8

Privacy and Trust in Electronic Commerce

Andy Gall and Beau Harrington

Introduction

Many inexperienced or first-time computer users are relying increasingly on electronic commerce to carry out simple everyday purchases and transactions. From paying one's credit card bills to purchasing Britney Spears tickets, the rise of Business-to-Consumer (B2C) electronic commerce has taken hold in the daily life of many Americans. E-commerce has proven to be successful in simplifying the buying and selling of goods, but this does not come without dangers. Consumers are required to furnish much more personal information to make an online purchase than would be required for a purchase at a brick-and-mortar store, even though an e-commerce transaction can be much riskier than buying offline. More fake and fraudulent sellers appear every day on the Internet, waiting for an unwitting user to provide their credit card number and personal information. Even legitimate online stores retain far more general and personally identifiable data about their customers than any traditional store would ever be able to assemble.

With such potential for the spread of a person's data, care must be taken to patronize only the sites that can reasonably guarantee the security of personally identifiable customer information. Every online store claims they safeguard customer info, but these claims can easily be baseless. How can one truly tell whether a certain site can be trusted?

This chapter will touch on the details of consumer profiling, direct marketing firms, and theft of personal information, and follow with a detailed look at how consumers determine what websites they trust. The ethical considerations of collection and exploitation of consumer profiles will also be examined.

Collection and Use of Personal Information

With the explosion of relatively cheap computing beginning in the late 1980s, more and more companies began to consider the business benefits that could be derived from the use of information technology. One of the first and most readily apparent applications was the retention of consumer information, including purchase records and eventually buying habits of individual customers. This data is compiled and analyzed to develop a profile of each customer, as well as the customer base as a whole; this is known as *consumer profiling*.

Supermarket chains were the first to implement consumer profiling techniques. Breakthrough developments in both computer power and storage technology made possible computer systems that automatically account for every item that leaves the store. After the new computer systems proved wildly successful with their original task, the supermarket chains upgraded them to track more information. These stores began tracking customer trends by issuing discount cards, allowing the observation of every individual shopper. Knowing the buying habits of all of their regular customers allowed supermarkets to tighten supply chains to keep just enough on hand to satisfy projected customer demand. This practice was proven to be successful, and when e-commerce usage began to take off, online "eBusinesses" followed suit and expanded further upon the idea of profiling. Thanks to the further developments in IT that came with the Internet boom, online B2C stores, such as Amazon.com, can easily keep a record of not only every product a customer buys, but every product they view, making it easy to compile a list of products that they may be interested in purchasing. This information can then be used in a variety of ways, including developing custom advertising material, e.g. banner ads for DVDs that have been browsed on Amazon two or more times but haven't purchased, or email bulletins for when a new book comes out from an author whose work has previously been purchased.

Profiling is not limited to purchase records. TiVo Corporation produces the TiVo digital video recorder (DVR), a device that allows an individual to record TV programs onto a hard drive and replay them later, similar to a VCR. A TiVo DVR device dials in to a central TiVo server nightly to download the newest programming information to use with the owner's cable or satellite service. However, a TiVo DVR also keeps a log of every button pressed on a user's remote, allowing the company to easily gather data on what shows are recorded most, what shows are re-watched most, and what parts of shows are replayed most frequently. This information is also transmitted to TiVo during its nightly call home. Using these techniques, TiVo was able to announce, within 36 hours of the end of the Super Bowl, that Janet Jackson's wardrobe malfunction was the most-replayed moment ever by TiVo owners (Reuters 2004).

While Amazon.com and TiVo Corporation compile information for internal purposes and improving the customer experience, some companies' intentions are not so benign. Many online marketing companies exist solely to sell the information they collect. These companies sell lists consisting of millions of email addresses and other personal information of consumers who, most likely unintentionally, clicked on a box or button that allows this information to be distributed and sold. The companies who purchase this information use it to market via telephone, email and direct mail, along with other methods. This usually translates into a bombardment of unwanted phone calls, emails, and envelopes.

Upon some research, the depth of these consumer databases is quite astounding: Claritas, a company that offers "customer targeting solutions," offers information on 62 distinct groups of individuals, based on hundreds of factors including age, affluence, presence of children, home value and location, and credit status. Group titles include "Winner's Circle", "Hispanic Mix", and "Urban Achievers". You can buy information on individuals in these demographics for prices as low as $65 per thousand names (EPIC).

