Privacy Protection in Electronic Commerce – A Theoretical Framework

Milena Head and Yufei Yuan
Michael G. DeGroote School of Business
McMaster University
Hamilton, Ontario, Canada
headm@mcmaster.ca; yuanyuf@mcmaster.ca

Head, M., Yuan, Y. (2001). "Privacy Protection in Electronic Commerce: A Theoretical Framework", *Human Systems Management*, 20, pp.149-160.

Abstract

In this paper, a theoretical framework for privacy protection in electronic commerce is provided. This framework allows us to identify the key players and their interactions in the context of privacy violation and protection. It also helps to discover the responsibilities of the key players and areas for further research.

Keywords: Electronic commerce, Privacy protection, Privacy policy, Privacy Violation, Self-regulation, Anonymity

Milena M. Head is an assistant professor of management science and information systems in the Michael G. DeGroote School of Business at McMaster University. Her research interests are in topics that relate to electronic commerce and human-computer interaction, including World Wide Web navigation, Web-based agents, electronic commerce intermediaries, online privacy, information retrieval and interface design. She holds a Ph.D. (1998) and a Master of Business Administration (1993) from McMaster University and a BMath (1991) from the University of Waterloo. She has published in *International Journal of Human-Computer Studies, Interacting with Computers*, and has presented articles at several conferences.

Yufei Yuan is a professor of information systems in the Michael G. DeGroote School of Business at McMaster University. He received his Ph.D. in Computer Information Systems from the University of Michigan in 1985. His research interests are in the area of matching problems, approximate reasoning with fuzzy logic, decision support in health care, Web-based negotiation support system, electronic commerce and privacy. He has published more than 30 papers in professional journals such as *Management Science, Fuzzy Sets and Systems, European Journal of Operational Research, Academic Medicine, Medical Decision Making, International Journal of Human-Computer Systems*, and others.

1. Introduction

The potential of electronic commerce has attracted the attention of many business and consumers. However, online shopping has not been adopted as quickly as expected. Internet users are concerned about the privacy of information they supply to Web sites [26], and this is one factor that has been holding them back from open acceptance of the electronic marketplace. Many people believe privacy protection in the United States is inadequate. A recent Harris Poll shows that 84% of Americans are concerned about threats to personal privacy, and 78% believe consumers have lost control over how their personal information is used [27]. Researchers at the Wharton School of Business claim that privacy and security concerns are actually driving people away from the Internet [18]. The cost of privacy violation to potential economic growth is rising in America. What was once seen as a threat to civil society is now a clear and present danger to the economic health of the country. Unless privacy is adequately protected, the revolutionary potential of the Internet may not be realized [10].

Information privacy is the "claim of individuals, groups, or institutions to determine for themselves when, and to what extent, information about them is communicated to others" [1]. Privacy protection should prevent non-permitted, illegal, and/or unethical use of private information. It is important to note that the right of privacy is not absolute. Privacy must be balanced against the needs of society. Criminals may use privacy protection to cover their crimes. The public's right to know surmounts the individual's right of privacy.

Security and privacy are often related to each other but they are not the same. In the computer security community there is still much confusion between privacy and security concepts. Privacy requires security, because without the ability to control access and distribution of information privacy cannot be protected. But security is not privacy. Information is secure if the *owner* of information can control that information. Information is private if the *subject* of information can control that information. Anonymous information has no subject, and thus ensures that information is private. Anonymity requires security and guarantees privacy, but is neither [3].

The complexity of manually collecting, sorting, filing, and accessing information from several different agencies was, in many cases, a built-in protection against the misuse of private information. However, in the Internet and Web environment, information about users can be easily collected, integrated and analyzed from different sources through the use of network, database, data warehouse and data mining technologies. The potential of privacy violation therefore becomes much higher. Technologies such as firewalls, public key encryption, secure sockets layer have been used to improve security, but they may not necessarily protect consumers' privacy.

Privacy protection is a very complex issue. It is not simply a technical, but mostly an economical, social, and legal issue, that involves multiple parties often with conflicting interests. From one side, businesses want to use information technology to identify, collect, and even trade customers' personal and preference information in order to make

profit. Unfortunately this may result in a violation of customers' privacy. From the other side, consumers may appreciate the personalized service from electronic commerce, but they worry about loosing their privacy. They look to government and third parties for protection. It is important for us to study how the different parties interact with each other in the context of privacy violation and protection.

In this paper, we develop a framework for privacy protection where we identify the key parties involved (Section 3) and their interactions (Section 4). Section 5 outlines privacy violations and Section 6 gives a description of current privacy protectors. We examine the responsibilities of each party in Section 7. Finally, we identify some potential areas for future research.

2. A Framework for Privacy Protection

Privacy issues have caught a great deal of attention from the media. However, to the best of our knowledge, an abstract framework of the privacy protection landscape (parties and their interactions) has not been reported in the literature. We present such a framework in Figure 1, where the major parties are represented by boxes, and their interactions are indicated by arrows. There are four main parties involved in the context of privacy protection: 1) the privacy subject, who wishes to control the dissemination of personal information to collectors; 2) the collector, who wishes to collect private information for business purpose; 3) the illegal user or violator, who illegally or unethically acquires, stores, sells or uses the subject's private information; and 4) the privacy protector, whose duty it is to safeguard the rights of the subject by stopping the violator and setting guidelines for the collector.

