# THE LARES INSTITUTE

***The Demographics of Privacy—A Blueprint for Understanding Consumer Perceptions and Behavior.***

***September, 2011.***

## TABLE OF CONTENTS

## I. Introduction

Privacy and information security is a fundamental business issue for companies, and as the most recent high-profile data breaches demonstrate, privacy mishaps can have a significant business impact, as well as lead to regulatory enforcement. Last year, the Federal Trade Commission released a report, "Protecting Consumer Privacy in an Era of Rapid Change: A proposed Framework for Businesses and Policymakers", in which the FTC suggested voluntary improvements to privacy practices. As noted by the opening sentences of the report:

> In today's digital economy, consumer information is more important than ever. Companies are using this information in innovative ways to provide consumers with new and better products and services. Although many of these companies manage consumer information responsibly, some appear to treat it in an irresponsible or even reckless manner. And while recent announcements of privacy innovations by a range of companies are encouraging, many companies – both online and offline – do not adequately address consumer privacy interests.[1]

This report had several recommendations for companies, including two of particular import—the adoption of "*Privacy by Design*" and providing consumers with greater choice regarding privacy.[2] This recommendation followed the landmark unanimous adoption of a resolution

[1] Protecting Consumer Privacy in an Era of Rapid Change: A proposed Framework for Businesses and Policymakers, (December 2010). The issues were further defined as follows: "Stakeholders emphasized the need to improve transparency, simplify the ability of consumers to exercise choices about how their information is collected and used, and ensure that businesses take privacy-protective measures as they develop and implement systems. At the same time, commenters and participants urged regulators to be cautious about restricting the exchange and use of consumer data in order to preserve the substantial consumer benefits made possible through the flow of information. Participants noted, for example, that the acquisition, exchange, and use of consumer data not only helps to fund a variety of personalized content and services, but also allows businesses to innovate and develop new products and services that offer consumers convenience and cost savings."

[2] "First, companies should adopt a "privacy by design" approach by building privacy protections into their everyday business practices. Such protections include providing reasonable security for consumer data, collecting only the data needed for a specific business purpose, retaining data only as long as necessary to fulfill that purpose, safely disposing of data no longer being used, and implementing reasonable procedures to promote data accuracy. Companies also should implement and enforce procedurally sound privacy practices throughout their organizations, including, for instance, assigning personnel to oversee privacy issues, training employees on privacy issues, and conducting privacy reviews when developing new products and services. Such concepts are not new, but the time has come for industry to implement them systematically. Implementation can be scaled to each company's business operations. Companies that collect and use small amounts of non-sensitive consumer data should not have to devote the same level of resources to implementing privacy programs as companies that collect vast amounts of consumer data, collect data of a sensitive nature, or engage in the business of selling consumer data.

Second, Commission staff proposes that companies provide choices to consumers about their data practices in a simpler, more streamlined way than has been used in the past. Under this approach, consumer choice would not be necessary for a limited set of "commonly accepted" data practices, thus allowing clearer, more meaningful choice with respect to practices of greater concern. This component of the proposed framework reflects the concept that it

regarding PbD by the 32nd International Conference of Data Protection and Privacy Commissioners.[3]

The voluntary adoption of PbD offers companies an important solution to certain privacy concerns, and it is a well-documented approach to privacy which has the objectives of "…ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage…"[4] These objectives are implemented by 7 Foundational Principles, including:

> The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.[5]

Thus, in addition to permitting personal control of information, PbD explicitly recognizes that improved privacy practices can create a competitive advantage for businesses, *but this competitive advantage can only be realized if the changes businesses make as they implement PbD are perceived by consumers as adding value*.

In order to implement PbD in a way that maximizes its utility as a tool to drive best practices, research needs to be done to integrate consumer attitudes and behaviors into privacy designs. This research, if completed, would permit companies to design privacy in a way to permit consumers to gain control of their information, and permit companies to better anticipate and prevent privacy issues before they happen. In short—research needs to be done to create a blueprint for PbD.

