

***INTERNET PRIVACY POLICIES: A COMPOSITE INDEX FOR  
MEASURING COMPLIANCE TO THE FAIR INFORMATION PRINCIPLES***

**Prepared by  
Felicia Williams, DBA  
Argosy University**

**September 2006**

**TABLE OF CONTENTS**

**List of Tables ..... iii**  
**Forward ..... iv**  
**Executive Summary ..... v**

I. Introduction ..... 1

**II. Background ..... 1**  
2.1 Privacy Concept..... 5  
2.2 Purpose of the Study ..... 5  
2.4 Research Questions ..... 7  
2.5 Research Hypothesis..... 7

**III. Research Method ..... 7**  
3.1 Research Design ..... 8  
3.2 Selection of Participants ..... 8  
3.3 Instrumentation ..... 9  
3.4 Privacy Policy Index- PPI..... 11  
3.5 Data Analysis..... 13  
3.6 Limitations..... 14

**IV. Findings..... 14**  
4.1 Research Question One ..... 14  
    Survey Question 1 ..... 14  
4.2 Research Question Two ..... 17  
    Survey Question 2 ..... 17  
    Survey Question 3 ..... 21  
    Survey Question 4 ..... 22  
    Survey Question 5 ..... 26  
    Survey Question 6 ..... 28  
    Survey Question 7 ..... 30  
    Survey Question 8 ..... 31  
    Survey Questions 9-10 ..... 31  
    Survey Question 11 ..... 32  
    Survey Question 12 ..... 33  
    Survey Question 13 ..... 34  
    Survey Question 14 ..... 35  
    Survey Question 15 ..... 37  
    Survey Question 16 ..... 38  
4.3 Research Question Three..... 40  
    PPI Application ..... 40  
4.4 Discussion of Results ..... 49

**V. Conclusion ..... 52**  
    5.1 Implications for Future Research ..... 54  
    5.2 Recommendations ..... 55

**Endnotes ..... 57**

**Appendix A: Survey Questions ..... 59**

**Appendix B: Survey Sample ..... 65**

**List of Tables**

Table 1: Privacy Policy Descriptions ..... 15

Table 2: Flesch Reading Ease Scores ..... 18

Table 3: Percentage of Firms Collecting Various Types of Personal Data ..... 19

Table 4: Percentage of Firms Collecting Various Types of Aggregated Data ..... 21

Table 5: Percentage of Firms Using Collection Technologies ..... 23

Table 6: Percentage of Privacy Policy Choices ..... 27

Table 7: Percentage of Firms Members of Privacy Seal Programs ..... 39

Table 8: Privacy Policy Index Compliance Rating Scale ..... 41

Table 9: Ranking of Firms by the Privacy Policy Index ..... 43

Table 10: Compliance Percentage Rating for each Principle ..... 45

## **Forward**

Imagine going into a book store and the moment you entered into the store, a person was assigned to follow and record your every move. The time and date you entered into the store was recorded. Every magazine, book, or paper you retrieved from the bookshelves and viewed was recorded. Every paged you turned to in the magazine, book, or paper, was recorded. As you moved from section to section, from isle to isle, the length of time you spent in each section and in each isle was recorded. Every person you spoke with on your journey of reading and acquiring knowledge was recorded. All of this recording and monitoring was done behind a veil of secrecy without your knowledge or consent. Welcome to the world of Internet privacy and the ongoing debate.

## **Executive Summary**

The privacy issues of online protection were reviewed by examining the privacy policies of the *Fortune* 500 firms. The survey questions were designed to examine the data collection practice statements contained within the privacy policies. A descriptive analysis of the results observed in 200 privacy policies is provided. Each firm was assigned a rating for each of the Fair Information Principles for an overall Privacy Policy Index (PPI) that measured the level of compliance to the Fair Information Principles. The firms were rated and rank in descending order based on the weight of their index score. Each index score was ranked in a compliance-rating category of fully compliant, compliant, partial compliant, and non-compliant. A firm with a *fully* compliant privacy policy received a score of 100.

Fourteen survey questions were used to formulate the PPI. The application of the PPI related to compliance to the Fair Information Principles proved positive. The PPI provides the basis for measuring compliance to the Fair Information Principles. The questions that were selected for the PPI computation objectively embodied and captured the various dimensions of the Fair Information Principles. The examination of each of the Fair Information Principles and the additional elements revealed several significant details.

### **Highlights of Results and Analysis**

- ❖ **Notice Principle:** Approximately, 24% of the firms failed to cover enough of the provisions of the Notice Principle in their privacy policies. Although there was an increase in the number of firms displaying privacy policies, the privacy policies were not written in plain, simple language, and were not comprehensible to the majority of the Internet users. There were significant differences in the

terminology used in each privacy policy. Each of the privacy policies differed across the different commercial Web sites. There was no standard format, standard hyperlink location, or standard data collection practice statements. However, the survey found that the number of firms displaying privacy policies was increasing over time.

- ❖ **Choice Principle:** Approximately, 88% of the firms failed to cover enough of the provisions of the Choice Principle in their privacy policies. Multiple options for opting-out were not provided. The privacy policies appear to give the firms the right to disseminate collected data to third parties with no evident means to opt-out of disclosure. Consumers were not given consent or choice opportunities when it comes to disclosing collected data to third parties. The firms automatically disclosed collected data to the third parties without notice to consumers. The survey found that a large portion of the firms did not provide consumers with an option of choice.
- ❖ **Access Principle:** Approximately, 53% of the firms failed to cover enough of the provisions of the Access Principle in their privacy policies. The individual right of consumers to review collected data helps to ensure that the data are accurate and complete. The survey found that a large portion the firms did not provide consumers with the opportunity to exercise their right to correct, amend, or delete inaccurate data.
- ❖ **Security Principle:** Approximately, 70% of the firms failed to cover enough of the provisions of the Security Principle in their privacy policies. The survey found that a large portion of the firms have not taken the effort to explain to consumers the security measures taken to ensure the security and protection of collected and stored data.
- ❖ **Enforcement Principle:** Approximately, 37% of the firms failed to cover enough of the provisions of the Enforcement Principle in their privacy policies. Many of the privacy policies did not provide consumers with contact information so that consumers could exercise their right to a method of recourse, redress, or a process to ensure that the privacy policies were enforced. The survey found that a large portion of the firms did not provide consumers with the opportunity to

exercise their right to verify and discuss collection practices, ask questions, register complaints, or remedy problems regarding the privacy policy or collected data.

***Additional Elements***

Two additional elements were also examined, the COPPA statement and membership into a privacy seal program. These two elements were identified during the review of literature pertaining to Internet privacy that could be useful in making the PPI more thorough. These two elements were not included in the index computation because the two elements are not included in the Fair Information Principles.

- ❖ ***Children’s Online Privacy Protection Act (COPPA):*** The examination shows that a significant pattern emerged concerning the additional elements. The findings revealed that the firms that are required to include a COPPA practice statement in their privacy policies are complying with the requirement and those firms that were not required to have a COPPA statement in their privacy policies are taking proactive steps to ensure they are also complying with the requirement. The firms who were required to have a COPPA statement in their privacy policies scored a PPI higher than those firms who were not required to have a COPPA statement in their privacy policies. The examination shows that a substantial percentage of the firms are accurately reflecting the COPPA statement in their privacy policies.
- ❖ ***Privacy Seal Programs:*** Only 10% percent of the firms were members of a privacy seal program. Approximately, 90.3% of the firms were not members of a privacy seal program, indicating that a substantial percentage of the firms are not in favor of a third party system of accountability. The findings revealed that the firms who were members of a privacy seal program scored a PPI higher than those that were not.

We live in a society where decision making is number driven. The PPI, even though not perfect, allows consumers to make an informed decision concerning compliance to the Fair Information Principles based on a number. The link between the PPI and compliance measurements will be a subject of significant interest to policy makers and consumers. The PPI, a different line of attack in the privacy debate, is a simple benchmarking tool that gauges the firm's best practice to comply with the standards.

The PPI is a tool whereby the consumer can assess compliance over time. However, additional work may be necessary to further refine the index. The PPI confirmed that the majority of the firms are not fully compliant the Fair Information Principles. The privacy policies do not cover all of the provisions of the Fair Information Principles. Although the privacy policies are compliant with some of the Fair Information Principles, there is plenty of room for improvement. This study provided the framework for future studies that seek to measure the level of compliance to the Fair Information Principles.

## **I. Introduction**

The Internet has been among one of the most important advances of the 20<sup>th</sup> century and its use is growing more prevalent. The Internet has unlocked numerous doors of information. Every bit of information the consumer sought has been found. Every door the consumer knocked on has opened. Every piece of information the consumer requested has been given. The Internet created a revolution in the ability to access information. Knowledge and information is power. In the quest to find knowledge and information, the question is, “Did the consumer lose a fundamental right-*the fundamental right of privacy*”?

The growth of the Internet, expansion into the global market, the increase in the e-commerce industry, and the rise of identity theft have cause consumers to pay more attention to the Internet privacy debate. Internet privacy can be a difficult challenge when attempting to create a marketing and global strategy. As consumer concerns increase, all firms must address the Internet privacy issue. Firms who fail to address Internet privacy will not be able to compete in the industry.

## **II. Background**

The Federal Trade Commission (FTC) conducted several hearings, workshops, and public meetings to investigate the issues associated with Internet privacy and data collection practices. Based on the results of the investigations, the FTC adopted a set of standards, The Fair Information Principles, for the management of collected data. The industry made a commitment to incorporate the standards into a privacy policy. The purpose of the privacy policy was to inform the consumer about data collection

practices. Internet privacy is a complicated issue due to the large number of people, institutions, organizations, and firms involved. The debate between the industry and the consumer is whether the key to protecting privacy is compliance with the standards or enacting privacy legislation.<sup>1</sup> The privacy policies have been at the heart of the Internet privacy debate.

Protecting privacy is dependent on consumer loyalty, and consumer loyalty is dependent on a comprehensive privacy policy.<sup>2</sup> A comprehensive approach to privacy protection includes a broad range of measures. These measures must be developed with the input of consumers, the industry, the government, and privacy advocates. This approach requires everyone involved to play an active role in protecting privacy.<sup>3</sup>

As a major player in the active role of protecting privacy, the FTC identified the standards as a method that would adequately present fair and adequate data collection practices. The standards are the data protection instrument that informs consumers of the type of data that is collected and used, provides consumers with a choice, gives consumers access to the collected data, informs consumers of the data collection security measures, and provides a method of enforcement when the industry does not comply with the standards.<sup>4</sup> The objectives of the FTC are to provide greater protection of personal privacy on the Internet, to protect consumers, and to increase the confidence in consumers.

In governing the use, collection, and dissemination of personal data, the privacy policy demonstrates the commitment to the privacy of the consumer. The privacy policy is a contractual commitment between the industry and the consumer to comply with the standards. The conflict between the industry and the consumer is what shaped the

standards. Consumers prefer standards that protect the right to privacy and the industry prefers standards that protect the right to collect and use data. A compromise between these two competing interest led to the standards written into a privacy policy. In order to ensure compliance with the standards, the privacy policy must consist of the following five Principles:

*Principle 1-Notice:* Those who collect data must disclose to consumers their collection practices before collecting, using, disseminating, and selling data. The privacy policy must provide consumers with a clear and conspicuous notice of data collection practices. The privacy policy must be easy to locate and written in plain and simple language.

*Principle 2-Choice:* Those who collect data must provide consumers with an option on the use, collection, and dissemination of collected data. The privacy policy must offer consumers choices regarding how the data are used. Consumers must be allowed to opt-out of the collection of data or opt-in to the collection of data. Consumers have the right to control the collected data and decline disclosure of data to third parties.

*Principle 3-Access:* Those who collect data must allow consumers access to the collected data. The privacy policy must offer consumers reasonable access to collected data. This includes the opportunity to review the data and to correct inaccuracies or delete information. The privacy policy must disclose any third party that will have access to the collected data. The consumer needs to know all those who have access to the collected data. Consumers have the right to know when personal data will be disclosed to third parties.

*Principle 4-Security:* Those who collect data must take appropriate steps to ensure the security of the collected data. Security involves measures to protect the collected data from lost, misuse, and unauthorized access. The measures include limiting access to the collected data, prevention of unauthorized access, encryption during transactions, and secure servers. The industry is required to protect the collected data. The consumer is looking for reassurance that the collected data are secure and protected.