The four parties interact with each other through three interrelated activities: 1) information collection activities; 2) privacy violation activities; and 3) privacy protection activities. Although information collection is necessary to provide many valuable business services, the excessive and inappropriate collection of personal information may damage customer confidence and drive them away. Privacy violation, motivated by profit or crime, may result in reputation damage or financial loss of the subject as well as the collector involved. Although government legislators and self-regulatory interest groups play an active and vital role in privacy protection, all parties have their share in a joint effort to uphold privacy rights.

To stimulate a healthy electronic commerce environment, privacy protection and business and public interests must be balanced. Analyzing the activities and information flows among the privacy parties helps us to better understand how privacy can be appropriately protected in the electronic marketplace. Our framework also helps us to better examine the key roles and responsibilities of various parties in fostering appropriate privacy practices, and allows us to identify areas requiring further research and understanding.

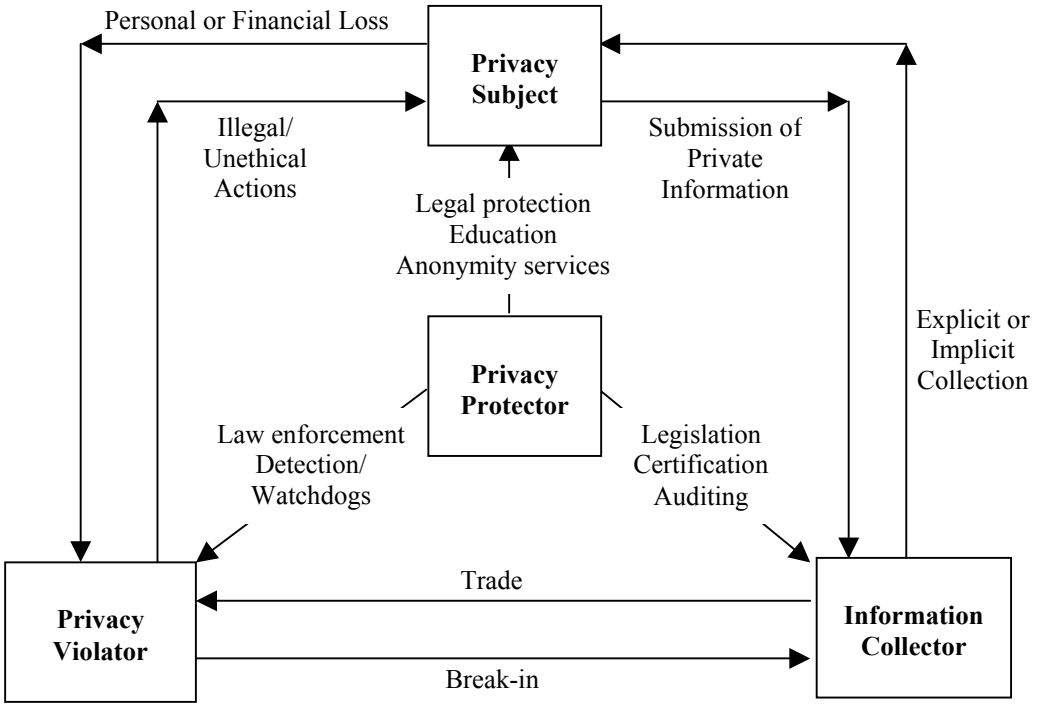

Figure 1 : A Theoretical Framework for Privacy Protection in Electronic Commerce

3. Privacy Parties

Privacy Subject
The privacy subject is an individual or organization that has a concern and the legal right to control the sharing of information about itself. For instance, a patient is a privacy subject who has a concern and the right to control the sharing of her health information. She may be willing to share her health information with a medical doctor but may not want other people to access it without her consent. Similarly, an online customer may not want a company to sell her purchase details to others.

Information Collector
The collector is an individual or organization that collects private information from privacy subjects. Information collection is often necessary to provide subjects with services. For instance, the government collects information about citizens' income and tax payments, banks collect information about clients' payment transactions and hospitals collect patient information for health care. Once the private information is gathered, it is the collector's legal responsibility to maintain its security and privacy.

Internet, database and data mining technologies allow collectors to compile extensive information about individuals from many different sources. The Government is one of the largest collectors and producers of these personal information dossiers. Virtually

every major event in an individual's life is recorded as a government document. Financial institutes such as banks, insurance and credit card companies hold detailed financial data of individuals and companies. Although hospitals hold a large amount information about their patients, much of their documentation is still paper-based and is not electronically shared. However, as more patient information becomes computerized, the sharing of this medical information will become a major issue.

Privacy Violator
The privacy violator is an individual or organization that illegally or unethically collects, distributes, and uses private information without the consent of the subject. For example, when a company sells consumers' email address to another company for online promotion without the permission of consumers, both buyer and seller companies become privacy violators. A more serious type of violator is the hacker who breaks in and steals personal information to commit fraud.

Privacy Protector
The privacy protector is an individual or organization that aims to protect the privacy of subjects. This includes government legislators and self-regulatory agencies that provide information, services and tools to enhance privacy awareness and protection. Details on privacy protectors are provided in section 6.

