December 2000

Trust and Quality Assurance in Business-to-Consumer Electronic Commerce: Enhancing Consumer Acceptance and Participation

Dat-Dao Nguyen
California State University

Dennis Kira
Concordia University Montreal

Trust and Quality Assurance in Business-To-Consumer Electronic Commerce: Enhancing Consumer Acceptance and Participation

Dat-Dao Nguyen , Glen L. Gray
Department of Accounting and Management Information Systems
California State University, Northridge CA 91330, USA

Dennis S. Kira
Department of Decision Sciences and Management Information Systems
Concordia University, Montreal H3G 1M8, Canada

Abstract
The growth of electronic commerce (e-commerce) has been inhibited by consumer fears and concerns about the risks, real and perceived. This paper discusses the risks associated with e-commerce transactions and the measures to gain consumers' trust in order to enhance their acceptance and participation. The quality assurance in e-commerce, and therefore the enhancement of consumer's trust and acceptance, should be a combination of self-regulation, technology, and legislation. Regulations similar to those for traditional businesses could be applied to the electronic commerce environment to protect consumers with the assurance regarding the existence of business entities and define the related liabilities to consumers.

Keywords: *Business-to-Consumer Electronic Commerce, Privacy, Reliability, Quality Assurance Services, Consumer Acceptance, Business Regulation*.

1. Introduction

Recently, with the proliferation of using computers to access to the Internet, the World Wide Web (the Web) has provided a new means to conduct online business, namely electronic commerce (e-commerce). This is affordable to everybody engaging in the selling or buying of goods and services. In e-commerce, one can have business-to-business (B2B) and business-to-consumer (B2C) transactions. This paper focuses on the relationship between sellers and consumers in B2C e-commerce.

In an estimation of e-commerce participation, Yankelovich Partners (1997) reported that 66% of their sample survey make online hotel or airline reservations, 55% bought computer hardware and software, 54% subscribed to online information services, 47% bought records, tapes, CD's and videos. The Direct Marketing Association (DMA) estimates that online sales approached $US 6 billion in 1998 and is expected to exceed $11 billion in 1999. They forecasted the growth in B2C e-commerce sales would exceed 60% per year through 2003 (Culnan, 1999). The DMA believes that more than 130 million Americans have made a purchase by mail or telephone, and many more are now choosing to shop online.

Online users are receptive to buying a variety of products over the Internet but often do not do so because of security fears. Yankelovich Partners (1997) reported that 91% of their survey sample said they would not provide information about their income, 85% would not provide their credit card number when shopping online, 74% were unwilling to provide their phone number, and 67% were unwilling to provide their address.

An opinion poll conducted by Business Week and Louis Harris & Associates in 1998 found that 78% of persons who use the Internet said that they would increase their use of the Internet if they believed their privacy were protected. A majority said that if a company explicitly guaranteed the security of personal information, they would be encouraged to register on the Web site, provide personal information, and purchase products and services (Culnan, 1999).

The growth of e-commerce has been inhibited by consumer fears and concerns about the risks, real and perceived. E-commerce will not reach its full potential unless consumers perceive that electronic transactions are secure and associated risks have been reduced to an acceptable level. This paper discusses the risks associated with e-commerce transactions and the measures to gain consumers' trust in order to enhance their acceptance and participation.

The remainder of this paper is organized as follows. Section 2 discusses some of the general, supplier and consumer risks associated with e-commerce and their negative impacts. Section 3 discusses a variety of assurance services and seal programs that help increase the confidence of e-commerce consumers. It also discusses three trade groups who are trying to improve consumer confidence through a variety of actions. Section 4 provides an overview of some research results regarding the consumers', businesses' and government agencies' attitudes toward e-commerce quality assurance activities. Section 5 presents our conclusions and direction for future research.

2. Risks Associated With E-commerce Transactions

When business transactions are conducted via the Internet, sellers as well as buyers may suffer from risks associated with the security of the media and those specifically related to non face-to-face and possible anonymous communication.

2.1. General Risks

General risks related to electronic transactions should be identified and controlled in order to enhance the integrity in e-commerce. Without proper controls, electronic transactions and documents can be easily changed, lost, duplicated, and incorrectly processed, thereby, causing disputes on terms of transactions and related payments.