*Principle 5-Enforcement:* Those who collect data must provide consumers with a method of recourse, redress, and a process to ensure that the privacy policies are enforced. The core Principles can only be effective if there is a procedure in place to enforce them. There should be regular audits and a modification process to ensure that adequate internal controls and enforcement measures are in place. Enforcement encompasses continuously reviewing and testing the effectiveness of the privacy policy. The privacy policy should be subject to frequent monitoring to ensure continued compliance to the standards. Consumers also have the right to be informed of a contact person or contact address where they can ask questions or register complaints regarding the privacy policy and collected data.<sup>5</sup>

Internet privacy and the collection of data are subjects of heated debate. Even before the arrival of online data collections, there was broad concern about the collection of data from marketing companies. The collection of data is not a new or unique concept. The unique capability of the Internet has made it possible to collect and disseminate collected data without the consent or knowledge of consumers.

## **2.1 Privacy Concept**

Internet privacy is autonomy. Internet privacy is the fundamental right of consumers to surf the Internet without having their privacy invaded and to be free from any external surveillance. Privacy is often thought of as a moral right or as a legal right. Justice Louis D. Brandeis gave the most famous definition of privacy, when he proclaimed privacy to be the “right to be left alone”.<sup>6</sup> But it is often more useful to perceive privacy as the interest individuals have in sustaining a personal space, free from interference by other people and organizations.<sup>7</sup>

The five Principles collectively provide consumers with control over collected data. The Principles balance consumers’ right to privacy with the need of the industry to collect data for legitimate business purposes. The industry has a stake in ensuring that consumers are content with the manner in which the industry handles collected data.<sup>8</sup>

## **2.2 Purpose of the Study**

Internet privacy is a broad subject and consumers must be prepared to protect themselves from all types of privacy invasion. The purpose of this study is to propose and demonstrate the application of a tool for measuring the level of compliance to the standards. The objective of the study is to develop a theoretical framework for measuring compliance by examining the practice statements contained within the privacy policies to provide consumers with a number that gauges the industry’s best practice to comply with the standards. Evaluating the adoption of and adherence to the standards and assigning a measurement tool showing the level of compliance will set the tone for the discussion of developing a standardized privacy policy.

Compliance is expected to increase with the progression of time. Compliance to the standards means there is a process in place that informs consumers of data collection practices. Noncompliance to the standards and inadequate collection practices can expose consumers to significant risks. The number one consequence of inadequate collection practices is identity theft. Identity theft is one of the fastest growing types of consumer fraud. In 2003, the FTC reported that 10 million consumers were victims of identity theft.<sup>9</sup> Approximately, 13% of consumers reported the theft of personal data occurred during an online transaction.<sup>10</sup> The lack of a comprehensive privacy policy has the potential to create an opportunity for the illegal use of collected data. The vast amount of data flowing through the Internet is astronomical. Everyday computer transactions reveal personal data such as a consumer's name, social security number, phone number, mailing address, e-mail address, and credit card data.<sup>11</sup> Reports and headlines concerning the lost, stolen, and compromised data from Bank America, Wachovia, Master Card, and Choice Point have heightened the fears and concerns about the protection of collected data.<sup>12</sup>

Not all collected data result in identify theft but inadequate collection practices can result in significant dangers. Consumers and the industry forget criminals are interested in personal data in order to use the data for illegal purposes. One of the best ways to build consumer confidence is to have a comprehensive privacy policy to assure consumers of adequate data collection practices with privacy protection.<sup>13</sup> The privacy policies are a self-regulatory process whereby the industry makes a promise to consumers to comply with the standards.

## **2.4 Research Questions**

This study addressed the following three questions:

1. How many firms display a privacy policy?
2. What information is provided in the privacy policy?
3. Does the privacy policy cover all of the Fair Information Principles?

The questions take into account the context within which the study is engaged and look forward to the possibilities inherent in the purpose of the study.

## **2.5 Research Hypothesis**

This study tested the following null hypothesis ( $H_0$ ) pertaining to whether the firms have gone beyond the basic requirements of compliance and are actively reviewing their privacy policies to ensure they are accurately attaining higher levels of compliance with the standards:

$H_0$ : The privacy policies are fully compliant with the Fair Information Principles.

$H_1$ : The privacy policies are not fully compliant with the Fair Information Principles.

## **III. Research Method**

This study introduces a means of measuring the level of compliance to the standards. Specifically, a PPI is proposed, not only as a measurement tool but also equips the consumer with the information necessary to evaluate privacy policies. The purpose of this chapter is to describe the research design, selection of participants, instrumentation, composite index development, and assumptions, procedures, and data analysis.

### **3.1 Research Design**

The research design presented in this chapter revolved around the three research questions and the null hypothesis. A descriptive research approach with a questionnaire survey was used. The study was modeled after the FTC studies with some revisions. Repeating prior research helps to establish the accuracy and reliability of previous studies and helps to determine if the findings are generalizable over time.<sup>14</sup> The format of the survey was a series of questions that examined the privacy policies of 200 of the *Fortune* 500 firms. The experiment resulted in dichotomous responses for which there were only two possible alternatives, *yes* or *no*. These responses were computed as a composite index score.

### **3.2 Selection of Participants**

A sample frame was generated from the 2005 *Fortune* 500 listing. To eliminate the possibility of potential bias in the results, the Excel random number generator was used to produce a random sample from the *Fortune* 500 listing. The random selection provided assurance that the sample was a representation of the population from which it was drawn. Therefore, the results have implications for generalization of the experiment back to the population. Random selection provided assurance that the variables were controlled and contributed to the validity of the study.<sup>15</sup>

Prior studies focused on commercial Web sites.<sup>16</sup> This study specifically examined a random sample from the corporate Web sites of the *Fortune* 500 firms. The firms are leaders and should have privacy policies that were synonymous with the standards and privacy protection because of their reputation for excellence. A listing of the *Fortune* 500 firms is provided in Appendix B.

### **3.3 Instrumentation**

The survey used in this study was used to examine and conduct a thorough, comprehensive, content examination of the privacy policies. The survey instrument (see Appendix A) was divided into two sections. Section One contained 16 survey questions. Prior studies examined the privacy policies as a unit analysis. In this study, the 16 questions were designed to observe each of the practice statements contained within in the privacy policies. This study is unique because the study combines several elements other researchers have studied separately.

Item 1 measured what proportion of the sample had a privacy policy displayed and observed the location of the privacy policy. Survey question 1 was used to answer research question one: How many firms display a privacy policy?

Items 2-4 measured information regarding the Notice Principle. As part of the Notice Principle, the privacy policies were examined for readability. The Notice Principle requirement states that the privacy policy should be written in plain and simple language-an easy-to-read policy. According to the U.S. Census Bureau, 75.8% of the Internet users reported some college education while less than 28.3% of the Internet users have the equivalent of high school education or less.<sup>17</sup> After the Internet population was identified, a statistical readability metric was employed to each of the privacy policies. The readability metric was used to observe if the privacy policies were written in plain and simple language and understandable by the average Internet user.

The readability metric, the Flesch Reading Ease Score (FRES), allowed an objective evaluation and comparison between the privacy policies. The FRES is a universally accepted standard metric tool for evaluating the complexity of texts. The

FRES provides an approximate score for the text's difficulty. The scores are based on a 100-point scale. The higher the score, the easier it is to understand the document.<sup>18</sup> The FRES is built into the Microsoft software package. The score is a formula based on the average number of syllables per word and words per sentence. For the purposes of this study, each privacy policy was ranked in the following rating category of identifying the educational level that would be needed to understand the privacy policy:

1. Postgraduate (0-29)
2. College (30-49)
3. High school or less (50-100)

Items 5-8 measured information regarding the Choice Principle. Items 9-10 measured information regarding the Access Principle. Items 11-12 measured information regarding the Security Principle and items 13-14 measured information regarding the Enforcement Principle. Survey questions 2-14 were used to answer research question two: What information is provided in the privacy policy? Items 15-16 were two additional elements that could be included in the index computation to make the index more thorough.

Survey question 15 examined compliance to the Children Online Privacy Protection Act, (COPPA). According to the COPPA, those in the industry who have a Web site that is directed at children and collect data from children are required by law to display a privacy policy.<sup>19</sup> The privacy policy must be fully compliant with the standards. This study observed the number of firms who do not meet the COPPA definition, but included the COPPA statement in their privacy policy.

Survey question 16 examined the privacy policies to observe whether the firm was a member of a third party certification process. The industry uses a third party certification process as an enforcement mechanism for trust, security, integrity, and accountability.<sup>20</sup> The study observed the number of firms that have taken the initiative to be associated with trust, security, integrity, and accountability by enrolling into a third party certification process. The study assessed whether the firms were signaling to consumers that their Web site was a credible Web site that could be trusted with personal data.

### **3.4 Privacy Policy Index- PPI**

In Section Two, the results of the responses to questions 1-14 were analyzed and a composite index was computed which was converted into a PPI. The PPI was used to answer research question three: Does the privacy policy cover all of the Fair Information Principles? The PPI was also used to validate the null hypothesis: The privacy policies are fully compliant with the Fair Information Principles.

The composite index is a statistic that has been computed from several weighed elements. The composite index is a “powerful tool used to identify the presence or absence of a required condition or to test the effectiveness of a proposed policy”.<sup>21</sup> In this present study, the composite index was used to identify the absence and the presence of the standards and determine the effectiveness of the industry’s privacy policies. The composite index scoring was chosen because it is deemed most suitable for this study after a check for validity.

The composite index must be “simple, information efficient, easy to understand and construct by the decision makers and the public for the purpose of policy making”.<sup>22</sup>

The development of the proposed composite index presented in this study met all of those requirements. The study demonstrates how the development of the PPI can serve as an effective tool for measuring compliance to the, the Fair Information Principles. An index score must show some relevance or usefulness. The PPI, in a statistical sense, serves as a comparative tool, providing consumers with the ability to gauge the firm's best practice to comply with the standards.<sup>23</sup>

The PPI is an independent measure, a qualitative and quantitative analysis of the privacy policies. The purpose of the PPI was simple: to provide consumers with a rating category that reflects the extent in which the industry was complying with the standards and providing adequate privacy protection. The PPI identified the level of compliance and reflected the overall performance of the industry based on the standards. The PPI was a sincere attempt to create an objective scoring system as an effective measurement tool. The data for computing the PPI were extracted from the privacy policies. The PPI is a weighted average of 14 key questions that combined provides a statistical method for accurate comparison and evaluation of the privacy policies with regards to the standards. The 14 content-validity questions were consistent with what was learned in the Literature Review. The criteria and the assessment for each element were incorporated into a weighed matrix analysis that permits a quantifiable evaluation process.

A PPI was calculated for each firm on a scale of 1 to 100, with 100 being the highest achievable score. To determine the level of compliance with the standards, a compliance rating scale for evaluating each of the five Principles was designed. The compliance rating scale was developed to access the survey results and target those

Principles that need improvement. The compliance rating scale was developed by studying published Internet privacy studies and literature. The results from the survey responses were scored and weighed so that each Principle carried an equal weight allowing for a perfect score of 20 for each of the Principles. The Principles were given equal weights because all the dimensions included in the PPI were equally important.

Each firm was assigned a rating for each of the Principles for an overall PPI that demonstrated the level of compliance to the standards. The firms were rated and ranked in descending order based on the weight of their index score. Each index score was ranked in the following compliance rating scales:

1. Fully Compliant (100)
2. Compliant (80-99)
3. Partial Compliant (51-79)
4. Non-Compliant (50 and below)

The compliance rating scales have been identified to assist consumers in understanding the PPI. Higher scores were an indication of higher compliance to the standards. A firm scoring 50 and below or less than the index average was evaluated as failing to comply with the standards. Lower scores were an indication that the firms have failed to implement the standards in their privacy policies and did not meet expectations.

### **3.5 Data Analysis**

During the week of February 5-February 11, 2006, an electronic copy of the privacy policies was obtained. Statistical tests were conducted to determine if there were significant differences between the Principles to validate the null hypothesis. Data analysis for the survey included presentation of descriptive statistics in tables, figures,

and text. The Statistical Package for Social Science (SPSS) program was used to compute the data. The findings chapter provides a statistical and descriptive presentation of each of the survey questions. The sampling error associated with this random sample survey is +/-5% at the 95% level of confidence.

### **3.6 Limitations**

The development of the PPI has two major limitations that confine the development of any index: (1) selecting the elements that make up the index and (2) assigning the proper weights to the elements. When selecting the elements that make up the index, several elements could be used in the computation that captures the various dimensions of compliance. The selection of the elements may differ depending on the type of elements used to formulate the index. The second limitation occurs when assigning the proper weights to the elements. The index encompasses the five Principles. The weight assignment to each Principle will also differ depending on the number of elements used to formulate the index.

## **IV. Findings**

### **4.1 Research Question One**

#### ***Survey Question 1***

Section One contained 16 survey questions. Survey question 1 was used to answer research question one: How many firms display a privacy policy? As a whole, 87.5% of the firms displayed a privacy policy informing consumers of data collection practices. Approximately, 12.5 % of the firms did not display a privacy policy. The vast majority of firms did follow the requirement to display a privacy policy. One firm displayed a privacy policy that consisted of legal restrictions and a disclaimer. The

privacy policy did not include any data collection statements nor did the privacy policy comply with any of the five Principles.