4. Information Collection Process

To conduct business and provide valuable services, it is often necessary to collect information from customers. The collector may collect private information from subjects explicitly or implicitly, and may integrate information from difference sources.

Explicit Collection: When a user visits a web site, information may be collected explicitly though the use of forms. For example, a customer may be required to provide personal information for user registration to download free software. To complete a business transaction, it is necessary to collect certain information, such as method of payment and shipping address. However businesses tend to collect more information than is absolutely necessary to complete the transaction. The electronic format of online shopping enables companies to amass large customer databases that can be used for customized target marketing. Web-gathered information about site visitors can help transform window shoppers into buyers.

Some customers may feel comfortable giving away their personal information but most are more cautious. Trust, which can be influenced by many factors, is critical to information disclosure. Cranor et al [6] found that Internet users are more likely to provide information when they are not identified. Some types of data, such as credit card numbers and social security numbers, are more sensitive than others, such as email addresses. The acceptance of persistent identifiers varies according to its purpose, and Internet users generally dislike unsolicited communication. It is valuable for businesses to understand users' privacy concerns, so that actions can be taken to build customer trust and willingness to disclose information.

Implicit Collection: The second type of information collection is implicit, which may be viewed as "covert" collection since privacy subjects often do not realize they are giving away personal information. When browsers send an HTTP request to view a Web page, Web servers can automatically collect information such as the subject's IP address, domain or host name, computer type, browser capabilities, as well as a trace of other Web pages visited and time spent on each page. FTP and e-mail application may also reveal the user's identity. Cookies are another implicit collection tool, where the Web server creates a small text file to be stored on the user's hard disk for the purpose of data gathering. Cookies can be used for online ordering, storage of userids, passwords and preferences, Website tracking, site personalization, and targeted marketing. Cookies are increasingly being used by advertisers to accumulate Internet user data and build user profiles.

Most users are not aware of the extent of automatic information gathering and tracking. Therefore customer trust is not affected until privacy protectors, such as advisors or watchdogs, expose these practices to the public. The public may then compare these actions to a spy following a customer in a department store while taking detailed notes on the customer's activities. Many people consider this practice a privacy violation, which has a large negative impact on trust. In fact, 86% of respondents in a recent survey [6] reported no interest in features that implicitly transfer their data to Web sites without any user intervention.

Integration from multiple sources: Customer data can be gathered independently or it can be integrated from different sources to establish a detailed customer profile for target marketing. For instance, customer preferences can be correlated to geographic location, income level, health status, and so on. This information is gathered because data has a monetary value. It may be used for customized target marketing to help transform window shoppers into buyers or it can be sold to other companies with similar motivations. If information is aggregated without identifying individuals, anonymity is maintained and privacy may not be violated. However, if the information includes the identity of individuals without consent from the subjects, privacy is breached and the collector also becomes a privacy violator.

Although the collection of personal information is necessary, excessive and inappropriate collection without subjects' consent will damage customers' trust and drive away their business. This can also open the door for possible privacy violations. According to Coursey (2001) the most serious danger to privacy comes from those that gather data for "other reasons – especially if they can assemble the data from multiple sources into complete consumer profiles. Imagine what someone would know about you if they could combine your credit card, banking, insurance, and utility bills with all the UPC scan information from your grocery shopping".

5. The Violation of Privacy

Privacy violation refers to the acquisition, storage, selling and use of private information without the awareness and/or consent of the subject. These actions can result in personal or monetary harm or damage. Businesses are economically motivated to collect and use great amounts of personal information because "personal details are acquiring enormous financial value. They are the new currency of the digital economy" [20]. Many may be tempted by the profit potential from the sale of personal data. The Internet is a new and expanding medium, where "companies say they need information on people to target their products, build their business models, and plan their marketing campaigns. The government, in turn, justifies its attack on private communications in the name of combating crime and terrorism" [10].

Illegal or Unethical Acquisition: Implicit or covert collection of personal data is performed daily by businesses seeking a competitive advantage. Acquisition becomes a privacy violation when it is collected without consent and the subject's identity remains associated with the personal information. For example, RealJukebox, an interactive application that helps users keep track of their CD libraries, was charged with a half-billion dollar lawsuit for invading its users' privacy rights. The program automatically uploaded the user's unique CD identifier without notification or permission.

Hackers are another class of violators. Individuals who "hack" into computer systems may do so for a variety of reasons: pleasure, entertainment, personal and monetary gain, as well as for philosophical, political and ideological reasons. Hackers may acquire information directly from the privacy subject, but more often they steal from the collectors' larger information databases.

Illegal or Unethical Storage: Information may be collected for use in the immediate future, or collected for long term storage. Long term storage of personal data affects people's rights to choose what information they wish to reveal about their past. For example, one may not want a future employer to have access to inappropriate newsgroup postings made during adolescence. In the recent Microsoft trial, e-mail communications sent over five years ago was some damaging evidence [25]. Repeatedly, email from years past is being used in litigation as evidence against companies at a cost of billions of dollars each year.

