E-Commerce Security

Theresa A. Kraft
thkraft@umflint.edu

Ratika Kakar
ratikak@umflint.edu

School of Computer Science,
University of Michigan – Flint
Flint, MI 48502, USA

Abstract

It is commonly believed that robust security improves trust and this will ultimately increase the use of Electronic Commerce (E-Commerce) (Kim, C., et al., 2009). This paper examines E-Commerce security by first investigating the recent market trends for E-Businesses and the key role E-Commerce plays in the retail market. Additionally, the current practices and trends of E-Commerce including the privacy and security aspects are researched and documented. The primary concern addresses the manner in which the information transactions are handled and the effect this has on the consumers' privacy. Various privacy concerns and arguments against and for these privacy issues are discussed. The legal aspects of these privacy concerns are also discussed and methodologies are evaluated with recommendations for possible solutions. The primary importance is how to protect the privacy of the users, while conducting businesses electronically. A key factor for the future success of E-Commerce is security, a requirement that is becoming more crucial in the current global E-Commerce environment.

Keywords: E-Commerce, E-Business, Security, Privacy, Identity Theft, Internet Based Technology, Privacy Enhancing Technology

1. INTRODUCTION

The web has become an indispensable tool covering several aspects of business, education and personal life. The Web "has changed the ways in which we buy products (e-commerce), socialize (on-line dating, social networking), understand the world (portals), acquire news (on-line media), voice opinions (Web Logs - blogs), entertain ourselves (everything from music downloads to on-line casinos), and go to school (on-line learning)" (Pressman, R., Lowe, D., 2009). The power of the internet also allows for the efficient, inexpensive collection of vast amounts of information without consumers' consent (Chung, W., and Paynter, J., 2008).

E-Commerce security must include a set of procedures, mechanisms and computer programs for authenticating the source of information and guaranteeing the process (Kim, C., et al., 2009). Consumer security fears about E-Commerce have resulted in retailers' loss of an estimated $2 Billion in 2006, according to a Gartner survey of 5,000 U.S. adults (Baseline, 2006). Approximately one-half of those losses ($913 million) could be attributed to people who avoided sites that seemed to be less secure and the rest (about $1 billion) came from consumers who were too afraid to conduct E-Commerce business at all. The report also includes on-line banking, where some 33 million U.S. adults have avoided on-line banking due to security concerns.

Another report by Forrester Research estimates the electronic retailers lost $15 Billion in 2001 because of consumer privacy concerns. Consumers do not trust E-Commerce sites to be secure and respectful of their privacy (Smith, R., and Shao J., 2007)

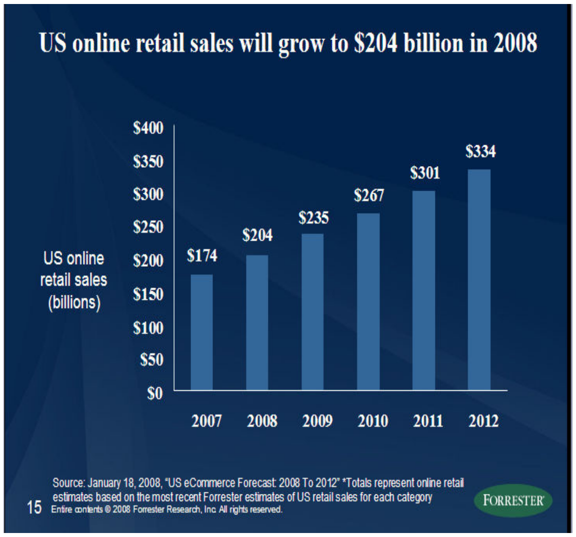
Despite these concerns, E-Commerce plays a very important role in the growth of industry, as an effective, convenient and faster method of doing business. As the trend of on-line transactions continues to grow, there will be increases in the number and types of attacks against the security of on-line payment systems. Such attacks threaten the system security, resulting in systems that may be compromised and less protected, resulting in consumer privacy issues. Consumers may be at the risk for losing their personal information, since they may be unaware of the security aspect of performing on-line transactions. Therefore, it is very important to make the Internet safe for buying and selling products on-line. Global privacy consistency is required, as Internet usage is largely unregulated, which means that laws in one country are not aligned with the laws in other countries.