Even companies with rigid privacy policies will get in on the act, especially if the entity on the receiving end of customer data is the United States Government. In 2002 and 2003, six of the ten largest airlines secretly turned over sensitive passenger information, including home phone numbers, credit card numbers and health data, to Transportation Security Administration contractors. Executives at Northwest, JetBlue and American as well as TSA directors denied the charges when initially questioned over the release of passenger data. Only after the preponderance of evidence to the contrary precluded any other explanation did they admit any involvement or wrongdoing (Singel 2004).

These trends in information retention and customer data sharing are regarded as merely an annoyance by most Americans. However, one of the largest threats to the security of personal information on the Internet is the storage of financial information on machines other than the user's own PC. When a user purchases goods from a site, he/she is often given the opportunity to store financial information such as credit card numbers online for quick future reference. Disturbingly, many customers don't bother to question the security measures the businesses take to keep that information private, or the validity of the company to whom they are providing this information.

If the financial information that these customers submit to the businesses is intercepted or stolen, it offers the holder free reign of that person's bank account or credit cards. Some websites go to great lengths to secure the information that is given to them to complete a transaction. Some smaller sites take hardly any measures to ensure the security of this extremely important information, some even going so far as to use unencrypted web forms to transfer address and credit card data. The net result is the same: companies with both simple and advanced security technologies have been the victims of information theft. Hackers use cracked sites to access other accounts, place orders with other users' credit cards, or even generate a list of all users and their associated information. But even with the highest of security standards enforced with every transaction, data is only protected from unauthorized access; the world's most perfect firewall cannot stop a trusted user on the inside. Such was the case when Jason Smathers, a 24-year-old software engineer at AOL, stole 92 million e-mail addresses and sold them to known spammers (Krim 2004). With computers nearly everywhere in a company, almost any employee can be regarded as a threat.

Determining Trust in E-Commerce

Contemplating all of the things that can go wrong, it seems that e-commerce is only for the adventurous. Considering the frequent sale or theft of personal information, it is a wonder that many venture onto the Internet for any commerce whatsoever. With seemingly endless threats to a consumer's privacy, how does one decide which sites are trustworthy with the sensitive data they hand over so often?

After some initial research, it was determined that some of the more measurable factors affecting a person's trust in a specific website: pricing, familiarity with the website, the encryption standard used, the site's reputation, the credit card verification service used, and presence and readability of a privacy policy. An online survey was distributed to over 200 people of all ages to determine exactly how much of each of these factors contributed to the decision. All information was analyzed to determine any possible correlations and to uncover any unclear relationships.

Some results seemed to contradict intuitive thought. For example, it was determined that males and females do not differ in the method they use to determine a site's trustworthiness. Considering the differences found between men and women in other studies of online habits, it is surprising to find that they act identically. In addition, it was assumed early on that many people would be humble about describing their computer experience. In a world where technology is ubiquitous, it is difficult to imagine anyone labeling themselves an expert. However, only nine people responded to a question requesting the level of experience with computers and the internet with anything but "expert." This particular result presented a rather large problem since much of the information gathered was to be from persons who considered themselves amateurs. To extract any available use from the data, further analysis had to be used to determine which users' information was useful. It was eventually determined that the level of computer experience was, in fact, unnecessary information. This is because much of the insecurity involved in using the internet was believed to be engendered from an overall insecurity of one's knowledge of the Internet and its inherent technologies. However, if no one feels that the Internet is an intimidating place, and that they are all experts, this insecurity doesn't exist. Since everyone, regardless of their level of expertise, feels they are competent, no difference exists between experience levels unless they regard their experience as insufficient. This was proven by the fundamentally different responses by the nine persons who did actually answer with something other than "expert." These few responded throughout of the survey with more caution, showing an overall fear of using the Internet to make purchases, a situation that was expected for many more than just three percent of all respondents.

