Global Information Assurance Certification Paper

The Perils of Privacy When a Dot-Com is Dot-Gone

Julie Hoke

GSEC Practical Assignment Version 1.3

Increasing amounts of effort and technology are focused on protecting vital data and sensitive information that travels through the Internet. New and improved security measures appear each day as consumers' concern and level of awareness grows. Internet shoppers accomplish a leap-of-faith as they enter credit card numbers or other sensitive information after being offered the warm and fuzzy reassurance of a tiny locked padlock or a magically unbroken key. Privacy policies are scrutinized to be sure that every effort is being made to protect what is being entrusted to the unseen recipient of valuable, sensitive, and confidential information. It is reassuring to know that so much energy is directed to protecting this vital data, but what happens to the information that is entrusted to these entities when a company decides to cease operations, sometimes in less than ideal conditions? What happens when an ultimately secure e-business is sold to an anything-for-a-buck enterprise? Is the private data left to float in cyberspace, or have precautions been taken to secure the information once it is no longer needed. Are privacy policies worth the screens on which they are displayed?

The market downturn in 2001 precipitated bankruptcy sales. Almost forty billion dollars was spent in 2001 to acquire almost 1,300 Internet companies. Over five hundred Internet companies ceased operations or declared bankruptcy last year. During all of this turmoil, it is hard to believe that the protection of sensitive customer information was a major concern. Protecting the customer's privacy is probably one of the last things on the mind of CEO struggling to find solvency and the network administrator who has just been handed a layoff notice is not inclined to make sure that the permissions on every database are at the proper level. When faced with these realities, it is hard to criticize individuals in these situations for not making the protection of information a top- priority concern, but who should pick up the reigns when this occurs?

Another issue that makes this even more of a concern is the fact Internet-based companies are not tangible like brick-and-mortar companies. Before Internet companies came along, it was not unusual for failed organizations to turn over customer's data. Doctors and banks have always followed this practice but people were fairly confident of what type of information was being exchanged and who would be receiving the information. The difference lies in the manner in which Internet companies collect and store the data. Some information that they gather is willingly given up, but other information stored in their databases is obtained by tracking visitors to their Web sites and recording their Web browsing and purchasing habits. These types of assets cannot be easily inventoried, and sometimes it may even be difficult to prove that they exist. It is hard to put a dollar value on intellectual properties and databases full of customer information. To further complicate matters, consumers are seldom aware of how much information about them exists in databases that not only track information that they willingly disclose through interactive Web forms, but also track their habits and trends and store that information as well.

Combine the turmoil of the dot-com failures and the vagueness of the assets that they can liquidate or turn over to another company, and the possibility of a privacy issue

steps into the forefront. This is a new unproven area for the government to step in and issue new laws and mandates. The Federal Trade Commission has been called to action, especially in the case of Toysmart.com when they tried to sell their assets that included customer information databases.

Recently, the decision has been made to concentrate on already existing privacy laws rather then introduce new legislation. The debate continues as to whether the government should step in before the situation eliminates the concept of privacy altogether, or government imposition that presents a hindrance to an Internet economy that has already been struggling recently.

Fortunately, attention has been given to this problem through government and private agencies. There are also things that individual consumers can do to protect themselves, but this problem is not resolved.

What is personal information is out there?

Just about every Internet site has a privacy policy. These policies assure online explorers that the information that they reveal will be kept in strictest confidence and will not be revealed or disclosed under any circumstances. This gives Internet consumers confidence to enter a wide variety of information ranging from addresses, telephone numbers, clothing preferences, “wish lists,” eating habits, and many other personal details. Some consumers are aware of the fact that this information is being stored for future use. What many consumers do not realize is not only the information that they willingly relinquish is stored, but other information about their personal Web-surfing habits may also be stored.

Most Internet companies use databases to build profiles about their customers. Most Internet sites collect some type of personal data, but few tell why the data is being collected and for what purpose.

The types of information fall into basic categories. The most frequent and import type of information collected is information related to contacting the individual. This involves names, e-mail addresses, telephone numbers, and addresses. It is usually apparent how and why this information is being collected.

