Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2009 Proceedings

Americas Conference on Information Systems (AMCIS)

2009

An Integrated Model for Personalization, Privacy and Security in eCommerce

Jerry Fjermestad
New Jeresey Institute of Technology, fjermestad@adm.njit.edu

Nicholas C. Romano, Jr.
Oklahoma State University, nicholas.romano@okstate.edu

An Integrated Model for Personalization, Privacy and Security in e-Commerce

Jerry Fjermestad
School of Management
New Jersey Institute of Technology
Newark, NJ 07102
Fjermestad@adm.njit.edu

Nicholas C. Romano, Jr.
Management Science & Information Systems
Spears School of Business
Oklahoma State University
700 N. Greenwood Ave.
Tulsa, Oklahoma 74106-0700
Nicholas.romano@okstate.edu

ABSTRACT

Customers and firms must understand and appreciate one another's personalization, privacy and security (PPS) vested interests. Customers and enterprises should establish and maintain sufficiently well implemented policies, mechanisms and behaviors to minimize unintended consequences of security breaches that breakdown relationships. An integrated model of personalization, privacy and security from both the customer's and enterprises point of view is presented. The objective is to assure value exchange appropriate levels of vigilance in both security and privacy but not at the expense of the value derived from personalization.

Keywords: Personalization, Privacy, Security, Integrated Model for e-Commerce

Introduction

New technologies are stimulating the global economy's evolution from one that is paper and pencil transactional-based toward one that is electronic commerce (EC) relational-based (Romano and Fjermestad 2007). EC relationships include: between enterprises and customers (B2C); enterprises (B2B); and customers (C2C) (Kalakota and Whinston 1996). Relational value exchanges are central to B2C EC success and competitive advantage. We propose an approach to integrate personalization, privacy and security (PPS) complementarities to increase value exchange. Customer data is a critical asset in the digital economy that provides businesses with new opportunities to widen their market share, improve customer retention rates, personalize services and products and build strategic, intimate customer relationships (Dinev and Hart 2006). However, personalization cannot be achieved at the expense of security and privacy without

having detrimental effects on an enterprise and its customers. We develop a model that leverages the commonalities among these three import EC dimensions to provide guidance on how to maximize all three and provide value for customers and enterprises.

An important question is whether or not firms consider consumer privacy expectations when developing policies to protect different data elements. We assert that firms could benefit from consideration of consumer expectations and willingness to reveal information before they establish security policies, measures and mechanisms to protect different information types. This would enable them to focus resources on protecting data in a personalized fashion that would engender consumer trust and minimize potential losses from breaches (Culnan and Armstrong 1999).

Personalization

EC personalization involves informational and product/service exchanges between customers and enterprises to increase value for both (Karat, et al. 2003). Customers tailor their EC experiences through personal information disclosure along a continuum from invisible anonymous to individualized differentiation (see Table 1) (Culnan and Armstrong 1999; Blom and Monk 2003; Karat, et al. 2003). Customers exchange information for personalization capabilities that match their expectations. Enterprises provide customers with personalization options that range from no differentiation to highly individualized 1-to-1 personalization (Lee, et al. 2000; Poulin, et al. 2006) Customer derived personalization value is the difference between the perceived cost (risk) to reveal the information and the perceived benefits gained from the exchange (Karat, et al. 2003). Enterprise derived value is the difference between the cost to collect the information and the increased profits from sales of products and services less any costs associated with release information through a security breach. Customer value is a combination of the tangible product/service value and the intangibles of personalization and maintenance of privacy, security, and trust in the relationship (Karat, et al. 2003).

Personalization changes the functionality, interface, information content, or distinctiveness of a system to increase the personal relevance to an individual and is therefore directly related to privacy (Blom and Monk 2003).

Privacy

Informational privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent their personal information is communicated to others (Lee, et al. 2000). Results of several surveys that have analyzed consumer perceptions and business privacy breach management suggest that customers consider their Social Security Numbers to be very sensitive and are unlikely to reveal them; however they are readily willing to share email and postal addresses (Romano and Fjermestad 2007). Table 1 illustrates the parallel natures of customer criticality and enterprise responsibility in terms of personalization, privacy and security along a continuum. Customer criticality involves identity disclosure that ranges from uncontrolled (pseudonyonymous- surfing) to sensitive (SSN) and Privacy Information Disclosure. Enterprise responsibilities include assuring that customer personally identifiable information is available only to authorized people, has integrity and is kept confidential.