---

is reasonable for companies to engage in certain commonly accepted practices – namely, product and service fulfillment, internal operations such as improving services offered, fraud prevention, legal compliance, and first-party marketing. Some of these practices, such as where a retailer collects a consumer's address solely to deliver a product the consumer ordered, are obvious from the context of the transaction, and therefore, consent for them is inferred. Others are sufficiently accepted – or necessary for public policy reasons – that companies need not request consent to engage in them. By clarifying those practices for which consumer consent is unnecessary, companies will be able to streamline their communications with consumers, reducing the burden and confusion on consumers and businesses alike." Protecting Consumer Privacy in an Era of Rapid Change:, pages v-vi.

[3] http://www.privacybydesign.ca/content/uploads/2011/02/2011-01-28-PbD-Toronto.pdf, page 17. Last visited August 12, 2011.

[4] http://privacybydesign.ca/about/principles/, last visited August 4, 2011. Dr. Ann Cavoukian, Ph.D, the Information & Privacy Commissioner of Ontario, Canada is the founder of PbD.

[5] http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf, last visited January 15, 2011.

While any single piece of research or article cannot hope to create this blueprint, this article does offer a starting point for further research, and for companies that want to better understand consumers' expectations regarding privacy. This study examines privacy from the individual perspective in two ways—it examines what people think about certain forms of privacy, and what they do about privacy, *i.e.* what steps they take to protect their privacy, and what privacy policies they read. This permits some examination of whether people who believe they are concerned about privacy actually are sufficiently concerned to change their behaviors. This article also offers some initial conclusions regarding consumer attitudes and behaviors, so that companies can better assess individual attitudes regarding privacy and incorporate these into PbD, or other information governance structures.

## II. A Description of the Study.

The study is based upon several surveys that asked consumers to: rank their sensitivity regarding certain forms of information, as well as privacy generally; self-report on their own privacy protective behavior; self-report on their review of certain policies and agreements; rate 100 data elements on a 1-10 scale of how sensitive certain forms of information were; and provide certain forms of demographic information.

Results from this survey are based upon an internet-based survey instrument that sent surveys to a representative sample of individuals, which resulted in a sufficiently large number of responses. These responses were part of three separate surveys which were sent to 954, 474, and 482 individuals in the United States, and 818, 420, and 399 responses were respectively received, for a response rate of 85.7%, 88.6%, and 83.6%. The margin of error of this survey is 5% at a 95% confidence level. The demographics of the survey sample generally track the U.S. Census, and are available upon request from the Lares Institute.

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings, such as non-response bias, as it is possible with any survey that individuals who did not participate would respond differently than those who did. Moreover, question wording, other survey concerns, and sampling error can result in error or bias in the findings of surveys. Finally, survey research is based upon the quality and integrity of confidential responses that the Lares Institute received from survey participants.

## III. Executive Summary.

There are certain clear patterns that become apparent when demographic issues and privacy are examined. First, age is one of the most relevant factors to predict both privacy sensitivity, as well as privacy protective behavior, but it is not a linear relationship, and the 46-65 age range is consistently the most privacy sensitive and protective group. Second, in a somewhat surprising finding, education levels were generally inversely related to self-reported sensitivity, and education level was clearly inversely related to individuals' privacy protective behavior. Third, income overall was not that significant in predicting sensitivity, but had relevance to predicting privacy protective behavior in the sense that higher income individuals were generally less likely to read privacy policies.

Fourth, there was consistency between self-assessed privacy sensitivity and other responses in the survey. When the mean rankings of data elements are examined and compared to respondents' self-reported privacy sensitivity, as shown below, the respondents who self-assessed themselves as being more sensitive regarding health information also consistently ranked health-related data elements higher on the 1-10 scale in 13 of 14 cases.

Fifth, consumers do not always review privacy policies, but generally review them in a pattern consistent with certain common consumer agreements, and the relative review of these policies appears to relate to how sensitive consumers perceive the information at issue to be.

