PRIVACY POLICIES: AN INVESTIGATION INTO BEST PRACTICES FOR INFORMATION SECURITY AND DATA PROTECTION

Edward D. Showalter, Randolph-Macon College, Ashland, VA 2305, (804) 752-3716, eshowalt@rmc.edu

Abstract

This paper overviews the concept of privacy and the evolution of laws relating to privacy policies. A sample of privacy policies from several companies (n>100) is reviewed on clarity, and readability. Several individual policies are highlighted and critiqued. Policies are also discussed as they relate to ethical criteria and privacy issues as outlined in Holtzman's (2006) "Seven sins against privacy."

Introduction:

Any consumer who has a bank account, investment account, credit card, customer loyalty card, or utility account has received one of the now ubiquitous slips of paper outlining a privacy policy. Nearly every website visited also has a privacy policy link. While there are no doubt many customers who carefully read these policies and make decisions based on the information contained therein, there are many more who give them at best a cursory glance before filing them away for future reference or who simply ignore them and/or toss them into the trash. This paper briefly overviews the concept of privacy, the evolution of some laws relating to privacy policies, and looks at a sample of privacy policies from several companies (n>100) in order to critique the policies and their presentation. Several criteria are used as the basis of the critique of these policies. Policies are also discussed as they relate to ethical criteria and privacy issues as outlined in Holtzman's (2006) "Seven sins against privacy."

Definition of Privacy

The definition of privacy varies with many factors including age group, culture and shifting social standards. What is considered private information by one person or group may be considered as fair game by another. Holtzman (2006) presents three basic views of privacy. Seclusion – the right to be hidden from the perceptions of others, Solitude – the right to be left alone and, Self-determination – the right to control information about oneself (Holtzman, 2006, 4) The purpose of a privacy policy is related to each view in some way. The most direct relationship is with the third view – that of self-determination, however companies which share information with others may potentially violate the first two views of privacy as well as the information becomes part of a target marketing or data mining process.
A privacy policy therefore should address information that is openly given to a firm through transactions or filling in forms, as well as information that is gathered indirectly (e.g. in the process of searching a website or by seeking information from a salesperson.)

Brief Evolution of Privacy Policy Law (some key legislation)

The complete evolution of legislation and common law applicable to privacy policies is too complex to be fully explored in this paper; however there are several key turning points and pieces of legislation that are worth note and are examined. There is no "right to privacy" guaranteed by the constitution although the 3rd and 4th amendments regarding the quartering of soldiers and search and seizure respectively are sometimes seen as establishing related rights.

Supreme Court Justices Warren and Brandeis published a seminal piece in the Harvard Law Review in 1890 arguing for the development of a right to privacy.

> "The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury. Nor is the harm wrought by such invasions confined to the suffering of those who may be the subjects of journalistic or other enterprise. In this, as in other branches of commerce, the supply creates the demand." (Warren and Brandeis, 1890)

Warren and Brandeis recognized over a century ago that a supply of private information would create a demand for that information, and such has certainly been the case. In their conclusion they recommend that laws to protect individual privacy should be established to bring the protection of criminal law to the issue of preventing invasions of privacy.

While many privacy protections were established at the state level over the following years, the most comprehensive legislation protecting privacy at the federal government level was the Privacy Act of 1974. (5 U.S.C. § 552a). In 1996 the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law 104-191) created a set of guidelines for gathering, protecting, transmitting and sharing health related information.

The most relevant legislation related to company privacy policies is the Gramm-Leach-Bliley Act (Public Law106-102;1999) regarding consumer information. This legislation addressed numerous financial institution issues, however for the purposes of this paper only those related to privacy policies are discussed.

The Gramm-Leach-Bliley Act (1999) defines six distinct types of privacy notices.
Initial: To customers not later than when relationship is established; To consumers prior to sharing nonpublic personal information

- Opt-Out: To consumers and customers prior to sharing information
- Short-Form: To consumers who are not customers, in lieu of full initial notice, prior to sharing nonpublic personal information about them
- Simplified: To customers if don't share NPI about current or former customers with affiliates or nonaffiliated third parties outside exceptions 313.14 and 313.15
- Annual: To customers for duration of the relationship
- Revised: To consumers, customers, and former customers (FTC, 2008)

According to the Gramm-Leach-Bliley Act (1999) privacy notices must be clear and conspicuous, reasonably understandable, and designed to call attention. As presented on the FTC website these terms are defined as follows:

