

Internet Privacy in E-Commerce: Framework, Review, and Opportunities for Future Research

J. Efrim Boritz¹, Won Gyun No², and R. P. Sundarraj^{2,3}

¹School of Accountancy, ²Department of Management Sciences, University of Waterloo,

³College of Business and Economics, Qatar University

¹jeboritz@uwaterloo.ca, ²wgno@uwaterloo.ca, ²rsundarr@engmail.uwaterloo.ca, ³rsundarraj@qu.edu.qa

Abstract

Increased Internet traffic and the sophistication of companies in tracking that traffic have made privacy a critical issue in electronic commerce (e-commerce). This has spawned a number of research works addressing Internet privacy from the perspectives of three main stakeholders – customers, companies and governments, as well as the interactions among them. The purpose of this paper is to analyze the extant studies and develop an understanding of the relationships among them. Accordingly, we review the research on Internet privacy in e-commerce that has been conducted in the fields of information systems, business, and marketing. We develop a framework for classifying the studies, review key findings, and identify opportunities for future research.

1. Introduction

The Internet, especially the Web, enables companies to engage in e-commerce activities as well as to collect, store, and exchange personal information obtained from visitors to their websites. Companies can use that information to gain greater insights into customers' behaviour, support marketing strategies, and meet their needs. However, companies can also intrude on customers' and other visitors' privacy, and this is becoming one of the main concerns of online shoppers [1, 2] as documented by several public opinion polls [3-5]. In response to customer concerns, e-commerce companies are paying increased attention to privacy [6, 7]. Their main challenge is to balance the competitive advantages provided by their use of personal information with the risk of alienating customers who are concerned about potential abuse of their personal information [8].

The major objective of this paper is to review the literature on Internet privacy in order to develop an understanding of the relationships among extant research studies that have been conducted in the fields of information systems, business, and marketing over the past decade. We use a comprehensive framework for classifying the studies, reviewing key findings, and identifying opportunities for future research.

The paper is organized as follows. First, we introduce a privacy research framework based on our literature

review. Next, we discuss gaps in our current understanding of Internet privacy which represent future research opportunities. We conclude with a brief summary of our review.

2. Privacy Research Framework

We reviewed 88 studies conducted between 1995 and 2006 addressing Internet privacy in an e-commerce and developed a framework for classifying and relating the research works that we examined.¹ We decided to restrict our review to journal articles only and thus exclude studies published in proceedings, book chapters or working papers. We also limit our review to e-commerce and exclude studies that investigate privacy in the context of health, social and political and similar non e-commerce settings because the relationship between users and organizations in these contexts significantly differs from that of customers and e-commerce companies.²

A privacy research framework (see Figure 1) was developed to classify prior studies and to identify research opportunities. The framework is organized around three main entities involved in Internet privacy: customers, companies, and governments.³

Customers are the main source of personal information. They may adopt privacy-enhancing actions (e.g., avoiding disclosure of information or providing false information) and/or privacy technologies (e.g.,

¹ The studies were collected through databases such as ProQuest and The ACM Digital Library, as well as through several search engines such as Google Scholar. An annotated bibliography of the 74 key studies is available at <http://webprivacy.uwaterloo.ca/bibliography.pdf>.

² For example, the personal information asked of patients in a hospital is more sensitive information (e.g., medical records such as HIV/AIDS) than that of customers in an online store. Furthermore, patients have limited opportunity to provide false information to the hospital while customers in an online retail store can easily fabricate their information.

³ Three main entities were identified based on the analysis of each study's research hypotheses. The results indicated that the hypotheses of 88 studies mainly examined three entities. That is, among 88 studies, 52 studies had hypotheses with respect to customer (e.g., how customers' privacy concerns influence their behaviour), 27 studies had hypotheses related to company (e.g., whether companies post privacy disclosures and the disclosures reflect fair information practices), and 14 studies had hypotheses regarding government (e.g., whether regulatory approaches influence companies' privacy practices.). Furthermore, several studies addressed three entities as major stakeholders involved in Internet privacy [e.g., 9, 10, 11].

privacy software) to protect their privacy. Their privacy concerns influence companies' privacy practices as well as government regulation. Companies are the biggest consumers of personal information. They use personal information to deliver products, study customer profiles, and offer personalized services. In response to customers' increasing privacy concerns, they may implement privacy protections such as privacy policy statements and privacy seals, and their privacy practices influence customers' privacy concerns and government regulations. Governments play two important but conflicting roles related to Internet privacy. Governments may seek to protect citizens' privacy but, at the same time, may need to use citizens' personal information to monitor and control individuals. To protect customer privacy, governments may promote privacy laws, oversee the implementation of these laws, educate the public about privacy issues, and encourage industry self-regulation. Such government activities affect customers' privacy concerns and companies' privacy practices.

The framework presented in Figure 1 shows all possible interactions between the three entities as well as the relationships between each entity.⁴ In the next section, we use this framework to discuss relevant literature and address directions for future research.⁵

3. Review and Research Opportunities

3.1. Customer Perspective

Public opinion polls have revealed a general desire among Internet users to protect their privacy [e.g., 3, 12, 13, 14]. Several studies have investigated three key privacy issues 1) what are the major dimensions of customers' privacy concerns, 2) what are the antecedent factors affecting such concerns, and 3) what are the consequences of customers' privacy concerns.

3.1.1. The Dimensions of Customers' Privacy Concerns. Prior literature has examined whether individuals' general attitudes about online privacy are constant or differ depending on the situation [e.g., 15, 16, 17]. Westin proposed a typology of individuals' concerns about privacy [17, 18]. He argued that individuals can be categorized into three groups: privacy fundamentalists, privacy unconcerned, and privacy pragmatists. The privacy fundamentalists are defined as being extremely

concerned about the use of their personal information and are unwilling to provide their information. Individuals in the privacy unconcerned group do not take their privacy into consideration and are willing to provide their personal information. The privacy pragmatists are concerned about their privacy, but less than privacy fundamentalists.

Dhillon and Moores [19] examined major issues that could point to individuals' potential concerns with respect to Internet privacy. Based on the brainstorming results of two panels (11 experts and 16 IS executives), they identified the five most important Internet privacy concerns (e.g., companies should eliminate spam and not sell personal information). Dhillon and Moores also identified eighteen means to address these fundamental Internet privacy concerns (e.g., enact stronger laws to protect consumer privacy and make spam illegal).

