Telecommunications Policy xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

Telecommunications Policy

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

A socio-technical analysis of China's cybersecurity policy: Towards delivering trusted e-government services

Huiping Zhang[a], Zhiwei Tang[a], Krishna Jayakar[b,*]

[a] *School of Political Science and Public Administration, University of Electronic Science and Technology of China, China*
[b] *Donald P. Bellisario College of Communications, Penn State University, USA*

ABSTRACT

This paper uses a socio-technical analysis framework to examine the potential impact of the 2016 Cybersecurity Law on e-government services in China. Based on prior survey results in the literature, the factors that affect user responses to e-government portals are identified. It then reviews the provisions of the Cybersecurity Law and identifies the factors that are likely to affect e-government operations. Open-ended interviews with cybersecurity and e-government experts are used to assess the possible impacts of the law.

1. Introduction

On November 7, 2016, the Chinese government released a comprehensive new National Cybersecurity Law (hereafter the CSL), with broad coverage of industrial sectors such as energy, transportation and information networks (National People's Congress [NPC], 2016). The Law has implications for disparate areas including data protection, privacy, and state surveillance, besides the security of information networks. On May 2, 2017, the Cyberspace Administration of China (CAC), charged with enforcing the CSL, produced new administrative rules for online products and services. Both the law and its administrative rules went into effect on June 1, 2017, and implementation is ongoing as this article goes to press.

E-government is only one of the several areas impacted by the law, but it presents certain unique challenges since it requires the interaction of technical systems and capabilities with human operators and users. Altering the technical and operational requirements for e-government, as the CSL has done, is likely to have wider ramifications for user acceptance, behaviors and satisfaction with e-government services. An appropriate framework for analyzing this process is socio-technical systems (STS) analysis, which has been to evaluate Information and Communication Technology (ICT) policies (Kim, Shin, & Lee, 2015; Kompella, 2017). As the extensive literature on STS has shown, the interaction of technical and social systems can result in novel and unpredictable outcomes (Bolton & Foxon, 2015; Fuenfschilling & Truffer, 2016; Geels, 2004; Geels et al., 2016; Geels & Schot, 2007; Walker, Stanton, Salmon, & Jenkins, 2008). Neither technical capability nor human behavior is “given,” but are iteratively modified and jointly optimized. From a theoretical perspective too, “socio-technical systems transitions,” catalyzed by new technologies or technical requirements, is a major strand of the STS literature. An analysis of the CSL on e-government services is therefore of both theoretical significance and practical importance.

This paper examines the potential impacts of the CSL and its operational rules on the provision of e-government services, utilizing an STS framework. A key element of the STS approach (discussed at greater length in the literature review below) is the focus on the social needs, expectations and psychology of workers and users (Engelstad, 1972; Rice, 1958; Thorsrud, 1967). New technologies and technical requirements are adapted to the social context of the organization, even as the technology shapes the environment within

* Corresponding author.
E-mail address: kpj1@psu.edu (K. Jayakar).

https://doi.org/10.1016/j.telpol.2018.02.004
Received 16 November 2017; Received in revised form 25 February 2018; Accepted 26 February 2018

which the human agents function. This “reciprocal shaping” of the social and technical environment of e-government, in light of the changes introduced by the CSL, is the subject matter of the paper. Therefore, in line with the STS framework, we ask the following questions: first, what technical aspects and organizational practices of e-government in China do citizens report as affecting their utilization of e-government services?; second, how does the CSL and its operational rules affect the technical and organizational aspects of e-government services in China, and in what manner?; and third, what is the likely impact of the CSL on delivering trusted e-government services, and increasing their utilization rates? Finally, inspired by the “human centered design” principle of STS theory, we seek to gain policy recommendations to improve e-government operations from the feedback of portal managers interviewed for this paper.