Illegal or Unethical Selling: The more times personal information is bought and sold over the Internet, the more likely it will fall into the wrong hands. GeoCities, which has several million members, was the first Federal Trade Commission case involving Internet privacy. In order to become a member of GeoCities (http://www.geocities.com), individuals were asked to complete an online form requesting personal information such as e-mail and postal addresses, interests and demographics. GeoCities mislead its members to believe this information would not be disclosed to third parties, when in fact this information was sold to target marketers for solicitations beyond those agreed to by the members [24]. Even the government can be a privacy violator. U.S. residents in Florida were surprised and angry when they learned that personal information, including

their pictures, collected for their state driver's license had been sold to a private company for a purpose that had nothing to do with securing permission to drive [21].

Illegal or Unethical Use: Whether information was gathered ethically or not, it is the use of this information that can result in violations with significant consequences. These violations directly affect the subject through the delivery of unsolicited "spam" mail or through more serious personal and/or monetary damage. For example, in the landmark privacy case, the U.S. Navy discharged sailor Timothy McVeigh after AOL violated its own privacy policy by confirming to a naval investigator that an anonymous user profile in which the word "gay" was used to describe a member's marital status belonged to McVeigh [17]. Hackers that perpetrate credit card fraud and identity theft are not only serious violators of privacy, but can impose severe personal and/or monetary consequences. The Privacy Rights Clearinghouse (http://www.privacyrights.org) estimates that over 400,000 thefts of identification occur each year at a cost of some $2 billion.

6. Protecting Privacy

Government legislation and self-regulation are two major mechanisms for privacy protection. The effectiveness of privacy protection, however, depends on the joint effort of all the parties involved.

6.1 Government Legislation

The focus of government in privacy protection is to legally recognize subjects' rights, to provide guidance and boundaries for collectors' acceptable behavior, and to provide warnings and legal consequences for violators' illegal and unethical behavior. In Europe, the European Community has taken aggressive legislative steps toward safeguarding privacy rights with respect to personal data processing. The European Commission has established a Directive on Personal Data Protection (Directive 95/46/EC) that grants members of the European Union the following rights [11]: the right to know the source of personal data processing and the purposes of such processing; the right to access own personal data; the right to rectify inaccuracies in own personal data; the right to disallow the use of own personal data (for example, in direct marketing). In addition to the European Union, Asia, Canada, and other regions have embraced stronger government legislation to protect privacy in cyberspace [4]. For example, Canada's Personal Information Protection and Electronic Documents Act (Bill C-6) will come into force on January 1, 2001. The act will help to meet the protection standards set by the European Union by establishing clear rules that govern the collection, use and disclosure of personal information in the private sector [22]. Organizations such as the OECD (Organization for Economic Co-operation and Development; http://www.oecd.org/), which has a twenty-nine country membership, are directed towards promoting an internationally coordinated approach to privacy policy making for global networks.

In contrast, the United States government has not taken any major actions towards regulating the gathering and sharing of personal information across the Internet. However, the Federal Trade Commission (FTC) has implemented the Children's Online

Privacy Protection Act (as of April 2000), which states "certain Web sites must obtain parental consent before collecting personal information from children under the age of 13" [13]. The FTC has outlined a federal privacy policy that would require Web sites to inform customers of their information practices (notice), offer choices on how their information is used (choice), provide access to stored information (access), and sufficiently protect their information (security) [14]. However this policy has not been introduced to Congress, as the focus in the United States is towards self-regulation [16]. The FTC's goal has been to encourage and facilitate effective self-regulation, with the belief that "greater protection of personal privacy on the Web will not only protect consumers, but also increase consumer confidence and ultimately their participation in the online marketplace". Interestingly, a recent Lou Harris & Associates survey shows that 80% of U.S. Internet users agree to allow industry and public-interest groups to self-regulate privacy rules and practices and to legislate only if the private sector fails to implement these policies [27].

6.2 Self-Regulation

We examine the privacy self-regulation initiatives along the categories of protection advisors, watchdogs, certification programs, and anonymity services. The examples provided in this discussion are used to illustrate concepts and are not meant to be a comprehensive listing of available products and services.

Protection Advisors: People may not be aware how to protect their privacy. Various organizations, associations and centers focus on supplying privacy education for subjects. By providing various sources of detailed online privacy information, subjects can make informed decisions on how and when they disseminate personal data. For example, the Electronic Privacy Information Center (http://www.epic.org) is a public interest research center in Washington, D.C that provides extensive information on civil liberty issues and privacy protection. The Privacy Rights Clearinghouse (http://www.privacyrights.org) offers a privacy survival guide that outlines how and when personal information should be provided. Users can also discover the amount of personal information that is stored in major industry and government databases. The Online Privacy Alliance (http://www.privacyalliance.org) is a diverse group of corporations and associations that lead, support and inform on self-regulatory initiatives. More specialized centers, such as Cookie Central (http://www.cookiecentral.com), are dedicated to provide information and resources for Internet cookies.

Various tools have been developed that allow Web users to monitor the information collected by Web sites and given by Web browsers. Enonymous Advisor (http://www.enonymous.com) queries each requested Web page and displays a privacy policy rating for the site. Users can then decide if they wish to continue searching the site and submit the requested personal information. "I Can See You" (http://privacy.net/anonymizer/) performs a privacy analysis of an individual's Internet connection. This is a free service that shows the user exactly what information is revealed while browsing Web pages. These tools help to educate the Web public about the degree of data collection through the Internet, and allow them to make an informed decision about their personal online privacy procedures.