2. BACKGROUND

The ability to use E-Commerce technologies was made possible in late 1970s. During this time, E-Commerce meant the execution of commercial transactions electronically with the help of Electronic Data Interchange (EDI) and Electronic Funds Transfer (EFT). In 1991, the Internet was opened for commercial use and started becoming popular in 1994 (E-Commerce Land, 2004). Subsequently, it took almost four years to develop security protocols like HTTPS. Amazon was one of the first E-Commerce businesses to establish a secure market.

Companies such as EBay, FedEx, Schwab, OnStar and Google know that using a web site to connect with customers is a key to success. Forrester's research into the Business to Consumer (B2C) E-Commerce market segment illustrates the overall growth of on-line retail and reinforces the importance of secure Web-based applications. The retail and travel portion of B2C E-Commerce exceeded $200 billion as of March 2007, with 60 million U.S. households that shop on-line.

The on-line Web-based presence is evolving into a critical element of the growth strategy for many consumer-facing industries (Malpuru S., 2007). More than 650,000 small, medium and large companies sell products and services utilizing the U.S. on-line marketplace. The on-line retail market is continuing to grow at an impressive rate fueled primarily by a steady stream of new on-line shoppers. “The on-line market is becoming less of a replacement for the brick and mortar retailing as it is a compliment and consumers are integrating the web into their multichannel shopping activities” (Johnson, C., 2005). The 2008 Forrester Outlook for E-Business predicts that the US On-line Retail sales will grow to $204 billion in 2008 and continue upward to $334 billion in 2012 as shown in Figure 1 (Johnson, C., 2008).



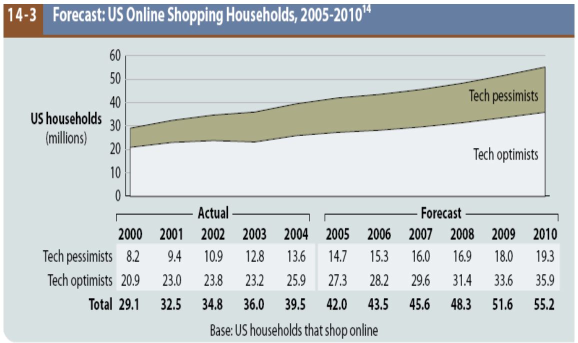
US online retail sales will grow to $204 billion in 2008

Source: January 18, 2008, “US eCommerce Forecast: 2008 To 2012” *Totals represent online retail estimates based on the most recent Forrester estimates of US retail sales for each category

Entire contents © 2008 Forrester Research, Inc. All rights reserved.

Figure 1: US On-line Retail Sales (Johnson, C. 2008)

The growth of on-line transactions is supported by increases in broadband access to the Internet, which is expected to reach 71 million households as DSL, Cable and Wi-Fi fight for the market share. “Three and half million more households shopped on-line in 2004 than in 2003, and we expect an additional 2.4 million household to shop on-line in 2005 en route to 48% of U.S. households shopping on-line in 2010” (Schadler, T., Golvin C., 2005). The forecast for the number of U.S On-line Shopping Households from the period of 2005-2010 is shown in Figure 2.



	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
Tech pessimists	8.2	9.4	10.9	12.8	13.6	14.7	15.3	16.0	16.9	18.0	19.3
Tech optimists	20.9	23.0	23.8	23.2	25.9	27.3	28.2	29.6	31.4	33.6	35.9
Total	**29.1**	**32.5**	**34.8**	**36.0**	**39.5**	**42.0**	**43.5**	**45.6**	**48.3**	**51.6**	**55.2**

Figure 2: US On-line Shopping Household (Schadler, T., Golvin, C., 2005)

E-Commerce businesses have been successful because they provide convenience, enable selection and expose transparency of price, geography etc. Factors contributing to the on-line success include allowing consumers to shop whenever they want without having to think about constraints like physical location or time. Moreover, customers can compare the prices of products on-line and find the best deals. This helps them to rely on the Web as a price-competitive channel.

E-Commerce is not a replacement of traditional commerce channels, but complements the traditional channels. Consumers are now able to do multichannel retailing. They can view the catalogs, visit stores and browse Internet sites. "Forrester's research shows that the key trends currently driving E-Commerce are the mainstreaming of on-line retail, retailers' move to data-driven merchandising, and personalization of experiences and products" (Johnson, C., 2005). The on-line retail market is viewed by consumers as convenient, less costly and ubiquitous. Consumers are more satisfied with the on-line choices they have.