Security can be enhanced with information technologies. Encryption helps prevent consumer personal information, such as credit card numbers and other vital information, from being intercepted and stolen during transmission. Firewalls and other security practices help protect customer information residing on the seller’s computer system from being intentionally or unintentionally disseminated to or being accessed by unauthorized third parties. Other standard controls on business functions of an information system also help to guarantee the accuracy of business transactions.

The general risks concerns while conducting online transactions are similar to the risks associated with traditional business transactions. Potential participants of traditional commerce as well as e-commerce may seek assurance that the business entity has effective integrity controls and a history of processing its transactions accurately, completely, and promptly, and billing its customers in accordance with agreed-upon terms. However, due to its non face-to-face nature, e-commerce imparts both suppliers and consumers with specific risks related to the actions of the other party.

2.2. Supplier Risks

E-commerce does not require face-to-face or person-to-person communication to facilitate business transactions. The anonymity of e-commerce and the ease of establishing an identity for online transactions can disguise the buyer's identity from the seller. But sellers want to protect against consumer frauds where customers deny (or repudiate) that they placed an order and/or use of the names of others (Swisher, 1998). Consequently, sellers tend to ask consumers information on their identities such as real names, demographic information, postal addresses, telephone number, e-mail addresses, and credit information.

In e-commerce transactions, some information gathering or tracking is normally in place when a user logs onto the Internet and navigates through the Web. The information can be collected directly from user who voluntarily provides when registering at the site or signing a guest book. Information on user can also be collected indirectly through the browser when user connects to the site or through a cookie file. Most information collected online is usage data on where user goes and how much time he/she spends at an individual site. Online service providers usually track sign-on and sign-off times for billing purposes. In principle, personal identifiable information is not gathered secretly. Although a code in a cookie file enables the site to label a particular user, it does not identify user buy name and address unless a person has provided the site with such information or set up browser preference to do so automatically.

However, collected information has not been used only to protect the business against losses from bad transactions. Most sellers sell the information on their clientele as a mailing list to other marketing services. This practice raises the issue on the privacy of e-commerce.

2.3. Consumer Risks

The ease of establishing an entity on the Internet poses the same risk to consumers as to sellers. Virtually, anybody can set up a Web site to conduct business in e-commerce. The appearance of a business on Internet can be deceiving, as one cannot evaluate a business performance based on well-designed electronic front store. Consumers do not know much about the history of a particular e-commerce business among multitude of online suppliers. On the Internet, consumers lack many of the traditional cues such as physical, brick-and-mortar front store, and person-to-person contact to build their trust in a business.

Consumers perceive that online businesses now have more opportunities to make use of consumers' personal information with sophisticated tools for collecting and data mining that information. Many sites are asking consumers to provide detailed personal information online. A number of sites are collecting information from consumers without their knowledge or permission. Some sites are providing access to personal information to others without proper authorization. There is a potential for misuse and/or abuse of consumer information by online business. Consequently, consumers are reluctant to provide their personal information, as they tend to mistrust the security of transaction over Internet. In addition, they are concerned about how to complain about the inaccuracy, incompleteness and unauthorized use of personal information.

Boston Consulting Group (1997) found that 76% of the survey sample expressed concern about sites monitoring browsing on Internet. 71% are more concerned about information transmitted over Internet than telephone. 72% are more concerned about Internet than mail.

39% are willing to pay more than 0.5% of selling price for privacy assurance, and 29% willing to pay extra cost for disclosure.

Consumers are also concerned about the assurance on the fulfillment of sales obligation by the supplier in terms of quantity, quality, delivery and cost, the ability to verify their order status, term of delivery, warranties and return policy. In addition, they are concerned about complaints on the sales and after-sales services

In a survey released by National Consumers League (Culnan, 1999), 88% of the respondents said that they are somewhat or very concerned about privacy. Although 76% believed that technology would make their lives easier and more convenient, consumers are still wary of providing sensitive information online. 73% said they were uncomfortable in providing credit card information, 73% were uncomfortable in providing other financial information, and 70% were uncomfortable in providing general personal information.

When asked if they had ever had a problem online with fraud or unauthorized use of their personal information, 7% of respondents from the above survey said yes, related to the use of their credit card information and other financial information online.

Consumers express strong concerns regarding privacy over the Internet: want to limit and control the spread of their information, see privacy and security as interrelated and overlapping issues, and generally are less willing to disclose more sensitive personal information to businesses they are not familiar with.

