason, 2009; Take, 2012). The discussion of governance structures for specific public policy issues, such as online privacy protection, is fairly limited. More exploration and insights in this regard can contribute to a deeper understanding of the internet governance issue.

To fill the research gaps, this paper, drawing on governance theory and internet governance literature, presents a comparative analysis of the national governance modes, with an emphasis on regulatory frameworks, of personal data protection in the context of e-government by the United States (US), Germany, and China. The objective is to examine the current status of the data protection issues in e-government, and contribute to the reflection on this issue by providing more insight into its governance mechanism and the impact of national context on the mechanism adopted. Given the shifting internet landscape and the potential tensions between networked governance, the dominant mode of coordination on the internet (Mueller, 2010), and traditional forms of government regulation in the area of privacy protection, this study also sheds light on important challenges to internet governance.

2. Conceptual framework and methodology

2.1. Privacy and information privacy in e-government

Being socially and culturally conditioned, the notion of privacy is highly dynamic and varies from context to context and culture to culture (Johnson, 1989). For this reason, there is a lack of a universally accepted definition of privacy in both the philosophical and legal literature (Introna, 1997). The definitions of privacy are often debated for various flaws. For instance, the US judges Warren and Brandeis (1890) first defined the right to privacy as the right "to be left alone", an approach which was later faulted as being too limited in that it "does not take enough cognizance of the subtle and complex social context where privacy is at stake" (Introna, 1997, p. 262). Despite the lack of an agreed version, a central element in the privacy definitions is the ability of individuals to choose if, when, and to what extent they interact with and reveal themselves to others (Connors, Harrison, & Akins, 2005).

In addition to looking for a specific definition, one useful approach to understand privacy is examining different privacy dimensions (e.g. Braman, 2006; Burgoon et al., 1989; DeCew, 1997). For instance, privacy can be divided into four aspects: *information privacy*, *bodily privacy*, *privacy of communications*, and *territorial privacy* (Privacy International, 2007a). Of the various metrics, *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 paper, the discussion of privacy focuses on *information privacy*, which in Europe is often referred to as *personal data*. Given the shifting landscape of the online information community, it is of increasing importance for the community members (data subjects and processors, policy-makers, privacy advocates and scholars) to fundamentally rethink what is information privacy and how this issue could be governed effectively.

There are three types of information privacy problems arising from e-government applications: *Collection problems*, *Use and disclosure problems*, and *Security problems* (McDonagh, 2002). Appropriate data protection measures should address each of these three aspects when e-government activities are carried out.

With regard to the first type of problems, every time a person visits a government website for browsing, information seeking, or conducting an online transaction, his/her personal information is purposely or

[1] A political economy approach would be an interesting avenue to explore this issue. While the paper does not aim at using a political economy framework, which would exceed the space available, this could be pursued in future studies on this subject. One reference that may shed light on a political economy approach towards this issue is Cassell's study of privatization in Germany and the United States (2003).