Age groups, like genders, traditionally differ in the way they treat many things, especially technology. This proved to be no different with trust and e-commerce. While the majority of respondents hailed from the 20-29 age group, enough (9%) were 40+ years of age to distinguish a relevant difference in practice. This particular age group seemed to be more cautious overall when considering any aspect of giving up financial or personal information. However, a surprising finding showed that despite this uneasiness, this age group did much less to determine a site's trustworthiness, but instead continued with their purchase process without reading the privacy policy, something that 26% of all respondents age 39 or less reported having read before making a decision.

Another interesting finding was that the look of the site was of reasonable importance to many users. Sites with less than remarkable web design were considered much less likely to be trustworthy. It could not be determined why this was the case, other than a basic assumption that the more professional a site looks, the less likely it is a small time hacker attempting to steal someone's money. This also assumes that the professionals are the ones that are trustworthy, but respondents also stated, as is discussed later, that they fear what these large e-commerce companies will do with their information once they receive it. This creates a paradox of sorts. In one respect, consumers feel safer the bigger the corporation, but in others, the smaller the corporation the more a consumer is able to trust it. The only possible logical solution to this perplexing situation is that the consumer is considering two different aspects of trustworthiness when taking these two aspects into consideration. It can be inferred from the results that the consumer fears predominantly the sale of personal information when they mention the large companies. With the smaller companies, however, it is likely that consumers fear being scammed. These issues can be resolved, but definitely not with ease. A step many corporations have taken, whether a one person limited liability corporation or a massive conglomerate, is to invest heavily in the design of their websites to alleviate the fear of the consumer. Once this is achieved, the only other way a business can alleviate a consumer's fears towards the distribution of personal information is to ensure the consumer, in plain language, that no information will be distributed. Some corporations find this impossible and only time will tell if this practice will come back to haunt them, or prove to be more important than an high level of consumer trust.

Although a consumer's familiarity with the site falls towards the bottom of things that they consider when deciding to give up personal information, it is definitely something that deserves recognition, according to the survey results. When asked if there were any other factors that aided in the decision, more than 6% of respondents included a familiarity of the site. This alone will not make the decision for someone, but of the 13 people who stated this was an issue, nine stated they would not even consider buying from someone who they've never heard of. Does a similar condition exist for "brick-and-mortar" operations? Most people would not think twice about purchasing from an unknown shop in the real world. This, once again, shows the inherent insecurity involved when purchasing from a vendor in cyberspace. This is believed to be because of accountability issues. When someone purchases something that is defective from a store, it is easy to hold that person responsible and confront someone regarding the issue. When someone purchases something over the Internet, however, one never knows who they are actually purchasing from, let alone whether they will be able to hold someone accountable. This is also assuming the consumer actually receives something at all. Some websites have been accused in the past of stealing a person's money, promising goods will be shipped, but never delivering. This is primarily why sites like eBay have such rigorous standards to adhere to when selling goods through their service. Other sites dealing with e-commerce must understand this, and offer some kind of guarantee that the merchandise the consumer orders will be delivered.

A positive reputation among consumers can help convince others that a site is safe and trustworthy: word of mouth increases the sites' trustworthiness even more than familiarity does. Over 9% of respondents stated the reputation of the website was the most important issue for them, and many reported having checked a site like resellerratings.com to determine past consumer's opinions of the site. This particular website is dedicated to providing the ratings consumers have given a particular website when purchasing goods or services. The power of this type of word of mouth advertising is evident with sites like newegg.com. Through the course of the survey, more than one out of eight people mentioned that their last purchase of a good or service over the Internet was from newegg.com. When asked what issues these specific people felt were important in aiding their decisions, 100% of them responded with either word of mouth or reputation. Some even went so far as to comment on resellerratings.com as the source of the reputation. How did the word of mouth reputation of newegg.com develop? The formation of a collective opinion regarding an e-commerce site is a complex process.

Circles of Trust: A Case Study

The global reach of the Internet allowed thousands of online stores to spring up and achieve profitability serving niche markets. Consumers desiring high-end computer accessories, once limited to just a few "brick-and-mortar" stores nationwide, now have their pick of dozens of online stores with full catalogues and low prices. The old problem of limited availability and selection has disappeared, but was quickly replaced with the question of which sites to trust. With few of these small stores having any history as an offline merchant, and fewer still able to fund television or radio advertising, peer opinions often become the sole source of legitimacy.

