# Chapter 7.7
# Online Information Privacy and Its Implications for E-Entrepreneurship and E-Business Ethics

**Carmen Gould**
*RMIT University, Australia*

**Fang Zhao**
*RMIT University, Australia*

## ABSTRACT

This chapter reports the results of a national survey which investigated Australian Internet users' attitudes and behaviours toward online information privacy using a typology that combines specific demographic and attitudinal measurements with behavioural data. The chapter contains a comprehensive examination of the internal, external/environmental, and behavioural dimensions of information privacy, incorporating a profile of each of the typologies' categories along with a general profile of total respondents. The implications of the findings for e-entrepreneurship and e-business ethics also are discussed.

## INTRODUCTION

In the e-business world, owning consumer data is essential to the development of customer relationships. **Consumer knowledge** can lead to value-added product offerings and marketing communications if businesses know what their customers already like and might need, reducing costs (Dembeck, 1999) and improving sales. Ultimately, collecting **consumer data** can help organisations enhance the level and quality of service or product they provide, enabling them to make gains in terms of competitiveness and efficiency. However, there also is a potentially negative cost because this practice can raise information privacy concerns and may have legal, ethical, and strategic implications.

Information privacy has been defined as:

*the claim of individuals…to determine for themselves when, how, and to what extent information about them is communicated to others. (Westin, 1967, p. 7)*

Arguably, the Internet has had the biggest impact upon information privacy than any other technology. "As a place to eavesdrop, cyberspace is without peer in all of human history" (Wright, 1993). For instance, the Internet can facilitate the explicit or covert collection of consumer data using a variety of methods. Being a fully digital medium, a consumer's lifestyle and profile can therefore be reduced to "bits and bytes" (Attaran, 2000), revealing a "digital persona" (Gindin, 1997) and presenting a variety of violations of social norms, one of which is invasion of information privacy. However, in its defence, the Internet also is an enabler of other privacy functions, such as physical privacy, through the states of solitude, and to some extent anonymity. Nevertheless, consumer online privacy concerns relating to the information practices of commercial entities are at an all-time high in public consciousness. Many consumers feel that their lives and personal preferences are being used and exchanged without their knowledge or consent, which has compromised the growth of e-commerce and inhibited consumer trust toward online business.

**Information privacy** is therefore now a core consideration of business policy, not only in order that organisations meet consumer ethical obligations or the legal requirements of Australian data protection legislation, but also because there are sound commercial reasons which indicate that fair information practices can be beneficial to business. In fact, it is commonly acknowledged that **consumer privacy** concerns have resulted in direct and indirect negative impacts on the commerciality of the Internet. For instance, Jupiter Communications indicated in 1999 that consumer concerns about privacy would effect a loss of $18 billion in e-commerce revenue by 2002 (cited in Scholtz, 2001).

Clarke (1999) suggests that there are three implications of how consumer privacy concerns can affect the sale of goods and services in the Internet environment:

- the opportunity cost of lost sales
- a shift in demand back to off-line business channels
- the intangible cost of privacy to consumers

In addition, those companies who do not comply with consumer privacy demands could encounter negative publicity and a decrease in share price (The Economist Intelligence Unit, 2001).

Clearly, if consumers believe that their privacy concerns are being addressed, then this could be beneficial to e-commerce. Therefore, Attaran (2000) asserts that businesses could view privacy as a threat and act defensively, or treat it as an opportunity and be proactive in maximising the gains. Many companies choose the latter, however reactionary "firefighting" may not have the desired effect of reducing privacy concerns. For instance, Meridien Research (2002) suggests that a lack of understanding of privacy issues in the finance sector has led to misdirected spending toward technical solutions such as encryption, arguing that they do little to mitigate the risks to consumers and merely serve to increase the costs associated with good privacy practice.

In contrast, Culnan and Bies (1999) argue that proactive privacy strategies can serve as a market segmentation variable. On a practical level, fair information practices also make good business sense; Citigroup reported how they had saved money by only sending direct marketing material to people who indicated that they wanted it (The Economist Intelligence Unit, 2001); Culnan and Armstrong (1999) found that organisations gain business advantage through customer retention when they use procedures to protect individual privacy, while a further argument supporting

## Related Content