Consumers also recognize that they have only weak control over dissemination of their personal information. Their willingness in providing personal information and engaging in e-commerce transaction is usually based on a subjective assessment of trust. The most common practice in case of doubt is either opting-out or disguising their identity. For example, 42% of consumers refuse to give registration information and 27% sometimes falsify information because of privacy concerns (Boston Consulting Group, 1997). Consumers generally disclose more information to businesses they have established relationship or are familiar with. They are less comfortable disclosing information to businesses they do not know well, particularly very sensitive information. If a site discloses its privacy practices, up to 18% of respondents would give information that they otherwise would not disclose.

Consumers indicate they would increase the depth and breadth of their Internet activity in responding to a privacy disclosure and assurance program. Assurance of non-dissemination of personal information would have a significant impact, increasing consumer willingness to participate in e-commerce by a factor of 2 to 3. Disclosure of privacy practices alone would have a more limited impact, increasing consumer willingness to participate by approximately 50%. The combined positive impact on e-commerce could reach US$ 6 billion by 2000 (Boston Consulting Group, 1997).

3. Quality Assurance and Trust Promotion Services

The problem in e-commerce assurance is there are no Web-specific rules that company must follow and that consumers can rely on to protect themselves. One observes a lack of uniformity in companies' stated privacy practices and policies regarding consumer information collected online and offline. The pressing issue is how can one create clear

privacy rules for everyone to abide by. Also consumer recourse is an important issue in national as well as in international context.

The criteria for Fair Information Practices proposed by U.S. Department of Health, Education and Welfare includes openness with no secret data collection, notice of use, limitations on secondary use, mean of correction, and appropriate security. Organization of Economic Cooperation and Development expanded this set into Fair Information Principles with purpose specification, use limitation, and individual participation (Culnan, 1999).

So far government agencies are reluctant to create new regulations for e-commerce transactions. However, it is impossible to assess the effectiveness of self-regulation based only on the basis of what Web sites say, rather than on what companies actually do. The issue is how to assess what actually happens to consumers' information, how easily they can access it, and how they can enforce the proper use of it. Also one needs the assurance on the reliability of e-commerce transactions in that business actually fulfills their obligations to their consumers.

Consequently, the need for assurance from an independent, neutral third party emerges. For example, Certified Public Accountants (CPAs) may be suitable agents for electronic commerce assurance, as integrity, objectivity, and independence are the attributes of the accounting profession. Or a similar non-government regulation in traditional commerce, such as the one provided by Better Business Bureau, is necessary to promote trust and enhance consumer acceptance of e-commerce.

This section reviews a variety of assurance services and seal programs that help increase the confidence of e-commerce consumers. Then it discusses actions of three trade groups who are trying to improve consumer confidence.

3.1 Better Business Bureau Online

The BBBOnLine Program is intrinsically tied to its parent organization, the Council of Better Business Bureaus (BBB). BBBOnLine Reliability was launched in 1997 as a way to help identify online businesses with a reliable track record in marketplace. A company in the BBBOnLine Reliability program must satisfy conditions such as being in business for at least one full year, being member of the BBB in its area, agreeing to BBB standards and dispute resolution procedures, being confirmed by a BBB representative on site on its adherence to the program requirements. To become a member of BBB, and consequently participating in BBBOnLine Reliability, a company must provide the BBB in its area with information about the business, its officers, and reference that support its reliability. It must also have a satisfactory complaint history with the BBB in its area. Once being approved by the BBB Board of Directors, the company can then display the BBBOnLine seal on its Web site. As of August 1999, over 3,600 companies have been approved to participate the program (BBBOnLine, 2000). BBBOnLine Reliability fees are based on the number of employees in the company.

BBBOnLine Privacy was launched in 1999 to award seals to online businesses that have been verified to be following good information practices. These practices include clearly posted privacy policies meeting rigorous privacy principles (such as notice to consumer, disclosure, choice and consent, access and security), monitoring and review by a trusted organization, and consumer dispute resolution. Companies that qualify must post privacy notices telling

consumers what personal information is being collected and how it will be used. Qualifying Web sites commit to abide by their posted privacy policies, and agree to a comprehensive independent verification by BBBOnLine. The privacy program also gives consumers a mechanism for resolving disputes. The participating company in this program is not required to be a member of BBB. Annual participation fees range from US$ 150 for companies with sales less than US$ 1 million to a few thousand dollars for companies with higher sales.