## IV. Privacy Sensitivity.

One key issue the study examined is what were individuals' perceptions regarding privacy—specifically how sensitive they were to privacy issues generally, and also regarding certain key categories of information. The results of the questions are discussed in general, and this data was examined for patterns based upon demographic categorization.

### *A. Privacy Sensitivity Generally.*

Respondents were first asked about how sensitive they were generally about privacy:

**Table 1.**

| Privacy Sensitivity | Total |
|---|---|
| Low | 6% |
| Medium | 15% |
| High | 79% |

There were no statistically significant results when these results were examined based upon income or age categorizations. However, when age was considered, there were some strong correlations between age and general privacy sensitivity, with those in the under 18-25 category having the lowest sensitivity at 67% in the high category, 79% in the 26-45 category self-identifying as having high privacy sensitivity, and 83% in the 46-65 category reporting they were highly sensitive to privacy generally. Additionally, at the Medium level, there was a statistically significant correlation between Under 18-25, versus 46-65. Thus, while there was a statistically significant correlation between being in the 46-65 and 26-45 categories, when compared to the youngest category, there was not a statistically significant correlation between the 66+ category and the Under 18-25 category. Moreover, in the Low sensitivity category, 66+ was almost the same as the Under 18-25 category, and the 66+ category was different in a statistically significant way from 46-65.

**Table 2.**

**Age**

| Privacy Sensitivity | Under 18-25 | 26-45 | 46-65 | 66+ |
|---|---|---|---|---|
| Low | 11% | 6% | 4% | 10% |
| Medium | 22% | 16% | 13% | 15% |
| High | 67% | 79% | 83% | 75% |

This result was confirmed when individual data elements were examined. As part of the survey, respondents were asked to rank the sensitivity of 100 data elements. When the mean score of each age cohort is examined, the 46-65 cohort had the highest mean ranking 68% of the time, the second highest 27% of the time, the third highest 5% of the time, and never was below the third highest mean ranking for any data element. Thus, the general finding that 46-65 has the highest sensitivity to privacy also appears when respondents were asked to rank individual data elements, which provides further validation for the conclusion that for privacy sensitivity generally, age is a predictor of privacy sensitivity, but it is not a direct linear relationship, as the 46-65 cohort was the most sensitive to privacy.

*B. Privacy Sensitivity--Health.*

For health sensitivity, demographic information was of more relevance. As a general matter, the respondents reported their sensitivity regarding health information as follows:

**Table 3.**

| Privacy Sensitivity--Health | Total |
|---|---|
| Low | 15% |
| Medium | 17% |
| High | 68% |

A response that someone was sensitive to health information showed a remarkable correlation to how respondents ranked the sensitivity of the health data elements when they were asked to rank the sensitivity of these data elements. Of the 100 data elements respondents were asked to rank, 14 were health-specific and if the mean sensitivity rankings of these elements is examined, a clear pattern emerges. The 14 health elements were examined by taking each sensitivity grouping—general, financial, health, and social media—and comparing the mean value for each group that self-identified as having high sensitivity regarding each category. Those that self-identified as highly sensitive regarding health information consistently ranked health information as more sensitive than those who were sensitive regarding other forms of information. This group had the highest mean value for the data elements in 13 of the 14 data elements, which demonstrates that respondents' general self-assessment strongly correlates to data sensitivity when individual data elements are examined.

Moreover, people who had a higher income were more sensitive regarding their health information than those at a lower income level, and this was the most predictive of health privacy sensitivity.

**Table 4.**

**Income**

| Privacy Sensitivity--Health | Lower | Middle | Upper |
|---|---|---|---|
| Low | 18% | 14% | 8% |
| Medium | 16% | 19% | 15% |
| High | 66% | 68% | 77% |

This conclusion was also seen when the 14 health data elements were examined. In each case, those with the highest income ranked the health data elements as more sensitive than those with a lower income.

Age was also predictive of privacy sensitivity, though it was not a direct linear relationship, with those in the 46-65 category being the most sensitive.