Some sites are a little less up-front about the information that they are collecting. They prompt visitors to disclose pieces of information in order to have a “more personal Web experience.” Web visitors eagerly give up information relating to their locale, age range, buying preferences, and taste in order to achieve this karma. The Web site presents an its-all-about-you attitude while the undercurrent its-all-about-us incentive is there to collect that information and use it as a marketing tool.

Another type of information that is being stored in Web site databases relates to cookies, which are small text files (usually around 50 to 150 bytes and always less than 4kb) downloaded from the Web site by the visitor’s browser. Cookies do not openly identify an Internet site visitor, but track movements from page to page within a Web site. Some Web sites use cookies to store customers information between visits and others use cookies to identify what Web site referred the visitor. All of this information can be collected and stored in a database.

Collecting and storing information about customers is nothing new. Before Internet-based businesses came along, information relating to customers and consumers has always been collected and stored in some manner. One major difference is Internet companies not only retain information relating to purchases completed, but also store information about those who do not purchase anything. In addition, personal information about the customer is collected related to *every* purchased made through the Internet. When was the last time anyone asked you for your name, address, telephone number, credit card number, and mother's maiden name when you bought a loaf of bread?

How is this information being protected?

Except in special instances, Internet sites are not required to have a privacy policy. (Brick and mortar companies are also not required to have privacy policies even though they collect customer information.) Privacy policies are offered so that visitors and consumers can have some degree of confidence when they disclose information. Failure comply with a privacy policy can be perceived as a deceptive trade practice and the Federal Trade Commission (FTC) is the United States governing body that must oversee compliance with these agreements. Members of 107th Congress of the United States have expressed opinions that some type of federal privacy legislation is needed because this is not best accomplished on a state-by state basis. Internationally, the 1948 Universal Declaration of Human Rights addresses territorial and communications privacy and acknowledges an individual's right to legal protection against invasion of their privacy.

Only two percent of all Internet sites had privacy policies in 1998. By the year 2000, increasing public concern over the matter of privacy resulted a privacy policy posted in almost every major Internet site dealing with customer information. For the most part, privacy policies specify that companies will not disclose information to a third party without first obtaining permission. Some privacy policies state that information will never be disclosed to a third party. A recent poll indicates that only three percent of all consumers bother to read the privacy policy, which is not surprising. Privacy policies tend to be full of legalese and difficult for the average consumer to understand.

Another development aimed at the protection of consumer's privacy is the establishment of third-party organizations such as TRUSTe and BBBonline to ensure adherence to privacy policies. These organizations offer various services that include confirmation, education, monitoring and review of Web sites, an avenue for consumer dispute resolution, a type of seal to be displayed on Web sites as evidence of membership, and a means to enforce compliance with privacy policies.

The World Wide Web Consortium, an international group formed to enable the Internet's growth and interoperation, is developing a platform for Privacy Preferences (P3P) project with the goal of a uniform privacy policy. The consortium is jointly managed by research groups in the United States, France, and Japan.

Has this type of information ever been threatened by bankruptcy or mergers?

There have been some notable instances of privacy violations through bankruptcy and mergers and the outcomes have varied. They have all served to illustrate the increasing need for some type of control over the transfer of data after an Internet business no longer exists.

Toysmart.com

Toysmart.com, LLC, and Toysmart.com, Inc., an Disney-owned Internet children's toy retailer, posted a privacy policy on its Web site in September 1999 that expressly stated that personal information that was voluntarily submitted by its customers, such as names, addresses, birth dates, and shopping preferences, are never shared with a third party. It assured customers that when they registered with Toysmart.com, their information would *never* be shared with a third party.

In May 2000, Toysmart.com announced that it was ceasing operations and selling its assets. TRUSTe contacted the FTC after this announcement. The FTC investigations revealed that Toysmart.com was practicing unfair and deceptive business practices and sued in district court. In January 2001, a bankruptcy judge ordered that all information was to be destroyed rather that be sold to a third party. After the bankruptcy case was closed, the customer information was to be destroyed within 30 days.

Craftshop.com

The Internet craft retailer, Craftshop.com, filed for bankruptcy and listed its customer list as an asset. It also was selling the actual name of the site and contended that as long as the name Craftshop.com was used, there would be no transfer to a third party. Following the actions taken by the FTC against Toysmart.com, Craftshop.com withdrew the customer list from the list of assets.