The description of the privacy policies are displayed in Table 1. The findings show a decrease of -6.5% ( $p < .001$ ) since 2003. The findings show a significant increase of 72.5% ( $p < .001$ ) since 1998. This marks an improvement. The evidence seems to suggest there is a significant increase in the number of firms displaying privacy policies over time. The findings were statistically significant. The number of those in the industry displaying a privacy policy since 1998 was encouraging. It is also noted that the format of each of the privacy policies differed across the different commercial Web sites. There was not a standard format. The privacy policies ranged from a one-paragraph format to a 20-page format, when printed.

**Table 1**

***Privacy Policy Descriptions***

<b>Variables</b>	<b>Frequency</b>	<b>Percent</b>	<b>95% CI*</b>
Privacy Policy ( $n = 200$ )			
Yes	175	87.5%	82.9, 92.1
No	25	12.5%	7.9, 17.1
Hyperlink from Home Page ( $n = 175$ )			
Yes	166	95%	91.6, 98.1
No	9	5%	1.9, 8.4

---

*Note.* \*CI = Confidence Interval.

Survey question 1a observed the location of the hyperlink to the privacy policies. The vast majority of the hyperlinks to the privacy policies were listed as privacy policy, privacy statement, or privacy notice. In this present study, as depicted in Table 2, 95% of the firms displayed the hyperlink to the privacy policy on the home page. The findings show a significant increase of 31% ( $p < .001$ ) since 1998. Approximately, 87% of the hyperlinks to the privacy policies were located on the bottom of the home page. Several of the hyperlinks, 8%, were located on the home page but in different locations. One firm had a hyperlink on the home page but the privacy policy did not include the firm's data collection practices. The researcher went to the firm's legal notice hyperlink and found the data collection practices under that link. Furthermore, 3% of the privacy policies were located under legal information and one of the hyperlinks were located under the firm's advertisement banner.

Approximately, 5% of the hyperlinks were not located from the home page. Several of the privacy policies were located under the following hyperlinks: under about us, terms of us, who we are, the firm's logo, and terms of agreement, whereas another privacy policy was located under a hyperlink to an entirely different Web site. In order to make sure that the consumer was aware of privacy policy, the privacy policy should be located on the home page. A privacy policy is not beneficial if the consumer is not able to locate it. A highly visible privacy policy is one that reassures consumers that the firms are concerned about the privacy of consumers. The findings show a pattern of improvement over time for those displaying a privacy policy and for those displaying the privacy policies on the home page. The findings were statistically significant.

## **4.2 Research Question Two**

### ***Survey Question 2***

Survey questions 2-16 were used to answer research question two: What information is provided in the privacy policy? The privacy policies were examined to observe whether the privacy policies were written in plain and simple language. To quantify the readability of the privacy policies, the FRES available in the Microsoft software was used. Table 2 depicts the findings of the examination. The FRES was statistically significant,  $t(174) = 33.8, p < .001$ . A college education was required to understand the privacy policies.

Of the 175 privacy policies examined, only 1% required the equivalent of a high school education or less, indicating that only 1% of the privacy policies met the guidelines for a clear and conspicuous privacy policy written in plain and simple language. Approximately, 30% of the privacy policies required the equivalent of postgraduate education. The audience reading the privacy policies mainly consists of adults with the equivalent of high school education or less.<sup>24</sup> The findings show that the privacy policies were less comprehensible to the majority of the Internet users. The results revealed that in order to understand the privacy policies, the consumer needed to have college education. The findings clearly demonstrate that the privacy policies did not meet the established guidelines of plain and simple language. The findings were consistent with the findings of Anton et al., 2003 and Jensen and Potts, 2004.<sup>25</sup>

**Table 2**

***Flesch Reading Ease Scores***

Variables	Flesch Reading Ease Score	Frequency ( <i>n</i> = 175)	Percent	95% CI*
Educational Level				
Postgraduate	0-29	53	30%	23.5, 37.1
College	30-49	121	69%	62.3, 76.0
High School or Less	50-100	1	1%	-0.55, 1.69

*Note.* \*CI = Confidence Interval.

Survey question 2 examined the privacy policies to observe whether the privacy policies included a practice statement explaining if the firm did or did not collect personal data, what data were collected, and the type of data collected. Table 3 shows the various types of personal data the firms collect. The number of those collecting various types of personal data (from 1998 to 2006) increased over time. The findings show that all firms (87.5%) collect some type of personal data from consumers. The findings remain consistent with the previous results of 92% in 1998 and 92.9% in 1999.

The firms collect a variety of personal data from consumers. The collection of the consumer's name increased from 68% in 1998 to 81.2% in 1999 to 85% in 2006 ( $p < .001$ ). The collection of the social security number increased from 3% in 1998 to 4.7% in 1999 to 13% in 2006 ( $p < .001$ ). The collection of the telephone number increased from 54% in 1998 to 82.9% in 2006 ( $p < .001$ ). These findings, showing an increase in the collection of various types of personal data over time, were statistically significant. The

findings demonstrate that a significant amount of personal data is being collected from consumers.

Ninety-seven percent of the privacy policies explained that the firm does or does not collect personal data. Approximately, 9% of the privacy policies did not list the type of data the firm collects. Although the privacy policies did not provide a complete listing of every type of data that the firm collected, consumers were informed of the type of data the firms collect and their data collection practices.

**Table 3**

***Percentage of Firms Collecting Various Types of Personal Data***

<b>Variables</b>	<b>Frequency (n = 175)</b>	<b>Percent</b>	<b>95% CI*</b>
Age/Date of Birth	17	10%	5.3, 14.1
Credit Card Number	37	21%	15.1, 27.2
Driver's License Number	7	4%	1.1, 6.9
Education	0	0%	0
E-Mail Address	146	83.4%	77.9, 88.9
Gender	10	6%	2.3, 9.2
Income	12	7%	3.1, 10.6
Mailing Address	146	83.4%	77.9, 88.9
Name	149	85%	79.9, 90.4
Occupation	9	5%	1.9, 8.4
Social Security Number	22	13%	7.7, 17.5
Telephone Number	145	82.9%	77.3, 88.4

---

*Note.* \*CI = Confidence Interval.

As shown in Table 4, many of the privacy policies included a practice statement explaining that the firm collected aggregated data. Aggregated data are statistical data that are automatically gathered at a Web site. Aggregated data allow the firm to measure how consumers use the Web site. Aggregated data consist of the Internet protocol address, number and frequency to a Web site, date, time, browse type, traffic patterns, and traffic areas.<sup>26</sup> Approximately, 30% of the privacy policies did not list the type of aggregated data that were collected. One privacy policy stated that the firm did combine personal data with aggregated data from third parties for the purposes of marketing products and services to consumers. Two firms did not collect personal data. The firms allowed consumers to browse their Web site anonymously. One of the firms only collected aggregated data in order to measure how consumers use the Web site whereas the other firm did not collect aggregated data.

If consumers were unaware of the amount of data that was collected, viewing the privacy policy validated the collection of data. The evidence seems to suggest that the collection of personal data was more prevalent among the firms than the collection of aggregated data. However, the collection of personal and aggregated data seems to be widespread among the firms.

**Table 4**

***Percentage of Firms Collecting Various Types of Aggregated Data***

<b>Variables</b>	<b>Frequency (n = 175)</b>	<b>Percent</b>	<b>95% CI*</b>
Browser	115	65.7%	58.7, 72.7
Date	113	64.6%	57.5, 71.7
Number of Visits	116	66.3%	59.3, 73.3
Operating System	118	67.4%	60.5, 74.4
Owner of Computer	9	5%	1.9, 8.4
Pages/Items Requested the Most	116	66.3%	59.3, 73.3
Preferences	115	65.7%	58.7, 72.7
Time	116	66.3%	59.3, 73.3

*Note.* \*CI = Confidence Interval.

**Survey Question 3**

Survey question 3 examined the privacy policies to observe whether the privacy policies included a practice statement explaining how the collected data were used. Consumers have a right to know for what purpose the collected data will be used. Overall, 93% of the privacy policies provided different explanations of how the collected data were used. There is evidence that the firms are making an effort to maximize fairness to inform consumers how collected data would be used.

Although the privacy policies did not provide a complete listing of how collected would be used, consumers were informed of the general purposes of collecting data. The following are some of the explanations of how collected data are, in general, used:

1. Complete purchase transactions
2. Conduct research
3. Customize advertising and Web sites
4. Identify high traffic areas
5. Inform the consumer of new products, services, promotions
6. Marketing and promotional purposes
7. Participate in online surveys
8. Record the consumer's activities/statistical analysis
9. Track the consumer through the Web site
10. Troubleshooting

**Survey Question 4**

Survey question 4 examined the privacy policies to observe whether the privacy policies included a practice statement explaining the use or non-use of collection technologies and the type of collection technologies that was used. The collection of data is accomplished by the use of several collection technologies: Cookies, Internet protocol (IP) address, and Web Beacons. In this current study, Table 5 provides a detailed breakdown of the frequency of the collection technologies the firms used.

Overall, 80% of the privacy policies included a practice statement explaining to the consumer the use or non-use of data collection technologies. Nineteen percent of the firms collected data but did not provide a practice statement explaining to consumers what type of collection technology was used to collect the data.

**Table 5**

***Percentage of Firms Using Collection Technologies***

Variables	Frequency ( <i>n</i> = 175)	Percent	95% CI*
Session Cookies	133	76%	69.7, 82.3
Persistent Cookies	136	78%	71.5, 83.9
Both	133	76%	69.7, 82.3
Internet Protocol Address	72	41%	33.9, 48.4
Internet Protocol Address and Persistent Cookies	136	76%	71.5, 83.9
Web Beacons	26	15%	9.6, 20.1
Web Beacons and Persistent Cookies	72	41%	33.9, 48.4
Pixel Tags	23	13%	8.1, 18.1
All Three	26	15%	9.6, 20.1

*Note.* \*CI = Confidence Interval.

There are two types of Cookies: Session Cookies and Persistent Cookies. The key difference between the two is the time of expiration. Session Cookies are stored in memory and are only available during an active session (while the consumer is on the Web site). The Session Cookies disappears forever as soon as consumers turn off their computers. Session Cookies do not permanently record data and are not stored on the computer hard drive of the consumer. Session Cookies expire at the end of the session.<sup>27</sup>

Persistent Cookies are stored on the hard drive of the computer and are read by the Web sites that placed the Cookie on the hard drive. The Persistent Cookie is read each time consumers visit a Web site. A Persistent Cookie will have a specific expiration date that is set by the Web site that created the Cookie. The specific expiration data could be tomorrow, next week, or 10 years from now. The Persistent Cookie will cease to function after the expiration date, or when the Cookie is overwritten with newer Cookies, or when consumers manually remove the Cookie.<sup>28</sup>

The use of Persistent Cookies to collect data received the highest rating. The examination revealed that 76% of the firms use Session Cookies, 78% of the firms use Persistent Cookies whereas 76% of the firms use both. Of these, less than 15% provided full explanation about what advantage the Cookie technology provides the consumer and what data the Cookie holds. The industry use Cookies to allow the system operator to perform necessary system maintenance and other essential system functions. The Cookie provides a detailed profile of the online activities of consumers. Privacy may be compromised if the use of Cookies is not revealed to consumers. The findings remain consistent since 1998. However, the findings show a slight decrease of -3% ( $p < .001$ ) since 2003. The findings were statistically significant.

Approximately, 41% of the privacy policies addressed the collection of data through the IP address (see Table 5). The IP address controls how messages on the Internet are broken down, sent, and reassembled.<sup>29</sup> The amount of information available about the consumer from the IP address varies greatly depending on how the consumer is connected to the Internet. The IP address is the consumer's unique identity. The firm

can combine the IP address with the identifiable data and reveal the identity of the consumer.<sup>30</sup>

The examination revealed that the firms may combine the IP address with the identifiable data. For example, one of the privacy policies proclaimed:

We collect information through technology to make our sites more interesting and useful to you. For instance, when you come to one of our sites, we collect your Internet protocol address. An Internet protocol address is often associated with the portal through which you enter the Internet, like your Internet Service Provider, your company, or your university. Standing alone, your Internet protocol address is not personally identifiable. At times, we also use Internet protocol addresses to collect information regarding the frequency with which our guests visit various parts of our site. *We may combine this information with personal identifiable data.*<sup>31</sup>

Approximately, 59% of the privacy policies did not explain to consumers the collection and use of the IP address. The collection of the IP address was included in the aggregated data and was automatically reported by the consumer's browser each time a Web page is viewed. This study observed that less than 5% of the privacy policies described its use of Cookies in combination with the aggregated data. A practice statement should have been included in all privacy policies to explain to consumers why and how the collection of the IP address was used.