Other studies investigated differences in privacy concerns across cultures and countries. For instance, Milberg et al. [20] examined whether nationality, information privacy regulatory approaches, and cultural values influence the level of information privacy concerns. Their survey of approximately 900 members of the Information Systems Audit and Control Association (ISACA) in roughly 30 countries found that the overall level of privacy concern for personal information varies across countries; for instance, individuals from Thailand have the lowest level of privacy concern, and those from Canada have the highest privacy concern.

3.1.2. Antecedents of Customers' Privacy Concerns. Two frequently-mentioned factors influencing customer's privacy concerns are: the type of information (e.g., demographics versus financial data) and the use of information (e.g., secondary use and sharing information with third-parties). Phelps, Nowak, and Ferrell [21] examined the relationship between customers' privacy concerns and their behaviour, as well as factors affecting their privacy concerns. Based on mail survey responses of 556 U.S. customers, they showed that the level of customers' privacy concerns is affected by the type of information requested, the way companies use personal information, and customers' desire for information control. From an online survey of 381 U.S. online users, Ackerman, Cranor, and Reagle [16] found that there were significant differences in customers' comfort levels across various types of information. They also found different levels of acceptance of persistent identifiers (i.e., cookies) depending on the purpose. Lastly, they found several important factors related to customers' decisions about information disclosure including the sharing of information with other companies, the use of information in an identifiable way, the kind of information collected, and the purpose for which the information was collected.

⁴ The various interactions and relationships in the framework are identified from prior studies. While each study has its own unique focus, the studies can collectively provide an extensive perspective on Internet privacy. Admittedly, this was a subjective process and may oversimplify the scope of some prior studies.

⁵ For the sake of brevity, we discuss only a few specific studies which are representative of the areas discussed in similar research.

Other researchers investigated the relationship between privacy concerns and other factors; for example, gender, [22-25], age [15, 22, 24, 26, 27], income level [23, 24], and education [15, 21, 23]. For instance, Sheehan's [15] analysis of an email survey of 889 U.S. online users indicated that online users' privacy concerns are influenced by their age and their level of education (e.g., well educated users tend to have higher level of privacy concern than less educated users). Sheehan [25] found that women are more concerned than men about privacy, but men are more likely than women to change their behaviour to protect their privacy.

3.1.3. Consequences of Customers' Privacy Concerns. Having examined the dimensions and antecedents of customers' concerns, we now turn to the consequences of privacy concerns. Sheehan and Hoy [28] found that U.S. online users are less likely to register for a Web site when their privacy concerns are high. In addition, as privacy concern increased, online users were more likely to provide incomplete information, to notify Internet Service Providers (ISPs) about unsolicited email, to request their name removal from mailing lists, and to send negative messages to those sending unsolicited email. Milne and Boza [29] examined the relationship between privacy concerns and trust. Based on the mail survey of 1,508 U.S. respondents, they showed that consumers' perceptions of trust and level of concern about privacy vary by industry, and that trust is negatively related to privacy concerns.

Some studies have addressed the interrelationships between customer behaviour and factors such as customers' beliefs about privacy, attitude, and intention. For instance, Lwin and Williams [30] developed a conceptual model to investigate a customer's behaviour in providing false information online. They used two theories: Multidimensional Developmental Theory of Privacy (MDTP) and Theory of Planned Behaviour (TPB) with an additional factor of perceived moral obligation. They conducted an empirical study to test the TPB portion of the conceptual model using a mail survey of 341 U.S. online users. Their results indicated that attitudes, perceived behavioural control, and perceived moral obligation influence customers' behaviour to provide false information, while subjective norm (the perceived social pressure) does not. Similarly, George [31] investigated whether privacy beliefs and trustworthiness of the Internet influence purchasing behaviour, as described in TPB. Based on a survey of 193 undergraduate students, he found that individuals' beliefs about trustworthiness of the Internet have a positive effect on their attitudes toward buying online, which in turn positively affects their purchasing behaviour.

3.1.4. Research Opportunities in Customer Perspective. The research works surveyed so far suggest

that consumers appear concerned about their privacy, and that such concerns may have negative effects on online transactions that could jeopardize the proliferation of e-commerce. While this literature contributes to our understanding about several privacy issues, there are several additional research opportunities:

- While a number of dimensions of privacy concern have been identified, which ones are most important to customers? Which of the fair information principles proposed by government are most central to consumers? (Suggested by Caudill and Murphy [32])
- Individuals are often willing to exchange their privacy for certain rewards [7, 32]. To what extent are customers willing to provide their personal information for rewards such as discount coupons and free gifts and do they perceive such tradeoffs as fair?
- Do individuals' privacy concerns actually cause individuals to engage in behaviour to protect their own online privacy? (Suggested by Sheehan & Hoy [28])
- Customers' privacy concerns differ across cultures. What makes individuals concerned about their privacy? Do the concerns exist because individuals in various cultures have different perceptions about their privacy?

3.2. Company Perspective

Customers' growing concerns about privacy have put pressure on e-commerce companies to develop customer-focused privacy practices [6-8]. The studies that we reviewed fall into two categories: those that describe companies' privacy practices and those that investigate the factors affecting those privacy practices.

3.2.1. Companies' Privacy Practices. Liu and Arnett [33] analyzed 497 Web sites of the Fortune 500 and found that approximately 50 percent of these Web sites provide a privacy policy. They found no industry differences in the use of privacy policies to address customer's privacy concerns. Although most of them address opt-out, access/correction, and internal privacy protection, many Fortune 500 Web sites failed to cover all four privacy principles (i.e., Notice/Awareness, Access/Participation, Choice/consent, and Security/Integrity) recommended by the US Federal Trade Commission (FTC) as representing fair information practices.

