

## Chapter 7.16

# Privacy and Security in the Age of Electronic Customer Relationship Management

**Nicholas C. Romano, Jr.**  
*Oklahoma State University, USA*

**Jerry Fjermestad**  
*New Jersey Institute of Technology, USA*

### ABSTRACT

This article presents a value exchange model of privacy and security for electronic customer relationship management within an electronic commerce environment. Enterprises and customers must carefully manage these new virtual relationships in order to ensure that they both derive value from them and minimize unintended consequences that result from the concomitant exchange of personal information that occurs in e-commerce. Based upon a customer's requirements of privacy and an enterprise requirement to establish markets and sell goods and services, there is a value exchange relationship. The model is an integration of the customer sphere of privacy, sphere of security, and privacy/security sphere of implementation.

### INTRODUCTION

New technologies have fostered a shift from a transaction-based economy, through an Electronic Data Interchange (EDI) informational-exchange economy, to a relationship-based Electronic Commerce (EC) economy (Keen, 1999). We have moved from “*first order*” *transactional* value exchanges through “*second-order*” *informational* value exchanges to “*third-order*” *relational* value exchanges (Widmeyer, 2004). Three important types of EC relationships have been identified: between enterprises and customers (B2C); between enterprises (B2B); and between customers (C2C) (Kalakota & Whinston, 1996). Additional relationships between Governments (G2G), enterprises (G2B), and customers (G2C) have become more important as EC and e-government have matured, and legislation, regulation, and oversight have

increased (Friel, 2004; Reddick, 2004); however, these are not the focus of this article. Relational value exchanges have become central to success and competitive advantage in B2C EC, and it is here that we focus on privacy and security in the age of virtual relationships.

Both enterprises and customers must carefully manage these new virtual relationships to ensure that they derive value from them and to minimize the possible unintended negative consequences that result from the concomitant exchange of personal information that occurs when goods and services are purchased through EC. The need to manage these relationships has resulted in the development of Electronic Customer Relationship Management (e-CRM) systems and processes (Romano & Fjermestad, 2001-2002). E-CRM is used for different reasons by enterprises and customers. It is important to understand how and why both of the players participate in “*relational value exchanges*” that accompany the economic transaction and informational value exchanges of EC.

Enterprises use e-CRM to establish and maintain *intimate virtual relationships* with their *economically valuable* customers to derive additional value beyond that which results from economic value exchanges to improve return-on-investment (ROI) from customer relationships.

Customers obtain goods, services and information (economic value) through EC for purposes such as convenience, increased selection and reduced costs. EC requires customers to reveal personal information to organizations in order for transactions to be completed. The exchange of information between customers and organizations leads to the possibility of privacy violations perpetrated against the customer. It is the responsibility of the organizations to provide privacy policies and security measures that will not endanger customer trust.

In this article, we present a series of models “*sphere of privacy model*,” “*sphere of security model*,” “*privacy/security sphere of implemen-*

*tation model*,” and then integrate them into the “*relational value exchange model*” to explain privacy and security in the context of e-CRM, from the perspective of both customers and enterprises, to provide guidance for future research and practice in this important area. It is important for both customers and firms to understand each others’ vested interests in terms of privacy and security, and to establish and maintain policies and measures that ensure that both are satisfactorily implemented to minimize damage in terms of unintended consequences associated with security breaches that violate privacy and lead to relationship breakdowns.

The remainder of this article is structured as follows: First, we explain why privacy and security are critically-important issues for companies and customers that engage in EC, and the consequences that can result from failure to recognize their importance or poor implementation of measures to ensure both for the organization and its customers. Second, we define privacy and security and their interrelationship in the context of CRM. Third, we present our relational value exchange model for privacy and security in e-CRM.

## **Customer Relationship Management Privacy and Security: Who Cares?**

*The data contained within a CRM application is often a company’s most critical asset, yet because of the pivotal role this information plays in day-to-day business activities, it is also often the most vulnerable to security breaches and disruptions (Seitz, 2006 p. 62).*

Before we explain and define privacy and security in detail and present our models and the relational value exchange model, we will describe the costs associated with failure to understand these concepts and failure to effectively ensure that both are protected in terms that firms and customers can understand: dollars and lost customers.

20 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:  
[www.igi-global.com/chapter/privacy-security-age-electronic-customer/36824](http://www.igi-global.com/chapter/privacy-security-age-electronic-customer/36824)

## Related Content

---

### Organizational Readiness Assessment for Knowledge Management

Kaveh Mohammadi, Amir Khanlariand Babak Sohrabi (2010). *Strategic Information Systems: Concepts, Methodologies, Tools, and Applications* (pp. 1712-1728).

[www.irma-international.org/chapter/organizational-readiness-assessment-knowledge-management/36785](http://www.irma-international.org/chapter/organizational-readiness-assessment-knowledge-management/36785)

### Countering Cross-Site Scripting in Web-based Applications

Loye Lynn Ray (2015). *International Journal of Strategic Information Technology and Applications* (pp. 57-68).

[www.irma-international.org/article/countering-cross-site-scripting-in-web-based-applications/129788](http://www.irma-international.org/article/countering-cross-site-scripting-in-web-based-applications/129788)

### Strategic Considerations for Emergency Preparedness and Management: An Editorial Essay

Murray Turoff (2010). *International Journal of Strategic Information Technology and Applications* (pp. 1-7).

[www.irma-international.org/article/strategic-considerations-emergency-preparedness-management/39109](http://www.irma-international.org/article/strategic-considerations-emergency-preparedness-management/39109)

### Fuzzy Modelling for Integrated Strategic Planning for Information Systems and Business Process Design

Dimitris K. Kardarasand Bill Karakostas (2009). *Strategic Information Technology and Portfolio Management* (pp. 59-77).

[www.irma-international.org/chapter/fuzzy-modelling-integrated-strategic-planning/29739](http://www.irma-international.org/chapter/fuzzy-modelling-integrated-strategic-planning/29739)

### A Survey on Bio-Inspired Method for Detection of Spamming

Mebarka Yahlali (2017). *International Journal of Strategic Information Technology and Applications* (pp. 1-19).

[www.irma-international.org/article/a-survey-on-bio-inspired-method-for-detection-of-spamming/209457](http://www.irma-international.org/article/a-survey-on-bio-inspired-method-for-detection-of-spamming/209457)