- "Clear and conspicuous" means that a notice must be reasonably understandable and designed to call attention to the nature and significance of the information in the notice.
- "Reasonably understandable" means clear and concise sentences, plain language, active voice.
- "Designed to call attention" means using headings, easily read typeface and type size, wide margins. On website: use text or visual cues to encourage scrolling down the page to view the entire notice; place notice on a frequently accessed page or via a clearly labeled link; ensure that there are no distracting graphics or sound. (FTC, 2008)

Sins Against Privacy

The legislation above is intended in part to address privacy and information concerns. These concerns are what Holtzman (2006) identified as the seven sins against privacy. This taxonomy develops a clear categorization of privacy violations. A given incident may violate multiple categories. The seven sins are:

- Intrusion – the uninvited encroachment on a person's physical or virtual space.
- Latency – the excessive hoarding of personal information beyond an agreed upon time.
- Deception – using personal information in a way that was not authorized by the person involved.
- Profiling – misusing data derived from raw personal information.
- Identity Theft - pretending to be someone else with the intent of harm or personal gain.
- Outing – revealing information about a person that they would rather remain hidden.
- Lost Dignity – revealing information (or failing to protect information) that may bring humiliation and a loss of self respect on an individual. (Holtzman, 2006, Chapter 1).

Types of information addressed by privacy policies

There are several types of information that can be obtained by companies as outside users access information from the company: Site Access information, Actively Provided information and Inactively Provided information. In addition each of these types can be categorized being Personally Identifiable information (PII) or non-PII.

Site Access information is the information required for a user's computer to access information provided by a company's web server. This primarily consists of IP addresses and Cookies used to facilitate site access. Cookies may do more than facilitate site access, and may provide the company with some PII and non-PII. In and of itself an IP address does not contain personally identifiable information but it may be possible to connect a user to the individual IP address of the computer they use.

Actively Provided information is user provided information openly provided to the company through user actions. These actions may simply be selecting certain links, or may be more identifiable such as filling out some sort of form providing requested information like names, e-mail addresses and demographic information. Much of this type of information is clearly identifiable with the user (PII) and is of the opt-in variety. A user only provides this type of information voluntarily through action. This type of information may be combined with site access information and retained on either the user's computer as a cookie or other type of file or by the company's computer.

Inactively Provided information is information provided by the user's computer to the company as the user accesses the site. This type of information may be accessed by the company through cookies or web-beacons and is often collected without the users active knowledge. Examples of this information may include information based on previous visits to the company's web site, or tracking information collected as a user goes from site to site. For instance if a user accesses a site through a search engine the company's server may track that information to determine how users find their sites. This type of information may be combined with site access and/or actively provided information and retained on either the user's computer or the company's server.

Method

Privacy policies are readily available and easily accessible. For the purposes of this study 120 privacy policies were collected and reviewed. These policies came both printed policies and policies available on the companies' web sites. Several categories of firms supplied these policies including banks and

financial institutions, retail sites, social networking sites, consumer credit sites, public institutions (libraries, motor vehicle divisions etc.) and utilities. The policies were of multiple types according to the criteria established by the Gramm-Leach-Bliley Act (1999). The policies to be analyzed for readability were downloaded from the companies' web sites.

Each policy, was assessed by the researcher according to its meeting the clear and conspicuous, readability and attention criteria set forth by the act. Prominence (a policy should be clear and conspicuous) was determined by its placement and accessibility from the home page of a firm, or in the case of a printed policy its position within a mailing. Readability (a policy should be reasonably understandable) was determined by entering the policy into a Microsoft Word document and measuring the policy's Flesch Reading Ease, and the Flesch-Kincaid Grade Level. While these tests may not be universally reliable they will provide an internally consistent measure for this study. The formulas used to determine readability are:

Flesch Reading Ease test
206.835 – (1.015 x ASL) – (84.6 x ASW)

Flesch-Kincaid Grade Level test
(.39 x ASL) + (11.8 x ASW) – 15.59
where:
ASL = average sentence length (the number of words divided by the number of sentences)
ASW = average number of syllables per word (the number of syllables divided by the number of words)

The readability test used is similar to the method used in a study by Proctor (2008) which found that the average reading level was above the 13th grade.

The number of and clarity of headings in each policy was also be recorded as a measure of the policies structure (design to call attention.)

