Chapter 3

Privacy Loss: An Expanded Model of Legal and Illegal Data Exchange

Joanne H. Pratt
Joanne H. Pratt Associates, USA

ABSTRACT

Considerable research shows that personal information privacy has eroded over the last 30 years. Prior research, however, takes a consumer-centric view of personal information privacy, a view that leads to the conclusion that the individual is responsible for his/her own information. This research presents a comprehensive personal information privacy model of extra-organizational data sharing and use in ecommerce and social networking. It incorporates how data is actually passed and leaked to entities of which the individual has no knowledge and no control. This research presents support for the existence of legal, illegal, and legally-grey area extra-organizational parties and the need for more complete comprehension of personal information privacy. In addition, the research identifies the magnitude of privacy violations in spite of legal and self-protection policies. The model can serve as a guide for privacy research and for social discussion and legislation to manage and regulate use of data once collected.

INTRODUCTION

Personal privacy is a vague concept generally applied to keeping confidential anything an individual does not want known (Solove, 2006; Spinello, 1998). This research adopts the definition offered by Westin (1967, p. 7.), who defines privacy as the claim to determine for oneself when, how and to what extent personal information is released.

That perspective leads to the assumption that we each have rights to keep private anything about us that we wish, ceding access rights in exchange for societal participation (Culnan & Bies, 2003). As Posner (2008, p.248) points out, “a person would have to be a hermit to be able to function in our society without voluntarily disclosing a vast amount of personal information to a vast array of public and private demanders.” To gain the benefits of citizenship and employment, and connectedness with “friends,” for example, we
cede rights of identity, domicile location, and family arrangements (Debatin, Horn, & Hughes, 2009). Through transactions we cede the rights to personal transaction information to aggregators who, until recently, limited their data collection and aggregation. Recently, because of new and maturing technologies, we are unknowingly giving away much more than just identity, location, and transaction information (Nissenbaum, 1998; Shilton, Burke, Estrin, Hansen, & Srivastava, 2008). Now our information can swiftly be integrated and aggregated, which was impossible before the Internet (Posner, 2008). Privacy is eroding as new technologies enable this massive collection, aggregation, and sale of everything about everyone (Spinello, 1998; Gleick, 1996; Inside Facebook Gold, 2010).

Data integration has led to functional, economic, and social benefits but also to abuses of individual privacy. Questions are being raised as to whether abuses to personal information privacy (PIP) are beginning to outweigh the benefits obtained by widespread data integration and sale (Thiesse, 2007; Stanton, Nemati, Chun, & Chen, 2007; Conger, Mason, Mason, & Pratt, 2005; Kling, 1995; Eldon, 2010). Legal data integrators are being pre-empted by illegal entities seeking accessibility to minutia on every facet of individuals’ lives.

To understand the implications of data release and integration, this research presents an expanded privacy model that contributes to the literature in several ways. First, it presents a model of data exchange that includes all parties: the 1st party individual holding personal private data; the 2nd party vendor/provider(s) to whom data is initially released; 3rd party legal data integrators, which include legally grey area government and private data miners, and 4th party illegal data collectors. While these constructs have individually been the topic of some research, none of the research found ties the subject matter to PIP, thus presenting an incomplete view of the data relationships among organizations. Second, the model in this research integrates and enlarges separate frameworks that model privacy and online transaction processing.

The article first presents an expanded PIP model, defining extra-organizational data-sharing entities along with the threats they pose to PIP. Then, proof of the existence and extent of losses to PIP from legal and legally grey area third parties and clearly illegal fourth parties is offered from the academic literature. Loss of control of PIP by the individual in varying degrees is illustrated with examples from current media, including loss that occurs from social networking. A review of privacy laws in the section, Safeguarding Privacy, describes the effectiveness of attempts to safeguard PIP by legislation, privacy-enhancing technologies, and self-protection. Finally, the importance of awareness of PIP issues for developing policy and possible actions are presented.

**AN EXPANDED MODEL OF INFORMATION PRIVACY**

**Decision Calculus**

The model begins with the decision calculus that the individual makes prior to releasing any personal information. Each box leading to the decision calculus in Figure 1 and the arrows depicting the relationships between them represent areas in which significant research has already been conducted (Culnan & Armstrong, 1999; Cheung, Chan, & Moez, 2005; Conger, et al., 2005; and Xu, Dinev, Smith, & Hart, 2008). The individual’s judgment of the vendor, medium, environment, consumer, and product or service characteristics enters into his or her calculation. Personal privacy as modeled by Culnan and Armstrong (1999) shows the individual as consumer disclosing information based on the expectation of achieving benefits that exceed risks. Published before web maturity, the 1999 model does not specifically treat online transactions. The model is presented from a corporate vendor/provider point of view.