Boo.com

The United Kingdom (UK) fashion Web site, Boo.com, sold assets to Fashionmall.com in June 2000. Among the assets that were included in the deal was data on 350,000 customers. Boo.com had a privacy agreement that complied with European laws and earned the TRUSTe seal. The chief executive of Fasionmall.com, Ben Narasin, assured that an e-mail notification was to be sent to each customer to obtain permission to maintain the mailing list. Due to the international twist to this case, though, it should be noted that even though it would have been illegal to give the customer information to a third party without their permission, once the information leaves a country, little can be done to prevent it from being sold to other parties. In this instance, there was not much UK Data Protection Registrar could do to protect this information.

More.com

In October 2000, HealthCentral.com agreed to purchase the online drugstore More.com. Among other assets acquired through the deal was the More.com customer database. This was in direct violation of the privacy policy posted on More.com's Web site that stated: "More.com does not give, sell or rent your personal information to third parties for purposes other than fulfilling your request. To better serve you, we use trusted third parties to fulfill and ship your order(s). We also use trusted third-party

business partners to distribute our electronic newsletters and send you promotional offers."[1] This raised privacy concerns, but HealthCentral.com and More.com maintained that the policy was not violated because the entire company was sold and HealthCentral.com should be considered a successor, not a third party. The fact that customer information not only consisted of names and addresses, but also contained sensitive medical information further complicated this situation. The transfer of customer information such as addresses and telephone numbers is definitely an issue, but that concern is compounded when sensitive information such as what drugs are being taken (evidence of a communicable, terminal, or psychiatric disorder) and what type of health insurance is carried is transferred to an unknown third party.

Essential.com

A Massachusetts telephone service, Essential.com, had been building a customer base of 70,000 since 1996. The firm bought services from New England companies at a wholesale price then sold the services to its customers at a discount. The entire process was accomplished online. In June 2001, the company filed for bankruptcy and funds are being solicited to recover losses and satisfy creditors. The privacy policy posted on the Internet site that assured that Essential.com does not sell, trade, or rent personal information. (A provision was added to the agreement in May 2001 that would allow information to be provided to companies, as needed, to achieve business objectives. Every effort was to be made to maintain the level of privacy protection.) The Massachusetts Attorney General blocked the sale of the information through a bankruptcy court order. Under the agreement, a new service must disclose its privacy policy to Essential.com customers and if they do not accept the service, they may transfer to another provider and the information must be destroyed. Essential.com was told not to give customer information to any third party for any reason.

Egghead.com

Egghead.com posted a privacy policy that stated it would *never* sell its customer data under any circumstance. The Internet retailer filed for Chapter 11 bankruptcy protection and entered into an agreement to sell its assets, which include customer data, to Fry Electronics, Inc. Fry agreed that customers would be notified of the pending transfer and be given the opportunity to refuse the transfer. The FTC did not oppose this agreement, although many states did dispute it. The $10 million sale stipulated that no fewer than ten percent of Egghead's active customers can refuse to transfer their personally identifiable data to Fry Electronics. Due to another Fry acquisition, Outpost.com, the deal apparently soured and Egghead was once again put on the selling block. Eventually, Amazon.com agreed to buy Egghead for $6.1 million. The deal did include customer data, but Amazon has stated that it will not use any of the information because it would be in direct violation of the Egghead's privacy policy. Egghead.com customers will be redirected to the Amazon.com site and all customer information will have to be re-entered. No information will go into Amazon unless the customer consents.

---

[1] Rosencrance, Linda, "Sale of More.com's customer list raises privacy concerns" http://www.cnn.com/2000/TECH/computing/10/27/online.privacy.idg/

An interesting side note to the Egghead.com and Toysmart.com controversies as they relate to Amazon.com. In September 2000, Amazon.com revised its privacy policy informing consumers that the information that they give is considered an asset and can be sold. It also provides for transfer of that information in the unlikely event that Amazon.com would be sold.