3. TECHNICAL DISCUSSION

3.1 Privacy concerns

The Internet Crime Complaint Center (IC3), which began operation on May 8, 2000, was established as a partnership between the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI). Their objective is to serve as a vehicle to receive, process, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. In 2008, the IC3 website received 275,284 complaint submissions (IC3, 2008). Complaints included auction fraud, non-delivery, and credit/debit card fraud as well as non-fraudulent complaints such as computer intrusions, spam/unsolicited e-mail, and child pornography. The total dollar loss from all referred cases of fraud was $264.6 million with a median dollar loss of $931.00 per complaint. E-mail (74.0%) and web pages (28.9%) were the two primary mechanisms by which the fraudulent contact took place.

The yearly comparison for complaints received by the IC3 for the period of 2000 to 2008 is shown in Figure 3. In 2008 there was a 33.1% increase compared to 2007 when 206,884 complaints were received. Dollar loss of referred complaints was at an all time high in 2008, at $264.59 million, compared to previous years as illustrated in Figure 4 (Internet Crime Complaint Center, 2008).

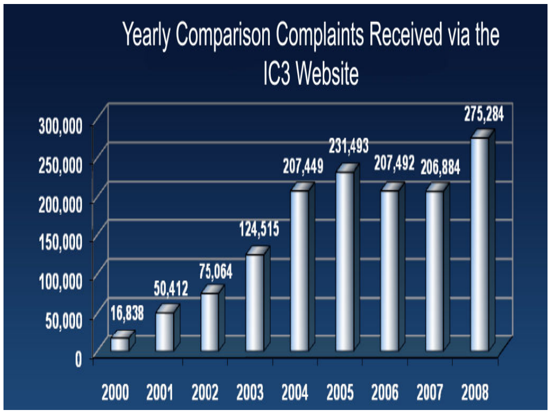


Figure 3: IC3 Web Site Yearly Complaint Comparison, (IC3, 2008).

In 2008, non-delivery of merchandise and/or payment was the most reported offense, comprising 32.9% of referred crime complaints. Auction fraud represented 25.5% of complaints while credit and debit card fraud made up an additional 9.0% of complaints. It is estimated that over 90% of all complaints were related to the Internet and online services.

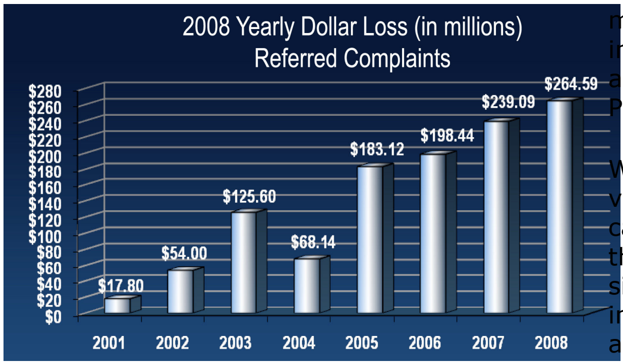


Figure 4: IC3 Web Site Yearly Complaint Dollar Loss (IC3, 2008)

In addition to Internet crime concerns, customers are also worried about the security of their personal information. Consumers' information may be collected without their consent. This raises their concerns regarding identity theft and privacy because they are worried about how their information might be used, stored, misused and retransmitted. Therefore, information security and privacy policies are very important aspect of on-line transactions.

One major privacy threat is capturing of information secretly without user's consent and using it for potentially malicious purposes. Consequently, this may lead to selling information to third parties. Stealing consumer identity information may also result in credit card theft. For Example, in 2007 T.J. Maxx disclosed in a Securities and Exchange Commission filing that more than 45 million credit and debit card numbers may have been stolen from its IT systems over an 18-month period. The data breach at the major retailer will cost the company $100 per lost record, according to database security firm IPLocks. "The effectiveness of the people who stole the information is critical here; they did it for a long time and they sold [the stolen information] out to multiple sources. Those credit card numbers are showing up in foreign countries" (Gaudin, S., 2007).

Cookies are another invasion of users' privacy. They keep track of the user's movements on the website and store it for later identification. Information stored in cookies can be combined with mailing lists and used for potentially damaging purposes. An example of this is America On-line, which "shares information about its users with various partners, including companies that do direct mailing and telephone solicitations" (Chung, W., and Paynter, J., 2002).