Only 15% of the privacy policies explained its use or non-use of the Web Beacons (see Table 5). Of these, less than 5% provided full explanation of what advantage the Web Beacons provided consumers. Thirteen percent of the privacy policies disguised its data collection practice of Web Beacons by using unfamiliar terminology such as Pixel Tag. Pixel Tag is an alternative name for Web Beacons.

The Web Beacons are invisible codes embedded in a Web page that are only used to collect data. If consumers were not aware of the Web Beacons terminology, the

consumers would not have a clue as to the use of Web Beacons. Web Beacons are only visible through specific detection software. Any Web site that uses Web Beacons should reveal to consumers its use and its purpose. The privacy policies did not explain to consumers how to detect the use of Web Beacons. The findings show that the use of collection technologies was widespread among the firms.

**Survey Question 5**

Survey question 5 examined the privacy policies to observe whether the privacy policies included a practice statement providing choices of how collected data are used. The privacy policies were observed to ascertain whether consumers have a choice and control over the collected data through measures, such as:

1. Opt-Out Statement- Where consumers can decline to have collected data disclosed to a third party.
2. Opt-in Statement- Where the firm asks for permission before disclosing collected data to a third party.

As shown in Table 6, the examination revealed that the privacy policies did provide the consumer with limited amount of choices. The consumer choices and control were limited to opting-out of tracking and opting-out of receiving marketing/promotional programs.

Less than 27% of the privacy policies allowed consumers to opt-out of collection of data. None of the privacy policies complied with the Choice Principle with the opportunity to opt-in. The firms did not ask consumers for their permission before collecting data. However, 15% of the privacy policies stated the firm would obtain permission before sharing or selling collected data. One privacy policy stated that the

firm used a third party service provider that also collected data. The third party service provider did provide consumers with the ability to opt-out of collection of data.

The vast majority of the privacy policies stated that the consumers signify their acceptance to the collection of data and to the privacy policy when consumers use the Web site. The privacy policies further explained that if the consumer does not agree with the terms in the privacy policy, then the consumer should not use the Web site.

**Table 6**

***Percentage of Privacy Policy Choices***

<b>Variables</b>	<b>Frequency (n = 175)</b>	<b>Percent</b>	<b>95% CI*</b>
Opt-In of Disclosure to Third Party	0	0%	0
Opt-Out of Collecting Data	48	27%	20.8, 34.0
Opt-Out of Disclosure to Third Party	51	29%	22.4, 35.9
Opt-Out of Tracking	91	52%	44.6, 59.4
Opt-Out of Promotional Material	74	42%	35.0, 49.6

---

*Note.* \*CI = Confidence Interval.

Approximately, 3% of the privacy policies provided consumers with a practice statement explaining whether the firm was complying with the privacy laws of European countries. In European countries, privacy is backed by enforceable privacy protection laws.<sup>32</sup> European laws require data collectors to ask for permission before using or sharing any collected data. Under the European Privacy Laws, consumers have a legal

choice. Consumers may opt-out of disclosing, using, and sharing of collected data. The evidence seems to suggest that not enough of the firms provide consumers with the opportunity to opt-out or opt-in to the collection data.

**Survey Question 6**

Survey question 6 examined the privacy policies to observe whether the privacy policies included a practice statement explaining whether the firm does or does not disclose data to a third party. The examination revealed that approximately, 83% of the privacy policies included a practice statement explaining whether the firm does or does not disclose data to a third party. The vast majority of the privacy policies stated the firms have the right to share any data with any third party for any reason. Seventeen percent of the privacy policies did not include a practice statement explaining whether the firm did or did not disclose collected data to third parties.

An overwhelming, 95% of the privacy policies stated that the firms did not sell, rent, or lease collected data without the consumer's permission but the firms did share data with a third party such as: parent companies, affiliates, subsidiaries, entities, companies working on their behalf, contractors, consultants, agents, law enforcement agencies, or direct marketers.

The privacy policies did not provide consumers with the names of the third parties or a hyperlink to the privacy policies of the third parties. Several of the privacy policies stated the firm shared data only with *reputable* third parties. The researcher was left with the question, "What *reputable* third party"? The privacy policies did not provide consumers with the name(s) of the reputable third party. The privacy policies should have provided consumers with name(s) of the third party so consumers could

review the privacy policy of the third party. The examination observed that the sharing of collected data was done without the consent or knowledge of the consumer. The examination provided support for the privacy advocates' argument that the sharing of collected data was done without the consent or knowledge of the consumer

The examination raised several questions with no apparent answers: What are the third parties privacy policies? Are the third parties adhering to the Fair Information Principles? How are the third parties storing the collected data? How does the third party prevent the unauthorized access and disclosure of the collected data? The firms in the study have failed to provide consumers with any information pertaining to disclosing data to third parties.

One privacy policy did not provide a statement explaining what data the firm collects but did reveal that the firm discloses collected data to a third party in order to compile demographic data about consumers, sales, and traffic patterns. Another privacy policy stated that the firm did not disclose any personal data to a third party, but did disclose and sell aggregated data to a third party.

The second part of survey question 6 examined the privacy policies to observe whether the privacy policies included a practice statement explaining whether the consumer had a choice about declining to participant. The researcher was interested in determining if the privacy policies allowed consumers to opt-out of disclosure of collected data to third parties. Only 29% of the firms allowed consumers to opt-out of disclosure of collected data to third parties (see Table 6).

Through examining the privacy policies, the study revealed that the firms automatically disclosed collected data to third parties without the consent or knowledge

of consumers. The findings were consistent with studies in the Literature Review.<sup>33</sup> The evidence suggests that the majority of the firms disclose collected data to third parties and the consumers did not have a choice about declining to opt-out of disclosure of collected data to third parties.

**Survey Question 7**

Survey question 7 examined the privacy policies to observe whether the privacy policies included a practice statement providing the consumer with choices of how to opt-out of tracking. Approximately, 52% of the privacy policies included a practice statement allowing the consumer to opt-out of tracking. The privacy policies stated that to opt-out of tracking, consumers would have to reject the Cookies. The privacy policies explained to consumers how to configure the Internet browser to reject the Cookies. Forty-eight percent of the privacy policies did not provide a practice statement allowing the consumer to reject Cookies or reveal to consumers how to reject Cookies.

Several of the privacy policies included a practice statement explaining the consequences of rejecting Cookies. If consumers rejected Cookies, consumers would not be able to order services and products from the firm nor could the firm process the order or services from consumers. Even though the privacy policy explained to consumers how to reject Cookies (opt-out of tracking), tracking continued to take place. The Web sites were designed to track the movements of consumers throughout the Web site. The evidence suggests that the majority of the firms did not give consumers the opportunity to exercise their right to choose when it comes to opting-out of tracking.

***Survey Question 8***

Survey question 8 examined the privacy policies to observe whether the privacy policies included a practice statement providing the consumer with choices of how to opt-out of marketing/promotional programs. Only 42% of the privacy policies provided the choice to opt-out of marketing/promotional programs such as receiving advertisement, contests, promotional events, sweepstakes, and surveys through e-mail or postal mail. Sending consumers unwanted marketing/promotional material is a nuisance. The findings show that a substantial percentage of firms did not give consumers the opportunity to exercise their right to choose when it comes to receiving marketing/promotional material through e-mail or postal mail.

***Survey Questions 9-10***

Survey questions 9-10 examined the privacy policies to observe whether the privacy policies included a practice statement providing the consumer the opportunity to review and/or correct collected data. It was found that 53% of the firms did not give the consumer the opportunity to review and/or correct collected data or recommend changes to data they believe to be inaccurate. Only 47% of the privacy policies allowed the consumer access to the collected data. The findings show a 4% increase ( $p < .001$ ) since 1998.

Several of the firms charged consumers for a copy of the report of collected data. Furthermore, the request could only be made in writing and the privacy policy did not indicate how much the report would cost. The findings show that a substantial percentage of firms did not give consumers the opportunity to exercise their right to correct, amend, or delete inaccurate data.

**Survey Question 11**

Survey question 11 examined the privacy policies to observe whether the privacy policies included a practice statement explaining how collected data are protected and stored. In response to the increase in identity theft, those who collect data should take appropriate steps to ensure the security of collected data. The core element of security is protecting collected data from theft or misuse from employees and third parties. One security breach of data stored in databases can release sensitive data to which thieves or hackers can get access. Security is the number one threat to the privacy of the consumer.

Fifty-nine percent of the privacy policies explained to consumers the measures used to maintain the security, protection, and storage of collected data. The vast majority of the privacy policies explained that collected data were stored in a secure, private database not connected to the Internet, and the collected data were protected from loss, misuse, or alterations. The examination revealed that 14% of the privacy policies did not explain the appropriate steps that the firms take to ensure the security of collected data. One privacy policy stated that the firm did not encrypt or provide secure servers for collected data nor did the firm scramble or decode the data once the data reached its Web site. The privacy policy further explained that personal data and e-mail communication sent to the firm might not be secure.

There are significant risks associated with the storage of collected data. As a result, the Security Principle places an obligation on the firm and the industry to ensure that collected data are transmitted and stored in a secure manner. Personal data are deemed highly sensitive to consumers and consumers require high levels of protection.

The evidence seems to suggest that not enough of the firms explained to consumers how collected data are stored and protected.

**Survey Question 12**

Survey question 12 examined the privacy policies to observe whether the privacy policies included a practice statement explaining the security measures taken to ensure the security and protection of credit card data during transactions. Approximately, 59% of the privacy policies did not provide a practice statement explaining the security measures taken to ensure the security and protection of credit card data during transactions.

Only 44% of the privacy policies explained the use of Secure Socket Layer (SSL) encryption when collecting and transferring credit card data. The privacy policies explained that the credit card data were also encrypted when the data were stored in the databases of the firms. The SSL encryption protects the security of online ordering and prevents credit card data from being intercepted and read as the data are transmitted through cyberspace.

The privacy policies further explained that the consumer knows when the SSL is working properly because the symbol of an unbroken key or closed lock is displayed at the bottom of the browser window. In the address window, at the top of the browser, consumers will also see the letters “https” instead of “http” which is an indicator of a secure browser. The SSL protocol is the industry standard and used by millions of Web sites to protect and encrypt online transactions.<sup>34</sup>

Only 4% of the firms, in the sample, were members of the VeriSign security program. VeriSign is one of the most trusted certifying authorities in the world. VeriSign

is used to ensure that the browser is communicating with an authentic Web site and not an imposter. Authentication is the process of verifying the identity of a Web site. VeriSign authenticates the Web site by issuing a certificate of verification.

When consumers place an order with a firm that is a member of VeriSign, personal data and credit card data are scrambled using a SSL encryption technology before the data are transmitted over the Internet. The SSL encryption makes it hard for credit card data to be stolen or intercepted while being transferred. VeriSign securely maintains all credit card transactions of all of its members.<sup>35</sup> The findings show that a substantial percentage of the firms have not taken the initiative to explain to consumers the security measures the firms have taken to ensure the security and protection of credit card data during transactions.

### ***Survey Question 13***

Survey question 13 examined the privacy policies to observe whether the privacy policies included a practice statement explaining whom to contact for asking questions. Seventy-one percent of the privacy policies included a contact person, a contact address, telephone number, or e-mail address for asking questions or registering complaints regarding the privacy policy or collected data. The researcher was disappointed to discover that 29% of the privacy policies did not include any contact information.

Just over 3% of the privacy policies referred consumers to the firm's privacy officer to ask questions or register complaints. Several of the privacy policies provided a statement informing consumers if they had questions concerning the privacy policy to contact the firm but the privacy policy itself did not provide any contact information. One

privacy policy provided contact information for the firm's ethics department so that consumers could file a complaint if they believed the firm had not followed the posted privacy policy. Several privacy policies referred consumers to the firm's webmaster for contact information. The webmasters were individuals who managed the Web site and not individuals who could answer questions or complaints concerning the privacy policies or collected data.

Without the ability to communicate with a firm, the consumers cannot exercise their right of access, choice, or security. Contact information makes the firms accountable. The evidence suggests that the firms did not provide consumers with the opportunity to exercise their right to verify and discuss collection practices, ask questions, register complaints, or remedy problems regarding the privacy policy or collected data.

***Survey Question 14***

Survey question 14 examined the privacy policies to observe whether the privacy policies included a practice statement explaining a process of modifying and or updating the privacy policy. Compliance with the standards is not a one-time occurrence. Enforcement encompasses reviewing and testing the effectiveness of the privacy policy continuously. The firms should subject themselves to frequent monitoring of their privacy policy.

Seventy-nine percent of the privacy policies included a practice statement explaining a process of modifying or revising the privacy policy. However, the vast majority of the privacy policies did not provide an effective date or a last revision date. Using February 1, 2006 as a date of calculation (the month the electronic copy of

privacy policies were obtained), the average age of the effective date of the privacy policies was 1 year and 3 months ( $M = 725.47$ ,  $SD = 481$ ).