Milne and Culnan [34] studied the changes and trends in voluntary privacy disclosures by analyzing four Web surveys conducted between 1998 and 2001, and found that the number of privacy disclosure statements increased over time, and also that the most popular sites had posted more privacy disclosures than their counterparts. Furthermore, they found a significant increase in disclosures about information collection, revealing information to third-parties, and choice. Gurau, Ranchhod, and Gauzente [35] examined the privacy

policies among three countries, and based on a Web site survey of French (93), UK (106), and US (92) Web sites they showed that there are differences among countries with respect to the form of data requested and information provided in the privacy policy disclosure. For example, the US sites provide more information about security of information than the French or British sites. While French sites collect data during transactions, the US sites are more focused on intrusive approaches such as data requests through pop-up windows.

3.2.2. Antecedents of Companies' Privacy Practices. Several studies have attempted to go beyond describing companies' privacy practices to identify the antecedents for those practices. For instance, Sarathy and Robertson [36] introduced a model of factors influencing privacy strategy which incorporates the environmental context, ethical perspective, and firm-specific considerations. According to the model, a company's privacy strategy is affected by its environmental context such as national history, culture, and existing and pending legislation. It is also influenced by the ethical frame of the firm and top management as well as firm-specific factors including information intensity of the business, age and experience of the firm, and corporate culture. Further, cost-benefit analysis plays a role in the privacy strategy adopted by the company. That is, the company adopts different strategies depending on the analysis of economic benefits (e.g., meeting customer needs and relationship management) and cost of compliance (e.g., the cost of granting access to data). Although this model was not empirically tested, Sarathy and Robertson used it as a framework to help firms develop a strategy for addressing privacy concerns.

3.2.3. Research Opportunities in Company Perspective. Research opportunities related to a company perspective include:

- While prior studies have examined stated privacy policy disclosures, research on the actual privacy practices of e-commerce companies is needed. For example, to what extent do companies' data collection activities comply with their stated privacy policies?
- Are the privacy policy statements currently disclosed by companies effective in dealing with consumer knowledge and control questions?
- How do companies' privacy practices affect short-term and long-term relationships with their customers?
- What are the differences between Web sites that post privacy policies and sites that do not? Do the sites with privacy policies share common characteristics? Do the Web sites with the best privacy disclosures have anything in common? (Suggested by Culnan [6])

3.3. Government Perspective

In this section, we review studies pertaining to government regulation of privacy, including regulation approaches and factors influencing regulation.

3.3.1. Regulation Approaches. Caudill and Murphy [32] discussed online privacy conceptually and summarized regulations on privacy in the United States. Then, they proposed ethical standards that need to be addressed in corporate ethical policy and public policy. Smith [37] investigated the differences in privacy approaches in the U.S. and Europe, identifying problems with the U.S. privacy approach such as the limitations of a voluntary approach to address privacy concerns and the secondary uses of personal information. Laudon [38] examined individual privacy and the market for personal information and discussed several problems of current privacy protection based on "fair information practices" proposed by the U.S. Federal Trade Commission. For instance, according to Laudon, fair Information practices leave individuals little or no control over the post-collection use of personal information (e.g., right for review and challenge). As one possible solution for such problems, he proposed a National Information Market (NIM) in which personal information could be bought and sold in a market, enabling individuals to receive fair compensation for the use of information about themselves.

Also, the privacy issues in e-government have been examined [e.g., 39, 40]. For instance, Belanger and Hiller [39] proposed a conceptual framework for e-government which incorporates the complexities of e-government by recognizing the various constituents (i.e., individuals, business, employees, and government) and the five e-government implementation stages (i.e., information, two-way communication, transaction, integration, and participation).

3.3.2. Factors Influencing Government Regulation. Milberg et al. [20] examined the interrelation among nationality, cultural values, and information privacy regulatory approaches. By analyzing survey responses from approximately 30 countries, they showed that the amount of government involvement (e.g., voluntary control, data commissioner, and regulation) is related to the cultural values identified by Hofstede [41] – uncertainty avoidance, individualism/collectivism, and power distance. That is, countries with a higher level of uncertainty avoidance or power distance tend to have higher levels of government involvement (e.g., regulation), but those with high individualism have less government involvement in regulating information privacy (e.g., voluntary control). Similarly, Milberg, Smith, and Burke [10] conducted a survey of 595 internal auditors from 19 different countries and demonstrated that countries with a higher level of power distance,

masculinity/femininity, and individualism/collectivism each tend to have less government involvement, but countries with high uncertainty avoidance have higher levels of government involvement in the regulation of information privacy practices.

3.3.3. Research Opportunities in Government Perspective. Previous studies on Internet privacy from a government perspective leave a number of gaps:

- Currently, each country adopts different fair information principles to manage privacy issues (e.g., PIPEDA from Canada and FTC principles from U.S.). It would be useful to examine whether a set of universal core privacy principles exist across countries. Such research could contribute to understanding privacy regulation approaches in various countries as well as developing international privacy standards.
- What factors influence government approaches to regulating privacy practices? Potential factors to investigate include economic trends (e.g., dot.com bubble), national security (e.g., the events of September 11 in U.S.), and the transfer of personal information across borders (e.g., U.S. and EU safe harbour).
- As e-government becomes more sophisticated, it requires increasing degrees of integration. This could raise privacy issues due to the exchange or disclosure of more sensitive personal information. Research is needed on what steps need to be taken and by whom to ensure that the government–public relationship is operated fairly in terms of the use and protection of personal information.

3.4. Customer–Company Interaction

Generally, in e-commerce, a customer searches one or more sites on the Internet, finds a suitable e-commerce site, and places an order. During this process companies have many opportunities to collect and use personal information. This personal information can be used to provide better services through customization; however, it may also be misused. Each company decides upon the degree of information that it will collect and use; however, companies' privacy practices are influenced by customers' privacy concerns and behaviour, as well as influencing these concerns and behaviour through privacy policy statements posted on company Web sites and related privacy practices. Two types of customer-company interactions have been studied: (1) the interaction between a company's privacy practices and customer behaviour, and (2) the interaction between a company's characteristics and customer behaviour.

3.4.1. Company's Privacy Practice and Customer Behaviour. Whether or not customers provide their personal information can be influenced, in part, by the

quality of companies' privacy practices (i.e., privacy policy disclosures or privacy seals). Palmer, Bailey, and Faraj [42] examined how firms use trusted third parties (i.e., privacy seals) and privacy statements to build trust on their Web sites. By analyzing a Web site survey of 102 publicly-traded U.S. companies, they showed that privacy statements and trusted third-party involvement can improve customers' trust. That is, by posting a privacy policy statement on their Web sites, companies can reduce their customers' perceived privacy concerns about providing personal information.