Web bugs are another invasion to users' privacy. They are invisible pieces of code that can be used to track users' movements on the Web, pilfer computer files and so on. The simplest form of web bug is a small graphic interchange format that works with cookies and sends information to third parties. Script-based executable bugs can be installed on the user's hard drive to collect information. If these Web bugs are placed on servers, they can be used to control the user's computer from the server. An example of this is the script-based executable bug, which launches multiple browser windows as the user tries to exit the website. Bugs are more invasive to privacy since they can be used to capture user's Internet Protocol (IP) address or install pernicious files on the user's hard drive. The primary privacy concern here is that "with a web bug, the user's computer can be fully exposed to malicious sites that can take any files or information from programs on the user's hard drive without his knowledge or consent (Chung, W., and Paynter, J., 2002).

3.2 Arguments against privacy concerns

Privacy concerns are controversial with many firms utilizing customer data for trend analysis. Firms collect information to provide customized services, identify buying trends and target good and services for specific markets. "Consumers must make choices on how much and what type of privacy they are willing to give up in exchange for outcomes that are valuable to them" (Storey V. C., et al., 2009).

Posner argues that information can have value and corporations will incur costs to discover it (Reis, S., 1984). "Since the corporate gains enhance the economy more than the individual gains", he concludes, "that defense of individual privacy is hard to justify as it can negatively impact these more important corporate gains" (Smith, R., and Shao, J., 2007). This is illustrated by the fact that many retailers collect data about their stores and their shoppers, and many use the information to try to improve sales.

A good example is Wal–Mart, which has access to information about a broad slice of America. The data are gathered item by item at the checkout aisle, then recorded, mapped and updated by store, by state, and by region. By its own count, Wal-Mart has 460 terabytes of data stored on Teradata mainframes. To put this in perspective, the Internet has less than half as much data, according to experts (Hayes, C., 2004). The storage of this large amount of data provides Wal-Mart with the opportunity to perform data mining, data analysis, and the discovery of trends to increase the efficiency and profitability of business. Wal-Mart found "that sales of strawberry Pop-Tarts increases by a factor of seven times the normal sales rate, ahead of a hurricane and the pre-hurricane top-selling item was beer" (Hayes, C., 2004).

3.3 Arguments for privacy concerns

Despite recent technological improvements, consumers still have concerns for their on-line privacy and many users are still reluctant to buy products on-line due to privacy and security reasons. Privacy concerns that must be addressed for improving consumer confidence in the web site include:

- Visits to web sites will be tracked secretly;
- E-mail addresses and other personal information will be captured and shared for marketing and other purposes without permission;
- Personal information will be sold to third parties without permission; and
- Credit Card Theft (Chung, W., and Paynter, J. 2002).

Although writing and enforcing a privacy policy and implementing other privacy enhancing mechanisms are time consuming and costly, a proactive stance makes the "firm appear more consumer focused in the eyes of the consumer, privacy advocates and potential government regulators" (Storey, V., C., et al., 2009).

3.4 Legislation and self regulation

Self-regulation should be used to handle privacy concerns but if it is inadequate, then legislation should be used as a last alternative to handle the issue. The legislation needs to be properly organized in order to be enforceable.

Websites should follow self-regulation if they do not want government involvement in privacy matters. The Federal Trade Commission (FTC) also prefers the websites to self-regulate since the technology changes rapidly. In 1998, the On-line Privacy Alliance was formed and published a self-regulatory policy for on-line companies. To implement privacy policies, a seal system was established. Seals are given only to selected websites that promote the three goals of seals and complies with the policies. The three goals of seals are:

1. Give on-line consumers control over their personal information.
2. Provide web publishers with standardized, cost effective solutions to satisfy businesses and address consumers' anxiety over sharing information.
3. Provide governmental regulators with evidence that the industry can self regulate.

TrustE™ is a self-regulatory privacy regime "that can build consumers' trust and confidence on the Internet through a program in which websites can be licensed to display a privacy seal or trustmark on their websites" (Chung, W., and Paynter, J., 2002). The TRUSTe organization allows E-Business sites to display a trustmark, indicating to consumers that the site adheres to the TRUSTe's privacy principles and practices, which are approved by the U.S. Department of Commerce and the FTC. E-Businesses displaying the trustmark must also allow oversight to ensure that they are compliant with the privacy practices (Smith, R., and Shao, J., 2007).