The sample privacy policies were not in effect during the *Privacy Online Report* in 1998. Rather, the privacy policies were written and displayed several years after the first Internet privacy study (*Privacy Online Report*) and therefore, should embody all of the provisions of the standards. Only 25% of the firms included an effective date on their privacy policies. The fact that over 75% of the privacy policies did not include an effective date is problematic.

The average age of the last revision of the privacy policies was 1 year and 1 month ( $M = 520.06$ ,  $SD = 478$ ). Only 30% of the firms included a revision date on their privacy policies. Less than 2% of the privacy policies included both an effective date and a date of the last revision. Thus, the evidence suggests that the firms are not subjecting themselves to frequent monitoring of their privacy policies to ensure continued compliance with the standards. A substantial percentage of the firms did not provide information about when the current privacy policies were created, updated, and/or what changes were made to the privacy policy.

Five percent of the privacy policies informed the consumer that the privacy policy would likely be changed and instructed consumers to check back frequently. For example, one privacy policy stated, the privacy policy was subject to change at any time and encouraged consumers to review the privacy policy regularly for any changes. The vast majority of privacy policies stated that the firm reserved the right to change, amend, or modify the privacy policies at any time at the firm's sole discretion and without any notice to consumers. Several of the privacy policies provided the consumer with

information regarding when the current privacy policy was created, updated, and listed changes that had been made within the previous 60 days. For example, several privacy policies stated that the privacy issues were changing rapidly and keeping up-to-date was not easy.

With the increase in the laws pertaining to how collected data should be managed, updating the privacy policy should be the number one priority of every firm. The firms have the right to change, modify, add, or remove portions of privacy policy at any time but any changes to the privacy policy should be posted and dated. The privacy policy should include an effective date and a revision date. Compliance with the standards, Fair Information Principles, is not a one-time occurrence. The findings show that a substantial percentage of the firms are not actively reviewing their privacy policies to ensure they are accurately reflecting the standards.

***Survey Question 15***

Survey question 15 examined the privacy policies to observe whether the privacy policies included a practice statement explaining how collected data are maintained according to the COPPA. The industry must make reasonable efforts to ensure that before data are collected from a child, a parent of the child must receive notice of the data collection practices and the parent must consent to those practices. The COPPA may set the tone for future privacy legislation for Internet privacy protection laws.

Only 2.3% of the privacy policies from the random sample were required to include a COPPA practice statement in their privacy policies. In most cases, the privacy policies required credit card verification as parental consent to use the Web site. While 97.7% of the firms in the random sample were not required to include a COPPA

statement in their privacy policies, 54.3% of the firms included the statement in their privacy policies. Of these, the privacy policies requested the parent's e-mail address in order to notify the parents to obtain permission for the children to use the Web site.

Several of the privacy policies referred consumers to the FTC's Web site for a detailed explanation of the COPPA requirements. The findings show that a substantial percentage of the firms are accurately reflecting the COPPA statement in their privacy policies.

### **Survey Question 16**

The last survey question 16, examined the privacy policies to observe whether the firm was a member of the privacy seal program. Security, integrity, and accountability also include having an oversight process. A member of a privacy seal program means there is a system of accountability--an oversight process. Those that disseminate collected data should implement a process to verify and address potential misuse of data.

Many organizations prefer third party enforcement processes as a method for achieving accountability and fostering consumer trust. Membership into a privacy seal program promotes consumer trust and confidence. However, those not enrolled in a privacy seal program must have a process in place that ensures security, integrity, and accountability that results in comparable consumer trust and confidence. Cranor, Reagle, and Ackerman<sup>36</sup> contented that a Web site with a privacy policy in conjunction with a privacy seal program greatly builds consumer confidence.

Each of the privacy policies were evaluated to ascertain how many of the firms were a member of a privacy seal program. As shown in Table 7, the examination

revealed that only 10% percent of the firms were members of a privacy seal program. One firm was a member of two privacy seal programs. Approximately, 6% of firms were members of the Better Business Bureau whereas 3% were members of TRUSTe and 1% of the firms were members of the Direct Marketing Association privacy seal programs.

**Table 7**

***Percentage of Firms Members of Privacy Seal Programs***

<b>Variables</b>	<b>Frequency (n = 175)</b>	<b>Percent</b>	<b>95% CI*</b>
Better Business Bureau	10	5.7%	2.3, 9.2
TRUSTe	6	3.4%	.7, 6.1
Direct Marketing Association	1	.06%	-.5, 1.7
No Membership	159	90.3%	86.6, 95.1

---

*Note.* \*CI = Confidence Interval.

The number of firms that were members of a privacy seal program decreased from 26% in 2003 to 9% in 2006 ( $p < .001$ ). This was disappointing news.

Approximately, 90.3% of the firms were not members of a privacy seal program. The findings show a decrease in the number of firms who were members of a privacy seal program. The findings were statistically significant, indicating that a substantial percentage of the firms are not in favor of a third party system of accountability.

### **4.3 Research Question Three**

In Section Two, the results of the responses to survey questions 1-14 were analyzed, a composite index score was computed, and converted into a PPI. The PPI was used for the following:

1. To answer research question three: Does the privacy policy cover all of the Fair Information Principles?
2. To validate the null hypothesis: The privacy policies are fully compliant with the Fair Information Principles.

#### ***PPI Application***

To determine the level of compliance with the standards (Fair Information Principles), a PPI was calculated for each firm on a scale of one to 100, with 100 being the highest achievable score. As shown in Table 8, each firm was assigned a rating for each of the Principles for an overall PPI that revealed the level of compliance to the standards. The firms were rated and ranked in descending order based on their weighted index score.

**Table 8**

***Privacy Policy Index Compliance Rating Scale***

<b>Rating</b>	<b>Description</b>
Fully Compliant (100)	Demonstrated a privacy policy that:  was reliable and covered all of the provisions of the standards, had an excellent level of compliance relating to the right to privacy and privacy protection, and applied best practices when developing, maintaining, and executing compliance to the standards.
Compliant (80-99)	was adequate and covered most of the provisions of the standards, had a good level of compliance relating to the right to privacy and privacy protection, applied some best practices when developing, maintaining, and executing compliance to the standards and needs improvement.

**Table 8 (continued)**

<b>Rating</b>	<b>Description</b>
Partial Compliant (51-79)	Demonstrated a privacy policy that:  was satisfactory and covered some but not enough of the provisions of the standards, had a fair level of compliance relating to the right to privacy and privacy protection, did not apply enough best practices when developing, maintaining, and executing compliance to the standards and needs improvement.
Non-Compliant (50 and below)	was unsatisfactory and failed to cover the provisions of the standards, the provisions were poorly implemented or ignored, had a poor level of compliance relating to significant risks to the right to privacy and privacy protection, did not apply best practices when developing, maintaining, and executing compliance to the standards, and greatly needs improvement.

---

The null hypothesis states that the mean PPI scores from the privacy policies will be equal to 95 ( $\mu = 95$ ). The average PPI mean score ( $M = 63.49$ ), ( $SD = 24.52$ ) was significantly lower than the mean score of ( $\mu = 95$ ),  $t(174) = 6.24$ . The results were statistically significant,  $p < .001$ , which resulted in rejection of the null hypothesis. Using the criteria in Table 9, the mean total score revealed that 34.9% of the privacy policies scored in the partial compliant range, indicating that the majority of the privacy policies do not cover all of the provisions of the standards and were not *fully* compliant with the standards. The majority of the privacy policies was satisfactory, covered some of the standards, showed a fair level of compliance, but did not apply enough best practices when developing, maintaining, and executing compliance to the standards.

**Table 9**

***Ranking of Firms by the Privacy Policy Index***

<b>Variables</b>	<b>PPI</b>	<b>Frequency (<math>n = 175</math>)</b>	<b>Percent*</b>
Fully Compliant	100	9	5.1%
Compliant	80-99	53	30.3%
Partial Compliant	51-79	61	34.9%
Non-Compliant	50 <	52	29.7%

---

*Note.* \* $p < .001$ .

Non-compliant was viewed from two aspects: Those who scored less than the index average and those who scored 50 and below. Approximately, 42.3% of the privacy policies scored less than the index average ( $p < .001$ ), indicating that the firms (52.6%) were complying with some of the standards. Less than 29.7% of the privacy policies scored less than 50 and below, also indicating the firms (65.2%) was complying with some of the Fair Information Principles. The findings show on average that 58.9% of the firms are complying with some of the Fair Information Principles but a substantial percentage of the privacy policies were not fully compliant with the Fair Information Principles. Fully compliant is defined as covering all of the provisions of Principles in a privacy policy as discussed in detailed on pages 6 and 7 of this study.

Only 5.1% of the privacy policies were fully compliant with the Fair Information Principles, achieving the highest score of 100. One privacy policy received the lowest score of 0. The ranges of scores were 0-100 with quite an even range. This suggests that the scoring criteria and weighing were valid measurements. Since the first report in 1998, all of the privacy policies should be fully compliant with the Fair Information Principles.

Each of the five Principles were checked for normality by descriptive statistics. There appears to be a great variation in the mean score between each Principle. Several of the firms received the highest score of 20 for each of the Principles. Table 10 summarizes the overall degree in which the firm achieved the highest score of 20 for each Principle. The break down of each Principle serves to identify the areas in which the firms may need to improve their privacy policies.

**Table 10**  
**Compliance Percentage Rating for each Principle**

Variables	Frequency ( <i>n</i> = 175)	Percent	95% CI*
Principle			
Notice	133	76%	69.7, 82.3
Choice	21	12%	7.2, 16.8
Access	83	43%	40.0, 54.8
Security	53	30%	23.5, 37.1
Enforcement	110	63%	55.7, 70.0

*Note.* \*CI = Confidence Interval.

The privacy policies achieved an average score for the Notice Principle, with a total mean score of 18.4 out of a possible 20 ( $p < .001$ ). This was a good average. Approximately, 76% of the privacy policies received the highest overall rating of 20 for the Notice Principle ( $p < .001$ ), indicating that 133 privacy policies met the guidelines for the Notice Principle. The findings show a significant increase of 22% ( $p < .001$ ) since 1998. Of all of the Principles measured, the Notice Principle scored the best. However, the findings show a substantial percentage of the firms have not complied fully or met the guidelines for the Notice Principle. The findings were statistically significant.

The firms achieved an average score for the Choice Principle, with a total mean score of 10.00 out of a possible 20 ( $p < .001$ ). This was a poor average. Approximately, 88% of the privacy policies scored less than the index average ( $p < .001$ ). Only 12% of the privacy policies achieved the highest overall rating of 20 for the Choice Principle,

indicating that 21 privacy policies met the guidelines for the Choice Principle. The findings show a significant decrease of 21% ( $p < .001$ ) since 1998. There was a great need for improvement among the firms with regards to the Choice Principle. The high number of firms scoring less than the index average is an indication that the Choice Principle is an area that needs improvement across the board. The findings show that a substantial percentage of the firms have not complied fully or met the guidelines for the Choice Principle. The findings were statistically significant.

The firms achieved an average score for the Access Principle, with a total mean score of 9.4 out of a possible 20 ( $p < .001$ ). This was a poor average. Fifty-three percent of the privacy policies scored less than the index average ( $p < .001$ ). Less than half, 43%, of the privacy policies achieved the highest overall rating of 20 for the Access Principle, indicating that 83 privacy policies met the guidelines for the Access Principle. Although the Access Principle scored less than the other Principles measured, compliance to the Access Principle shows significant growth from 9% in 1998 to 43% in 2006. However, the high number of firms scoring less than the index average is an indication that the Access Principle is an area that needs improvement across the board. The findings show that a substantial percentage of the firms have not complied fully or met the guidelines for the Access Principle. The findings were statistically significant.

The firms achieved an average score for the Security Principle, with a score of 10.3 out of a possible 20 ( $p < .001$ ). This was a poor average. Approximately, 70% of the firms scored less than the index average ( $p < .001$ ). Only 30% of the privacy policies achieved the highest overall rating of 20 for the Security Principle, indicating that 53

privacy policies met the guidelines for the Security Principle. The high number of firms scoring less than the index average is an indication the Security Principle is an area that needs improvement across the board. The findings show that a substantial percentage of the firms have not complied fully or met the guidelines for the Security Principle. The findings were statistically significant.

The firms achieved an average score for the Enforcement Principle with a total mean score of 15.00 out of a possible 20 ( $p < .01$ ). This was a good average. Approximately, 63% ( $p < .001$ ) of the privacy policies received the highest overall rating of 20 for the Enforcement Principle, indicating that 110 privacy policies met the guidelines for the Enforcement Principle. The findings show that a substantial percentage of the firms have not complied fully or met the guidelines for the Enforcement Principle. The findings were statistically significant.