Miyazaki and Krishnamurthy [43] found that a firm's participation in a privacy seal program favourably influences customers' perceptions of a Web site's privacy policy and the level of information disclosure. In contrast, Moore's [44] survey of 143 students found that few of them consider privacy seals as important in deciding to trust a Web site. Moores also found that although participants have a basic understanding about privacy seals and about the function of seals, quite a number of them did not know how a seal is obtained and failed to recognize non-genuine privacy seals.

Earp et al. [45] studied whether there is a gap between the information provided in companies' privacy policy statements and the information that users want to know about Internet privacy. By analyzing privacy policy statements on 50 U.S. companies' Web sites and conducting a survey of 827 U.S. Internet users, they showed that the information addressed in Web site privacy policy statements does not fully provide the information that users want to know. That is, the three information items most frequently included in privacy statements are 1) security 2) how data is collected, and 3) consent about information collection. But users are most concerned about 1) transfer or sharing of their personal information, 2) information about what information is collected and how it is used, and 3) how organizations store and maintain their personal information.

3.4.2. Company Characteristics and Customer Behaviour. Several researchers have explored whether or not company characteristics such as the trustworthiness of their Web site affect customers' willingness to provide personal information as well as purchasing behaviour. Earp and Baumer [26] studied consumers' behaviour and online privacy. By conducting an online survey of 415 U.S. respondents, they showed that the type of Web site (i.e., retail, financial, or medical/health) and brand status (e.g., well-known versus unknown Web sites) influence individuals' willingness to provide information. Swaminathan, Lepkowska-White, and Rao [46] also examined factors affecting online purchasing behaviour. Their analysis of 428 email responses indicated customers' online purchasing behaviour is influenced by three factors: the perceived reliability of a vendor, the

convenience of placing an order and contacting the vendor, price competitiveness and access to information.

3.4.3. Research Opportunities in Customer – Company Interaction. Research opportunities related to this interaction include:

- Do companies benefit by addressing customers' concerns about privacy? Companies posting well-developed privacy policies might affect customers' propensity to visit their Web sites often and to transact more. Therefore, are companies more likely to address privacy concerns if they gain benefits through building strong customer relationships?
- The studies on customers' behaviour usually used a survey methodology to measure self-reported privacy behaviour, rather than actual behaviour. Are individuals' stated actions/intentions consistent with their actual behaviour [47, 48]?
- Currently, many companies develop and disclose a privacy policy statement in their Web sites. It is expected that reading such privacy policy statements can reduce customers' perceived privacy risks associated with the disclosure of their personal information. However, it is not clear how customers perceive the privacy policy statement and whether the statement successfully addresses their concerns.
- While seals are meant to raise consumer confidence in a company's Web site, the fact is that they are not popular among companies, nor is it clear how customers perceive privacy seals. Interesting questions include: Are there specific situations in which seals are perceived as useful? Are there differences in characteristics of companies participating in seal programs and those not participating in seal programs?

3.5. Customer – Government Interaction

Customers express their privacy concerns through public opinion, and governments respond to customers' privacy concerns by way of regulations. However, only a few studies have examined this relationship.⁶

3.5.1. Customer's Privacy Concern and Government Approach. Sheehan and Hoy [49] examined whether the underlying dimensions of customers' privacy concerns are addressed in FTC privacy principles. By conducting an e-mail survey of 889 U.S. online users, they showed that many underlying dimensions of customers' privacy

concerns are addressed in the principles. However, they also found that two possible dimensions related to customers' privacy concerns are not addressed in FTC privacy principles: 1) the exchange of information for compensation and 2) users' established relationships with online entities (i.e., familiarity with entity).

3.5.2. Research Opportunities in Customer – Government Interaction. Few studies have examined the relationship between customers and governments. Promising research opportunities include the following:

- Customers' concerns about privacy are influenced by several factors and keep changing, so as to keep up with social and technical changes. However, it usually takes a considerable amount of time for a new regulation to be effective. Can government regulation itself satisfy customers' privacy concerns and is it an effective approach to protect customers' privacy?
- Do customer concerns influence government regulation approaches? How do such concerns affect governments' approaches?
- Various regulations have been enacted to protect individuals' privacy across countries: for example, Health Insurance Portability and Accountability Act (US), Personal Information Protection and Electronic Documents Act (Canada), and Data Protection Directive (EU). Are customers are aware of the legislation and what is the impact of government regulation on customers' privacy concerns and their behaviour?

3.6. Company – Government Interaction

While government regulation is affected by customers' privacy concerns, it could also be influenced by companies' practices and industry self-regulation.

3.6.1. Company's Privacy Practice and Government Approach. Milberg, Smith, and Burke [10] found that high levels of privacy concern are associated with greater preferences for strong laws over self-regulation and that regulatory approach is associated with both the corporate privacy management environment and regulator preferences. That is, countries with higher levels of governmental involvement tend to have tighter corporate privacy environments (e.g., strong corporate privacy policies and practices, and senior management attitudes) and greater regulator preferences (e.g., preference for government regulation over corporate self-management).

Johnson-Page and Thatcher [50] studied privacy policy discourses on Business to Customer (B2C) Web sites in nine countries (US, Canada, Germany, Hungary, UK, China, Singapore, Brazil, and Venezuela) across five industries (newspapers, online retailers, Internet service providers, banking and financial services, Internet service

⁶ Although most studies addressed in this section did not examine a particular casual relationship (e.g., how customer concerns influence government regulation approaches), they were classified into this section. Since such studies examined the relation between customer and government, they are somewhat akin to the interaction between customer and government.

providers, and telecommunications). The analysis of 149 B2C Web sites indicated that privacy policies are more commonly found in countries which establish a market economy with clear business regulations and in which customers not only have more access to the Web, but also have more experience in using it.