The European Commission (EC) decided to harmonize data protection regulation across the member states of the European Union (EU) and proposed the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. All members of the EU transposed this legislation into their internal law by 1998. This legislation required that personal data could only be allowed to be transferred to non-EU countries if the country provided an adequate level of protection (Smith, R., and Shao, J., 2007). To satisfy this requirement the EC and the U.S. Department of Commerce adopted the "Safe-Harbor" framework in 2000. Under the safe harbor agreement, U. S. companies can choose to register and enter the safe harbor by self-certifying annually, and agree to comply with the agreement's rules and regulations. EU organizations must ensure and check that the U.S. company is participating with the Safe Harbor agreement prior to sending out the personal information.

3.5 Technological solutions

Technologies to protect individual privacy can generally be split into two main methods: those that attempt to preserve an individual's privacy by enabling anonymous communication channels and those that attempt to minimize the amount of personal information given to an e-business during the on-line interaction (Smith, R., and Shao, J., 2007). Anonymous communication channels attempt to unlink the individual and their personal information, for example, allowing the user to create a virtual identity or scrubbing the data stored by the organization to remove the identity details.

Platform for Privacy Preferences (P3P) attempts to minimize the amount of personal information exchanged and is a protocol for privacy protection on the Web. The World Wide Web Consortium (W3C) is the governing body issuing the standard. The beneficial aspect of P3P is users don't need to read the privacy policies of the websites. "P3P enables websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents" (World Wide Web Consortium, 2007). P3P works through browsers, and it alerts the user when the website collects information about the user. It also tells the consumer what information is being collected by the website. Thus, the websites can express their privacy policies and the users can express their privacy preferences. The users can also go off the website if the website is collecting information about them and users can choose the websites where they want their information released.

Thus, P3P is a smart technology, which allows users to make informed and wise decisions about releasing their information, and protects their privacy. The main philosophy of P3P is that individuals will have to give up some privacy in order to complete transactions with an E-commerce site, but they would be able to at least make an informed choice about which E-commerce sites, they would interact with. P3P is a technology to help consumers and guide their decision-making about whom to trust (Smith, R., and Shao, J., 2007).

E-Commerce transactions take place in an open environment that cannot be trusted since the network is highly vulnerable to outside security threats. This network can be made secure with the help of cryptography. Implementing cryptography can hide content of electronic transactions, detect changes in electronic transactions and confirm the source of electronic transactions (E-commerce Working Group, 2009). Cryptography can be applied through encryption and digital signatures. Cryptography is an effective method of securing E-Commerce transactions that take place over the Internet.

Secure Sockets Layer (SSL) is a commonly used protocol used to encrypt messages between web browsers and web servers (E-commerce Working Group, 2009). It encrypts the datagrams of the Transport Layer protocols. SSL is also widely used by merchants to protect the consumer's information during transmission, such as credit card numbers and other sensitive information. SSL is used to provide security and data integrity over the Internet and thus plays an important role. SSL has now become part of Transport Layer Security (TLS), which is an overall security protocol.

Transport Layer Security (TLS) is a protocol that is used for securing the communications among the applications and their users on the Internet. During the communication between the server and the client, the Transport Layer Security ensures that no message is tampered with and that no third party is able to eavesdrop. TLS consists of two layers – TLS Record Protocol and TLS Handshake Protocol. TLS Record Protocol provides connection security. TLS Handshake Protocol allows the authentication of server and the client, and the negotiation of an encryption algorithm and cryptographic keys, before the exchange of data.

A Virtual Private Network (VPN) can also be created using encryption (E-commerce Working Group, 2009). It is a secure way for machines to communicate though a public network, privately. VPN emulates a private network by specifying endpoints for the secured tunnel and encrypting all of the data that passes through it. The Internet is the backbone for VPNs. Tunneling is a virtual point-to-point connection created through a public network. The four critical functions of Virtual Private Network are authentication, access control, confidentiality and data integrity.

Virtual Private Networks (VPNs) as depicted in Figure 5 offer significant benefits for a company. It extends connectivity to remote sites, thereby reducing the cost and improves the productivity by providing global networking opportunities. VPNs reduce transit time and transportation costs and provide telecommuter support and broadband networking capability.