The requirement that customers submit personally identifiable information was found to be a primary factor that discouraged online shopping (Dinev and Hart 2006). Two thirds or more of customers who initiated online shopping procedures did not complete the transactions primarily due to a reluctance to reveal personally identifiable information (Dinev and Hart 2006). Two dimensions of privacy concern have been validated: customer personal information access (unauthorized use) and information abuse (theft) (Dinev and Hart 2006).

Security

Information assets must be protected to ensure business continuity, minimize business damage and maximize return on investments (ROI) and business opportunities. The goals of information security include confidentiality preservation, information asset integrity and availability control. Business value is maintained through effective implementation of policies that protect information assets from theft, manipulation and corruption. Security is risk management.

EC security requires having the necessary hardware, software, network controls, data encryption, policies and procedures in place for an enterprise to ensure that all consumer information is kept confidential, has integrity and is available only to those authorized for EC use.

Privacy and security are related in many ways. Enterprises and consumers must be prepared for increasingly hostile public networks. Enterprises (see table 1.) require the well known levels of perimeter, network, host, application and data security.

Table 1 Complementarities among identity, personalization, privacy, security and technology levels				
Customer Criticality		**Enterprise Responsibility**		
Identity Disclosure	**Privacy Information Disclosure**	**Personalization**	**Security Level**	**Privacy/Security Technology**
Invisible, Anonymous	**Uncontrolled** (pseudonyonymous- surfing) [Cookies off Cookies on TV show, favorite snack]	Non-Differentiation	Perimeter	Hardware/Software
Identified	**Registered** Full Name Email Address Single CC# Transaction Data	Micro	Network	Network Security
Associated Differentiation	**Personal** [Phone #; Income Demographics; Intentions Associations; Non-transactional-behavioral data]	Nano	Application	Process & Procedures
Individualized Differentiation	**Sensitive** [Transaction Data SSN Stored Credit Card #]	1 to1 Personalization	Data	Encryption

Table 1 illustrates the interrelationships between personalization, privacy and security across the levels of data, security strategy and technologies required to achieve appropriate vigilance. Our model implies that some information is less important to secure (i.e. email address) while other information, consumer's SSN, is absolutely critical to secure. Kuper (2005) suggests that enterprises initially focused on perimeter security, but as they learned from persistent attacks they moved from the edge down deeper, layer by layer, to secure the very data itself through encryption. Different technologies are required at different levels and the most crucial level, data, requires encryption to ensure that it is not released (Rust and Kannan 2003). Security at the perimeter level includes firewalls and malware prevention software that may offer enough protection for data that is less sensitive than data at the inner levels (Earp and Baumer 2003).

Both enterprises and customers must also consider risks, costs and possible consequences of personally identifiable information releases. Enterprises that foster a willingness in individuals to disclose personally identifiable information must consider collection of it as a "social contract" in which customers exchange money for products or services; and personal information for intangible benefits such as higher quality service described above (Culnan and Armstrong 1999) and personalization benefits. This is the value exchange. Customers maintain social contracts while perceived benefits exceed perceived risks. Information practices that address perceived risks result in positive customer experiences with a firm over time and this increases the customer's perception of the firm's trustworthiness; while practices that fail to address customer perceived risks can lead to negative customer experiences and decreased perceptions of trustworthiness.

Personalization Privacy and Security (PPS) Integration

Enterprises and customers must manage virtual relationships vigilantly to maximize value derivation and minimize unintended negative consequences from personally identifiable information exchanges. EC has led to electronic customer relationship management (eCRM) system and process development (Romano and Fjermestad 2007). Enterprises and customers use eCRM for different purposes that make it imperative for firms to understand how and why both players participate in "***value exchanges***" that accompany transactional and informational ones. Firms must understand what each customer values in PPS and personally identifiable information terms and then implement their policies, mechanisms and capabilities accordingly and in an adaptable, personalizeable fashion. Failure to consider the PPS values in terms of customer personally identifiable information disclosure preferences and criticality can result in lack of trust, damaged relationships and customer relationship termination.