**Table 5.**

**Age**

| Privacy Sensitivity--Health | Under 18-25 | 26-45 | 46-65 | 66+ |
|---|---|---|---|---|
| Low | 24% | 17% | 9% | 21% |
| Medium | 24% | 16% | 15% | 16% |
| High | 51% | 67% | 75% | 63% |

This conclusion was confirmed when the health data elements were examined, with those in the 46-65 category ranking the 14 health elements as the most sensitive 11 times, compared to other age groups. This is consistent with the finding that while being in this age cohort is predictive of sensitivity regarding health information, income had a stronger correlation to health information sensitivity.

Education level was also inversely predictive of health privacy sensitivity, with those who did not have a college degree being more sensitive regarding health information, with those who had a college or graduate degree being less sensitive in so far as less respondents in this cohort reported being highly sensitive than those without a college degree.

**Table 6.**

**Education**

| Privacy Sensitivity--Health | No College Degree | College Degree or Graduate Degree |
|---|---|---|
| Low | 14% | 16% |
| Medium | 14% | 18% |
| High | 72% | 66% |

In conclusion, age again was predictive of health sensitivity, with the 46-65 cohort being the most sensitive, but income was the most relevant factor to consider for health privacy sensitivity. As we will see in other areas, a higher education level was predictive of a lower sensitivity to health privacy.

*C. Privacy Sensitivity--Financial.*

Financial information was the category that respondents were the most sensitive about, with 90% reporting that they were highly sensitive regarding financial information.

**Table 7.**

| Privacy Sensitivity--Financial | Total |
|---|---|
| Low | 5% |
| Medium | 5% |
| High | 90% |

From a demographic perspective, age was the only factor that was predictive of financial privacy sensitivity, with the 46-65 cohort again being the most sensitive.

**Table 8.**

**Age**

| Privacy Sensitivity--Financial | Under 18-25 | 26-45 | 46-65 | 66+ |
|---|---|---|---|---|
| Low | 8% | 4% | 4% | 8% |
| Medium | 9% | 5% | 4% | 6% |
| High | 83% | 91% | 92% | 86% |

*D. Privacy Sensitivity--Social Media.*

Finally, respondents were asked to self-assess their privacy sensitivity regarding social media. Overall, respondents were generally less sensitive regarding social media privacy, with 58% falling into the "high" category, compared to 90% with financial privacy.

**Table 9.**

| Privacy Sensitivity--Social Media | Total |
|---|---|
| Low | 18% |
| Medium | 24% |
| High | 58% |

Income and education were not predictive of sensitivity regarding this issue, and age was only predictive in a limited way. 25% of respondents in the under 18-25 category, compared to 16% in the 26-45 cohort self-reported as having a low sensitivity regarding social media privacy.

**Table 10.**

**Age**

| Privacy Sensitivity--Social Media | Under 18-25 | 26-45 | 46-65 | 66+ |
|---|---|---|---|---|
| Low | 25% | 16% | 17% | 20% |
| Medium | 25% | 25% | 24% | 24% |
| High | 50% | 59% | 59% | 56% |

In sum, generally people were less concerned about social media privacy, and contrary to some popular belief, younger respondents were not significantly less concerned about social media privacy than other age-ranges.

*E. Demographics and Privacy Sensitivity--In Summary.*

Conclusions can be drawn regarding privacy sensitivity and demographic information that demonstrate there are certain correlations. Age is one of the most important factors in determining privacy sensitivity, but the relationship is not a directly relational one in the sense that higher age does not predict higher sensitivity. Instead, we consistently see that one age range, 46-65 is the most sensitive to privacy, with those younger, and older, being less sensitive. Income was slightly predictive of privacy sensitivity as it had a significant impact on health privacy sensitivity, but it had no other statistically significant correlation to privacy sensitivity.

Education level, where it was relevant, had an inverse relationship to privacy sensitivity, which is a result we will see replicated in other data. Finally, the belief that younger people "cared less" about privacy in social media is not supported by these results. While younger people self-assessed as being less sensitive to social media privacy issues than older respondents, there was not a statistically significant variance based upon age.