Newegg.com is regarded as the top seller of specialist computer equipment in the United States, both in sales volume and customer trust. Gamers and computer professionals thirsting for high-performance parts have come to trust them for fast service at the lowest prices but how was this trust created? The answer is the peer influence exerted by the large Internet community of computer enthusiasts; the different parts of the community coming together to create a "circle of trust." Social networks, specialized online bulletin boards, weblogs, e-commerce rating sites, and even search engines play a role in determining which sites can be assumed to be safe. The breadth of the circle ensures that the message of trust or distrust for a specific company is accurate, and is spread to nearly everyone involved in the community, no matter what the medium (Good 2004). Earning high marks within the relevant circle of trust can dramatically increase sales figures for an online merchant. Chris Gahan, a semi-professional gamer from Toronto, had this to say:

> I first learned about newegg.com when I mentioned to some fellow gamers on [an Internet bulletin board] that I was in the market for a new hard drive. When I asked him how he knew I would not get ripped off, he said he'd seen reports of dozens of successful transactions on various gaming boards. I went ahead and ordered… from newegg.com and was so pleased with their price and service that I recommend them to anyone I can.

This is a clear demonstration of the effectiveness of two parts of the trust circle: social networks and bulletin boards. A dissection of these and other elements of the circle of trust follows.

Social networks. Internet-based social networks are simply groups of people that meet and interact using a specific piece of software. One of the simplest is AOL Instant Messenger with its famous buddy list, a quick listing of all friends on the network. More complex social networks have emerged recently, such as the wildly popular Friendster and the Google-run Orkut. These new networks allow users to organize into groups based on nearly any shared interest. For example, Orkut has several hundred food groups, some with thousands of members. These groups provide a central information repository for members. Newegg.com is held in high regard in hundreds of such computer and game-centric groups.

Online bulletin boards. Community bulletin boards allow any visitor to learn from the knowledge of the community, by viewing old messages or posting messages asking for advice. Many of the most popular boards have special sections for posting information on transactions with Internet-based companies selling related products. Community members are eager to help others, posting hot deals from sites held in high regard and warning those who might purchase from an unreliable or untrustworthy site. This information is archived, often indefinitely, and is readily accessible with a keyword search.

Weblogs. Otherwise known as blogs, weblogs allow anyone to publish a journal for others on the Internet to read, comment on, or even link to from their own blogs. Due to their personal nature, reviews of products and shopping experiences are common. Particularly positive, negative, or informative reviews will be commented on and linked by other bloggers, which from there will be discussed and linked by even more bloggers. In the case of newegg.com, their status as a top computer hardware supplier is already cemented. Another weblog post affirming the reliability of newegg.com hardly merits discussion. Weblog discussion of newegg.com consists mostly of sharing the latest special offers and clearance sales, further confirming newegg.com's status as the leader in their market segment and driving their sales even further.

E-commerce rating sites. Mentioned earlier, e-commerce rating sites allow users to rate their purchase from an online merchant with both numerical ratings and comments on their experience. In addition to an overall rating, the site also asks buyers to rate pricing, customer service, and shipping speed. When a visitor requests information on a particular site, the average of all the user ratings is displayed, as well as complete listing of buyer comments. Rating sites were the first of the elements of the circle of trust to appear on the web – they were in full swing long before weblogs or Google took off. Newegg.com is one of the best performers on the biggest rating site, resellerratings.com.

Search engines. Although not readily apparent, search engines serve an important role in the circle of trust. Search sites like Google provide a vast archive of user impressions, indexing social networks, weblogs, bulletin boards and rating sites. Easy access to a wide variety of sources allows for easy comparison of site reviews from all over the Internet. Delving further into the archive yields meta-reviews: essentially, an appraisal of the reviews themselves.

Further Survey Findings

One of the most surprising findings from the survey was the amount of respondents who reported immediately noticing the use, or lack thereof, of a secure encryption standard. This is one of the most effective methods a website can use to ensure the safety of the information being transmitted. 65% of those surveyed said they notice almost immediately whether a site is using Secure Sockets Layer (SSL). It is only visible to the user through the use of the Secure HTTP protocol (e.g.: https://...) or an icon appearing in the browser's status bar, usually a lock or key denoting a secure connection has been made. Even with their apparent awareness of the presence of website security, only 45% of respondents, regardless of the security standards used, felt comfortable with what the website would do with the information once it was securely transmitted. From this data it can be concluded that people are less worried about someone stealing the information on its way to the site; rather, most are worried that the information will deliberately be given away or sold. In fact, less than 15% of respondents stated they were not worried about what the receiving party would end up doing with their information. It seems, although the e-commerce industry is still growing, online merchants may have lost the trust of consumers by selling their information so profusely and so willingly.