The World Wide Web Consortium (W3C)'s Platform for Privacy Preferences Project (P3P) attempts to provide a framework for informed online interactions. The P3P initiative provides a way for a Web site to encode its data-collection and data-use practices in a standardized, machine-readable XML format. Users would not need to read the privacy policy at every site they visit, since these policies could be interpreted by user agents that automate decision-making when appropriate. The implementation of this standard would allow Web users to clearly understand what data is collected by sites they visit, how that data is used, and what data/uses they may "opt-out" of or "opt-in" to [7]. The P3P would not be a final solution, but a complement to other technologies as well as legislative and self-regulatory approaches to privacy [23].

Privacy Watchdogs: The focus of the privacy watchdog, such as EPIC (Electronic Privacy Information Center) and Alert (http://www.epic.org/alert/), is to identify violators and publicize their actions to alert privacy subjects. The CDT (Center of Democracy and Technology) unveiled a Privacy Watchdog site to help Internet users communicate their privacy concerns to Web sites and join an ongoing campaign to monitor the privacy practices of businesses operating online. "The CDT Watchdog site is a way for consumers to show that privacy matters. This tool lets users send a clear privacy message to the business community," says Deirdre Mulligan, CDT Staff Counsel (http://watchdog.cdt.org). The vigilance of watchdogs, such as the media, is the most powerful tool to correct or stop the improper behaviour of the violator. The DoubleClick case is a good example of how the publication of unethical practices can result in the quick reaction and correction of the violator [9].

Certification Programs: The focus of certification programs is to encourage the collectors to follow acceptable privacy principles, which will help to build trust among privacy subjects. Certification programs provide guidelines for privacy disclosures and associate a trusted and branded "seal" with sites that follow those guidelines [2]. Web sites that display a trust label seal convey a message to users that they openly disclose their information collection and dissemination procedures, and that this disclosure is assured by a credible third-party regulator. A recent Louis Harris & Associates Survey [27] indicates that 79% of Internet users believe that such privacy auditing programs would improve online privacy practices.

The two most popular trust label programs are TRUSTe (http://www.truste.org) and BBBOnLine (http://www.bbbonline.org). The TRUSTe "trustmark" is awarded to sites that adhere to established privacy principles and are willing to comply with oversight and consumer resolution procedures. Similarly, the BBBOnLine Privacy Program offers a "seal" to companies that post their online privacy policies that meet the core principles of the Better Business Bureau (disclosure, choice and security), monitors compliance and presents specific consequences for non-compliance. WebTrust (http://www.webtrust.net/) is a less known initiatives administered by professional accountants, which offers a certification program to assure Web users that their transactions are safe and secure and their privacy is protected.

Trust label programs can only succeed if they are vigilant in their monitoring and strict in upholding their privacy standards. RealNetworks had a TRUSTe privacy seal when their RealJukebox application was automatically uploading users' unique CD identifier without their notification or permission. In this case, RealNetworks was not violating the privacy policy of TRUSTe, which only dealt with information collected through a Web site, not information collected by an interactive program. Similarly, GeoCities remained a member of TRUSTe even while its privacy practices came under question by the FTC. In fact, TRUSTe has not seriously disciplined any site, creating the impression that they are not willing to scorn their members and sponsors [16]. It is also important for these self-regulatory initiatives to be linked to a familiar and trusted organization, and efforts must be made to raise their customer awareness. A recent survey [6] showed that people do not seem to understand privacy seal programs.

Anonymity Services: While privacy is the ability of subjects to protect information, anonymity is the privacy of identity. Anonymity is essential to protect free speech. It can be used to protect activists of human rights, challengers of political policy, writers of controversial material, and others where revealing an individual's identity may threaten their life or wellbeing. However anonymity also opens the door for criminals to plan and coordinate attacks in an environment where authorities have no way to find and stop them.

Various organizations provide anonymity services for sending and receiving e-mail messages, surfing the Web, and online payment. The focus of the anonymity service is to block the violator's collection actions and to provide subjects with self-defense tools that hide private information from violators and collectors.

Anonymous E-mail

An anonymous remailer service can hide e-mail sender and recipient information from eavesdroppers. Messages are resent through several servers (called remailers) such that any server along the remailing chain can only see the address of the previous remailer, not the originator. Message encryption can be included at each link of the chain for further privacy and more sophisticated remailers use a constant-length message, to prevent eavesdroppers from matching up incoming and outgoing messages by size. Message recipients may also remain private by posting messages encrypted by the recipient's public key to large mailing lists or newsgroups. Some examples include Cypherpunks Remailers (http://www.CSUA.Berkeley.EDU/cypherpunks/remailer/), Mixmaster Remailers (http://www.publius.net/mixmaster-list.html), the W3- Anonymous Remailer (http://www.gilc.org/speech/anonymous/remailer.html), and Private Idaho (http://www.eskimo.com/~joelm/pi.html).