Enterprises employ eCRM to manage "***intimate virtual relationships"*** with "***economically valuable"*** customers to derive value beyond that generated transactionaly to increase customer ROI. Customers acquire goods, services and information through EC and derive value from convenience, increased selection and reduced costs. Customers must reveal some personally identifiable information to organizations to complete transactions; however this leads to potential customer privacy violations. Organizations are responsible to provide effective privacy policies and security measures that don't endanger customer trust and yet maintain confidentiality, availability and integrity of PII at a level that matches the customer's preferences and criticality.

We present personalization, privacy and security "zone" models and integrate them into the "***value exchange model***" for eCRM from customer and enterprise perspectives to provide future research and practice direction in this important area. Figure 1 depicts PPS zones as spheres with the intersection of the different levels and concepts each contributes as a multi-colored polygon.

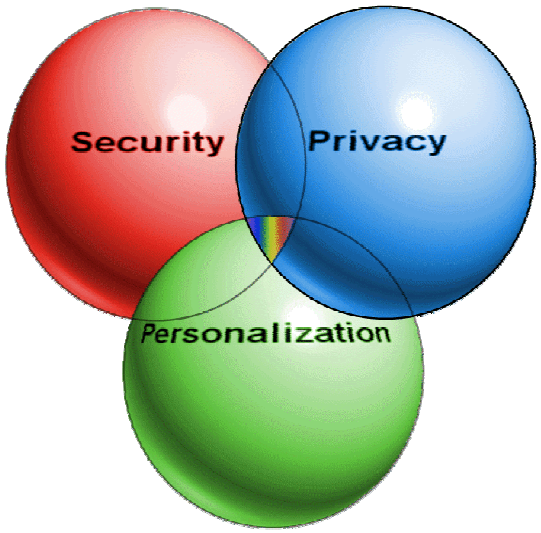

Figure 1. Personalization, Privacy and Security Integration

Value Exchange Model

Figure 2 presents the "***value exchange***" model from a process perspective that integrates customer and enterprise PPS zones. Enterprises must provide adequate security to attract and retain customers to succeed in EC. Customers will churn if they feel their privacy has been or may be compromised.