3.6.2. Research Opportunities in Company – Government Interaction. Regulations must balance companies' personal information needs and customers' concerns about privacy requires taking into account companies' information gathering activities and the context in which the information is used. Although some researchers have examined the relationship between company and government, there are several potential research opportunities:

- For most companies, regulation will form the basis for developing a privacy policy. Do companies provide the privacy protections required by governments?
- It is expected that existing and pending regulations influence companies' privacy practices. To what extent do recently enacted and pending privacy regulations impact Internet privacy?
- Are companies' privacy practices in one country different from those of other countries due to various regulation approaches? The differences in privacy regulations may pose a significant regulatory challenge for companies looking to multiple markets around the world. Do companies with business units in less strict regulation countries have less comprehensive privacy practices than for units in strict regulation countries?

3.7. Customer – Company – Government Interaction

Internet privacy involves interactions among customers, companies, and governments. Customers provide personal information, and companies collect and use the information for marketing purposes or customizing their services. Customer concerns about potential abuse of privacy lead to governmental involvement through laws or self-regulation, which in turn influences companies' privacy practices. Studies that have examined this relationship are rare. Culnan and Bies [9] is one study that addressed relationships among customer, company, and government. In their research, Culnan and Bies discussed consumer privacy from a justice perspective and explained three types of justice factors related to consumer privacy (i.e., distributive justice, procedural justice, international justice). They argued that the violation of these factors may lead to consumers' privacy concerns. In addition, Culnan and Bies explained fair information practices in justice concerns and three implementation alternatives for implementing fair information practices (government

regulation, self-regulation, and technological solutions). Research in this area is just beginning to emerge.

3.8. Other Factors

While most prior research has focused on privacy issues among customers, companies, and government, some attempts have been made to address privacy issues in terms of new technologies and social or economical perspectives.⁷ For example, Kenny and Korba [51] argued that Digital Rights Management is a potential tool for the management of personal information. Cranor, Arjula, and Guduru [52] examined the role of the Platform for Privacy Preferences (P3P) in customers' privacy behaviour. The AT&T Privacy Bird⁸ was used as a P3P user agent. Based on an email survey of 331 AT&T Privacy Bird users, they showed that the use of the AT&T Privacy Bird guides users to read privacy policies more often, as well as protects their privacy more proactively.

Other researchers address privacy issues in social or economical perspectives [e.g., 53, 54] and the role of the accounting profession in privacy assurance services [e.g., 55, 56, 57]. For instance, Rust, Kannan, and Peng [54] studied the erosion of privacy on the Internet. By using a simple economic model with assumptions that there is no government intervention and privacy is left to free-market forces, they showed that over time, the amount of privacy will decline, and customers will bear more expenses to maintain their privacy. Hunton et al. [56] investigated the effect of e-commerce assurance on financial analysts' earnings forecast and stock price estimates. By analyzing a survey of 37 financial analysts and conducting an experiment of 87 analysts, they found that financial analysts issue more positive earnings forecasts and stock-price estimates when an e-commerce company acquired e-commerce assurance and vendor- and outcome-based risks were high (i.e., the company is unknown and the perceived outcome risk from transactions is high).

Several research opportunities in this area include:

- How do customers perceive new privacy protection technologies? Currently, a variety of technology tools are being developed to help customers protect their privacy. However, there is no reliable evidence indicating that privacy protection technologies improve user privacy. How do customers perceive privacy

⁷ The studies addressed in this section are placed outside the model as other factors because they are qualitative research works which address the impact of new privacy protection technologies, the economical aspects of privacy, and the role of privacy assurance services.

⁸ The AT&T Privacy Bird is software designed to help Internet users stay informed about the privacy policies of Web sites they visit. It reads privacy policies written in Platform for Privacy Preferences (P3P) and informs the Web site's policies by displaying a bird icon. That is, a green bird icon is appeared for Web sites that match users' privacy preference, but a red bird icon is shown for Web Sites that do not.

protection technology tools and do such tools can reduce customers' privacy concerns?

- What are the short-term and long-term consequences of loss of privacy to individuals and to society as a whole?

3.9. Summary and Conclusion

The spread of e-commerce and related technologies has enabled and encouraged companies to collect and store customers' personal information. The privacy of accumulated customer information is a growing concern for customers, companies, and governments. In this paper, we reviewed prior research on Internet privacy in the fields of information systems, business, and marketing. Based on our review of 74 key studies, we introduced a privacy research framework based on all possible interactions between customers, companies and governments. Figure 1 and Table 1 provide a summary of our review.

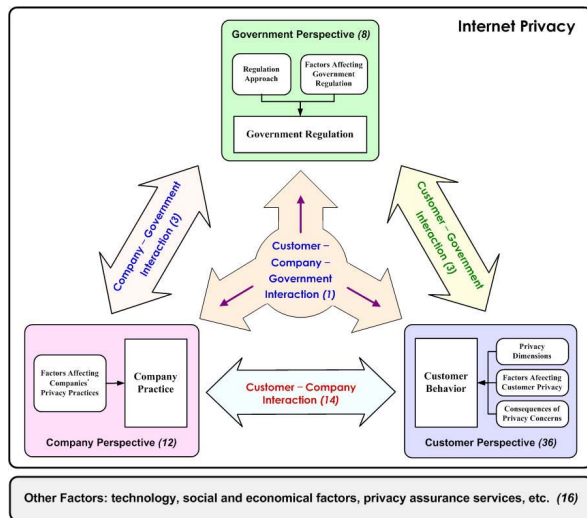


Figure 1. Privacy Research Framework

Figure 1 depicts eight major research areas in Internet privacy, and table 1 classifies the prior studies on Internet privacy according to their contributions in eight major research areas. The numbers in parentheses in Figure 1 indicate how many of the studies reviewed here fall into a given classification. Thus, 32 studies have addressed the customer perspective, 12 have addressed the company perspective, and 6 have addressed the government perspective. In addition, 13 studies have investigated the customer-company interaction, 3 studies have addressed the customer-government interaction, 3 studies have addressed company-government interaction and 1 study has focussed on the three way interaction of customer-company-government. In addition, 11 studies addressed privacy issues with respect to other factors such as technology and economic perspectives.