Voter.com

Voter.com was founded in 1999 by former Clinton advisor Craig Smith. In February 2001, it announced that it was closing due to financial conditions. It posted an asset sale document on its Internet site that included a 170,000-member subscription list that included the typical information in addition to the person's party affiliation. This sale was in accordance with the Voter.com privacy policy that provides for the selling of the list to an organization that will provide personalized political information. This transfer of information still presents questions as to the consumers expectations of privacy as they enter information online.

Engage

CMGI, the majority holder of Engage, an online ad agency, announced in August 2001 that it planned to withdraw a $50 million line of credit. It prompted concern that the company would try to sell off its media business that would bring along a database of over 88 million anonymous customer profiles. The database was built through cookie technology that tracks Internet user habits and builds anonymous profiles. There has been increasing concern relating to the selling of cookies (not the Girl Scout variety). The transfer of this personal information through a sell or acquisition is a privacy concern. The concern stems from the fact that cookies can be retroactively identified and eventually associated with name if a form had been completed on a previous Web page. Therefore, the promise of anonymity becomes void. This means that not only has Engage been monitoring Internet habits without permission, but also with the new developments, they would be trying to sell this valuable information. This debate is a double-edged sword. Will Engage be able to sell its database, and do those cookies contain valuable personal information? The company announced later in August 2001 that the decision was made not to sell the customer profiles and it was discontinuing the profiling service.

What have we learned?

Unfortunately, there are no unified laws or broad court rulings that provide a clear answer to the question, "Can companies facing bankruptcy sell customer data?" This is even more distressing as more and more Internet companies are facing economic peril. There is a new proactive movement among e-businesses, as they face economic difficulties, to send e-mail notices to customers, asking permission to transfer their information or decline the sale. This tactic was used by four failed dot-coms: Webvan, eToys, Wine.com, and Garden.com. These companies asked to transfer information that they earlier promised not to disclose. The understanding would be that if they receive permission from the customers, they are honoring their privacy policies. When customers are given the option to have their information transferred, it serves to decrease the value of the asset. Seldom will 100 percent of the customers agree to have their information transferred. At times, it has been proven wise to provide the customers the option to not have their information transferred. In the case of Wine.com,

orders had already been placed and there were outstanding club memberships and gift certificates, so Sand Hill transferred the customer information unless the customer opted out of the sale.

Bankruptcy cases present another problem. It must be noted that a bankruptcy judge has the power to declare all previous agreements and contracts null and void in order to raise necessary funds to keep a company solvent. Currently, even though privacy legislation has been proposed, there are no specific laws to directly address the issue of the transfer of customer information in the event of an Internet-based company bankruptcy or merger. The FTC is dealing with this on a case-by-case basis. The FTC takes into consideration such things as the type of data that is to be transferred, is it being transferred to a company that is similar in nature with a comparable privacy policy, is it a stand alone asset, or a part of a packaged asset sale.

What is the Government Doing?

New legislation has been introduced, but none has passed Congress to become law. The U. S. Senate passed the "Bankruptcy Reform Act of 2001" (S. 420) on March 15, 2001 by a vote of 83-15. This amendment addresses the sale of personal information in the event of bankruptcy. This amendment was introduced in direct response to the Toysmart.com incident. This amendment is sponsored by Patrick Leahy, a Democrat from Vermont. The corresponding House bill (H. R. 333) proposes a more conservative version of the same bankruptcy legislation. Due to events of September 11, 2001, the government has directed most of its efforts to the surveillance of terrorism and Internet privacy bills have been presently put on hold.

The new chairman of the FTC under the Bush administration, Timothy Muris, stated that he would not support any new Internet privacy legislation. Instead, Mr. Muris spoke of his intentions to emphasize the enforcement of the existing privacy laws. This stance disappointed privacy advocates who had hoped to build on U. S. privacy rules that do not offer enough protection to consumers. During the year 2001, about 100 privacy bills were introduced in Congress, but none of them was taken up in committee. Muris believes that instead of introducing new legislation, it was time to evaluate the existing privacy laws and find an effective means of enforcing those laws. It is imperative that companies that post privacy policies are legally obligated to adhere to them or they are in violation of the FTC rules the outline deceptive practices. The FTC plans to increase by 50 percent, the enforcement of laws directed at businesses that violate privacy policies. Muir intends to increase the number of full-time FTC employees dedicated to privacy matters from 36 people to 60. He also proposes an investment in data mining software that has the ability to cross-reference privacy complaints.