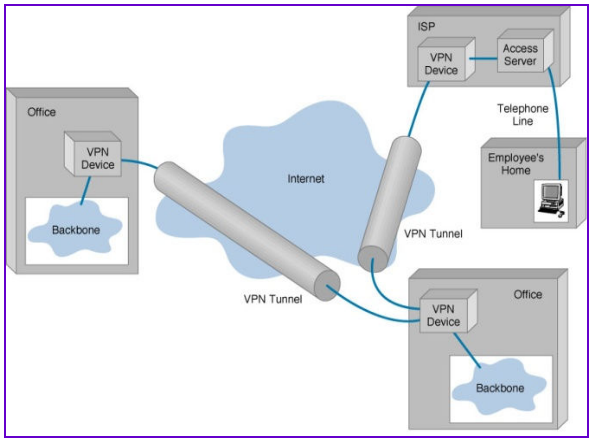


Figure 5: Basic Architecture of Virtual Private Network

Another encryption technique is digital signatures, which provide confirmation of the source of an electronic message and the detection of any changes in the message (E-Commerce Working Group, 2009). Using this technique, forgery can be prevented by proving the authenticity of an electronic transaction. Digital signatures can also prevent impersonation by confirming the identity of the user and providing repudiation including proof of transmission and receipt of transactions. Thus, digital signatures are built into web servers and web browsers with the help of encryption through SSL.

A PKI (Public Key Infrastructure) is required for digital signatures to function correctly (E-commerce Working Group, 2009). Digital certificates are issued by Certification Authorities (CAs) to users after they have confirmed their identity. A PKI is based on digital certificates and assumes the use of public key cryptography.

Public key cryptography is a techniques used to authenticate the sender or encrypt the message. PKI may use one or two different keys at the same time – private key and public key. A PKI consists of Certificate Authority (CA), Registration Authority (RA), directories where the certificates are held and a certified management system. The Certificate Authority issues and verifies the digital certificates. A Registration Authority acts as the verifier for the certificate authority before a digital certificate is issued to a requestor. A certificate includes the public key or information about the public key. Some PKI leaders are RSA, Verisign, GTE CyberTrust, Xcert and Netscape

Electronic payments (in the form of debit/credit cards) should be secured during electronic transactions. SSL is being widely used to encrypt debit/credit card details. SET (Secure Electronic Transactions) is an alternative technique. It uses encryption and enables the authentication of both users and merchants through digital signatures. S/MIME (Secure/Multipurpose Mail Extensions) protocol can also be used as an alternative technique. S/MIME is a standard for secure email and can be used to secure electronic payments. S/MIME provides authentication, message integrity and privacy, and data security. Proprietary systems provide another alternative by providing users with an electronic wallet that stores card details on PC.

Consumers are also looking for ways to protect their privacy themselves (Chung, W., and Paynter, J., 2002). They delete cookies so that their movements are not tracked. Tools like Anonymizer™ can also be used to protect the privacy of users. It is a tool that is used to keep the movements of the users untraceable. This allows the users to surf the web anonymously without giving out their personal information and IP addresses.

Web bug repellents are also being developed by companies to protect the consumers. "Personal Sentinel helps surfers to wash the bugs out of the page by alerting consumers to the risk level of any given website by listing the number of web bugs (Chung, W., and Paynter, J., 2002). Eliminating the threat of web bug, by using repellents would be a great milestone in protecting the privacy of consumers as they pose a great security threat to the users.

3.6 Robust Solutions

A robust solution combining many individual solutions, may be the ideal recommendation to provide adequate privacy and security to consumers. Such a robust solution will consist of legislation, self-regulation and technical solutions, integrated together to achieve this goal. As an example, P3P does not help in protecting data, therefore, the addition of self-regulation and legislation can help in assuring consumers that their information would be protected. In this way, all the solutions combined would give the high level of desired privacy to consumers. Technical solutions and self-regulation may help in enhancing the protection of consumers' privacy, but are not enough. Legislation is also required to address the overall issues of consumer privacy and security.

The global economy requires companies to operate under different principles in different countries leading to country specific law and regulations. The net result is that a global company will be forced to comply with different requirements across other countries. For example, Personal Information Protection and Electronic Documents Act (PIPEDA) manages privacy issues in Canada whereas FTC manages privacy issues in the U.S.A. Ideally an effective, global and consistent set of privacy legislation can be developed, when these different governments and policy makers from different countries come together. There are certain global projects already under way, such as Automotive Industry Action Group (AIAG) in U.S.A. (Mears, J., et al., 2002). AIAG is working on industry standards and prefers the Open Application Group's Business Object Documents to work on XML (eXtensible Markup Language) technical elements.