## V. Demographics and Privacy Protective Behavior.

Another way to examine privacy and demographic issues is to analyze certain privacy protective behaviors and examine if there are any demographic correlations. While as noted above, certain age groups are more sensitive to privacy issues, that did not necessarily translate to a correlation in privacy protective behavior.

Respondents were asked a number of questions that related to privacy and information security protective activities, which were based in part upon the FTC's recommendations for consumers to avoid identity theft.[6]

### *A. Social Security Cards.*

The first question respondents were asked was whether they carried their Social Security card in their wallet. Overall, 27% did and 73% did not.

**Table 11.**

| | Total |
|---|---|
| Yes | 27% |
| No | 73% |

There was not a statistically significant variance in these numbers based upon income, though higher income people tended to carry their Social Security number card less than lower and middle income respondents.[7]

[6] http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt01.shtm, last visited August 7, 2011.

[7] Education level was not predictive of this behavior.

**Table 12.**

**Income**

| | Lower | Middle | Upper |
|---|---|---|---|
| Yes | 28% | 30% | 21% |
| No | 72% | 70% | 79% |

However, age was predictive of whether people carried their Social Security card in a way that was surprising given the results of the questions regarding privacy sensitivity. The least privacy sensitive group—Under 18-25 carried their Social Security card in their wallet much less than the older groups, which were all more privacy sensitive than the youngest group.

**Table 13.**

**Age**

| | Under 18-25 | 26-45 | 46-65 | 66+ |
|---|---|---|---|---|
| Yes | 14% | 23% | 31% | 45% |
| No | 86% | 77% | 69% | 55% |

*B. Virus Protection.*

Respondents were asked if they took steps to protect their computer from viruses and other security threats. Overall, 92% of respondents did take steps to protect their computer, and 8% did not. Education level was not significant for this question, but both income and age were important to consider. Upper income respondents protected their computer 97% of the time, compared to 89% of lower income respondents.

**Table 14.**

**Total**

| | |
|---|---|
| Yes | 92% |
| No | 8% |

**Income**

| | Lower | Middle | Upper |
|---|---|---|---|
| Yes | 89% | 94% | 97% |
| No | 11% | 6% | 3% |

In contrast to the question regarding Social Security numbers, age was predictive of whether people took steps to protect their computer from security threats, with older respondents taking steps more often than younger respondents.

**Table 15.**

**Age**

| | Under 18-25 | 26-45 | 46-65 | 66+ |
|---|---|---|---|---|
| Yes | 78% | 92% | 95% | 95% |
| No | 22% | 8% | 5% | 5% |

*C. Password Habits.*

Respondents were also asked if they used information such as their mother's maiden name, their birth date, or the last four digits of their Social Security number as a password for their credit card, bank account or phone account. There were not statistically significant differences based upon an examination of demographic information, and overall 18% of people did use such information as their password, and 82% did not.

**Table 16.**

| | Total |
|---|---|
| Yes | 18% |
| No | 82% |

*D. Verification of the Identity of Businesses.*

Respondents were also asked whether they took steps to verify the identity and legitimacy of businesses that asked for PII, and overall 81% did, and 19% did not. There was a statistically significant variance based upon age, with only 69% of respondents who were in the under 18-25 age range responding that they did check this information, 85% of the 46-65 age demographic responding that they did check this information, and 90% of the 66+ age range verifying this information.

**Table 17.**

**Total**

| | |
|---|---|
| Yes | 81% |
| No | 19% |

**Table 18.**

**Age**

| | Under 18-25 | 26-45 | 46-65 | 66+ |
|---|---|---|---|---|
| Yes | 69% | 79% | 85% | 90% |
| No | 31% | 21% | 15% | 10% |

*E. Secure Storage of PII.*

Respondents were asked if they kept PII in a secure location in their home, and overall 76% did, and 24% did not, and interestingly, people with no college degree were more likely to keep their information in a secure location than those that had a college or post-graduate degree.