Table 1. Summary of Reviewed Studies

	Research Framework	Study
<i>Customer Perspective (36)</i>	The Dimensions of Customers' Privacy Concerns (9)	[1, 10, 15, 16, 19, 20, 49, 58, 59]
	Antecedents of Customers' Privacy Concerns (16)	[15, 16, 21-27, 60-66]
	Consequences of Customers' Privacy Concerns (11)	[8, 28-31, 58, 66-70]
<i>Company Perspective (12)</i>	Companies' Privacy Practices (11)	[6, 32-35, 50, 71-75]
	Antecedents of Companies' Privacy Practices (1)	[36]
<i>Government Regulation (8)</i>	Regulation Approaches (6)	[7, 32, 37-40]
	Factors Influencing Government Regulation (2)	[10, 20]
<i>Customer - Company Interaction (14)</i>	Company's Privacy Practice and Customer Behaviour (11)	[8, 42-45, 76-81]
	Company Characteristics and Customer Behaviour (3)	[26, 46, 82]
<i>Customer - Government Interaction (3)</i>	Customer's Privacy Concern and Government Approach (3)	[10, 20, 49]
	Company's Privacy Practice and Government Approach (3)	[10, 50, 72]
<i>Customer-Company-Government Interaction (1)</i>	Customer-Company-Government Interaction (1)	[9]
<i>Other Factors (16)</i>	Privacy General (4)	[11, 53, 83, 84]
	Technology (7)	[51, 52, 85-89]
	Economic Perspective (2)	[54, 90]
	Privacy Assurance Services (3)	[55, 56, 80]

Note: (NN) indicates number of studies

References

- [1] H. J. Smith, S. J. Milburg, and S. J. Burke, "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly*, vol. 20, pp. 167-196, June 1996.
- [2] A. M. Porter, "Buyers want Web Privacy," *Purchasing*, vol. 129, pp. 22-25, September 2000.
- [3] Harris Interactive, "Most People Are "Privacy Pragmatists" Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits." vol. 2004, 2003.
- [4] Federal Trade Commission (FTC), "Privacy online: Fair information practices in the electronic marketplace - A report to Congress," Washington, DC May 2000.
- [5] Zogby, "UPI-Zogby International Poll: Most Americans Worry About Identity Theft." vol. 2007, 2007.
- [6] M. J. Culnan, "Protecting Privacy Online: Is Self-Regulation Working?," *Journal of Public Policy & Marketing*, vol. 19, pp. 20-26, Spring 2000.
- [7] B. Shapiro and C. R. Baker, "Information technology and the social construction of information privacy," *Journal of Accounting and Public Policy*, vol. 20, pp. 295-322, Winter 2001.
- [8] M. J. Culnan and P. K. Armstrong, "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science*, vol. 10, pp. 104-115, January 1999.

