

2002

An empirical study of web surfers' privacy concerns

Jack Cook

Rachel Curtin

Follow this and additional works at: <https://scholarworks.rit.edu/other>

Recommended Citation

Cook, Jack and Curtin, Rachel, "An empirical study of web surfers' privacy concerns" (2002). Accessed from <https://scholarworks.rit.edu/other/435>

This Conference Paper is brought to you for free and open access by the Faculty & Staff Scholarship at RIT Scholar Works. It has been accepted for inclusion in Presentations and other scholarship by an authorized administrator of RIT Scholar Works. For more information, please contact ritscholarworks@rit.edu.

AN EMPIRICAL STUDY OF WEB SURFERS' PRIVACY CONCERNS

Jack Cook, Ph.D., CFPIM

Associate Professor of Information Systems
College of Business, Rochester Institute of Technology

Rachel Curtin

Jones School of Business, State University of New York at Geneseo

Just imagine how you would feel if you found out that someone secretly followed you for months. This person knows your name, address, and birth date, but it does not stop there. They have discovered what medications you currently take, that you plan to vacation in Cocoa Beach, Florida from March 10th to the 18th, what kind of music you listen to, even how old your children are and the fact that you think your spouse is cheating on you. Do you think that this only happens to people in the movies? Think again. This is but a sample of what marketers and websites can deduce from tracking you online.

In 1998, "the FTC reported to the U.S. Congress that the most basic fair information practice -- notifying individuals when information is collected -- wasn't practiced by a majority of surveyed web sites. The FTC surveyed 1,400 commercial web sites and found that while 85 percent of the sites collected personal information, only 14 percent provided any details of their information practices, and only two percent did so through a formal privacy policy (Sullivan 2000, p. 32)." This was only four years ago. While companies have changed how they conduct business and collect data over the Internet since the time of this report, consumers still have reason to distrust web sites. One example of a company that was criticized for the way that information was collected was RealNetworks. RealNetworks provides streaming video and audio through Web browsers. The initial release of RealNetworks' RealJukebox sent data about what CDs consumers listened to back to the company (Graven 2001). It was also discovered that RealNetworks' software collected information about the content users requested from their browser -- all without the users' permission (Rubin 2000).

This research addresses the question: How willing are Internet users to provide personal information to web sites? The objective of this research is to determine how willing consumers are to share personal information under different conditions, as well as how informed the average consumer is regarding what specific information is collected by web sites and how this information is used.

This survey will be of interest to a broad spectrum of different groups, including, most notably, e-businesses and consumers. E-businesses would find this survey useful in gauging how willing consumers are to provide personal information and what impact does online privacy policies have on consumers' willingness to share their personal information. Consumers would find this survey interesting, as it may open their eyes as to what is really going on in cyberspace when they log on the net.

LITERATURE REVIEW

Research has uncovered some startling facts concerning consumer privacy. Larry Ponemon, the head of Pricewaterhouse Coopers's privacy practice, estimates that 80 percent of companies do not comply with their own

privacy policies. Even though he attributes most of these breaches to human error, it is still unsettling (Petersen 2001). In addition, there are many other examples of e-businesses invading consumer privacy. Just recently, Windows Media Player for Microsoft Windows XP has been in the news. Everything that is watched or listened to through the player is recorded on a Microsoft server. Of course, Microsoft claims the data is not used and only facilitates personalization, but it makes one wonder. Some companies have even been found using Spyware to find out how an individual uses his or her computer when offline.

Many people do not shop online. They do not trust e-businesses. And it is not just those new to the web that are weary of how companies use consumer information and how that information is protected. According to Hoffman, Novak and Peralta (1999, p. 84), "It is dramatically apparent that negative perceptions regarding security and privacy increase along with levels of online proficiency." According to a survey by PeopleSupport, an Internet customer service provider, about 19% of Internet users shop online once a week, 22% do so once a month, and 43% are infrequent Internet shoppers (Hinde, 1998).

Not surprisingly, consumers are more likely to make a purchase online if they trust the web site. So what exactly entices a consumer to trust an e-business? A comprehensive privacy policy, written clearly and in plain English, is a start. Initial trust in an unfamiliar web site is also influenced by a perceived connection between the web site in question and well known web site. Noteberg, Christiaanse, and Wallage (1999) have found that assurance services, such as a credit card's assurance or the computer industry's assurance, also positively affects the likelihood of purchase.

