Chapter 70
Management of Privacy and Security in Cloud Computing: Contractual Controls in Service Agreements

Deniz Tuncalp
Istanbul Technical University, Turkey

ABSTRACT

There are a number of risk domains that are relevant for information privacy and security in cloud-based scenarios and alternative deployment models, which require implementation of a number of controls. However, cloud service providers often take a one-size-fits-all approach and want all their customers to accept the same standardized contract, regardless of their particular information security and legal compliance needs. Taking ISO 27001 Information Security Management standard as a guide, we have employed the Delphi method with a group of cloud computing experts from around the world who are subscribed to the "Cloud Computing" group on LinkedIN to identify the most applicable controls in a generic cloud service provider – customer context. Based on these results, we use a sample of cloud computing customer service agreement as a case study to further discuss related contingencies. As a result, this chapter argues that a more balanced approach is needed in service contracts to ensure the maintenance of necessary service levels and the protection of cloud users.

INTRODUCTION

The widespread diffusion of information and communication technologies (ICTs) has significantly altered the way people live and work. People spend significant portion of their time on and around computers in their daily lives. Companies utilize ICTs to perform and support all their business processes. ICTs are critical for the performance of the immediate operations, and the long-term survival of the organizations. The worldwide diffusion of ICTs not only brings personal, social and commercial changes, but also carries new risks to contemporary society. Compared to the functioning of the society in the pre-computer era, both personal and business uses of ICTs involve: generating, storing, processing, and transferring much larger amounts of information. The

DOI: 10.4018/978-1-4666-9466-8.ch070

development and expansion of ICTs, therefore, affects individuals' right to information privacy. It is necessary to balance the societal benefits promised by new technology infrastructures and related business models with individual rights to information privacy and organizations need for information security. Thus, an adequate level of information privacy and security control is essential to ensure public and commercial trust in online services. This is especially crucial for the success of new technologies when they are first launched for public use.

INFORMATION PRIVACY AND SECURITY

In this chapter, information security is discussed in the context of privacy protection or the general personal data protection. For the purpose of this study, personal data protection is used as personal information privacy protection that includes the protection of data privacy and data security.

Warren and Brandeis (1890) defined the right to privacy as the right "to be left alone". Burgoon et al. (1989) distinguished four types of privacy violations: physical, interactional, psychological/informational, and impersonal. 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. 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 study, the discussion of privacy is limited to information privacy, which is often referred to as personal data.

Regarding personal information, Smith, Milberg, and Burke (1996) identified four dimensions of concerns about organizational privacy practices:

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 (Chang & Ramachandran, 2014).

The concept of information privacy emerged in the 1960s and 1970s, at about the same time as data protection (Bennett, 2002). 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, particularly on the Internet. Personal information privacy in the digital age has increased in salience and has been discussed in various fields, such as public policy, law, and Internet study worldwide (e.g., Baumer, Earp, & Poindexter, 2004; Banisar & Davies, n.d.; Baumer, Earp, & Poindexter, 2004; Bennett, 2002; Buchanan, Paine, Joinson, & Reaps, 2007; Zwick, 1999).

Information Security is "the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities" (International Organization for Standardization [ISO], 2005). ISO has published ISO 27001 standard in 2005 to provide guidance to organizations that want to manage their information security with a management system