In addition to these measures each policy was assessed on critical content relating to the protection of personal information including the type of information gathered, the length of time information is kept, policies for sharing information, disclaimers and other criteria to be developed.

Findings

The findings based on the review of the policies were not surprising based on the highly charged and regulated environment in which these policies are created. The vast majority of the policies reviewed were either of the initial or short form variety. The Annual policies reviewed connected to financial institutions (Banks, Investment Firms and Credit Cards) tended to be substantially longer and more complex than the web site policies for social networking and most type of web sites. All the policies seem to be conspicuous and designed to call attention. Links were available on the home page of nearly every company reviewed, although there were a few that were listed as "Legal Notices" rather than privacy policies, and several (approximately 5% of those reviewed) required more than one click to access the full policy. One policy in particular, the web-policy for Wachovia Bank, was structured as a series of separate pages (within a frame) and required multiple clicks to read through the entire policy. It is of interest to note that the page for SEINFORMS does not have a privacy policy linked either on the website or on the conference paper submission form.

Clarity of the policies reviewed varied widely. BEA systems presents a clear concise policy that is fairly readable in less than 160 words, although the Flesch-Kincaid reading level was just under the 12th grade

level (11.58). KPMG at the 13th grade level was also quite readable and understandable, although the word count was fairly high at 1820. The range for word count was 158 (BEA systems) to 5461 (Sprint). ATT was the next largest at 5313. The mean for word count was 1831, and the mean reading level was 13.7. Of the policies analyzed for readability (n=110) only 10 had a reading level score less than the 12th grade level, and only two were below the 11th (Accenture and Specialized Bicycles.)

BEA respects your right to privacy and your right to limit information exchanges to only those you initiate, if you so desire. We do acquire certain personal information from private individuals in the course of business, and may at times share this personal information with our partners. We use this information to better serve you and facilitate your use of our web site.

BEA may also acquire a private individual's personal information from registration forms, product order information, or e-mail messages to us. The BEA web server also records visitor IP addresses and domain names for reporting and site usage analysis. This information is reported internally and then purged when required.

If you supply BEA with your e-mail address, postal address or phone number through our site you may receive promotional or informational communications from BEA or one of our partners. To manage your profile or opt-out from BEA communications, please fill out this request form.

BEA Privacy Policy
Accessed 8/2/2008 from www.bea.com

Readability scores tended to track reading level scores (.87 correlation) and ranged from a high (most readable) of 55.85 to a low (least readable) of 19.42 with a mean of 40.38. The most readable policy again belonged to Specialized Bicycles. The least readable was Northrop Grumman's.

An excerpt from Specialized Bicycles policy shows how the policy is not only readable, but targeted for the intended audience.

Introduction

We're bike geeks. We live and breathe bikes and cycling. We believe the only thing better than going on a good ride yourself is helping others have the ride of their life. That's what Specialized is all about. For that reason, we thought you might want to know what our Privacy Policy is, and what it means to both of us.

The Overview

Our number one goal is to keep you psyched on cycling and stoked on Specialized. So, we responsibly use technology to help us learn more about what you like, and what you don't, so we can get you the right products at the right price at the right time.

Specialized respects your privacy. The only information that we collect about you is that which you choose to submit to us either through a product registration form, signing up for our Rider Club, by placing an order, submitting a résumé or through other interactive forms. We will always give you an opportunity to decline to receive further information.

The Nuts and Bolts (and cookies)

Our site does contain links to other sites. If you are concerned with their privacy practices, please check their sites individually. We are not responsible for their privacy practices.

Excerpt from Specialized Bicycle's Privacy Policy
Accessed 8/2/2008 from www.specialized.com

Relationship of Privacy Policies to Holtzman's Seven Sins

The seven sins against privacy outlined by Holtzman (2006) are Intrusion, Latency, Deception, Profiling, Identity Theft, Outing, and Lost Dignity. Most privacy policies reviewed do not specifically address all of these issues, however several are addressed indirectly. The majority of companies specifically state that any information provided by the individual to the company is voluntary, so Intrusion is avoided. Latency, on the other hand, is rarely addressed. Information provided to a company is often kept well beyond its usefulness to the company. For instance, Social Security Numbers, which may be needed to initially check the credit-worthiness of a customer, may be retained indefinitely. In and of itself this may not pose a problem, but in the event of a breach of data security, this information may be obtained by outside entities. Most privacy policies contain some sort of disclaimer that protects them in the event of such a security breach, and the remedy is usually limited to the notification of the breach to the customer.