According to another recent survey, 71 percent of Americans feel that there should be new laws enacted to protect their privacy online. The U.S. government, however, has been slow to act. The government believed that the computer industry would heed consumers' cries for more respect of their privacy and increased security when information is in fact gathered. In reality though, not all companies have heeded consumer demands regarding privacy. The Federal Trade Commission (FTC) has been the leading government force for consumer online privacy. In the FTC's May 2000 report, a follow up to the initial 1998 report, the Federal Trade Commission identified four recommendations that are suppose to be guidelines for the collection and use of information from consumers (Gillin 2000). These four recommendations are:

- 1) Notice: the consumer should be given notice as to how the information is collected, what the information is going to be used for, and what, if any, third parties have access to the information;
- 2) Choice: the consumer should be given a choice, as in opt-in or opt-out;
- 3) Access: the consumer should be allowed to access the information collected about them to correct any inaccuracies;
- 4) Security: the company should take steps to ensure the information collected is secure.

As a result of the efforts of the FTC and a number of consumer privacy lobbying groups, a few laws have been passed regarding consumer privacy in the United States. However, the U.S. still has a long ways to travel before consumer privacy gains the level of protection it deserves. "U.S. privacy statutes have primarily focused on protecting consumers' financial data (Gramm-Leach-Bliley Act), health information (Health Insurance Portability and Accountability Act), and their children's personal information (Children's Online Privacy Protection Act) (Rombel 2001, p. 28)."

While many businesses may genuinely act in the customers' best interests by improving service and targeting marketing efforts, the same practices may cross the line between what is public and what is private personal information (Sullivan 2000). Only after e-businesses and consumers come to a mutually beneficial agreement as to how consumer information can be collected and used will the Internet be able to flourish and the consumer freely able to enjoy the full benefits that the World Wide Web has to offer.

METHODOLOGY

A convenience sample was taken for the purposes of this pilot study. The sample collected contained 232 people in four different categories. The first category contained students at the State University of New York at Geneseo in two sections of a Management Information Systems class. They accounted for 36 of the 232 people surveyed. The second group was made up of both friends and family of students in the class. This included 88 of the 232 surveyed. The third group contained professionals at an APICS professional development meeting. This accounted for 49 of those surveyed. The rest were graduate and undergraduate students in a Systems Analysis and Design class at the Rochester Institute of Technology. The average age of participants was between 30-39. The sample was 55.2 percent male and 44.8 percent female. Of those surveyed, 190 were White, 19 were Asian, 9 were Black/African American, 3 Hispanic, 3 people classified themselves as other and 9 did not specify. On average, most respondents had completed some college. The average income was between \$50,000 – 74,999.

HYPOTHESES

Hypothesis 1: Respondents will be more willing to provide sensitive information to web sites as the information becomes more relevant to their surfing activities.

For the purpose of this survey, a few items have been selected as "sensitive data", or data that can be used far beyond the scope of a web site. For example, a social security number can be used to access a vast amount of information including new credit cards and loans. Other data categorized as sensitive include name, email address, zip code, phone number, credit card number and income.

It is predicted that as information becomes more relevant to a respondent's Internet experience, the more willing a respondent will be to provide sensitive information. A respondent will be increasingly likely to provide a web site his or her credit card number when purchasing, but not very willingly provide that same data to a web site that does not customize the site to meet a surfer's needs.

Hypothesis 2: Respondents will feel uncomfortable to learn that web sites are sharing their information with third parties, yet a majority of respondents will choose to *opt-in*, or receive either emails or direct mailings from third parties.

In an effort to maintain their privacy, respondents will say that they are uncomfortable with the thought of web sites sharing information with third parties. However, either due to the fact that a respondent does not know that *opt-in* gives a web site permission to share information with third parties or respondents perceive value in receiving marketing from third parties, it is predicted that 50 percent or more of respondents will choose to *opt-in*.

Hypothesis 3: Respondents will feel more comfortable sharing information if the web site displays a privacy policy, even if the respondent does not read it.

A privacy policy on a web site can reassure visitors that the web site will take steps to secure personal information. Knowing that a web site is concerned with their privacy, respondents will feel more comfortable about sharing sensitive information.