It has been claimed that companies in BBBOnLine Reliability make a commitment to high levels of ethical business practices and customer satisfaction that are not required by other seal programs. For instance, BBBOnLine Reliability can review advertising claims made on the Web sites of applicants to see whether they meet basic BBB truth-in-advertising standards. BBBOnLine Reliability representatives visit the workplace of each BBBOnLine Reliability participant to verify the company's location and its ability to deliver what is promised on the Web site. Companies in BBBOnLine Reliability should commit to work with their customers and the BBB to resolve disputes that might arise, including going through an arbitration process monitored by the BBB should a consumer choose so. Businesses that repeatedly violate their own policies will have their seal revoked. They will be publicly identified and the most serious or frequent offenders will have the violations reported to the proper government agency.

3.2 TRUSTe's Trustmark

The Trustmark is an online branded seal awarded to sites that adhere to established privacy principles and agree to comply with ongoing TRUSTe oversight and consumer resolution procedures. Annual license fee starts from US$ 299 for companies with annual revenue less than US$ 1 million to US$ 4,999 for companies with annual revenue more than $US 75 million. In January 2000, TRUSTe announced that it has awarded its 1000th Privacy Seal (TRUSTe, 2000).

The principles advocated by TRUSTe include:
- Adoption and implementation of a privacy policy that takes into account consumer anxiety over sharing personal information online.
- Notice and disclosure of information collection and use practices.
- Choice and consent, giving users the opportunity to exercise control over their information.
- Data security and quality and access measures to help protect the security and accuracy of personally identifiable information.

TRUSTe licensees agree to post a comprehensive privacy statement and implement fair information practices. Consequently, the Web site should tell a consumer exactly what personal information is being gathered, how it will be used, with whom it will be shared, the choices available to consumer regarding how collected information is used, the safeguards in place to protect the information, and how consumer can correct any inaccuracies in his/her information. TRUSTe promises to monitor licensees for compliance with program principles and posted privacy practices through a variety of measures.

To resolve complaints raised by consumers, licensees agree to cooperate with all TRUSTe reviews and inquiries. Depending on the severity of the violation, this process could result in a Web site compliance review by an outside CPA firm, revocation of the Trustmark, termination from the TRUSTe program, breach of contract proceedings, or referral to the appropriate federal authority.

With the TRUSTe Watchdog program, a consumer can complain on the privacy violation of a TRUSTe licensee after contacting the Web site directly and not getting a complete satisfaction on the dispute. However, TRUSTe can process and resolve only issues pertaining to violation of a licensee's posted privacy policy or misuse of Trustmark. It is not within the TRUSTe charter to process consumer complaints or issues regarding general online security and Internet privacy rights, or matters involving a Web site's specific commerce, online ordering, and other non-privacy related company procedures.

3.3 WebTrust

Public accounting profession has developed a set of principles and criteria for B2C e-commerce, referred to as WebTrust (AICPA/CICA, 1999). These principles and criteria reflect fundamental standards for business practices, transaction integrity, and information protection. A business entity conducting e-commerce that meets these principles and criteria will be provided with a WebTrust Seal of assurance to display on its Web site. Consumers can click on the seal to view the report prepared by a CPA and other relevant information on the e-commerce site that they plan to do business with. As of December 1999, 25 sites are awarded WebTrust seals.

WebTrust Principles include:
- Business and information privacy practices: the entity should disclose its business and information privacy practices for e-commerce transactions in matters such as orders, subsequent returns and warranty claims. The entity should follow its disclosed practice and agree to third party arbitration to settle customer complaints. It should also disclose the use, protection, maintenance of private customer information along with consumer recourse provisions. The principle does not include representation as to the quality of goods or services provided or their suitability for any customer's intended purpose.
- Transaction integrity: the entity should maintain effective control to provide reasonable assurance that customer transactions using e-commerce are completed and billed as agreed. These controls address matters such as transaction validation; the accuracy, completeness, and timeliness of transaction processing and related billings; the disclosure of terms and billing elements; and appropriate transaction identification.
- Information protection: the entity should maintain effective controls to provide reasonable assurance that private customer information obtained from an e-commerce transaction is protected from uses not related to the entity's business. The issues relate to privacy and security matters such as encryption and protection of private customer information during and after the transaction, requesting permission of customers to use their information for purposes other than those related to the entity's business, obtaining customer permission before storing, altering, or copying information on the customer's computer.