An analysis was conducted to explore the relationship between the PPI score and those privacy policies with a COPPA practice statement. The analysis was conducted to determine if any patterns emerged. The total mean PPI score of those firms that are required to include a COPPA practice statement in their privacy policies were 83.75 ( $p < .001$ ). The findings indicate that the privacy policies ranked in the rating category of compliant. The findings were statistically significant. The evidence shows that the firms are complying with the COPPA.

The total mean PPI score of those firms that are not required to included a COPPA practice statement in their privacy policy but did include the COPPA statement in their privacy policies were 70.55 ( $p < .001$ ). The findings indicate that the privacy policies ranked in the rating category of partial compliant. The evidence seems to

suggest that the firms that were not required to have a COPPA statement in their privacy policies are taking proactive steps to ensure they are complying with the COPPA.

A positive, significant pattern of relationship emerged. The findings show that the firms who were required to have a COPPA statement in their privacy policies scored a PPI higher than those firms who were not required to have a COPPA statement in their privacy policies. The relationship is highly significant.

A similar analysis was conducted to explore the relationship between the PPI score and membership in a privacy seal program. The analysis was conducted to also determine if any patterns emerged. The total mean PPI score of those firms that were members of the privacy seal program was 82.33 ( $p < .001$ ). The findings indicate that the privacy policies ranked in the rating category of compliant.

The total mean PPI score of those firms that were not members of the privacy seal program was 61.72 ( $p < .001$ ). The findings indicate that the privacy policies ranked in the rating category of partial compliant. A positive, significant pattern of relationship emerged. The findings show that the firms who were members of a privacy seal program scored a PPI higher than those that were not. The relationship is highly significant.

Overall, the findings show that a substantial percentage of the firms complied with some of the Fair Information Principles in their privacy policies but the privacy policies, as a whole, did not fully comply with all of the Principles. Much more work is needed to achieve widespread compliance of the standards into a privacy policy.

#### **4.4 Discussion of Results**

As stated previously, the purpose of this study was to propose and demonstrate the application of a tool for measuring the level of compliance to the Fair Information Principles. The first research question investigated whether the firms displayed a privacy policy. The second research question investigated the contents of the privacy policies and the third research question investigated whether the privacy policies complied with all of the Fair Information Principles and assigned a PPI score to each of the privacy policies.

The findings showed a pattern emerging. There is a significant increase within the industry to display privacy policies. The increase in the number of firms displaying privacy policies may be a direct response to consumer outcry from the many Internet privacy studies, consumer concerns, and the news media reports concerning lost, stolen, and compromised data. Increased attention to Internet privacy and privacy protection has caused many in the industry to engage in strategies that build consumer confidence in data collection practices.

The firms have adopted a strategy to combat privacy fears by displaying privacy policies. At the same time, the findings reveal there is an increase in the number of firms collecting several types of personal and aggregated data. Thus, while the firms are making an effort to display a privacy policy, there has been a significant increase in the collection of data. However, displaying a privacy policy and complying with *all* of the Fair Information Principles are two different topics. Consumers want to conduct business with those firms they can trust. A privacy policy that is fully compliant with all of the Fair Information Principles is an important element of trust.

The study demonstrated that the PPI serves as an effective tool for measuring compliance to the Fair Information Principles. The survey supplied factual data on the compliance level of the privacy policies. The application of the PPI related to compliance to the Fair Information Principles shows that the contents of the privacy policies were inconsistent with the Fair Information Principles. The PPI scores revealed that the firms' privacy policies failed to cover enough of the provisions of the Fair Information Principles. The examination also revealed that privacy policies were not written in plain and simple language. The privacy policies did not have a standard format to follow, there was no standard hyperlink location, and there were no standard data collection practice statements. A standard format would provide the firms with a level playing field and allow consumers to easily determine the data sharing and collecting practices of the industry.

Although there was an increase in the number of firms with privacy policies, the privacy policies in this study were only partially compliant with the Fair Information Principles. The PPI scores revealed how extensively the firms were partially complying with the Fair Information Principles. The evidence strongly suggests that additional strategies to protect the privacy of the consumer are warranted. This includes educating the public about the importance of reviewing the privacy policies, issues surrounding privacy implications, and privacy solutions.

In this present study, another interesting finding was that the vast majority of the privacy policies stated the firms did not sell, rent, or lease collected data but the firms did share data with a third party such as: parent companies, affiliates, subsidiaries, entities, companies working on their behalf, contractors, consultants, agents, law

enforcement agencies, or direct marketers. However, the privacy policies did not provide consumers with the names of the third parties or a hyperlink to the privacy policies of the third parties, which did not demonstrate a commitment to limiting the use of collected data or provide consumers with the opportunity to exercise their right to choose.

While one might argue that there is not enough justification for privacy legislation because of the increase in the industry, the rate of growth was not accessed for those firms who were non-compliant. If the consumer had an accurate overall picture of the privacy policies compliance status, there is a greater likelihood that strategies of prevention would be implemented. The PPI scores provide an accurate overall picture of the privacy policies compliance status and identify those areas where the privacy policies need improvement. While there is a growing concern about the importance of compliance to the Fair Information Principles, the matter does have a greater urgency. The lack of privacy legislation may only result in continuing distrust of consumers in the industry and consequently harm the growth of the industry.

In addition, the low compliancy number reported in this study suggests there is a need for some type of privacy legislation. This study as well as previous studies,<sup>37</sup> indicate that effective protection cannot take place without strict enforcement of the privacy policies. Perhaps, enforcement is needed for a safe shopping environment. Such enforcement could be standard but also allow for flexibility and could ensure adequate protection of Internet privacy. Penalties might be necessary in cases where the privacy legislation is violated. The implementation of privacy legislation could ensure

the protection of Internet privacy, the industry reaches its full potential, and consumer confidence is built.<sup>38</sup>

## **V. Conclusion**

Internet privacy is not just a consumer concern. The risks associated with Internet privacy, such as identity theft, makes Internet privacy everyone's concern. Identity theft is pushing privacy issues to the forefront. Internet privacy is a complex, multi-faceted issue with no easy solution. The Internet privacy dilemma needs a solution that is flexible but also works effectively across global borders. The firms have had ample opportunity to display a privacy policy and comply fully with the Fair Information Principles. It seems that the firms view the privacy policy as an unwelcome restriction on the scope of the data that they can collect from consumers. Nevertheless, all firms, regardless of size, structure, and the amount of personal data collected and the type of collection activity engaged in, are obligated to display a privacy policy and ensure proper compliance procedures are set in place.

The PPI did show that a substantial percentage of the firms are compliant with some of the Fair Information Principles. The findings show that the majority of the privacy policies were satisfactory, covered some but not enough of the provisions of the Fair Information Principles, had a fair level of compliance relating to the right to privacy and privacy protection, did not apply enough best practices when developing, maintaining, and executing compliance to the Fair Information Principles and need improvement. This study concludes the privacy policies do not actively reflect *all* of the provisions of the Fair Information Principles. The findings highlight the pressing need to better incorporate the Fair Information Principles into the privacy policies.

Despite the findings, the Fair Information Principles are the essential components of Internet privacy. The Fair Information Principles and the privacy policies have been woven into the fabric of the privacy debate. The firms in the industry may have to pay more attention to privacy concerns in order to build and maintain a loyal consumer base because of the privacy debate. The firms are responsible for full compliance with the Fair Information Principles. Full compliance with the Fair Information Principles will create an environment of trust. To achieve full compliance, the firms must create and execute privacy policies and procedures that comply with all of the Fair Information Principles.

Steps to remedy the low PPI scores and non-compliance level, may require a comprehensive strategy that focuses on privacy legislation. The evidence seems to suggest that compliance to the Fair Information Principles alone does not adequately protect the privacy of the consumer. This research may provide empirical support for the need to implement privacy legislation to ensure enforcement of the Fair Information Principles.

Privacy policies have a significant impact on how the consumer perceives the firms. The presence of a privacy policy seems to increase the consumer's willingness to conduct online business.<sup>39</sup> The privacy policy should be a mandate and not an option because Internet privacy is a necessity. The vast majority of the privacy policies in this study need to be improved. The privacy policies are lacking in informing the consumer about basic data collection practices. This is almost certain that consumers might not do business with the firms who have failed to meet the basic requirements of complying with the Fair Information Principles. "Although security concerns are a major deterrent

to online shopping, concerns regarding the secondary use of data loom large and also discourage consumers from engaging in online relationship exchanges”.<sup>40</sup> The findings show that the PPI is a means of accessing compliance with the Fair Information Principles. The statistical findings are similar to those reported by the FTC. The low PPI scores display a very negative attitude towards Internet privacy and ignore consumer concerns when it comes to Internet privacy. The number of privacy policies, in this study, that are not fully compliant with the Fair Information Principles represent a small portion of those in the industry. It is troubling to note that on a larger scale, the number of privacy policies that are not fully compliant with the Fair Information Principles may mirror these results. All efforts must be pursued to ensure maximum compliance to the Fair Information Principles. The FTC, the consumers, the privacy advocates, and the industry must work closely together to ensure that full compliance to the Fair Information Principles is met.

### **5.1 Implications for Future Research**

The findings in this study have implications for future research. The significance of the study goes beyond its contribution to measuring compliance. The PPI is a tool with which consumers can assess compliance over time. The study set out to demonstrate that a tool for measuring compliance is not only important but also capable of monitoring those in the industry and holding the industry accountable. The PPI is not perfect but does take into account every aspect of the Fair Information Principles. The PPI focuses on the dimensions of Internet privacy that are of the utmost concern, full compliance to the Fair Information Principles.

Specific research needs to be completed to refine the PPI. The PPI has been simplified as much as possible. The survey questions and the weights used in formulating the PPI could be expanded to include those variables that have been omitted from the computation. The Literature Review suggests that other questions could be used in the PPI computation. Since all five Principles are inextricably linked, it is essential to select questions for the PPI computation that objectively embody and capture the various dimensions of the Fair Information Principles. The research is the first attempt to consolidate in one index, the various dimensions of the Fair Information Principles. The selection of questions and weights that make up the PPI may need revision. Nevertheless, with continued improvement and refinement, the PPI will grow in impact and validity. The researcher expects the PPI to evolve over time. The PPI will continue to evolve as future researchers learn from experience. Perhaps someday, the PPI will be just as important as the privacy policy itself.

## **5.2 Recommendations**

The results of this analysis was limited to a study of 200 privacy policies and not designed to be an exhaustive examination of the Fair Information Principles. The results of this research can be generalized. The Privacy Policy Index is an effective tool for measuring the level of compliance to the Fair Information Principles. Consumers may have a good reason to be concerned about their privacy while online.

Three recommendations are offered to the industry to serve as guidelines for those in the industry seeking to improve their level of compliance to the Fair Information Principles. The following are requirements:

1. A third party information practice statement that explains third party collection, sharing, and security practices.
2. A process by which consumers could opt-out of disclosure of data to third parties.
3. A privacy policy with a standard format for all in the industry to follow.

This study shows that the privacy policies do not actively reflect *all* of the provisions of the Fair Information Principles. A platform for privacy protection may have to be applied within the context of forcible privacy legislation. If the privacy policies are to be effective, there is a need for privacy legislation that ensures that the practice statements in the privacy policies reflects actual practice. Privacy legislation can guarantee consumers a minimal amount of privacy protection across the board. What is essential are rating systems and services, such as the tool proposed in this dissertation.

Surveys have revealed that consumers will conduct business with the firms that safeguard the privacy of consumers. Consumer trust does make a difference in the industry. The industry is dependent on consumer confidence. There must be a balance between legitimate data collection needs and consumer privacy. A standardized privacy policy and a tool for measuring compliance help consumers understand what data are collected and why. Privacy education can increase the awareness of consumer rights, the obligations of the industry, and the role the industry must play in protecting the privacy of consumers.

***The right to privacy is a fundamental right and if consumers  
give up that right that right may be gone forever.***

## **Endnotes**

---

<sup>1</sup>Smith, M. (2004). *Internet privacy overview and pending legislation: Report for congress* (RL31408). Congressional Research Service, The Library of Congress, Washington, DC.

<sup>2</sup>Brown, M., & Muchira, R. (2004). Investigating the relationship between privacy concern and online purchase. *Journal of Electronic Commerce Research*, 5(1), 62-70.

<sup>3</sup>Microsoft (2005). *A guide to privacy at Microsoft*. Retrieved February 15, 2006 from Microsoft Web site: <http://download.microsoft.com/download/c/0/d/c0ddb7d5-287d-4b65-88d4-c0ee1b94adbb/privacyguide.doc>

<sup>4</sup>Federal Trade Commission (1998). *Privacy online: A report to congress*. Washington, DC: Federal Trade Commission, 7-11.