A global effort is already being undertaken with the European Union activities for Digital Business Ecosystem (DBE) (Dini, P., and Nicolai, A., 2003). The European Union (EU) Framework Program 6 (FP6) with its Digital Business Ecosystem (DBE) Project and other Web Science Research Initiatives have established the foundation of a digital, decentralized and interdisciplinary environment for Small and Medium Enterprises (SMEs) in Europe. The DBE Project, which started in 2002, is constantly maturing and has strong potential to be applied on a global scale.

4. CONCLUSIONS

E-Commerce sales are rising but privacy issues are coming into light as more and more consumers become concerned about the protection of their personal information. Privacy is an important issue that needs to be addressed to ensure the future growth of E-Commerce. Surveys have shown that E-Commerce is losing a significant amount of income due to the privacy and security concerns of its potential user base. E-commerce businesses must have the "ability to give consumers control of their privacy in an attempt to create an acceptable level of trust, which is essential" (Smith, R., and Shao, J. 2007).

On-line companies need to gain customer's trust to retain their existing E-Commerce market share and provide for growth. To ensure security, the companies need to adopt privacy policies for safeguarding the consumer's information. In order to achieve this, legislation, self-regulation, technical solutions and robust solutions should be implemented.

5. OPPORTUNITIES FOR FUTURE RESEARCH

Addressing the issue of protecting consumers' privacy opens the door for many research opportunities. Different research efforts are currently being undertaken related to E-Commerce companies, the government, the interaction between the consumer and the E-Commerce company, the interaction between the consumer and the government, and the interaction between the E-Commerce company and the government.

Research opportunities related to the company perspective are:

- Research needs to be done on the actual privacy practices of E-Commerce companies.
- How do the privacy practices of companies affect their relationship with consumers in the short term and long term?
- Do the privacy policies released by companies deal with consumers effectively?
- What is the difference between the websites that post privacy policies and the websites that do not? Do the sites that post privacy policies have anything in common? (Efrim Boritz, J. et al., 2008).

Research opportunities related to government prospective are:

- Countries adopt different privacy policies. Research should be done to find out if any universal privacy practices exist across countries. Research should also be done to develop international privacy standards.
- What factors influence government to regulate privacy practices?
- What steps need to be taken to ensure that the information of consumers is protected by the government and used fairly? (Efrim Boritz, J. et al., 2008).

Research opportunities related to consumer-company interaction are:

- Do companies benefit by addressing the consumers about their privacy concerns? Would the companies be more willing to address privacy concerns if they gain benefits?
- Are the actual actions of users in synch with their stated actions?
- When the websites post the privacy statements on their websites, how do the users perceive it, and does it address their concerns?
- How do the users perceive the privacy seals on the websites? Are there any specific situations where these seals are useful? Are there any differences between the companies that have privacy seals on their websites and those that do not have them? (Efrim Boritz, J. et al., 2008)

Research opportunities in consumer-government interaction are:

- Since the consumers' concerns regarding privacy keep changing and it takes time for the new regulation to be effective, is the self regulation approach effective to consumers' privacy concerns and is it an effective approach to protect the privacy of consumers?
- Do consumers' concerns influence government regulations?
- Different regulations are being implemented in different countries. What is their impact on consumer's concerns regarding privacy? (Efrim Boritz, J. et al., 2008).

Research opportunities in company-government interaction are:

- Regulation forms the basis for most companies in order to develop their privacy policies. Do the companies follow the privacy regulations stated by the government?
- What impact do the enacted and pending regulations have on the privacy policies of the companies?
- Due to different regulations in the countries, are the privacy policies in one company different from the privacy policies in other countries? The differences in the privacy policies may be a challenging task for companies trying to establish global markets. Do the company's business units in counties with less strict regulations have less comprehensive policies than business units in counties with strict regulations? (Efrim Boritz, J. et al., 2008).

These research opportunities would provide a new set of insights and results, which would be beneficial to understanding the core issues and lead to the appropriate steps to safeguard the existing systems.

6. RECOMMENDATIONS

The topic of E-Commerce Security provides an abundance of research opportunities. The authors recommend that the research should be continued. The development of new standards in order to protect the privacy of the consumers is very important and critical to the continued growth of E-Commerce. Proper laws should be legislated to ensure consumer privacy, since it has been shown that self-regulation is not always ideal.

Laws in other countries should also be researched and standard international policies should be adopted at a global level. Consumers, companies and the government should work together with integrity to protect the privacy rights of the consumers.