CPAs are in the business of providing assurance services (Gray and Debreceny, 1998; Nagel and Gray, 1999). An audit opinion signed by a CPA is valued because these professionals are experienced in assurance matters, subject matters, and are recognized for their independence, integrity, discretion, and objectivity. Depending on annual revenue of the related business entity, the cost to obtain a WebTrust seal may run from US$ 5,000 to 50,000. The seal must be refreshed at least every 90 days. The CPA may judge on the extent and type of testing for seal refreshment.

3.4 Online Privacy Alliance

The Online Privacy Alliance (OPA) is an ad hoc organization of more than 80 global companies formed in 1998 committed to promoting the privacy of individuals online. Its purpose is to define privacy policy and to foster an online environment that respects consumer privacy. It advocates that the best way to create public trust is for the organization to alert consumers to the organization's practices and procedures through participation in a program that has an easy to recognize symbol or seal.

To address consumer concerns about privacy a company should post a privacy policy that follows the guidelines such as those suggested by the OPA. Then the company should join a seal program such as BBBOnline, TRUSTe, or WebTrust. Validation by an independent trusted third party that organizations are engaged in meaningful self-regulation of online privacy may be necessary to grow consumer confidence. The symbol or seal can be used to connote both compliance with privacy policies and an easy method for consumers to contact the seal providers.

3.5 DMA Privacy Promise

The Direct Marketing Association (DMA) is a trade association for businesses interested in interactive and database marketing, dedicated to helping its members increase their effectiveness and profitability. It includes 4,500 members from small business entrepreneurs to Fortune 100 companies. The DMA Privacy Promise seeks to raise privacy practices by ensuring that DMA members adhere to certain privacy practices. It is a public assurance that, by July 1, 1999, all members of DMA will follow certain specific practices to protect consumer privacy. Those practices are designed to have a major impact on those consumers who wish to receive fewer advertising solicitations.
Companies displaying the DMA Member logo commit to the association's Privacy Promise, which includes the following principles:
- Provide customers with notice of their ability to opt out of information rental, sale or exchange with other marketers.
- Honor customers request of not to share their information with other marketers.
- Honor customers request of not to receive mail, telephone or other solicitations.

Furthermore, DMA members are assumed to adhere to a whole range of other ethical business practices administered by the DMA and backed by a peer review program that enforces these practices (DMA, 2000).

3.6 Individual Reference Services Group

The individual reference services industry helps users to find people and verify identities. Individual reference services provide their customers with access to databases containing information obtained from public records from government agencies, publicly available information from non-governmental sources, and proprietary or non-public sources. These services play an important role in facilitating law enforcement, fraud prevention and detection, and other business transactions and legal proceedings.

The Individual Reference Services Group (IRSG) is composed of leading companies in the individual reference services business. In December 1997, IRSG pledged to adopt self-regulatory principles governing the dissemination and use of personal data. In close

consultation with the Federal Trade Commission, the IRSG has developed a comprehensive set of self-regulatory principles backed by audits and government enforcement.

Companies that sign on to the IRSG principles commit--among other things--to: acquire individually identifiable information only from sources known as reputable, restrict their distribution of non-public information through safeguards appropriately calibrated to the type of use made of the information, educate the public about their database services, and furnish individuals with information contained in services and products that specifically identifies them, unless the information is publicly available or a matter of public record, in which case the companies will provide the individuals with guidance on how they can obtain the information from the original source (IRSG, 2000). Companies abiding by these principles will be subject to annual outside assurance reviews conducted by qualified independent professional services, such as accounting firms, law firms, or security consultants. Reviewers will use criteria developed by PriceWaterhouseCoopers L.L.P. and approved by the IRSG. A summary of the assurance report will be made publicly available.

4. Attitude toward E-commerce Quality Assurance

Assurance services are in place to address major concerns of consumers and business partners engaging in e-commerce such as security of data, business policies, transaction processing integrity, and privacy of data (Greenstein and Feinman, 2000). Some services are more sophisticated in that they require an audit of a professional CPA, others are just a posting of a statement of promise. However, parties in e-commerce have different views on the quality assurance either as a technical issue related to data security, or ethical and legal issue related to business policies and transaction integrity. Overall, the Georgetown Internet Privacy Policy Stud*y* (Georgetown Study) found that about 9.5 % of the survey sample provide consumers with the type of notices required by the Online Privacy Alliance, Better Business Bureau, and TRUSTe (Culnan, 1999).