All sites, from the tiny ones run by just a few people to the massive ones like amazon.com, need credit card verification services if they wish to maximize their sales and the size of their customer base. Ensuring the security of credit card information requires a secure connection utilizing high-grade encryption. If security surrounding credit card transactions is lax, almost anyone can gain easy access to one's credit card information during transfer. Sites like PayPal and VeriSign have spent millions of dollars developing products whose sole purpose is to perform this one small step, absolutely necessary to complete a secure transaction. Regardless of the vast importance of keeping this information out of the wrong hands, respondents showed that the credit card verification company used by an e-commerce site was of little importance to most people. Only 8% were "concerned" with the credit card verification process during their last online transaction, while over

90% of respondents noted that they felt “comfortable” when providing their credit card information. Although this already seems to be fairly under control in the e-commerce industry, it was concluded that any site that performs online transactions without a secure (SSL) connection is in serious need of update. Regardless of the type of credit card verification company used, it is evident that the lack of one altogether is a red flag in the minds of the majority of Internet consumers.

Possibly one of the largest discoveries when analyzing the information was the proportion of respondents who claimed to have read the privacy policy on the site where they purchased their last goods or services online. 24% of all participants stated having read the policy prior to making a decision. Considering the difficulty of locating a link to the privacy policy on many sites, and the length and legal jargon of most policies, it is surprising that anyone reads the policy at all. Older Internet users seem less likely to do so: none of the 40+ year olds who took the survey reported having ever looked at a privacy policy online. Out of the respondents who did read the policy during their last transaction, 25% did feel that the policy was too long to understand or to finish reading.

Sites with privacy policies that were deemed too long and complicated took a credibility hit in the eyes of the potential customer. The power of a privacy policy comes from simplicity and strong words. If a consumer cannot understand what the policy is stating, the consumer feels that the privacy policy is hiding privacy concerns under a thick layer of legalese. Fifty-four percent felt that the wording of the privacy policy made them feel more comfortable about purchasing from the site. Of the more than half of the respondents that felt this way, not one claimed their privacy policy was difficult to understand or read.

To no one’s surprise, price has proven to be of immense importance in the eCommerce industry. When asked if there were any other factors that influenced the decision, many respondents needed only one word to explain their motivation: price. Although the study provided many valuable insights as to what factors were most important when a customer decides to send personal and financial information to a company online, the one factor that overrides all others is a low price. The better the bargain, the more red flags the consumer is willing to overlook. If a site is willing to give something of value away for free, it is possible to get an unreal amount of information from a consumer as payment.

Freeipods.com offers a free iPod or iPod Mini MP3 player to anyone willing to give up their personal information and sign up five of their friends, and participate in a trial for companies such as AOL and Blockbuster. Although according to *Wired News Online* (Kahney 2004), this is a legitimate offer. It simply proves that citizens are more than willing to give up privacy and anonymity for capital benefit. This creates a problem when people don’t understand the massive level of distribution that will happen with the information they provide in order to cash in. Most people who give up their information aren’t concerned, but not because they know the facts. Usually, it is primarily because of an overall ignorance to the practices of e-commerce businesses. Soon after signing up to get an iPod, a consumer will quickly find a slew of seemingly unsolicited e-mails and direct mail advertisements, as well as phone calls throughout the day unless they are included in the national do-not-call registry.

Ethical Concerns

Consumers have the power to resolve the issues at hand; they just haven't exercised it. As discussed earlier, it is common and widespread for businesses of all kinds to profile their customers in order to better appeal to their tastes. This collection of information has been largely accepted due to the clever marketing on the corporations' part. If consumers pay more attention to these issues, they could effectively force the corporations into not collecting and distributing mass amounts of data about their customers. The only thing consumers by-and-large would have to sacrifice is a small amount of time and money. In other words, quit using the grocery store discount cards, read the privacy policies of online vendors, if they are too long, purchase from somewhere else. Consumers will always lose if they place their demand for products at a low price above their privacy and anonymity. The fact that Albertson's grocery store chain, one of the last remaining chains priding themselves on not using discount cards, recently scrapped the policy further proves that price is more important in most peoples' minds than privacy.