The sin of Deception is usually addressed in privacy policies by language that allows the company to use the information in various ways. It is unlikely, however, that most customers knowingly authorize every way that a company may use the information. While the language of the privacy policies legally avoids deception, there may be ethical arguments depending on the individual company's use.

The sin of profiling is more difficult to address from a corporate standpoint, as it is the misuse of derived data that is addressed. Data Mining may allow companies to use derived data to provide improved products, services and communications to customers. Often customers are given an opt-in or opt-out opportunity by the privacy policies regarding the receipt of communications related to these offers, however the privacy policies often indicate that the customers data will be used to facilitate the development of the new offerings.

The last three sins addressed by Holtzman, Identity Theft, Outing, and Lost Dignity, are typically not issues that are of direct concern but rather arise from the failure to protect gathered and stored data. As mentioned before many companies use language in their privacy policies to hold themselves harmless in the event of such a data breach. An example of such language is below:

All information gathered on our website is stored within a database accessible only to Comcast and its specifically authorized contractors and vendors. However, as effective as any security measure implemented by Comcast may be, no security system is impenetrable. We cannot guarantee the complete security of our database, nor can we guarantee that information you supply won't be intercepted while being transmitted to us over the Internet.

Excerpt from Comcast Privacy Policy
Accessed 8/2/2008 from www.comcast.com

Conclusions and Recommendations

The purpose of this investigation was to assess privacy policies acccording to certain ethical and legal criteria. Legislation requires privacy policies to be clear, accessessble and readable. While privacy policies as they now exist may meet most legal critera, that determiniation can only be made by the courts and the legislative process. From an academic perspective, however, there is room for improvement especially in the readablity of the policies. Many are quite lengthly and the reading level is quite high. Shorter more straightforward sentences may make the policies more understandable to the consumer.

The content of the policies could be improved as well. Many companies collect more information than they need to facilitate either information sharing or transactions. In addition to gathering the information much of it is retained longer than needed, allowing future opportunities for misuse of the information to exist.

When creating policies for gathering information companies should ask themselves what information is needed, for what purpose, and for how long; then construct appropriate policies and clarify for the consumer the reasoning behind the policies.

Recommended Best Practices

1: Connect Privacy Policy to Mission
2: Collect only data that is needed
3: Limit the retention of data
4: Use appropriate language – Avoid unnecessary complexity
5: Provide examples of how data might be used
6: Clearly identify who has access to data, and why.

Selected References

Bhasin, Madan Lai. (Feb 4, 2008). Guarding privacy on the internet privacy policy, government regulations and technology solutions. International Journal of Internet Marketing and Advertising. 4.2/3 p. 213.

FTC: Federal Trade Commission (2008). The Gramm-Leach-Bliley Act Privacy of Consumer Financial Information. http://www.ftc.gov/privacy/glbact/glboutline.htm . Accessed 3/24/2008.

Holtzman, David H. (2006). Privacy Lost. San Francisco: Josey-Bass.

Lwin, May; Wirtz, Jochen and Williams, Jerome D. "Consumer online privacy concerns and responses: a power – responsibility equilibrium perspective. " Journal of the Academy on Marketing Science 35.4 (Winter 2007):p572-585.

"Many people unaware of internet data tracking." (March 2008). Choice (Chippendale, Australia) 5(1). p. 5.

"Nationwide survey reveals 87 percent of consumers question safety of personal information, yet many unknowingly engage in risky behaviors" (April 30, 2008) Business Wire. New York.

Peterson, Diane; Meinert, David; Criswell II, John and Crossland, Martin. (2007). Consumer trust: privacy policies and third party seals. Journal of Small Business and Enterprise Development. Bradford. Vol 14, Iss. 4 pg. 654.

Pollach, Irene. (2007). What's wrong with online privacy policies?. Association for Computing Machinery. Communications of the ACM. New York. September 2007. Vol 50, Iss 9. Pg 103.

Proctor, Robert W., Ali, M. Athar, Vu, Kim-Phuong L. (2008). Examining Usability of Web Privacy Policies. International Journal of Human-Computer Interaction, Vol. 24 Issue 3, p307-328.

Warren and Brandeis (1890). The Right to Privacy. Harvard Law Review. Vol. IV. December 15, 1890. No. 5

Wilcon, Tim, (March 24,2008). Bitten by a privacy policy. Information Week. Manhassett. Iss 1178 pg. 21.