4.1 Consumers

Many researches and surveys reflect strong consumer desire to control the spread of their personal information. Privacy disclosure increases consumer willingness to give information. If a site discloses its privacy practices, up to 18% of respondents would give information that they otherwise would not disclose. Assurance of non-dissemination of personal information has a much more significant impact. If a site assures non-dissemination of personal information, up to 45% of respondents would give more sensitive information they otherwise would not disclose (Boston Consulting Group, 1997).

Consumers are concerned about controlling the privacy of their personal information on the Internet. Privacy concerns result in multiple negative effects on e-commerce: low rates of consumer participation, falsification of personal information given online, potential for government intervention. Consumers would welcome Internet privacy assurance and they would modify their behavior accordingly. However, the increase in the number of sites that post privacy statements is not necessary evidence that consumer privacy protection is assured on the Internet. No survey has revealed what actually happens to consumers' information, how easily consumers can access it, and how one can enforce the proper use of it.

Yankelovich Partners (1997) found that 78% of their survey sample had a favorable impression on a seal program to improve security and accountability on the Internet. The fact

that professionals, such as CPAs, are providing such service is a key factor in creating user acceptance. 46% of online users in the survey stated that if a Web site received the CPA WebTrust seal, they would be more likely to conduct an online transaction. However, 47% stated that the seal would likely make no difference on their online transaction. One notes that this survey was conducted to assess the prospective acceptance before current seal programs were implemented.

In their comments to the Georgetown Study (Culnan, 1999), *National Consumers League* expresses the concern that it is impossible to assess self-regulation based merely on the basis of what Web sites say, rather than on what companies actually do with the information they collect. *Privacy Rights Clearinghouse* proposes that the standards for determining the adequacy of online privacy policies of Federal Trade Commission or appropriate agency must include enforcement mechanisms and they should provide meaningful redress for consumers' grievances. *Consumer Federation of America & Consumer Action* states that consumers support legislation to protect their privacy online.

4.2 E-commerce Businesses

E-commerce businesses express their interest in a privacy assurance program. However, they are less certain about specific benefits to their businesses. Smaller companies seeking trusted brand recognition see the highest value. Larger companies want a proven, credible program before signing on.

In general, businesses have lower expectations than consumers about the impact of privacy assurance. Smaller businesses believe privacy programs could increase the size of their customer base up to 30%, whereas medium to large businesses expect a 16% increase (Boston Consulting Group, 1997). Online businesses perceive less direct value to their business than indicated by consumers. Many may mistake privacy concerns for security issues. Some believe that their brands will carry them through. Others avoid the involvement in any regulation program because of the requirement of binding arbitration for customer disputes.

However, *IBM* stated that the most important relationship in e-commerce is the trust that the businesses have with each customer (Culnan, 1999). In e-commerce, businesses who demonstrate little or no concern to their consumers interest will find themselves being abandoned, while those who demonstrate such respect will find their customers' loyalty being strengthened. Consumers may go competitors who have reliable system to support fair business practices. They may even stay with traditional business and not participate in e-commerce at all. It is the responsibility of online businesses to take action in order to build consumer trust in e-commerce and further the development of the electronic marketplace

Building consumer trust in e-commerce is beyond technical solutions for security and authentication issues. It should address consumer concerns about the privacy of their information with the disclosure of information practices and the assurance of good business practices.

4.3 Assurance Service Providers

The TRUSTe organization comments that it is much easier to educate a site about what should be in a privacy statement once the site has already accepted a privacy statement as a

necessary part of doing business on the Web (Culnan, 1999). However, some businesses believe that the display of a privacy statement is window dressing. A comment in the Georgetown Study (Culnan, 1999) revealed that, for example, before the survey sponsored by FTC in 1998, the DMA had developed a "Privacy Policy Generator" to help its members create and post a Privacy Policy Statement "in a matter of minutes". This generator gave the marketers an "add water and stir" recipe for providing consumers with information on how data were gathered and used online. This practice results in a speedy ad-hoc posting of privacy policies but not the long-term effort and commitment needed to ensure actual privacy.