Hypothesis 4: The majority of people surveyed will say that they sometimes use false identities when registering for web sites.

What are some of the reasons that people would use false identities? One could be that they feel uncomfortable giving out certain personal information. Or maybe consumers do not trust some Internet sites and they feel uneasy providing them personal information.

Hypothesis 5: The majority of people will say that they should always have the choice whether to receive e-mails and other information from web sites.

People desire options. They do not want anything forced upon them. Next, we analyze the survey results.

ANALYSIS

The survey began with some basic background information about Internet usage. It was found that the majority of those surveyed spent less than three hours a week surfing the Internet, not including idle time, email, or chatting. Of those surveyed, 19.6 percent spent less than one hour a week, 31.8 percent spent less than three hours per week but more than one, 19.6 percent spent less than five hours per week but more than three, 19.1 percent spent less than ten hours but more than five, and 10.3 percent spent ten or more hours surfing the Internet per week. Only 21.2 percent of the respondents have been surfing the net for less than two years. Almost 53.7 percent of those surveyed had been surfing the Internet for less than five years, but more than two. Approximately twenty-five percent of those surveyed had been surfing for more than five years. It was also found that 85.3 percent of our sample had purchased consumer goods on the Web within the last six months. More specifically, 31.9 percent of the respondents had spent less than \$100 online in the last six months, and 31.3 percent had spent less than \$500 but more than \$100 in the last six months online. And finally, 22.1 percent had spent more than \$500.

This study found that almost 91.6 percent of all respondents have provided personal information to a web site such as name, email, street address, phone number, social security number, or credit card number, just to name a few. Additionally, of all respondents, 52 percent admitted to registering for and regularly using three to six web sites. One might very well conclude that people are very willing to provide information to web sites, but how much is too much and what information exactly are consumers willing to give?

The study found that what information a consumer provides a web site depends on the level of customization. More information will need to be provided to a web site a consumer is purchasing from, as opposed to a web site at which a consumer is just browsing. Sixty and one-half percent of all respondents said that they would be very willing to provide their name to a web site, as long as they were purchasing from that site; contrasted with only 37.3 percent if the web site customized, and 23.6 percent if the web site did not customize. Sixty-seven percent of respondents claimed they would provide a web site their email address if they were purchasing something, as opposed to 33.8 percent if a web site was only customizing, and 23.3 percent if the web site did not customize. The same theory holds true for other sensitive data including phone number and credit card number (see Table 1).

Table 1. Percent of People Very Willing to Provide Information

Data Collected	Web Site Does Not Customize	Web Site Personalizes or Customizes	Purchase from Web Site
-----------------------	------------------------------------	--	-------------------------------

<u>Name</u>	23.6 percent	37.3 percent	60.5 percent
<u>Email Address</u>	23.3 percent	33.8 percent	67.3 percent
<u>Phone Number</u>	4.0 percent	5.9 percent	41.6 percent
<u>Credit Card Number</u>	1.5 percent	2.0 percent	38.8 percent

There is some information, however, that consumers feel are too sensitive to provide a web site regardless of whether they are purchasing or not. This study found the two things that consumers are least willing to provide are a social security number and his or her mother's maiden name. Only 9.4 percent of all respondents said that they were very willing to provide a social security number, even if they were purchasing an item; and only 11.8 percent were very willing to provide his or her mother's maiden name under the same circumstances.

The results suggest that customers are willing to provide some information, but there remains the question of why they do not. Perhaps consumers are afraid that the information will be shared with third parties. In fact, only 14.7 percent of respondents said that they were either very comfortable or even somewhat comfortable with web sites sharing information with third parties. However, 45 percent of all respondents said that they prefer to *opt-in*, or request to receive direct marketing, from these same third parties.

This survey also found that people feel more comfortable with a web site that has a privacy policy, regardless of whether they read it or not. In fact, 58.4 percent of all respondents either strongly agreed or agreed with the idea that a privacy policy ensures comfort, even though only 4.4 percent of those surveyed always read the privacy policy when they first arrive at a web site. 23.2 percent sometimes read the policy after they first arrive at a web site, followed by 30 percent who rarely and 42.9 percent who never read the privacy policy.