Federal Trade Commission (1999). *Self-regulation and privacy online: A report to congress*. Washington, DC: Federal Trade Commission.

Peslak, A. (2005). Internet privacy policies: A review and survey of the *Fortune* 50. *Information Resources Management Journal*, 18(1), 29-41.

<sup>5</sup>Federal Trade Commission, 1998.

<sup>6</sup>Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193-220.

<sup>7</sup>Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Association for Computing Machinery*, 42(2), 60-67.

<sup>8</sup>Culnan, M., & Armstrong, P. (1999). Information privacy concerns, procedural fairness and impersonal trust: An empirical investigation. *Organization Science*, 10(1), 104-115.

<sup>9</sup>Federal Trade Commission (2003). *Identity theft survey report*. Washington, DC: Federal Trade Commission, 4.

<sup>10</sup>*Ibid*, 31.

<sup>11</sup>Federal Trade Commission, 1998.

<sup>12</sup>Levy, S., & Stone, B. (2005, July). Grand theft identity. *Newsweek Magazine*, 38-47.

<sup>13</sup>Brown, & Muchira, 2004.

Furnell, S., & Karweni, T. (1999). Security implications of electronic commerce: A survey of users and businesses. *Internet Research*, 9(5), 372-382.

<sup>14</sup>Milne, G., & Culnan, M. (2002). Using the content of online privacy notices to inform public policy. *The Information Society*, 18(5), 345-359.

<sup>15</sup>Christensen, L. (2004). *Experimental methodology* (9<sup>th</sup> ed.). Boston: Pearson, 234-240.

<sup>16</sup>Peslak, 2005.

<sup>17</sup>U.S. Census Bureau (2005). *Computer and Internet use in the United States*. Washington, DC: US Census Bureau.

<sup>18</sup>Anton, A., Earp, J., Vail, M., Jain, N., Gheen, C., & Frink, J. (2006). An analysis of web site privacy policy evolution in the presence of HIPPA. *IEEE Security & Privacy*, North Carolina State University, Technical Report #TR-2001-21;

Crosier, K. (2004). How effectively do marketing journals transfer useful learning from scholars to practitioners? *Marketing Intelligence & Planning*, 22(5), 540-545.

<sup>19</sup>Federal Trade Commission (2000a). *How to protect kids' privacy online*. Washington, DC: Federal Trade Commission.

<sup>20</sup>Peslak, 2005.

<sup>21</sup>Kumar, R., Manning, E., & Murch, B. (1993). *The challenge of sustainability*. Ontario, Canada: Center for Sustainable Future at the Foundation for International Training, 113.

<sup>22</sup>Ibid, 118.

<sup>23</sup>Kumar, Manning, & Murch, 1993.

<sup>24</sup>U.S. Census Bureau, 2005.

<sup>25</sup>Anton et al., 2006.

Jensen, C., & Potts, C. (2004). *Privacy policies as decision-making tools: An evaluation of online privacy notices*. Atlanta, GA: Georgia Institute of Technology, College of Computing.

<sup>26</sup>Smith, R. (2003). *Online profiling a consumer's perspective*. Washington, DC: Federal Trade Commission, 3.

<sup>27</sup>Webopedia (2006b). Online computer dictionary for computer and Internet terms and definitions. "Session Cookie." Retrieved January 10, 2006 from Webopedia Web site: [http://www.webopedia.com/TERM/S/session\\_cookie.html](http://www.webopedia.com/TERM/S/session_cookie.html)

<sup>28</sup>Webopedia (2006a). Online computer dictionary for computer and Internet terms and definitions. "Persistent Cookie." Retrieved January 10, 2006 from Webopedia Web site: [http://www.webopedia.com/TERM/P/persistent\\_cookie.html](http://www.webopedia.com/TERM/P/persistent_cookie.html)

<sup>29</sup> Smith, 2003, 3.

<sup>30</sup> Ibid, 3.

<sup>31</sup>Walt Disney (2003). *Privacy policy*. Retrieved February 9, 2006 from Walt Disney Web site: [http://disney.go.com/corporate/privacy/pp\\_wdig.html](http://disney.go.com/corporate/privacy/pp_wdig.html)

<sup>32</sup>Bygrave, L. (2004). Privacy protection in a global context: A comparative overview. *Scandinavian Studies in Law*, 47, 319-348.

<sup>33</sup>Cranor, L., Reagle, J., & Ackerman, M. (1999). Beyond concern: Understanding Net user's attitude about online privacy. *AT & T Labs Research Technical Report*, 1-19.

Culnan, 1999, *Georgetown Internet privacy policy survey: Report to the federal trade commission*. Washington, DC: Federal Trade Commission.

Earp, J., Anton, A., Smith, L., & Stufflebeam, W. (2005). Examining Internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management*, 52(2), 227-237.

Federal Trade Commission (1998).

Federal Trade Commission, 1999.

Federal Trade Commission (2000b). *Fair information practices in the electronic marketplace: A report to congress*. Washington, DC: Federal Trade Commission.

Hildebrand, M., & Klosek, M. (2005). Recent security breaches highlight the important role of data security in privacy compliance programs. *Intellectual Property and Technology Law Journal*, 17(5), 20-24.

Hoffman, D., Novak, T., & Peralta, M. (1999). Building consumer trust online environments: The case for information privacy. *Communications of the Association for Computing Machinery*, 42(4), 80-85.

Milne, G., Rohm, A., & Bahl, S. (2004). Consumer's protection of online privacy and identity. *The Journal of Consumer Affairs*, 38(2), 217-232.

Peslak, 2005.

<sup>34</sup>Webopedia, 2006a.

<sup>35</sup>VeriSign (2004). *The number one sign of trust on the Internet*. Retrieved March 12, 2006 from VeriSign Web site: <http://www.verisign.com/static/013506.pdf>

<sup>36</sup>Cranor, Reagle, & Ackerman, 1999.

<sup>37</sup>Culnan, 1999;

Federal Trade Commission, 1998.

Hildebrand, & Klosek, 2005.

Hoffman, Novak, & Peralta, 1999.

<sup>38</sup>Federal Trade Commission, 2000b.

<sup>39</sup>Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, 19(1), 27-41.

<sup>40</sup>Hoffman, Novak, & Peralta, 1999.

## **Appendix A: Survey Questions**

## PART I: PRIVACY POLICY

### 1. Does the firm display a privacy policy?

Yes

No

### 1a. Where is the hyperlink to the privacy policy located?

Bottom of Home Page

Top of Home Page

Middle of Home Page

Right Hand Side of Home Page

Left Hand Side of Home Page

Under Advertisement Banner

Under Legal Information

Other/Different Hyperlink

## PART II. CONTENTS OF THE PRIVACY POLICY

### PRINCIPLE 1: NOTICE

### 2. Does the privacy policy provide a practice statement explaining if the firm does or does not collect any personal data?\*

Yes

No

### 2a. Does the privacy policy provide a practice statement explaining what data the firm collects?\*

Yes

No

**2b. What type of personal data does the firm collect?**

Age or Date of Birth

Credit Card

Drivers License

Education

E-mail Address

Gender

Income

Mailing Address

Name

Occupation

Social Security Number

Telephone Number

**2c. What type of aggregated data does the firm collect?**

Browser Type

Date

Number Visits

Operating system

Owner of Computer

Pages & Items Requested the Most

Preferences

Time

**3. Does the privacy policy provides a practice statement explaining the use of collected data?\***

Yes

No

**4. Does the privacy policy provide a practice statement explaining the use or non-use of collection technology?\***

Yes

No

**4a. What type of collection technology does the firm use for collecting data?**

Cookies

Persistent Cookies

Session Cookies

Internet Protocol Address

Web Beacons/Web Bugs and/or

Pixel Tags

PRINCIPLE 2: CHOICE

**5. Does the privacy policy provide a practice statement giving choices of how collected data are used?\***

Yes

No

**6. Does the privacy policy provide a practice statement explaining whether the firm does or does not disclose data to a third party?\***

Yes

No

**6a. Does the privacy policy provide a practice statement giving choices of how to opt-out of disclosing data to a third party?**

Yes

No

**7. Does the privacy policy provide a practice statement giving choices of how to opt-out of tracking?\***

Yes

No

**8. Does the privacy policy provide a practice statement giving choices of how to opt-out of receiving marketing/promotional programs?\***

Yes

No

### PRINCIPLE 3: ACCESS

**9. Does the privacy policy provide a practice statement explaining how to review collected data?\***

Yes

No

**10. Does the privacy policy provide a practice statement explaining how to correct collected data?\***

Yes

No

### PRINCIPLE 4: SECURITY

**11. Does the privacy policy provide a practice statement explaining how collected data are protected?\***

Yes

No

**12. Does the privacy policy provide a practice statement explaining the security measures taken to ensure the security and protection of credit card data during transactions?\***

Yes

No

PRINCIPLE 5: ENFORCEMENT

**13. Does the privacy policy provide a practice statement explaining whom to contact for asking questions?\***

Yes

No

**14. Does the privacy policy provide a practice statement explaining a process for modifying and updating the privacy policy?\***

Yes

No

*Note: \*Used in the Privacy Policy Index computation.*

ADDITIONAL ELEMENTS

**15. Does the privacy policy provide a practice statement explaining how collected data are managed according to the Children Online Privacy Protection Act?**

Yes

No

**16. Does the firm belong to a privacy seal program?**

Yes

No

**Appendix B: Survey Sample**

2005 Rank	FIRM	2005 Rank	FIRM
1	WAL-MART STORES	46	SAFEWAY
2	EXXON MOBIL	47	LOCKHEED MARTIN
3	GENERAL MOTORS	48	MEDCO-HEALTH SOLUTIONS
4	FORD MOTOR	49	MOTOROLA
5	GENERAL ELECTRIC	50	INTEL
6	CHEVRON TEXACO	51	ALLSTATE
7	CONOCO- PHILLIPS	52	WELLS FARGO
8	CITIGROUP	53	MERRILL LYNCH
9	AMERICAN INTERNATIONAL GROUP	54	WALT DISNEY
10	IBM	55	CVS
11	HEWLETT-PACKARD	56	AT&T
12	BERKSHIRE HATHAWAY	57	CATERPILLAR
13	HOME DEPOT	58	NORTHROP GRUMMAN
14	VERIZON COMMUNICATIONS	59	GOLDMAN SACHS GROUP
15	MCKESSON	60	SYSCO
16	CARDINAL HEALTH	61	PEPSICO
17	ALTRIA GROUP	62	AMERICAN EXPRESS
18	BANK OF AMERICA CORP.	63	DELPHI
19	STATE FARM INSURANCE	64	PRUDENTIAL FINANCIAL
20	J.P. MORGAN CHASE & CO.	65	WACHOVIA
21	KROGER	66	DUPONT
22	VALERO ENERGY	67	SPRINT
23	AMERISOURCEBERGEN	68	NEW YORK LIFE
24	PFIZER	69	VIACOM
25	BOEING	70	INTERNATIONAL PAPER
26	PROCTER & GAMBLE	71	JOHNSON CONTROLS
27	TARGET	72	TYSON FOODS
28	DELL	73	CAREMARK
29	COSTCO WHOLESALE	74	J.C. PENNEY
30	JOHNSON & JOHNSON	75	HONEYWELL
31	MARATHON OIL	76	INGRAM MICRO
32	TIME WARNER	77	BEST BUY
33	SBC COMMUNICATIONS	78	FEDEX
34	DOW CHEMICAL	79	ALCOA
35	ALBERTSON'S	80	HCA
36	MORGAN STANLEY	81	TIAA-CREF
37	METLIFE	82	SUNOCO
			MASS. MUTUAL LIFE
38	WALGREEN	83	INSURANCE
39	UNITED TECHNOLOGIES	84	MERCK
40	UNITED HEALTH GROUP	85	ST. PAUL TRAVELERS
41	MICROSOFT	86	DUKE ENERGY
42	UPS	87	BELLSOUTH
43	LOWE'S	88	HARTFORD FINANCIAL
44	ARCHER DANIELS MIDLAND	89	WEYER HAEUSER
45	SEARS ROEBUCK	90	MCI