E-mail account providers are realizing the increasing concern over privacy issues among the Internet community. For example, ZipLip Plus (https://www.ziplip.com) offers a Web-based secure and private e-mail account where the sender can prohibit messages from being copied, pasted, forwarded, printed or screen dumped by the recipient. Messages do not travel Internet lines, but are centrally stored on a secure server to be accessed only by intended recipients. Public/private key encryption can be used to hide

message content as well as the sender and recipient information. Storage centralization allows the sender to control the only existing copy of the message and ensure complete deletion.

Anonymous Web Surfing

An effective way to surf the Web anonymously is through proxy servers. Proxy servers sit between Web users and the sites they visit. Instead of capturing the user's personal information, Web servers can only see the proxy's identification. Proxy servers are often found in corporate environments and personal versions may be purchased for home use, however various public proxy server networks have also been established to conceal personal identities. For example, Anonymizer (http://www.anonymizer.com) serves as a surrogate for the Web user blocking Web servers from gathering personal information or tracking surfing behavior. URL encryption also prevents logging by Internet service providers. Freedom, a privacy system launched by Zero-Knowledge (http://www.zks.net), uses encryption and untraceable digital identities called "nyms" to route Web communication through a globally distributed network of anonymous servers. The Lucent Personalized Web Assistant (http://www.bell-labs.com/project/lpwa/) is a pseudonym agent that creates different, but consistent, aliases for each Web site and removes the personal information that browsers automatically send with each request.

Cookies are a common tool to identify and track Web users. Most current Web browsers allow the user to specify their preferences for cookie control. In Netscape's Navigator, users can "accept all cookies", "accepts only cookies that get sent back to the originating server", "disable cookies", or be warned before accepting a cookie. Similarly, in Microsoft's Internet Explorer users can set security levels that determine if cookies are enabled, disabled, or prompted. It is important to note that most Web browsers enable cookie acceptance by default, and some sites will not provide access to users that do not accept their cookies. Internet tools have been developed that give Web users more flexibility and control over their cookie management. For example, the Internet Junkbuster Proxy (http://www.junkbusters.com) blocks unwanted banner ads and protects Web surfing privacy from cookies. Cookie Crusher (http://www.thelimitsoft.com /cookie.html) controls cookies before they are placed on the user's hard drive, and Cookie Cruncher (http://www.RBAworld2.com/index.shtml) allows the user to view, edit, and delete Internet cookies through an easy to use interface.

Anonymous Payment

Outside of the Internet, cash is the most effective means for maintaining anonymity in payment. Check, debit and credit transactions allow financial institutions to track purchasing behavior. On the Internet, the anonymity of cash can be reflected in digital cash or smart cards. eCash Technologies Inc. (http://www/ecash.net) is striving to develop a worldwide standard for digital currency. The blind signature encryption technology of eCash ensures privacy of transactions, since the bank cannot link the identity of the user to the electronic coin. Banks can prevent the double spending of electronic coins by maintaining a list of spent coins and verifying if coins are already on this list. More advanced digital cash systems have been proposed that use restrictive blind signatures, fair blind signatures, and blind weak signatures (see [5] for details).

The microprocessor chip on the smart card can store many different types of information, but the smart cash card is used to replace coins and paper money with the same level of anonymity. Although it has not been widely accepted, the technology exists to insert smart cards into computer compatible readers to transfer anonymous cash. However, if digital cash or smart card payment is made over a non-anonymized IP connection, the merchant will be able to track the customer's IP address. Total anonymity in payment must also utilize an anonymous proxy service, as discussed above.

Today's electronic commerce is almost totally dependent on electronic credit card transactions. The success of anonymous payment methods, such as digital cash and smart cards, will depend on their widespread adoption by customers and merchants. It is also important to remember that anonymous payment can be misused by criminals for money laundering, blackmailing and illegal purchases [5].

7. Responsibilities of Each Party

It is important to emphasize that the effectiveness of privacy protection relies on the joint effort of each party.

Privacy Subjects
The ultimate responsibility of privacy protection lies within the subjects. They should be aware that the Internet is a public medium where their personal data may be collected or tracked. They should be careful to disseminate information, verify requester credibility when information is required, and provide no more information than is absolutely necessary. Company's privacy policies should be read, cookies can be disabled, and public anonymity services can be utilized. Web users may also take actions to remove their names from mailing lists, by contacting organizations such as the Direct Marketing Association's Mailing Preference Service (http://www.the-dma.org/). Unfortunately, the use of privacy-protecting technology requires time and skills that many users of the Web do not have [3]. It is clear that subjects will be less likely to have their privacy violated when they have increased awareness and actively protect their privacy rights.

Information Collectors
The collectors should realize the importance of privacy protection to the success of their business. They should clearly state what information they will collect from users and how this information will be stored and used. Users should be given information dissemination choices and collectors should ensure that their data is secure and their stated policies are followed. The Georgetown Internet Privacy Policy Survey [8] found that 92.8% of Web sites gather at least one type of personal identifying information (name, e-mail address, postal code), but only 65.9% of sites post either a privacy policy notice (a comprehensive disclosure describing policies and practices about collecting and using consumer information) or an information practice statement (shorter statements focusing on a more limited aspect of privacy). A very strong majority (96%) of Internet shoppers believe that it is important for business Websites to post notices explaining how personal information provided during the buying of products and services be used [27].