Overall, the results indicate that consumers are at least somewhat concerned with their privacy. For an example, respondents claimed that that they would only provide certain information if the circumstances were appealing. One such circumstance is if they were purchasing from a web site and information was necessary to process the order. Out of those people that were surveyed, 46.5 percent said that although they value both privacy and convenience, when given a choice, they preferred privacy over convenience. Twenty six percent said they were indifferent between the two.

Consumers are aware that web sites collect personal information. We found that 27.2 percent of the respondents believe that 50-74 percent of the most popular websites collect personal information. Another 26.7 percent believe that 75-89 percent of these websites collect personal information. And still another full 25.2 percent of the people surveyed believe that between 90-100 percent of popular websites collect personal information. Only 20.8 percent of the respondents thought that less than 49 percent of the most popular websites collect personal information from consumers. The actual percent of popular sites that collect data about surfers is above 90 percent.

We also discovered that most consumers do not use false identities to register for web sites. Of those surveyed, four percent always use false identities, 45.7 percent sometimes use false identities, 11.6 percent rarely use false identities, and 38.7 percent never use false identities. It is

interesting to note that although consumers are well aware that websites collect personal information, over half of the respondents rarely or never use false identities to protect themselves from prying electric eyes.

Of those surveyed, 85.6 percent felt that web sites should always give customers choices about having collected information disclosed to outside third parties. Only 1.5 percent said that they should never give customers a choice. It was also found that 85.5 percent felt that web sites should always give consumers choices about whether they want to be contacted by the organization for marketing or other communications (other than those communications related to processing an order or responding to a customer's question). When consumers are given a choice to receive e-mails from a web site, eight percent always opt to receive the e-mails, while 38.6 percent sometimes opt to receive them and 53.5 percent rarely or never choose to receive the e-mails. However, when given the choice to receive e-mails from third parties, 91.1 percent rarely or never opt to receive them.

LIMITATIONS

As with any research, limitations exist with this pilot study. It is necessary to understand a few basic limitations that the researchers faced. Among the most important ones were (1) the sample may not reflect the whole population since it is a convenience sample, and (2) the survey was quite long and respondents became impatient with the amount of time involved.

A good majority of the respondents had some technical background and this may have biased the results. In order to have had a better representation of the population, researchers should randomly select individuals from the population as a whole.

Since many respondents were busy, comments were made that the survey was too lengthy. Although researchers were trying to capture as much data as possible, it is always important to remember the needs of the respondent by considering the time needed to complete the survey. When a survey becomes too long, respondents become agitated and are less willing to take adequate time to finish the questionnaire. In this study, a few respondents stopped after approximately question ninety and did not finish taking the survey.

FUTURE RESEARCH

There are other opportunities to do more research in this area. An interesting topic would be to find out why people are so unwilling to give some personal information. Through this survey, we found what information people were willing and unwilling to provide online. To expand on this, we could ask different questions to try to ascertain their reasoning for their differences in willingness.

REFERENCES

Gillin, Donna. "The Federal Trade Commission and Internet Privacy: Internet Privacy Threatens Both Online and Offline Research," *Marketing Research*, Fall 2000, pp. 39-41.

Graven, Matthew P. "Leave Me Alone," *PC Magazine*, 16 Jan. 2001, pp. 151-159.

Hinde, Stephen. "Privacy and Security-The Drivers for Growth of E-Commerce," *Computers & Security*, 17 (1998), pp. 475-478.

Hoffman, Donna L., Thomas P. Novak, and Marcos Peralta. "Building Consumer Trust Online," *Communications of the ACM*, Apr. 1999, pp. 80-85.

Noteberg, A., E. Christiaanse, and P. Wallage. "The Role of Trust and Assurance Services in Electronic Channels: An Exploratory Study." *Proceeding of the Twentieth International Conference on Information Systems*, Dec. 1999, pp. 13-15.

Petersen, Andrea. "Private Matters: It Seems That Trust Equals Revenue, Even Online." *Wall Street Journal*, 12 Feb. 2001, night final ed., pp. R24+.

Rombel, Adam. "Navigating the Privacy Law Divide." *Global Finance*, Jan. 2001, p. 28.

Rubin, Aviel D. "None of Your E-Business: Protecting Your Privacy in Cyberspace." www.webtechniques.com, Apr. 2000, pp. 55-58.

Sullivan, Dan. "Protect Customers' Web Privacy." *E-Business Advisor*, Apr. 2000, pp. 28-33.