- [9] M. J. Culnan and R. J. Bies, "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues*, vol. 59, pp. 323-342, July 2003.
- [10] S. J. Milberg, H. J. Smith, and S. J. Burke, "Information privacy: Corporate management and national regulation," *Organization Science*, vol. 11, pp. 35-57, January-February 2000.
- [11] G. R. Milne, "Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue," *Journal of Public Policy & Marketing*, vol. 19, pp. 1-6, Spring 2000.
- [12] Business Week, "Business Week/Harris Poll: A Growing Threat." vol. 2004, 2000.
- [13] Harris Interactive, "Privacy On and Off the Internet: What Consumers Want," Privacy & American Business, Hackensack, NJ. February 7 2002.
- [14] M. J. Culnan, "The Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission," Georgetown University, Washington, DC June 1999.
- [15] K. B. Sheehan, "Toward a typology of Internet users and online privacy concerns," *Information Society*, vol. 18, pp. 21-32, January 2002.
- [16] M. S. Ackerman, L. F. Cranor, and J. Reagle, "Privacy in e-commerce: examining user scenarios and privacy preferences," in *1st ACM conference on Electronic Commerce*, Denver, Colorado, United States 1999, pp. 1-8.
- [17] A. F. Westin, "Social and Political Dimensions of Privacy," *Journal of Social Issues*, vol. 59, pp. 431-453, July 2003.
- [18] Louis Harris and Associates and A. F. Westin, "E-commerce & Privacy: What Net Users Want," Privacy & American Business, Hackensack, NJ June 1998.
- [19] G. S. Dhillon and T. T. Moores, "Internet Privacy: Interpreting Key Issues," *Information Resources Management Journal*, vol. 14, pp. 33-37, October-December 2001.
- [20] S. J. Milberg, S. J. Burke, H. J. Smith, and E. A. Kallman, "Values, Personal Information Privacy, and Regulatory Approaches," *Communications of the ACM*, vol. 38, pp. 65-74, December 1995.
- [21] J. Phelps, G. Nowak, and E. Ferrell, "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy & Marketing*, vol. 19, pp. 27-41, Spring 2000.
- [22] C. J. Dommeyer and B. L. Gross, "What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies," *Journal of Interactive Marketing*, vol. 17, pp. 35-51, Spring 2003.
- [23] D. O'Neil, "Analysis of Internet Users' Level of Online Privacy Concerns," *Social Science Computer Review*, vol. 19, pp. 17-31, March 2001.
- [24] T. R. Graeff and S. Harmon, "Collecting and using personal data: Consumers' awareness and concerns," *The Journal of Consumer Marketing*, vol. 19, pp. 302-318, July 2002.
- [25] K. B. Sheehan, "An investigation of gender differences in on-line privacy concerns and resultant behaviors," *Journal of Interactive Marketing*, vol. 13, pp. 24-38, Autumn 1999.
- [26] J. B. Earp and D. Baumer, "Innovative Web use to learn about consumer behavior and online privacy," *Communications of the ACM*, vol. 46, pp. 81-83, April 2003.
- [27] G. R. Milne and A. J. Rohm, "Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-In and Opt-Out Alternatives," *Journal of Public Policy & Marketing*, vol. 19, pp. 238-249, Fall 2000.
- [28] K. B. Sheehan and M. G. Hoy, "Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns," *Journal of Advertising*, vol. 28, pp. 37-51, Fall 1999.
- [29] G. R. Milne and M.-E. Boza, "Trust and concern in consumers' perceptions of marketing information management practices," *Journal of Interactive Marketing*, vol. 13, pp. 5-24, Winter 1999.
- [30] M. O. Lwin and J. D. Williams, "A Model Integrating the Multidimensional Developmental Theory of Privacy and Theory of Planned Behavior to Examine Fabrication of Information Online," *Marketing Letters*, vol. 14, pp. 257-272, December 2003.
- [31] J. F. George, "The theory of planned behavior and Internet purchasing," *Internet Research-Electronic Networking Applications and Policy*, vol. 14, pp. 198-212, July 2004.
- [32] E. M. Caudill and P. E. Murphy, "Consumer Online Privacy: Legal and Ethical Issues," *Journal of Public Policy & Marketing*, vol. 19, pp. 7-19, Spring 2000.
- [33] C. Liu and K. P. Arnett, "An Examination of Privacy Policies in Fortune 500 Web Sites," *Mid-American Journal of Business*, vol. 17, pp. 13-21, Spring 2002.
- [34] G. R. Milne and M. J. Culnan, "Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998-2001 U.S. Web Surveys" *Information Society*, vol. 18, pp. 345-359, October-December 2002.
- [35] C. Gurau, A. Ranchhod, and C. Gauzente, "'To legislate or not to legislate': a comparative exploratory study of privacy/personalisation factors affecting French, UK and US Web sites," *The Journal of Consumer Marketing*, vol. 20, pp. 652-664, 2003.
- [36] R. Sarathy and C. J. Robertson, "Strategic and Ethical Considerations in Managing Digital Privacy," *Journal of Business Ethics*, vol. 46, pp. 111-126, August 2003.
- [37] H. J. Smith, "Information privacy and marketing: What the U.S. should (and shouldn't) learn from Europe," *California Management Review*, vol. 43, pp. 8-33, Winter 2001.
- [38] K. C. Laudon, "Markets and Privacy," *Communications of the ACM*, vol. 39, pp. 92-104, September 1996.
- [39] F. Belanger and J. S. Hiller, "A framework for e-government: privacy implications" *Business Process Management Journal* vol. 12, pp. 48 - 60, 2006.
- [40] S. H. Holden and L. I. Millett, "Authentication, Privacy, and the Federal E-Government" *The Information Society*, vol. 21, pp. 367 - 377, November 2005.
- [41] G. H. Hofstede, *Culture's Consequences: International Differences in Work-Related Values*. Beverly Hills, Calif.: Sage Publications, 1980.
- [42] J. W. Palmer, J. P. Bailey, and S. Faraj, "The Role of Intermediaries in the Development of Trust on the WWW: The Use and Prominence of Trusted Third Parties and Privacy Statements," *Journal of Computer-Mediated Communication*, vol. 5, March 2000.
- [43] A. D. Miyazaki and S. Krishnamurthy, "Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions," *Journal of Consumer Affairs*, vol. 36, pp. 28-49, June 2002.
- [44] T. T. Moores, "Do consumers understand the role of privacy seals in e-commerce?," *Communications of the ACM*, vol. 48, pp. 86-91 March 2005.
- [45] J. B. Earp, A. I. Anton, L. Aiman-Smith, and W. H. Stufflebeam, "Examining Internet privacy policies within the context of user privacy values," *IEEE Transactions on Engineering Management*, vol. 52, pp. 227-237, May 2005.
- [46] V. Swaminathan, E. Lepkowska-White, and B. P. Rao, "Browsers or Buyers in Cyberspace? An Investigation of Factors Influencing Electronic Exchange," *Journal of Computer-Mediated Communication*, vol. 5, December 1999.
- [47] R. P. Horton, T. Buck, P. E. Waterson, and C. W. Clegg, "Explaining intranet use with the technology acceptance model," *Journal of Information Technology*, vol. 16, pp. 237-249, December 2001.
- [48] B. Szajna, "Empirical Evaluation of the Revised Technology Acceptance Model," *Management Science*, vol. 42, pp. 85-92, January 1996.
- [49] K. B. Sheehan and M. G. Hoy, "Dimensions of Privacy Concern Among Online Consumers," *Journal of Public Policy & Marketing*, vol. 19, pp. 62-73, Spring 2000.
- [50] G. F. Johnson-Page and R. S. Thatcher, "B2C data privacy policies: Current trends," *Management Decision*, vol. 39, pp. 261-271, May 2001.