Although many Web sites may provide a privacy policy, users do not always find them understandable and some are being accused of not practicing what they preach. Even popular sites such as yahoo.com, webmd.com and onhealth.com have been distributing lists of e-mail addresses and other information after explicitly specifying they would not [19]. In its report to Congress, the FTC states that "there is often a one-way mirror effect: Web sites ask users to provide personal information, but users have little knowledge about how their information will be used. This lack of knowledge leads, understandably, to confusion and mistrust" [12]. Not surprisingly, 91% of Internet users and 98% of online shoppers believe that an official annual audit should be conducted to determine how well companies follow their privacy policies [27]. To build and maintain consumer trust, it is important for the collectors to publicly provide a clear and complete privacy policy, to strictly adhere to this policy, and to allow annual audits for compliance. Only then can privacy subjects make informed decisions on what information they wish to disseminate.

Privacy Violators

The violators should act legally and ethically and stop disregarding personal privacy rights. Unfortunately, the nature of the intentional violators, such as hackers, is to act against the interests of other parties. They assume no responsibility, and it remains up to the other privacy parties to take action to stop their violating behavior. Violators that unintentionally breach privacy rights, must educate themselves and make efforts to adhere to fair privacy practices.

Privacy Protectors

The protectors play the most active role in privacy protection. Their success, however, depends on how well they can influence other parties' behavior. More and more businesses have realized the importance of privacy protection for the success of their own business. IBM, the second largest advertiser on the Web, is leading a charge for more privacy on the Internet by removing its advertising from American or Canadian sites that do not cite clear privacy policies [15]. Similarly, online shoppers should refuse to purchase products or services from such sites. When collectors and violators realize that they cannot profit by practicing unfair privacy procedures they will be forced to change their ways.

8. Conclusions and Directions for Future Research

The incredible and continuing growth of the Internet has led to many new and innovative methods to gather and share information. It is not be surprising that the Internet's impact and effect on freedoms is profound as well. While the monetary cost of collecting, storing and utilizing data is diminishing rapidly, the cost to personal privacy is continuously escalating. "Covert" collection occurs constantly and data that was once carefully hidden may be only a few mouse clicks away.

We have developed a theoretical framework for privacy protection in electronic commerce in order to better understand the key roles and responsibilities of various parties to foster fair information practices. Protecting privacy rights on the Internet is a

critical step towards user acceptance and adoption of an electronic marketplace. Although the protectors play the most active role in privacy protection, it is the responsibility of the privacy subjects to be aware of potential violations and adequately shelter their personal data. It is the responsibility of the collectors to provide clear and complete privacy policies, which must be strictly followed and audited for compliance. Moreover, we emphasize that it is the responsibility of every party to foster privacy protection through their actions and online behavior.

Our framework also allows us to determine some areas that required further investigation and understanding. Although this is not a comprehensive list, the following are some questions that remain to be answered in future research.

1. The United States and Europe currently have a different emphasis on government legislation and business self-regulation for privacy protection. Will government legislation provide better protection than business self-regulation, but cause unnecessary interference for the free market? How can we take the advantages of both approaches to promote the better protection and healthy growth of e-commerce?

2. To what degree are self-regulatory services and tools being used? We have examined a number of self-regulatory initiatives, but have little indication of the extent of their use by privacy subjects. For example, most users may lack the technical savvy to properly utilize anonymity services. Do people trust a business more with a trust label certificate? Although these services and tools have the potential to protect privacy, they are of little value if they are not known, utilized, or trusted by the general public.

3. What are the effects of long-term storage and dossier gathering, or centralization, of personal information? While certain information may be accurate in the context and time it was initially collected, it may be inaccurate when referenced in a different time and context (in a process of centralization). What is a reasonable time frame to store personal information and to what extent should this information be centralized?

4. How can we balance two somewhat conflicting interests: business' interests to collect as much personal information as possible and consumer's interests to kept their information private? Can the conflict be resolved by compensating customers for providing their personal information?

5. How can we protect people's privacy and at the same time allow government and business to track and stop crime and fraud? Should the government be allowed to access encryption keys to monitor criminal activity?

6. How is privacy collected and/or violated by smaller Internet players? What protection is appropriate? The samples of most privacy surveys tend to be drawn from a subset of the larger or most popular Web sites [8]. However, there are

many smaller companies and sites that emerge and disappear quickly on the Internet. It would be valuable to investigate the degree of privacy loss to these smaller sites and examine the viability of their control through traditional government and self-regulation effort.

7. Do we have enough privacy protection? Have we overemphasized its risk and damage? If not, to which extent do we need to establish online privacy protection so that it will no longer be a major huddle for e-commerce growth?

8. What is the corporate attitude towards online privacy? Public attitudes toward online privacy have been documented in numerous surveys [27], however little is known about the corporate point of view. Privacy protection is not only for consumers. It is very common for employees to use the Internet on a daily basis. What are the attitudes of employers and what steps are being taken to protect their employees' online privacy?

9. How can we provide adequate privacy protection when crossing international boarders? Laws, ethics and cultures vary around the world. The Internet is a global medium and we need to understand how differences in culture and government regulation should influence privacy policies and business practice.

10. What are the characteristics, motivations and practices of privacy violators? In order to stop the privacy violator, we must understand their characteristics, motivations and practices. Although this information may be more difficult to collect, we must understand the nature of violators before we can effectively alter their unethical behavior.