**Table 19.**

**Total**

| | |
|---|---|
| Yes | 76% |
| No | 24% |

**Education**

| | No College Degree | College Degree or Graduate Degree |
|---|---|---|
| Yes | 83% | 72% |
| No | 17% | 28% |

*F. Shredding of Information.*

Respondents were asked if they shredded documents such as charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, or expired credit cards, before they threw them away. Overall, 58% did, 12% did not, and 30% did some of the time. Income was predictive of this behavior, but education level was, again in an inverse way, with 66% of those with no college degree shredding this information, compared to 54% of those with a college or graduate degree.[8]

Age was also predictive of this behavior, with 47% of those in the under 18-25 category shredding this information, 22% not shedding it, and 31% sometime shredding it, compared to 52%, 10% and 38% in the 26-45 category, and 64%, 11%, and 25% in the 46-65 category respectively.

[8] The impact of education level was the opposite when one considers the "sometimes" category.

**Table 20.**

| Total | | Age | | | | |
|---|---|---|---|---|---|---|
| | | | Under 18-25 | 26-45 | 46-65 | 66+ |
| Yes | 58% | Yes | 47% | 52% | 64% | 65% |
| No | 12% | No | 22% | 10% | 11% | 10% |
| Sometimes | 30% | Sometimes | 31% | 38% | 25% | 25% |

*G. Deposit of Mail.*

A final question regarding whether respondents deposited mail in a secure location was asked. Overall, only 15% did, 63% did not, and 22% did some of the time. Here, income level was predictive of this behavior, with upper income respondents being more likely to deposit mail in a secure location. In contrast to some other areas, a higher education level was predictive of privacy protective behavior as respondents with a higher education level were less likely to use unsecure methods.[9]

**Table 21.**

| Total | | Education | | |
|---|---|---|---|---|
| | | | No College Degree | College Degree or Graduate Degree |
| Yes | 15% | Yes | 15% | 16% |
| No | 63% | No | 70% | 59% |
| Sometimes | 22% | Sometimes | 15% | 25% |

*H. Conclusions.*

Overall, the 46-65 cohort tends to be more privacy protective when these behaviors are examined, with the exception of the practice of carrying a Social Security card on their person. Higher income is somewhat predictive of privacy protective behavior, but higher education levels tend to have an inverse relationship to privacy protective behavior.

[9] While the use of secure mailing did not vary across education level, the failure to use it did—70% for those with a lower education level, compared to 59% of those with a higher education level, and this was also true for those that sometimes used secure mailing, with 15% of those without a college degree sometimes using secure mail, and 25% of those with a college or graduate degree sometimes using secure mail.

### *I. Do People Read Privacy Policies?*

The final area that was examined regarding privacy-related conduct by individuals was whether people read privacy policies, particularly when the review of these documents in compared to other agreements individuals regularly enter. A number of questions regarding different types of privacy policies and other contracts are discussed below. It should be noted that the data is useful to examine in two ways. The raw numbers are helpful in the sense of understanding what people self-report about their review of agreements, and how demographic factors influence this issue. Perhaps as important is an analysis of the relationship between the numbers of people that self-report they review these documents is also helpful because it permits some conclusions to be drawn about the relative review of these documents in comparison to other commonly-enforced consumer transactions.

### *J. Review of Financial Privacy Policies.*

Respondents were asked whether they read the privacy policies they received from their bank, credit card company, or other financial institution and 44% said they had read them, 12% said they had not reviewed them, and 44% had reviewed some of them.

**Table 22.**

| | Total |
|---|---|
| Yes | 44% |
| No | 12% |
| Some of them | 44% |
| I am unaware whether I receive these privacy policies | 0% |
| I have not received any such policies | 0% |

Income level was inversely predictive of whether people read these policies, with 8% of middle income respondents saying they had not reviewed them, compared to 19% of upper income respondents who had not reviewed these policies.

**Table 23.**

**Income**

| | Lower | Middle | Upper |
|---|---|---|---|
| Yes | 45% | 47% | 34% |
| No | 12% | 8% | 19% |
| Some of them | 42% | 45% | 47% |
| I am unaware whether I receive these privacy policies | 0% | 0% | 0% |
| I have not received any such policies | 1% | 0% | 0% |

Education level was also inversely predictive of whether people read these privacy policies, with 54% of people without a college degree reading these policies, compared to 39% of individuals with a college or graduate degree who read these policies.