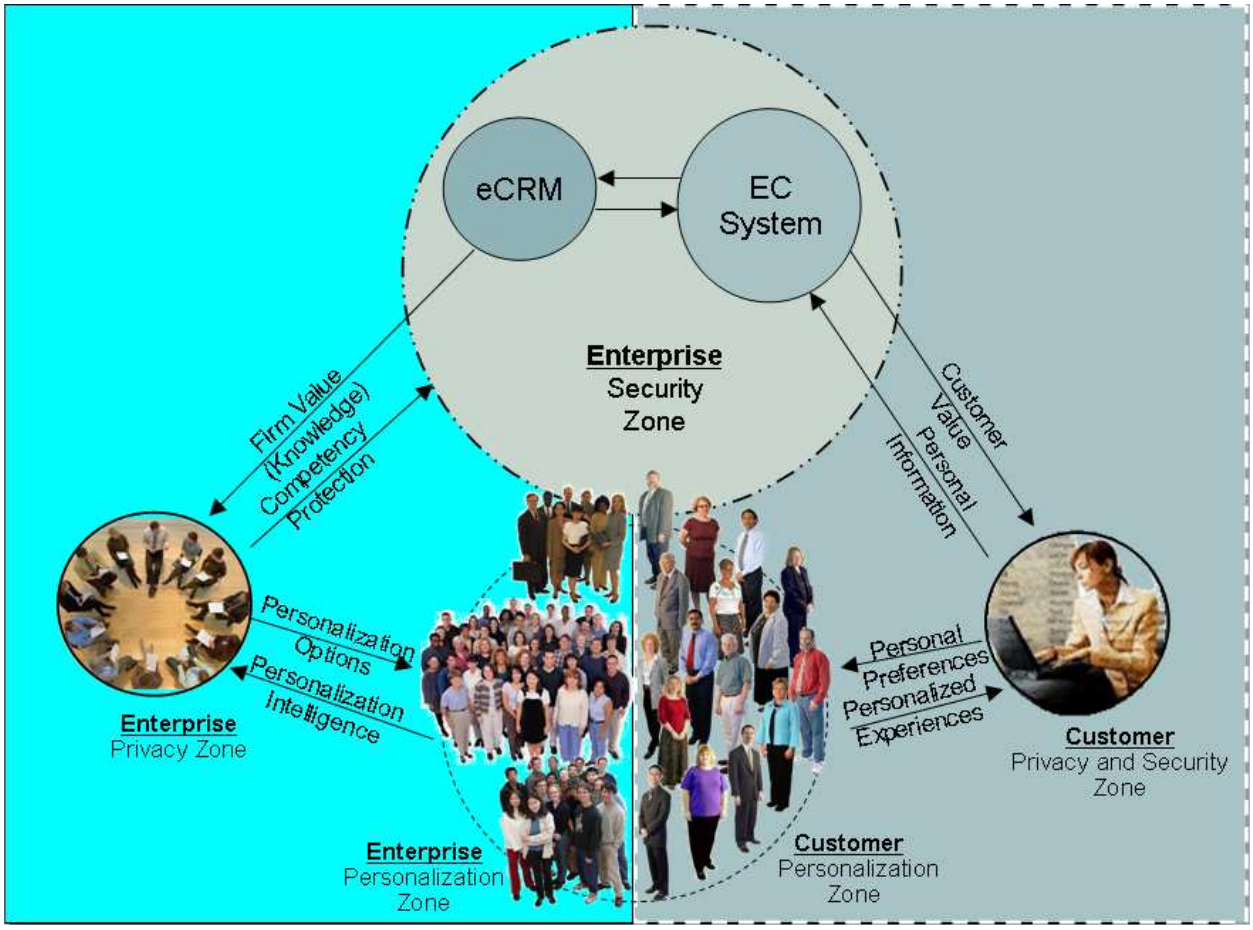

Figure 2 Value Exchange Model.

The relational value exchange model illustrates how customers obtain information, evaluate or buy products or services through the EC system and then provide required personally identifiable information from the customer privacy zone. Simultaneous with the customer's inquiry or purchase (customer's value exchange) the eCRM system is updated (enterprise's value exchange). The enterprise's privacy/security zone assurances and mechanisms should be adapted based upon detailed internal and external analysis of the overall EC system and all three zones for each customer if possible. This would provide personalization of security and privacy for customers at a level heretofore unheard of that provides the customer with direct input as to how the firm will control their personally identifiable information and how it is to be secured. We believe that this model can improve value to the firm by reducing losses when data breaches occur, increasing customer trust, reducing customer churn and providing a higher level of security that will lower breach occurrence.

Personalization Zone
The personalization zone in Figure 2 interacts with the privacy and security zones. The objective is to provide different levels of customer disclosure that map to the enterprise's responsibility to collect, maintain, and secure personally identifiable information.

Privacy Zones
The enterprise must ensure availability, integrity, and confidentiality of all personally identifiable information that it collects and simultaneously enable extensive customer personalization. The enterprise in return gains value from collection of customer intelligence through the eCRM system.

Security Zones
The enterprise security zone (Figure 2) contains the EC and eCRM systems which interact to provide value through customer knowledge to the enterprise. The enterprise provides defense from security attacks from the perimeter level to the data level through a firewall to encryption, respectively.

Implications for Enterprises and Customers
Enterprises collect additional personally identifiable information from online transactions to improve sales and service effectiveness (Rust and Kannan 2003). Virtual relationship management has become one of the most significant issues that confront modern enterprises in the information age. Companies must balance competing goals to maintain consumer privacy and security with increased sales of goods and services through advanced IS (i.e. eCRM, business intelligence, and data mining) and provision of personalization of customer interactions.

Consumer's desire benefits (i.e. reduced time and cost and personalization) from EC; but many remain unwilling to reveal data items such as SSN and credit card numbers to acquire these benefits. Consumers have already begun to demand that enterprises safeguard their personally identifiable information with the same vigilance that they do. The implications are that together consumers and enterprises must establish effective virtual relationships and communicate their PPS desires and act accordingly.

Conclusions and Implications for Research and Practice
This paper presents an integrated model of personalization, privacy and security for EC. Our work supports, enhances and extends Karat, et al.'s (2003) personalization value model that suggested personalization is a critical feature for EC. Personalization alone is not sufficient; but must be employed in concert with privacy and security to reap the benefits for both consumers and enterprises.

Our relational value exchange model defines consumer levels of personalization, privacy and security in terms of willingness to reveal different personally identifiable information items with the expectation that the enterprise will provide the required level of security. The deepest level

corresponds to any personally identifiable information that consumers are almost never comfortable revealing, such as their SSN or credit card numbers. Consumers will not reveal such information unless they completely trust the recipient. The next level (identifiable) corresponds to personally identifiable information that many consumers are very comfortable revealing, such as their email address or zip code. These levels correspond with the potential seriousness of consequences if consumers' information ends up in the wrong hands. Release of SSNs or credit card numbers can result in identity theft and monetary losses; while release of an email address may only result in additional spam email. Both are negative consequences; but clearly the former has potentially more serious consequences than the latter.