Many companies are already following this research trend and boosting their sales online. Many more are likely to follow and achieve large profits. It is imperative that companies understand achieving success and sustaining competitiveness in the highly volatile and demanding E-Commerce market "lies in their ability to securely protect their information assets and IT infrastructure" (Diamin, M. T., et al., 2009).

The scope of E-Commerce security must be one of a strategic governance activity and requires a more coordinated and focused effort from the national and international society, governments and the private sector. A good, hard, dedicated effort from the companies and the government is desired to win the trust of the consumers. Both technical protections and security statements are significant factors for improving consumers' perceived security, which is positively related to consumers' perceived trust and increase E-Commerce usage (Kim, C., et al., 2009).

In summary, E-Commerce Security should be considered with utmost importance and appropriate steps should be taken to implement comprehensive security practices on E-Commerce sites. It is in the best interest of the E-Commerce entire community to follow good privacy practices, implement good security methods, and protect consumers' information in the interest of growing the E-Commerce activity and helping the industry improve.

7. REFERENCES

Baseline (2006), "Gartner: $2 Billion in E-Commerce Sales Lost Because of Security Fears", Nov 27, 2006, Ziff Davis Media Inc.

Chung, W., Paynter, J.,(2002), "Privacy issues on the Internet," IEEE, *2002, Proceedings of the 35th Annual Hawaii International Conference on System Sciences,* pp 9, 7-10 Jan. 2002 retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=994191&isnumber=21442

Damini, M. T., Eloff, J. H. P., Eloff, M. M., (2009), "Internet Security: The Moving Target", *Computers & Security* (article in press).

Dini, P., and Nicolai, A., (2003), "The Digital Business Ecosystem - FP6 IST E- Business Integrated Project", retrieved from http://www.digitalecosystems.org/cluster/dbe/dbe_summary_cc.pdf

E-Commerce Working Group, Universal Postal Union, "E-Commerce Security", retrieved from http://www.upu.int/security/en/E-commerce_security_en.pdf

E-Commerce Land, (2004), "History of Ecommerce" retrieved from http://www.ecommerce-land.com/history_ecommerce.html

Efrim Boritz, J.; Won Gyun No; Sundarraj, R.P., (2008), "Internet Privacy in E-Commerce: Framework, Review, and Opportunities for Future Research," *IEEE, Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*, 204, 7-10 Jan. 2008.

Gaudin, S. (2007), "Estimates put the T. J. MAXX Security Fiasco at $4.5 Billion", *Information Week,* May 2, 2007.

Hayes, C. L., (2004), "Wal-Mart appetite for data raises concerns" *New York Times*, Nov. 26, 2004.

Internet Crime Complaint Center, Bureau of Justice Assistance, Federal Bureau of Investigation, The National White Collar Crime Center, Internet Crime Complaint Center, 2008 Internet Cyber Crime Report, Retrieved July 27, 2009 from http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf

Johnson, C., (2005), "Topic Overview: US Online Retail", Forrester Research Inc., Cambridge, MA, 1-7.

Johnson, C., (2008), Teleconference: The 2008 Outlook for E-Business, Forrester Research Inc., Cambridge, MA, 1-39.

Kim, C., Tao, W., Shin, N., Kim, K. S., (2009), An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications*, (article in press).

Mears, J., Connor, D., Martin, M., (2002), September 11: One year later--what has changed. *Network World*, 19(35), 1, 12+. Retrieved November 23, 2008, from ABI/INFORM Global database. (Document ID: 158530181).

Mulpuru, S., (2007), Topic Overview: US On-line Retail, Forrester Research Inc., Cambridge, MA, 1-7.

Pressman, R., Lowe, R. (2009), WEB Engineering A Practitioners Approach, McGraw Hill Higher Education, New York, N.Y.

Reiss, S. P., (1984), Practical data swapping: the first steps, *ACM Transactions on Database Systems,* 9(1), 20-37.

Schadler, T., Golvin, C., (2005), The State of Consumers and Technology: Benchmark 2005, Forrester Research Inc., Cambridge, MA, 1-25.

Smith, R., Shao, J., (2007), "Privacy and e-commerce: a consumer-centric perspective", *Electron Commerce Res*, 7, 89-116.

Storey, V., C., Kane, G., C., Schwaig, K., S., (2009), "The Quality of On-line Privacy Policies: A resource-Dependency Perspective", *Journal of Database Management Systems*, 20(2), 19-37.

World Wide Web Consortium, (Oct. 2007), "Platform for Privacy Preferences (P3P) Project", retrieved from http://www.w3.org/P3P