One possible reason for non-participation from e-commerce businesses is that some sophisticated assurance services may be too costly for a small business entity. In addition, a business may reluctant to undergo a process of auditing their business practices to obtain a trust seal if it is not enforced by government agencies or required by prospective consumers.

4.4 Government Agencies

The Federal Trade Commission (FTC) told the House Commerce Subcommittee on Telecommunications, Trade and Consumer Protection in 1998 that unless industry can demonstrate that it has developed and implemented broad-based and effective self- regulatory programs, additional governmental authority would be appropriate and necessary (FTC, 1998).

Following this warning, FTC announced its intention to monitor progress of self-regulation. Comments to the Georgetown Study (Culnan, 1999) remarked that, before the 1999 survey sponsored by FTC, the Online Privacy Alliance, Better Business Bureau, TRUSTe, and the DMA announced a campaign to encourage thousand of companies and Web site owners to adopt privacy policies as a "last-ditch effort to avoid new laws that could stunt the growth of e-commerce". There is a wide belief that government agencies will be judging the success of self-regulation by the number of companies posting privacy policies on their Web sites.

However, the Georgetown Study (Culnan, 1999) found fewer than 10% of the sample Web sites meet the minimal fair information practices standards supported by the FTC, professed by the industry self-regulation proponents, and expected by consumers. Industry self-regulation seems failing to protect consumers or foster consumer confidence. Further failure by Congress and the FTC to enact comprehensive privacy protections may hinder the development of e-commerce.

5. Conclusions

The quality assurance in e-commerce, and therefore the enhancement of consumer's trust and acceptance, should be a combination of self-regulation, technology, and legislation. Opinions voiced by consumer organizations show that the issue of consumer's trust and acceptance is not purely technical but it relates to the integrity of a business conducting online transactions online. In engaging in e-commerce, consumers are concerned as much about their interest as they are in traditional business.

A business entity whether conducting transaction online or in traditional manner has many of the same characteristics and responsibilities. Consequently, traditional business regulations could be applied in the e-commerce environment to protect consumers with the assurance on the existence of business entities and the related liabilities to consumers.

Although we have discussed the most recent information about the implementation of consumer protection measures by business entities conducting online transactions, there is still potentially significant research to be conducted related to the success and failure of those measures. In future research, we will discuss a theoretical framework on consumer trust and participation in e-commerce setting. Then we will address the consumer perception on the existing as well ideal protections and assurances related to e-commerce. This will help in designing and implementing efficient measures to guarantee a fair business and foster the participation in e-commerce.

References

AICPA/CICA. *WebTrust Principles and Criteria for Business-to-Consumer Electronic Commerce, October 15, 1999 Version 2.0*, (http://www.aicpa.org/webtrust/princrit.htm), 1999.

BBBOnLine. *BBBOnLine FAQs*, (http://www.bbbonline.org), 2000.

Boston Consulting Group. *eTrust Internet Privacy Study* (http://www.ftc.gov/bcp/privacy/wkshp97/comments1/etrust/), 1997.

Culnan M.J. *Georgetown Internet Privacy Policy Study, August 1999*, (http://neptune.gsb.georgetown.edu/culnan/gippshom.htm), 1999.

Direct Marketing Association (DMA). *The DMA's Privacy Promise*, (http://www.the-dma.org), 2000.

Federal Trade Commission (FTC). *Consumer Privacy On The World Wide Web,* (http://www.ftc.gov/os/1998/9807/privac98.htm), 1998.

Gray G. L., and Debreceny, R. "The Electronic Frontier," *Journal of Accountancy*, May 1998, pp.32-38.

Greenstein M., and Feinman, T. M. *Electronic Commerce: Security, Risk Management and Control*, Irwin McGraw-Hill, Boston, 2000.

Individual Reference Services Group (IRSG). *Industry Principles*, (http://www.irsg.org), 2000.

Nagel K.D., and Gray, G. L. *Electronic Commerce Assurance Services*, Hartcourt Professional Publishing, San Diego, CA, 2000.

Online Privacy Alliance. *Facts*, (http://www.privacyalliance.org), 2000.

Swisher, K. "Seller Beware," *Wall Street Journal*, December 7, 1998.

TRUSTe. *The TRUSTe Program*, (http://www.truste.org) , 2000.

Yankelovich Partners. *Electronic Commerce Assurance: Attitudes Toward CPA Trust*, (http://www.aicpa.org/webtrust/yankel.htm), 1997.