Electronic commerce has the potential to revolutionalize the way consumer business is conducted. However, the future growth of the electronic marketplace will, to a certain degree, depend on our better understanding of and solutions for privacy protection.

References

[1] M.H. Agranoff, Controlling the Threat to Personal Privacy*, Journal of Information Systems Management*, Summer 1993.

[2] P. Benassi, TRUSTe: An Online Privacy Seal Program, *Communications of the ACM*, February, 42(2), 1999, pp. 56-57.

[3] L.J. Camp, Web Security and Privacy: An American Perspective, http://www.ksg.harvard.edu/people/jcamp/webpriv.htm.

[4] J.W. Cioffi, The Legal and Policy Framework for Global Electronic Commerce: Conference Summary and Report, http://e-conomy.berkeley.edu/pubs/summary /0399ecom.html, 1999.

[5] J. Claessens, B. Preneel, and J. Vandewalle, Anonymity Controlled Electronic Payment Systems, *Proceedings of the 20th Symposium on Information Theory* in the Benelux, Haasrode, Belgium, May 27-28, 1999, pp. 109-116.

[6] Coursey, D., Your Privacy: Uncle Sam Isn't the Real Threat. Here's Who Is, ZDNet AnchorDesk, January 26, 2001, http://www.zdnet.com/anchordesk/stories/story/0,10738,2678867,00.html

[6] L.F. Cranor, J. Reagle and M.S. Ackerman, Beyond Concern: Understanding Net Users' Attitudes About Online Privacy, *AT&T Labs-Research Technical Report TR 99.4.3*, 1999, http://www.research.att.com/library/trs/TRs/99/99.4/99.4/.

[7] L.F. Cranor, M. Langheinrich, M. Marchiori, M. Presler-Marshall, and J. Reagle, The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, *W3C Working Draft 10*, May 2000, http://www.w3.org/TR/P3P/.

[8] M.J. Culnan, *Georgetown Internet Privacy Survey: Report to the Federal Trade Commission*, 1999, http://www.msb.edu/faculty/culnanm/gippshome.html.

[9] C. Dembeck, Online Privacy Inside and Out, *E-Commerce Times*, April 25, 2000, http://www.ecommercetimes.com/news/articles2000/000425-1a.shtml.

[10] Editorials, Privacy: The Key to the New Economy, *Business Week*, New York, March 1998.

[11] European Commission, *Directive 95/46/EC of the European Parliament*, 1999, http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html.

[12] Federal Trade Commission, *Privacy Online: A Report to Congress*, 1998, http://www.ftc.gov/reports/privacy3/.

[13] Federal Trade Commission, New Rule Will Protect Privacy of Children Online, 1999, http://www.ftc.gov/opa/1999/9910/childfinal.htm.

[14] Federal Trade Commission, *Final Report of the FTC Advisory Committee on Online Access and Security*, May 15, 2000, http://www.ftc.gov/acoas/finalreport.htm.

[15] K. Girard, IBM to Pull Web Ads Over Privacy Concerns, *CNET News.com*, 1999, http://news.cnet.com/news/0-1005-200-340588.html.

[16] G. James, The Price of Privacy, *Upside*, April 2000, pp. 182-190.

[17] J. Kornblum, Navy, AOL settle privacy case, *CNET News.com*, June 12, 1998, http://news.cnet.com/news/0-1005-200-330209.html.

[18] C. Levin, Web Dropouts : Concerns About Online Privacy Send Some Consumers Off-Line, *PC Magazine*, January 19, 2000, http://www.zdnet.com/pcmag/stories/trends/ 0,7607,2423811,00.html.

[19] M. McGinity, Surfing Your Turf, *Communications of the ACM*, April, 43(4), 2000, pp. 19-21.

[20] A.L. Nggroni, Privacy and the prying eyes of cyberspace, Mortgage Banking, 60(7), 2000, pp. 76-81.

[21] R. O'Harrow, Jr., Fla. Governor Cancels Sale of Driver's License Photos to Company, *Washington Post*, February 2, 1999, http://www.euronet.nl/~rembert/echelon/.

[22] Privacy Commissioner of Canada, *BillC-6 : A Private Sector Privacy Law*, 2000, http://www.privcom.gc.ca/english/02_06_e.htm.

[23] J. Reagle, and L.F. Cranor, The Platform for Privacy Preferences, *Communications of the ACM*, 42(2), 1999, pp. 48-55.

[24] E. Turban, J. Lee, D. King, and H.M. Chung, *Electronic Commerce: A Managers Perspective*, Prentice Hall: NJ, 2000, pp. 349.

[25] C. Walker, E-mail cleanup: Take a lesson from Microsoft: Clean up your mail files or you could be all washed up, *eWEEK*, October 26, 1998, http://www.zdnet.com/eweek/stories/general/0,11011,364129,00.html.

[26] H. Wang, M. Lee, and C. Wang, Consumer Privacy Concerns about Internet Marketing, *Communications of the ACM*, 41(3), 1998, pp. 63 - 70.

[27] A. Westin, D. Maurici, E-Commerce & Privacy: What Net Users Want, *Louis Harris & Associates Survey*, June 1998.