Our model represents the levels of security required by enterprises to support customer privacy ranging from the deepest internal data to the externally focused perimeter. The Perimeter level requires hardware and software (i.e. routers and firewalls) to provide a modest level of protection; while at the data level more secure technologies such as encryption or perturbation are required to ensure more vigilant protection of consumer privacy. The enterprise privacy/security zones are comprised of the firm's policies, mechanisms, and assurances. Many enterprises provide privacy and security policies statements on their websites that enable customers to determine how vigilantly the firm will protect their privacy before entering into any transactions; however we have yet to find any firms that ask customers at what level of security they prefer the firm to secure different types of personally identifiable information.

The integrated relational value exchange model is built upon the interrelationships among the three zones. The customer exchanges personally identifiable information to obtain value (reduced time and cost, and goods, services or information). The enterprise gains competitive advantage from the increase in their customer knowledgebase. Enterprises must provide competent protection for customers' personally identifiable information at various levels of vigilance that match the customer's privacy expectations to retain customers over time. In order to validate the model data on personalization, privacy and security from the major social-networking and e-commerce sites.

Customers and data about them are a major asset for many enterprises. The relational value exchange model illustrates that enterprises must maintain the delicate balance between appropriate use of customer data for competitive advantage through personalization and vigilant protection of that same data through security and privacy mechanisms. Customers are only a mouse click away from an enterprise's competitors. Customers also have responsibilities to be careful and vigilant when they choose to reveal personally identifiable information to receive EC benefits in exchange. They must provide accurate and reliable information and also verify that a firm is trustworthy and employs adequate security levels before they reveal any personally identifiable information. They should also think carefully about what information is required for a given transaction and provide only necessary details. This enables customers to make more informed queries and purchases and at the same time helps the enterprise market to them and to other customers more effectively through mechanisms such a recommender systems, cross selling and preference discounts. Firms that appropriately secure information that consumers do not want revealed while also providing meaningful personalization will have a competitive advantage over those that do not. Personalization without security and privacy will in the long

run cause customers to abandon their relationships with an enterprise. We assert that enterprises must integrate personalization, privacy and security to succeed in EC.

REFERENCES

Blom, J. O. and A. F. Monk (2003). "Theory of personalization of appearance: why users personalize their PCs and mobile phones." Human Computer Interaction 18(3): 193-228.

Culnan, M. J. and P. K. Armstrong (1999). "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation." Organization Science 10(1): 104-115.

Dinev, T. and P. Hart (2006). "Privacy Concerns and Levels of Information Exchange: An Empirical Investigation of Intended e-Services Use." E-Service Journal 4(3): 25-59.

Earp, J. B. and D. Baumer (2003). "Innovative web use to learn about consumer behavior and online privacy." Communications of the ACM 46(4): 81-83.

Kalakota, R. and A. B. Whinston (1996). Frontiers of electronic commerce. New York, NY, USA, Addison Wesley Publishing Co.

Karat, C. M., C. Brodie, et al. (2003). "Personalizing the user experience on ibm.com." IBM Systems Journal 42(2): 686-701.

Kuper, P. (2005). "The state of security." IEEE Security and Privacy 3(5): 51-53.

Lee, C. H. S., A. Barua, et al. (2000). "The complementarity of mass customization and Electronic commerce." Economic Innovation and New Technology 9(2): 81-109.

Poulin, M., B. Montreuil, et al. (2006). "Implications of personalization offers on demand and supply network design: A case from the golf club industry." European Journal of Operational Research 169(3): 996–1009.

Romano, N. C. Jr. and J. Fjermestad (2007). "Privacy and Security in the Age of Electronic Customer Relationship Management." International Journal of Information Security and Privacy 1(1): 85-106.

Rust, R. T. and P. K. Kannan (2003). "E-service: a new paradigm for business in the electronic environment." Communications of the ACM 46(6): 37-42.

Volonino, L. and S. R. Robinson (2004). Principles and Practice of Information Security. Upper Saddle River, NJ, USA, Pearson Prentice Hall.