- [51] S. Kenny and L. Korba, "Applying digital rights management systems to privacy rights management," *Computers & Security*, vol. 21, pp. 648-664, November 2002.
- [52] L. F. Cranor, M. Arjula, and P. Guduru, "Use of a P3P user agent by early adopters," in *Workshop On Privacy In The Electronic Society*, Washington, DC, 2002, pp. 1-10.
- [53] A. Ben-Ze'ev, "Privacy, emotional closeness, and openness in cyberspace," *Computers in Human Behavior*, vol. 19, pp. 451-467, July 2003.
- [54] R. T. Rust, P. K. Kannan, and N. Peng, "The Customer Economics of Internet Privacy," *Journal of the Academy of Marketing Science*, vol. 30, pp. 455-464, Fall 2002.
- [55] M. Greenstein, M. and J. E. Hunton, "Extending the Accounting Brand to Privacy Services," *Journal of Information Systems*, vol. 17, p. 87, Fall 2003.
- [56] J. E. Hunton, T. Benford, V. Arnold, and S. Sutton, G., "The Impact of Electronic Commerce Assurance on Financial Analysts' Earnings Forecasts and Stock Price Estimates," *Auditing*, vol. 19, pp. 5-22, 2000.
- [57] M. D. Odom, A. Kumar, and L. Saunders, "Web Assurance Seals: How and Why They Influence Consumers' Decisions," *Journal of Information Systems*, vol. 16, pp. 231-250, Fall 2002.
- [58] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research*, vol. 15, pp. 336-355, December 2004.
- [59] K. A. Stewart and A. H. Segars, "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research*, vol. 13, pp. 36-49, March 2002.
- [60] S. Bellman, E. J. Johnson, S. J. Kobrin, and G. L. Lohse, "International Differences in Information Privacy Concerns: A Global Survey of Consumers," *Information Society*, vol. 20, pp. 313-324, November 2004.
- [61] G. Chakraborty, V. Lala, and D. Warren, "An empirical investigation of antecedents of B2B Websites' effectiveness," *Journal of Interactive Marketing*, vol. 16, pp. 51-72, Autumn 2002.
- [62] D. L. Hoffman, T. P. Novak, and M. Peralta, "Building consumer trust online," *Communications of the ACM*, vol. 42, pp. 80-85, April 1999.
- [63] X. M. Luo, "Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory," *Industrial Marketing Management*, vol. 31, pp. 111-118, February 2002.
- [64] A. D. Miyazaki and A. Fernandez, "Consumer Perceptions of Privacy and Security Risks for Online Shopping," *Journal of Consumer Affairs*, vol. 35, pp. 27-44, June 2001.
- [65] J. Phelps, G. D'Souza, and G. Nowak, "Antecedents and consequences of consumer privacy concerns: An empirical investigation," *Journal of Interactive Marketing*, vol. 15, pp. 2-17, Autumn 2001.
- [66] T. Diney and P. Hart, "An extended privacy calculus model for E-commerce transactions," *Information Systems Research*, vol. 17, pp. 61-80, March 2006.
- [67] B. Berendt, O. Gunther, and S. Spiekermann, "Privacy in E-commerce: Stated preferences vs. actual behavior," *Communications of the ACM*, vol. 48, pp. 101-106, April 2005.
- [68] J. F. George, "Influences on the intent to make Internet purchases," *Internet Research-Electronic Networking Applications and Policy*, vol. 12, pp. 165-180, May 2002.
- [69] C. Koyuncu and D. Lien, "E-commerce and consumer's purchasing behaviour," *Applied Economics*, vol. 35, p. 721, January 2003.
- [70] C. Liu, J. T. Marchewka, and C. Ku, "American and Taiwanese Perceptions Concerning Privacy, Trust, and Behavioral Intentions in Electronic Commerce," *Journal of Global Information Management*, vol. 12, pp. 18-40, January-March 2004.
- [71] M. S. Desai, T. C. Richards, and K. J. Desai, "E-commerce policies and customer privacy," *Information Management & Computer Security*, vol. 11, pp. 19-27, March 2003.
- [72] K. Jamal, M. Maier, S. Sunder, and P. Healy, M., "Privacy in E-commerce: Development of Reporting Standards, Disclosure, and Assurance Services in an Unregulated Market," *Journal of Accounting Research*, vol. 41, p. 285, May 2003.
- [73] T. T. Moores and G. S. Dhillon, "Do privacy seals in e-commerce really work?," *Communications of the ACM*, vol. 46, pp. 265-271, December 2003.
- [74] G. R. Milne, M. J. Culnan, and H. Greene, "A Longitudinal Assessment of Online Privacy Notice Readability," *Journal of Public Policy & Marketing*, vol. 25, pp. 238-249, Fall 2006.
- [75] P. O'Connor, "AN INTERNATIONAL COMPARISON OF APPROACHES TO ONLINE PRIVACY PROTECTION: IMPLICATIONS FOR THE HOTEL SECTOR," *Journal of Services Research*, vol. 6, pp. 7-25, July 2006.
- [76] D. L. Hoffman, T. P. Novak, and M. Peralta, "Information Privacy in the Marketplace: Implications for the Commercial Uses of Anonymity on the Web," *Information Society*, vol. 15, pp. 129-139, May 1999.
- [77] G. J. Nowak and J. Phelps, "Direct marketing and the use of individual-level consumer information: Determining how and when 'privacy' matters," *Journal of Interactive Marketing*, vol. 11, pp. 94-108, Fall 1997.
- [78] A. D. Miyazaki and A. Fernandez, "Internet Privacy and Security: An Examination of Online Retailer Disclosures," *Journal of Public Policy & Marketing*, vol. 19, pp. 54-61, Spring 2000.
- [79] M. A. Eastlick, S. L. Lotz, and P. Warrington, "Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment," *Journal of Business Research*, vol. 59, pp. 877-886, August 2006.
- [80] V. Lala, V. Arnold, S. G. Sutton, and L. Guan, "The impact of relative information quality of e-commerce assurance seals on Internet purchasing behavior," *International Journal of Accounting Information Systems*, vol. 3, pp. 237-253, 2002.
- [81] K.-L. Hui, B. C. Y. Tan, and C.-Y. Goh, "Online information disclosure," *ACM Transactions on Internet Technology*, vol. 6, pp. 415-441, November 2006.
- [82] C. Ranganathan and S. Ganapathy, "Key dimensions of business-to-consumer web sites," *Information & Management*, vol. 39, pp. 457-465, May 2002.
- [83] H. Q. Wang, M. K. O. Lee, and C. Wang, "Consumer privacy concerns about Internet marketing," *Communications of the ACM*, vol. 41, pp. 63-70, March 1998.
- [84] J. Kalvenes and A. Basu, "Design of Robust Business-to-Business Electronic Marketplaces with Guaranteed Privacy," *Management Science*, vol. 52, pp. 1721-1736, November 2006.
- [85] A. I. Antón, J. B. Earp, and A. Reese, "Analyzing Website Privacy Requirements Using a Privacy Goal Taxonomy," in *10th Anniversary IEEE Joint International Conference on Requirements Engineering (RE)*, 2002, pp. 23-31.
- [86] P. Ashley, S. Hada, G. Karjoth, and M. Schunter, "E-P3P privacy policies and privacy authorization," in *The 2002 ACM Workshop on Privacy in the Electronic Society*, Washington, DC, 2002, pp. 103-109.
- [87] L. F. Cranor and AT&T Labs-Research, "P3P: Making Privacy Policies More Useful," *IEEE Security & Privacy*, vol. 1, pp. 50-55, November-December 2003.
- [88] R. Grimm and A. Rossnagel, "Can P3P help to protect privacy worldwide?," in *The 2000 ACM Workshops on Multimedia* Los Angeles, California, United States, 2000, pp. 157-160.
- [89] H. Hochheiser, "The platform for privacy preference as a social protocol: An examination within the U.S. policy context," *ACM Transactions on Internet Technology (TOIT)*, vol. 2, pp. 276-306, November 2002.
- [90] T. Vila, R. Greenstadt, and D. Molnar, "Why we can't be bothered to read privacy policies models of privacy economics as a lemons market," in *5th International Conference on Electronic Commerce* Pittsburgh, Pennsylvania, 2003, pp. 403-407.