On the FTC's Web site, businesses are encouraged to post privacy notices and honor those agreements. The FTC's agenda includes a focus on privacy concerns as they relate to a bankruptcy or reorganization.

Difficulties in government legislation can lie in the nature of the Internet. There are no geographical limitations and it is difficult for companies to identify and comply with a myriad of privacy regulations.

What Can Consumers Do to Protect Themselves?

Even though the effectiveness of privacy policies can be disputed, consumers should always look for the privacy policy and read it thoroughly. If it mentions the possibility of the transfer of the information that is entered, the benefits of entering the information must be weighed against the risk. It is also wise to look for the TRUSTe, BBBonline or other similar "seal of approval." Verify that the seal is what is represented to be by carefully studying the endorser's standards on their Web site.

One of the most important things that a consumer can do is to research the viability of a company when doing any type of business online or when entering any type of personal or sensitive information. In the "real world" we tend to deal with businesses that have been around for a while and have established a reputable history. You can transfer that common sense to Internet shopping, sometimes literally. Many of the stores that consumers have come to trust while shopping at the mall are available to sell their goods or services online as well. This is definitely no guarantee…remember that Toysmart.com was owned by Disney.

If you, as consumer, must enter a large amount of sensitive information on an Internet site when performing activities such as applying for a loan or insurance, consider the added precaution of consulting the Better Business Bureau or the attorney general's office to make sure that there are no claims against the company. Just because a company is not listed does not indicate that there are no problems. It just indicates that no one has bothered to file a complaint.

It is a good idea for consumers to pay attention to Internet gossip. When a company is suffering financial problems, it is seldom kept a secret. A quick Internet search or Web sites that monitor such activities and newsgroups might provide valuable information. Financial pages and Internet sources are may also indicate when is facing impending bankruptcy.

To avoid the compilation of a profile through cookies, reject unnecessary cookies. Most browsers now provide this capability and if these cookies are rejected, Internet sites are not able to build and store profiles based on cookies.

Anonymizers are tools that have been created to help Internet users preserve their anonymity while browsing Internet sites. They are a type of protection that relay Internet traffic through an intermediary server. They hide any type of identifying information that might be obtained by the Web site, such as the IP (Internet Protocol) address, identification of the type of browser software, and Internet browsing tendencies. They also block sites from placing cookies or any other unwanted files on the computer.

Many Internet companies offer the option to remove your name from lists of information that they are permitted to share with third parties. This is usual an option that is available online and when offered, choose to "opt out." Some companies go even further by only sharing the information on these types of lists only when they are given permission to do so. This is the "opt in" method. When given either option, take it. Companies are notorious for making these options difficult by hiding them so that you must scroll to find them or presenting the default selection as one that would have consumers agreeing to share information.

Companies have also resorted to slightly unethical tactics to gather personal information. Internet sites may have contests with enticing prizes that prompt the visitor

to enter personal information in order to enter the contest. It is a good idea to avoid this type of disclosure altogether. If it sounds to good to be true, it probably is.

When filling out Internet forms of any type, do not give out any more information than is required. Almost every Internet form has fields in addition to the ones that are necessary to complete the transaction. These fields usually include information about preferences, buying habits, income, lifestyle, and other personal information. This information is valuable for marketing and can become part of a company's assets if it is sold or if it decides to sell the assets due to bankruptcy. Only complete the required fields. They are usually marked, but it is not always obvious.

Do not use debit cards for online transactions. It is bad enough to have your credit card number to be sold to an unscrupulous company, but it would be much worse if your debit card information is transferred to another entity.

It is important that parents educate their children about divulging information online. Too many times sites that are directed to children prompt them enter information to access special areas or to be included in a special club. Children should be instructed not to enter any information without first consulting a responsible adult. Congress has passed the Children's Online Privacy Protection Act that prohibits Internet sites from gathering information from children under the age of thirteen without parent's consent. This act goes a long way to protect children and their personal information, but it is no guaranteed that every Internet site will comply with the act.

Lastly, be smart. Do not enter any information if you are not confident that it will be used as you intend it to be used. If you are required to enter information in order to enter a specific area of the Internet site, and you do not feel comfortable entering that particular piece of information, lie. They have no way of knowing that you do not live at 123 Maple Street, Normaltown, New York.