2005 Rank	FIRM	2005 Rank	FIRM
91	CISCO SYSTEMS	136	PREMCO
92	COCA-COLA COMPANY	137	EXPRESS SCRIPTS
93	BRISTOL-MYERS SQUIBB	138	DELTA
94	LEHMAN BROTHERS HOLDINGS	139	ANHEUSER-BUSCH
95	ELECTRONIC DATA SYSTEMS	140	MANPOWER
96	PLAINS ALL AMERICAN PIPELINE	141	TJX
97	WELLPOINT	142	COMPUTER SCIENCES
98	NEWS CORP	143	U.S. BANCORP
99	NATIONWIDE	144	LOEWS
100	ABBOTT LABORATORIES	145	EXELON
101	HALLIBURTON	146	STAPLES
102	COMCAST	147	MAY DEPARTMENT STORES
			AMERICAN ELECTRIC
103	RAYTHEON	148	POWER
104	SUPERVALU	149	UNITED STATES STEEL
105	3M	150	COUNTRYWIDE FINANCIAL
106	DEERE	151	DOMINION RESOURCES
107	CENDANT	152	ELI LILLY
108	AETNA	153	EASTMAN KODAK
109	GEORGIA-PACIFIC	154	QWEST
110	TECH DATA	155	PROGRESSIVE
	LIBERTY MUTUAL INSURANCE		
111	GROUP	156	OFFICE DEPOT
112	AUTONATION	157	NEXTEL COMMUNICATIONS
113	KMART HOLDING	158	AFFLAC
114	SARA LEE	159	OFFICEMAX
115	GENERAL DYNAMICS	160	WHIRLPOOL
116	MCDONALD'S	161	CHUBB
117	PUBLIX SUPER MARKETS	162	HUMANA
118	VISTEON	163	FIRST ENERGY
119	AMR	164	SOLETRON
120	GOODYEAR TIRE	165	WILLIAMS
121	CONAGRA	166	TEXAS INSTRUMENTS
122	CIGNA	167	CONSTELLATION ENERGY
123	COCA-COLA ENTERPRISE	168	WASTE MANAGEMENT
124	NORTHWESTERN MUTUAL	169	TENET HEALTHCARE
125	WYETH	170	MASCO
126	AMERADA HESS	171	MBNA
			PACIFICARE HEALTH
127	LEAR	172	SYSTEMS
128	RITE AID	173	NIKE
129	UAL	174	UNION PACIFIC
130	GAP	175	SANMINA-SCI
131	WASHINGTON MUTUAL	176	MARSH & MCLENNAN
132	XEROX	177	TESORO
			TRW AUTOMOTIVE
133	FEDERATED DEPARTMENT STORES	178	HOLDINGS
134	EMERSON ELECTRIC	179	DIRECTV GROUP
135	KIMBERLY-CLARK	180	SOUTHERN

2005 Rank	FIRM	2005 Rank	FIRM
181	PULTE HOMES	226	AES
182	WINN-DIXIE STORES	227	EATON
183	ILLINOIS TOOL WORKS	228	CONSOLIDATED EDISON
184	KOHL'S	229	PROGRESS ENERGY
185	HEALTH NET	230	OMNICOM GROUP
186	OCCIDENTAL PETROLEUM	231	CIRCUIT CITY STORES
187	EDISON INTERNATIONAL	232	CONTINENTAL AIRLINES
188	PACCAR	233	NAVISTAR INTERNATIONAL
189	NUCOR	234	KELLOGG
190	NORTHWEST AIRLINES	235	SEMPRA ENERGY
191	USAA	236	PPG INDUSTRIES
192	TOYS "R" US	237	BAXTER INTERNATIONAL
193	TRANSMONTAIGNE	238	AMERICAN STANDARD CLEAR CHANNEL COMMUNICATIONS
194	SUN MICROSYSTEMS	239	COMMUNICATIONS
195	TXU	240	LIMITED BRANDS
196	PG&E CORP.	241	FLUOR
197	GENERAL MILLS	242	CALPINE
198	CHS PUBLIC SERVICE ENTERPRISE GROUP	243	DEVON ENERGY
199	GROUP	244	ARVINMERITOR
200	BRUNSWICK NO SANTA FE	245	GENUINE PARTS
201	DANA	246	MEDTRONIC
202	PEPSI BOTTLING	247	LUCENT TECHNOLOGIES
203	D.R. HORTON	248	INTERNATIONAL STEEL GROUP
204	CENTEX	249	YUM BRANDS
205	DEAN FOODS	250	RELIANT ENERGY
206	CAPITAL ONE FINANCIAL	251	GUARDIAN LIFE INSURANCE
207	ARROW ELECTRONICS	252	ASHLAND
208	UNUMPROVIDENT	253	PRINCIPAL FINANCIAL
209	CENTER POINT ENERGY	254	LIBERTY MEDIA
210	COLGATE-PALMOLIVE	255	MURPHY OIL
211	NATIONAL CITY CORP.	256	XCEL ENERGY
212	AMGEN	257	CUMMINS
213	FPL GROUP	258	BEAR STEARNS
214	LENNAR	258	UNOCAL
215	GILLETTE	259	H.J. HEINZ
216	TEXTRON	260	ENTERPRISE PRODUCTS
217	AVNET	261	FIDELITY NATIONAL FINANCIAL
218	AON	262	SMURFIT-STONE CONTAINER
219	ARAMARK	263	APPLE COMPUTER
220	ORACLE	264	SCHERING-PLOUGH
221	ENTERGY	265	ALLTEL
222	SMITHFIELD FOODS	266	EMC
223	FIRST DATA	267	MEADWESTVACO
224	MARRIOTT INTERNATIONAL	269	CSX
225	UNITED AUTO GROUP	270	APPLIED MATERIALS

2005 Rank	FIRM	2005 Rank	FIRM
271	KINDER MORGAN ENERGY	316	EASTMAN CHEMICAL
272	SONIC AUTOMOTIVE	317	FIFTH THIRD BANCORP
273	SUNTRUST BANKS	318	SOUTHWEST AIRLINES THRIVENT FINANCIAL FOR
274	DILLARD'S	319	LUTHERANS
275	R.R. DONNELLEY & SONS	320	SAKS
276	SAIC	321	REYNOLDS AMERICAN
277	AUTOMATIC DATA PROCESSING	322	COX COMMUNICATIONS PNC FINANCIAL SERVICES
278	AVON PRODUCTS	323	GROUP
279	LAND O'LAKES	324	JABIL CIRCUIT
280	DOLLAR GENERAL	325	IAC/INTERACTIVE
281	AIR PRODUCTS & CHEMICALS	326	FEDERAL-MOGUL
282	ASSURANT	327	DYNEGY
283	GANNETT	328	PERFORMANCE FOOD GROUP
284	BJ'S WHOLESALE CLUB .	329	AUTOLIV
285	SAFECO	330	BAKER HUGHES
286	NORFOLK SOUTHERN	331	SHERWIN-WILLIAMS
287	ROHM & HAAS	332	INTERPUBLIC GROUP
288	PEPCO HOLDINGS	333	ANADARKO PETROLEUM
289	CROWN HOLDINGS	334	VF
290	AGILENT TECHNOLOGIES	335	BARNES & NOBLE
291	ECHOSTAR COMMUNICATIONS	336	ONEOK
292	OWENS-ILLINOIS	337	NCR
293	BANK OF NEW YORK CO.	338	LYONDELL CHEMICAL
294	NORDSTROM	339	CNF
295	US AIRWAYS GROUP	340	MOHAWK INDUSTRIES
296	DTE ENERGY	341	STATE STREET CORP.
297	CAMPBELL SOUP	342	WELLCHOICE
298	PARKER HANNIFIN	343	UNISYS
299	PHELPS DODGE	344	PPL
300	KB HOME	345	SPX
301	FORTUNE BRANDS	346	ESTEE LAUDER
302	KEYSPAN	347	CDW
303	AMAZON.COM	348	TRIBUNE
304	NEWELL RUBBERMAID	349	OWENS CORNING
305	L-3 COMMUNICATIONS	350	AUTOZONE
306	DANAHER	351	WORLD FUEL SERVICES
307	YELLOW ROADWAY	352	BOSTON SCIENTIFIC
308	ITT INDUSTRIES	353	BURLINGTON RESOURCES
309	FIRST AMERICAN CORP.	354	DOVER
310	NORTHEAST UTILITIES	355	KEYCORP
311	NISOURCE	356	CMS ENERGY
312	BB&T CORP.	357	MONSANTO
313	AMERICAN FAMILY INSURANCE	358	ASBURY AUTOMOTIVE GROUP
314	EL PASO	359	BLACK & DECKER
315	PRAXAIR	360	BALL

2005 Rank	FIRM	2005 Rank	FIRM
361	GROUP 1 AUTOMOTIVE	406	EMCOR GROUP
362	ALLIED WASTE INDUSTRIES	407	AUTO-OWNERS INSURANCE
363	LINCOLN NATIONAL	408	GOODRICH
364	PILGRIM'S PRIDE	409	BRINK'S
365	FOOT LOCKER	410	MAYTAG
366	AVERY DENNISON	411	CHARLES SCHWAB
367	APACHE	412	CINERGY
368	HARLEY-DAVIDSON	413	CIT GROUP
			FISHER SCIENTIFIC
369	DOLE FOOD	414	INTERNATIONAL
370	LEXMARK INTERNATIONAL	415	IKON OFFICE SOLUTIONS
371	COVENTRY HEALTH CARE	416	JONES APPAREL GROUP
372	STARBUCKS	417	TEREX
373	FAMILY DOLLAR STORES	418	LIZ CLAIBORNE
374	AGCO	419	LAIDLAW INTERNATIONAL
375	MCGRAW-HILL	420	REGIONS FINANCIAL
376	AK STEEL	421	LONGS DRUG STORES
377	BRUNSWICK	422	CARMAX
378	SLM	423	JACOBS ENGINEERING GROUP
379	KERR-MCGEE	424	MIRANT
380	AMEREN	425	ERIE INSURANCE GROUP
381	RYDER SYSTEM	426	TRIAD HOSPITALS
382	QUEST DIAGNOSTICS	427	OWENS & MINOR
383	MATTEL	428	NEWMONT MINING
384	LEGGETT & PLATT	429	ROCKWELL AUTOMATION
385	W.W.GRAINGER	430	TIMKEN
386	DARDEN RESTAURANTS	431	W.R. BERKLEY
387	ADVANCED MICRO DEVICES	432	YORK INTERNATIONAL
388	BECTONDICKINSON	433	USG
389	KELLY SERVICES	434	BED BATH & BEYOND
390	CHARTER COMMUNICATIONS	435	GOLDEN WEST FINANCIAL
391	MELLON FINANCIAL CORP.	436	HERSHEY FOODS
392	PITNEY BOWES	437	HUGHES SUPPLY
393	WPS RESOURCES	438	SMITH INTERNATIONAL
394	CABLEVISION SYSTEMS	439	MICRON TECHNOLOGY
395	PACIFIC LIFE	440	STARWOOD HOTELS & RESORTS
396	HARRAH'S ENTERTAINMENT	441	BIG LOTS
397	OGE ENERGY	442	C.H. ROBINSON WORLDWIDE
398	QUALCOMM	443	CONSECO
399	RADIOSHACK	444	NVR
400	ENERGY EAST	445	CLOROX
401	CAESARS ENTERTAINMENT	446	NTL
402	HORMEL FOODS	447	MOLSON COORS BREWING
403	ROUNDY'S	448	ENBRIDGE ENERGY PARTNERS
404	COMMERCIAL METALS	449	MGM MIRAGE
405	TEMPLE-INLAND	450	STRYKER

2005 Rank	FIRM	2005 Rank	FIRM
451	AVAYA	476	NASH FINCH
452	ROSS STORES	477	TOLL BROTHERS
453	TENNECO AUTOMOTIVE	478	SCANA
454	H&R BLOCK	479	WHOLE FOODS MARKET
455	ECOLAB	480	CORNING
456	ENGELHARD	481	SEALED AIR
457	HOVNANIAN ENTERPRISES	482	MAXTOR
458	UNIVERSAL HEALTH SERVICES	483	REEBOK INTERNATIONAL
459	OMNICARE	484	UGI
460	AFFILIATED COMPUTER SERVICES	485	GUIDANT
461	JEFFERSON-PILOT	486	HOST MARRIOTT
462	GRAYBAR ELECTRIC	487	ADVANCE AUTO PARTS
463	MUTUAL OF OMAHA INSURANCE	488	SERVICE MASTER
464	LEVI STRAUSS	489	WESCO INTERNATIONAL
			TELEPHONE & DATA
465	HENRY SCHEIN	490	SYSTEMS
466	MDC HOLDINGS	491	LEVEL 3 COMMUNICATIONS
467	PATHMARK STORES	492	BRINKER INTERNATIONAL
468	UNITED STATIONERS	493	STATER BROS. HOLDINGS
			WESTERN & SOUTHERN
469	RYLAND GROUP	494	MUTUAL
470	COOPER TIRE & RUBBER	495	GATEWAY
471	WISCONSIN ENERGY	496	WM. WRIGLEY JR.
472	AMERICAN FINANCIAL GROUP	497	PEABODY ENERGY
473	BEAZER HOMES USA	498	WENDY'S INTERNATIONAL
474	COLLINS & AIKMAN	499	KINDRED HEALTHCARE
475	BORDERS GROUP	500	CINCINNATI FINANCIAL

Note. Adapted from "Largest U.S. Corporations," 2005, *Fortune*, 151(8), p. F1.