Personal Information Privacy: 
A Multi-Party Endeavor

Sue Conger, University of Dallas, USA

ABSTRACT

Individuals can no longer manage their own personal information privacy. Rather, organizations with which individuals interact must recognize vulnerabilities and actively manage their data to guarantee known data sharing and to prevent data leakages. A more complete model of consumers’ personal information privacy that includes not only data gathering, but also data sharing and data leakage is presented and defended here.

Keywords:  data leakage; data sharing; personal information; personal information privacy

INTRODUCTION

Every day, we read of some new data loss of millions of individuals’ personal information (PI) (Albrecht, 2002; Driscoll, 2007; Konitzer, 2006; Zeller, Jr., 2005). As losses amass, the realization that Personal Information Privacy (PIP) is not manageable by individuals becomes clearer. This lack of management is exacerbated by the lack of clear or binding agreements on the parameters of collection or usage of PI data between individuals and organizations with which they interact.

Privacy has many facets and can be defined in many ways. Personal privacy generally applies to keeping confidential anything an individual does not want known, such as a person’s location (Solove, 2006). For our purposes, privacy is “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” (Westin, 1967). Westin’s definition is appropriate by its applicability to both individuals and institutions, and its focus on information. Therefore, in this research, this definition describes information privacy.

PI management historically has been the responsibility of individuals forging contracts with organizations, health providers, governments, and other organizations (hereafter referred to as organizations) for protection of their data (Smith & Milberg, 1996) with responsibility of government to protect the individual (Swire, 1997), and the responsibility of organizations to manage internal PIP use (Smith & Milberg, 1996). These views have all been valid in the past but PIP threats have expanded beyond the organization to its data-sharing partners. PIP depends on the security practices of multiple organization in multiple jurisdictions (Majores, 2006). Further, PI needs to be thought of as
having a life of its own once it moves beyond immediate the individual-vendor relationship (Anonymous, 2006). In this research, we build on past privacy research to develop a model of data sharing from the individual to the organization and from the organization to its data-sharing partners.

The premise of this research is that the individual-to-organization transaction link, while still needing research, is well understood. However, what businesses do with the data, once collected, is less understood and is becoming more important to privacy maintenance (cf. Albrecht, 2002; Zeller, Jr., 2005). Organizations, having spent billions creating secure corporate silos, do not operate in a silo-like vacuum. Rather, organizations routinely share data with business partners and legal entities that in turn, share that data with other organizations. In this data-sharing environment, we develop two groups of data sharing partners with which organizations interact and the need for organizations to actively manage or prevent different types of data access and use. Once the full extent of data movement is understood, it is clear that organizational policies and procedures need extension and regulation to control multi-party access.

In the next sections, PIP research to date is summarized and the expanded model and supporting arguments are presented. Extra-organizational data sharing entities and the PIP threats posed by them are detailed. Then, suggestions for further research are developed and actions of individuals seeking to protect themselves are proposed.

PERSONAL INFORMATION PRIVACY MODELS

PIP research relating primarily to transaction relationships is summarized in this section. This research is representative of the enormous body of work relating to ‘information technology and privacy,’ which yields over 350 scholarly articles on Proquest. The World Wide Web (Web), a new technology 15 short years ago, changed many of the issues relating to PIP and furthermore, maturing Web and emerging technologies enable new abuses of data that require more formalized, or more regulated, data and data relationship management.

Before Web technology matured to support interactive transaction processing, research concentrated on organizational data gathering, usage, and access practices, seeking to articulate the issues relating to PIP and organizational data gathering and use. Post-Web maturity research shifted focus to Internet transactions that generate more and different data, use more and different methods of data collection, and have different persistence issues.

**Personal Privacy Before Web Transaction Technology Maturity**

Research published before Web capabilities for transaction processing matured had few references to Web information gathering practices (Culnan & Armstrong, 1999). Much research in the 1990s sought to determine the scope of the privacy problem and how to frame privacy issues (Conger et al., 2005; Culnan, 1993; Culnan & Armstrong, 1999; Loch & Conger, 1996; Smith & Milberg, 1996). Privacy, at a minimum, concerned collection, unauthorized secondary use, ownership, accuracy, and access (Culnan & Armstrong, 1999; Loch & Conger, 1996; Smith & Milberg, 1996).

Culnan & Armstrong’s (1999) privacy leverage model (see Figure 1) relates corporate use of consumers’ collected personal data to the trust that either leads to retention or defection of customers. Culnan’s model demonstrates an understanding of the issues in organizational data collection and use but assumes solid control over all use and also assumes firm’s have some policy (whether explicit or not) on PIP protection. Transaction decisions are based on a ‘privacy calculus’ that is an idiosyncratic trade-off between trust, risk, cost/benefit, and other consumer psychographic characteristics (Bhattacherjee, 2001; Bhattacherjee & Premkumar, 2004; Culnan & Armstrong, 1999; Gauzente, 2004; McKnight et al., 2004; Park
Augmented Reality Apps for Tourism Destination Promotion
www.igi-global.com/chapter/augmented-reality-apps-for-tourism-destination-promotion/179813?camid=4v1a