To answer these questions, we structure the paper as follows. First, in the section that follows, we review the literature, providing a summary of existing studies on China's cybersecurity law and outlining the socio-technical analysis framework. In the next section, we review prior survey research on citizen attitudes towards e-government in China and elsewhere, with the goal of identifying the critical issues that users name as the determining factors in their decision to utilize e-government services. Next in Section 3, we turn to China's 2016 CSL, first discussing the legal definition of e-government portals under the law, and then identifying the provisions applicable to them. Next in Section 4, we turn to the third research question of the paper: the likely impact of the CSL on e-government services, relying on in-depth, anonymized interviews with cybersecurity experts to identify potential impacts. In section 5, we present our conclusions and recommendations.

2. Literature review

2.1. China's cybersecurity policy

In recent years, China's efforts at economic restructuring and technological upgradation through the application of ICTs such as Big Data, Cloud Computing, and the Internet of Things have met with a major obstacle in cybersecurity. China has been an attractive target of cyberattacks and cybercrimes (Kim, Wang, & Ullrich, 2012; Kshetri, 2013a; China Software Testing Center, 2017). Simultaneously, a crisis in ensuring the privacy and security of personal data has become more and more serious. Citizens are not willing to share personal data when utilizing online services (Wang & Yu, 2015), which hampers the adoption and application of the emerging ICTs. China's strategy emphasizing “cybersecurity and informatization are two wings of one body” is a direct outcome of this challenge (Parasol, 2017).

China's cybersecurity policy had been always considered to be fragmented, vague and difficult to enforce. For instance, there was no dedicated legislation clearly defining the specific rights of personal privacy, which were instead protected under the right of reputation in the Civil law (Wu, Lau, Atkin, & Lin, 2011). On data privacy, Kshetri (2014) indicated that the provisions were ambiguous and ineffectively enforced in China. In this context, the CSL was a landmark legislation that sought to clarify and systematize a fragmented and disorganized regime for cybersecurity. Some observers have pointed out that the law is not entirely new and has merely codified rules and regulations that were already in effect (Mozur, 2016). Nevertheless, the Law as a systematic and broad-based legislation covering all aspects of cybersecurity, is expected to be consequential for business as well as network operations (Mozur, 2016; Wee, 2017). The CAC and other agencies or institutions subsequently issued a series of rules, measures and standards to enhance the enforcement of the CSL. Now that the law has become operational, it is essential to examine its implementation and impact.

In assessing China's cybersecurity policy, the literature has mostly focused on the impact on technology innovations, market growth and international relations. Many studies pointed it out that China's Internet censorship and cyber control had affected the ICT's productive utilization (Feng & Guo, 2013; Kshetri, 2014, 2015), and hindered foreign firms' development in China (Kshetri, 2015; Parasol, 2017). Cybersecurity policy had become an important issue in international relations (Kshetri, 2013b; Parasol, 2017; Wharton & Lin, 2015). However, few studies have analyzed the impact of China's cybersecurity policy from the point view of e-government, which is where this paper intends to make its contribution.

2.2. Socio-technical analysis

Sociotechnical theory (STS) originated in the 1950s as a means of coming to terms with the non-linear and unpredictable effects that accompanied the introduction of new technologies into organizations (Trist & Bamforth, 1951; Trist, 1956). According to STS, technical and social systems are interrelated. Whereas technical systems are designed to achieve certain performance parameters, social systems comprised of human beings do not always behave predictably. The interaction of technical capabilities with the social system, and the continuous behavioral adjustments to the technical environment create complex, unpredictable and non-linear patterns of interaction. STS posits that social and technical systems are jointly optimized (Walker et al., 2008). In addition to the social and technical systems, early theorists considered whether the ‘economic system’ should be included as a separate element of the model; eventually this argument was rejected, on the grounds that economic factors are better understood as influences on the social and technical dimensions of the system (Emery, 1959; Kelly, 1978; Trist, Higgin, Murray, & Pollock, 1963).

Over the next decade, field work based on Trist's STS Model led to increasing focus on the social needs, expectations and individual psychology of workers and work groups. Rice’s (1958) research on the introduction of modern weaving technology in Indian textile mills found that there was a mismatch between the needs of the technology (collaborative team work in which each individual plays only a small part) and the psychological needs of workers (specialized, individual work within clearly demarcated task boundaries), leading to loss of productivity. In the absence of attention to worker needs and expectations, individuals may experience