Future Considerations

Privacy has long been among the major concerns for Internet users and is one of the main reasons that non-Internet users avoid the Internet. Seventy-five percent of Americans fear that their personal information could be stolen or used improperly. In order to gain the public confidence, steps must be taken to ensure the privacy of Internet users. Much has to be decided. It must be determined whether the government should, and can, step in to calm Internet users' fears and bolster a sagging industry. In the meantime, it is up to the Internet buyer to beware.

Bibliography

(1) Brown, Andrew, "If all is lost, can a dot.com sell your soul?" http://www.cnn.com/2001/WORLD/asiapcf/east/02/16/hongkong.customer/

(2) Christie, Jim, "Companies saw bankrupt dot-com buying binge in 2001" http://www.forbes.com/newswire/2002/01/09/rtr475576.html

(3) Consumer Privacy Guide.org "Consumer Privacy Guide Top Steps" http://www.consumerprivacyguide.org/topthings/

(4) CyberAtlas "Americans show Net security concern" http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905357501&rel=true

(5) Davsion, Paul, “Congress May Limit the Selling of Dying Dot-com’s Data” http://detnews.com/2001/technews/0102/07/b04-184955.htm

(6) DiSabatino, Jennifer “Essential.com Stopped from Selling Customer Data” http://www.pcworld.com/features/article/0,aid,57884,00.asp

(7) Farmer, Melanie, “Toysmart suspends auction of customer list” http://news.cnet.com/news/0-1007-200-2359462.html

(8) Federal Trade Commission, “FTC Sues Failed Website, Toysmart.com, for Deceptively Offering for Sale Personal Information of Website Visitors” http://www.ftc.gov/opa/2000/07/toysmart.htm

(9) Gartner, James, “New Congress to Push Privacy” http://www.ecommercetimes.com/perl/story/15138.html

(10) Gunn, Moira, “Hey, who's in charge of my data?” http://www0.mercurycenter.com/svtech/news/indepth/docs/mg072500.htm

(11) Heim, Kristi, “Amazon acquires assets of bankrupt Egghead, plans relaunch of site” http://www.siliconvalley.com/docs/news/depth/amazon120501.htm

(12) Hoffman, Ivan “Privacy Issues: New Wrinkles”. http://www.ivanhoffman.com/policies.html

(13) Lorek, Laura “Grim Reapers Prey on Dot-Com Failures” http://www.zdnet.com/zdnn/stories/news/0,4586,2600179,00.html

(14) Olsen, Stephanie, “Privacy watchdogs mull Engage's future” http://news.cnet.com/investor/news/newsitem/0-9900-1028-6831796-0.html?tag=ltnc

(15) Regan, Keith, “Honesty about E-Privacy, Truly the Best Policy” http://www.ecommercetimes.com/perl/story/story-start

(16) Rodger Will, “All That Data, All That Secrecy “ http://www.wired.com/news/politics/0,1283,42406,00.html

(17) Rosencrance, Linda, “Sale of More.com's customer list raises privacy concerns” http://www.cnn.com/2000/TECH/computing/10/27/online.privacy.idg/

(18) Ross, Patrick, “Senate protects consumer data” http://news.cnet.com/news/0-1005-200-5160763.html?tag=bplst

(19) Sandoval, Greg, “Failed dot-coms may be selling your private information” http://news.cnet.com/news/0-1007-200-2176430.html

(20) Scribbins, Kate, “Privacy@net An international comparative study of consumer privacy on the internet” http://www.consumersinternational.org/news/pressreleases/fprivreport.pdf

(21) Steer, David, “Privacy Of Online Data Still Elusive” http://www.privacyplace.com/news/00news/01_January/01_17/privelusive.php

(22) Stepanek, Marcia, “Privacy Isn’t a Priority at Bankrupt Dot-coms” http://www.businessweek.com/bwdaily/dnflash/july2000/nf00720b.htm?scriptFramed

(23) Thibodeau, Patrick, “FTC Chief Suggests Pause in Push for Privacy Laws” Computerworld, http://www.pcworld.com/news/article/0,aid,64804,00.asp