With the majority of people blindly accepting the requests for information from corporate online vendors, a slew of ethical considerations are engendered. Many online vendors, when confronted about the pervasiveness of consumer profiling, respond merely with the fact that it remains legal. Every sound adult on this planet understands the discrepancies between legal and ethical constraints. Although it is legal in most states to commit adultery, most would say it is seriously immoral and unethical. The business world has somehow recently all but abandoned ethics when making strategic decisions. If businesses continue to act with capital gain as their primary motivation, consumers need to counter this with a demand for up-front, succinct policies and agreements. The conventional corporate school of thought is that consumers should look after themselves when making these important decisions. There is no simple solution to this problem, but it is vital for corporations to maintain a level of trust from their customers. If the trust eventually erodes, businesses will be forced to abandon their ludicrously unethical practices, and equilibrium will somehow be reached. The current state of business practices is thus completely in the hands of the consumer.

The other large ethical implication when dealing with online vendors is the possibility of theft of identity or private information. Although it was shown that this is not a main concern from most experienced users of the internet, it is still an issue that should remain one of the top priorities of online vendors. Despite the large threat that exists, many online e-commerce websites perform transactions with no security measures whatsoever. Some are relatively large websites selling many goods over the Internet. With the technology readily available to secure these transactions, it is simply unethical to not provide the consumer with a secure connection for sending financial information.

Conclusion

Although many people feel they are more than competent enough to use the Internet to take care of many regularly scheduled financial tasks, evidence points to the fact that their confidence has little backing. Many people do not understand what happens when a credit card transaction takes place over the internet, nor do they understand the social and ethical implications they might be facing. However, only a minority of people actually expressed any level of concern when asked if they were concerned if these issues might exist. It was determined that age seems to play more of a part than gender in determining the habits of surfing and purchasing goods or services on the web.

In addition to the more commonly understood factors that play a part in attracting buyers (e.g.: advertising, brand name, professional look, etc.) the single most important issue an online consumer considers is the reputation of a website, as determined predominantly by word-of-mouth. This has shown to be so powerful, some have gone so far as to state they would not purchase goods or services over the Internet from a vendor they have never heard of. This is an issue that does not exist in brick-and-mortar locations, and was probably the most considerable result of the research. However it was determined that, due assumedly to a prevailing capitalist mentality, only price had the power to override a poor reputation. An item sold at a below average cost, or even free, was determined to have immense power when asking consumers to provide personal, or even financial, information! Many ethical issues are also engendered by the practices of online vendors. These include unclear and lengthy privacy policies, stealthy collection of information, and not providing an easy method to perform financial transactions with a high level of security. The e-commerce industry thrives on trust, but it is quickly eroding the confidence of its consumers, which can be seen by the inherent feeling of insecurity when purchasing goods and providing sensitive information online.

Works Cited

Reuters. “TiVo: Jackson stunt most replayed moment ever.” CNN.com. 3 Feb 2004. http://www.cnn.com/2004/TECH/ptech/02/03/television.tivo.reut/ index.html

EPIC (Electronic Privacy and Information Center). “Privacy and consumer profiling.” EPIC.org. Undated. http://www.epic.org/privacy/ profiling/

Singel, Ryan. “More False Information from TSA.” Wired News. 23 Jun 2004. http://www.wired.com/news/politics/0,1283,63958,00.html? tw=wn_tophead_1

Krim, Johnathan. “Insider Case at AOL Shows Vulnerability.” The Washington Post. 26 Jun 2004. http://www.washingtonpost.com/wp-dyn/articles/A6703-2004Jun25.html

Good, Robin. “Circles of Trust: Influence Indicators on the Internet.” RG News. 28 July 2004. http://www.masternewmedia.org/news/2004/07/28/circles_of_trust_influence_indicators.htm

Kahney, Leander. “Making Free iPods Pay Off.” Wired News. 2004 Aug 18. http://www.wired.com/news/mac/0,2125,64614,00.html