**Table 24.**

**Education**

| | No College Degree | College Degree or Graduate Degree |
|---|---|---|
| Yes | 54% | 39% |
| No | 5% | 16% |
| Some of them | 41% | 45% |
| I am unaware whether I receive these privacy policies | 0% | 0% |
| I have not received any such policies | 1% | 0% |

*K. Financial Privacy Policy Review--Conclusions.*

With financial privacy policy review we see that income and education level were inversely predictive of policy review since individuals with higher incomes and higher education levels reviewed these policies less than individuals with lower incomes and education levels. Age was not predictive of financial privacy policy review.

*L. Health Care Privacy Policy Review.*

Overall, 52% of respondents read the privacy policies they received from their health care providers, 12% did not, and 35% read some of them. This number is higher than the financial privacy policy review and the highest number seen for privacy policy review.

**Table 25.**

| | Total |
|---|---|
| Yes | 52% |
| No | 12% |
| Some of them | 35% |
| I am unaware whether I receive these privacy policies | 1% |
| I have not received any such policies | 1% |

As with financial privacy, both income and education level were inversely predictive of whether people read privacy policies. 56% of middle income respondents read these privacy policies, while only 41% of upper income respondents had read them.[10]

**Table 26.**

**Income**

| | Lower | Middle | Upper |
|---|---|---|---|
| Yes | 52% | 56% | 41% |
| No | 11% | 8% | 22% |
| Some of them | 35% | 33% | 37% |
| I am unaware whether I receive these privacy policies | 1% | 1% | 0% |
| I have not received any such policies | 2% | 1% | 0% |

Education was also inversely proportional to privacy policy review, with 59% of those with no college degree reviewing health-related privacy policies, compared to 48% of respondents who had a college or graduate degree.

[10] This finding was also seen in the number of people that had not read the privacy policies, with only 11% of lower income respondents reporting that they did not read these privacy policies, compared to 8% of middle income respondents, and 22% of upper income respondents.

**Table 27.**

**Education**

| | No College Degree | College Degree or Graduate Degree |
|---|---|---|
| Yes | 59% | 48% |
| No | 12% | 12% |
| Some of them | 27% | 38% |
| I am unaware whether I receive these privacy policies | 1% | 1% |
| I have not received any such policies | 1% | 1% |

Age was predictive of whether individuals read health privacy policies, with only 37% of respondents in the under 18-25 demographic reading them, 52% in the 26-45 age-range reading them, and 56% of the 46-65 age-range reading these privacy policies.

**Table 28.**

**Age**

| | Under 18-25 | 26-45 | 46-65 | 66+ |
|---|---|---|---|---|
| Yes | 37% | 52% | 56% | 48% |
| No | 14% | 11% | 12% | 12% |
| Some of them | 47% | 35% | 31% | 33% |
| I am unaware whether I receive these privacy policies | 2% | 1% | 0% | 3% |
| I have not received any such policies | 0% | 1% | 1% | 5% |

*M. Health Privacy Policies--Conclusions.*

We again see further evidence that income and education level is inversely related to health privacy policy review, and see here, in contrast to financial privacy, that age is a factor that must be considered. Once again, we see that the 46-65 cohort has the highest reported level of privacy policy review.

*N. Cable Company Privacy Policies.*

Overall, the review of privacy policies from cable companies was lower than those of other areas. 25% of respondents had reviewed the privacy policies they received from cable providers, 35% did not, and 31% reviewed some of them. This conclusion was consistent with the findings when respondents were asked to self-assess their sensitivity regarding information regarding their television viewing habits, because this data element ranked 99 out of 100 data elements based upon consumer perception of sensitivity.

**Table 29.**

| | Total |
|---|---|
| Yes | 25% |
| No | 35% |
| Some of them | 31% |
| I am unaware whether I receive these privacy policies | 3% |
| I have not received any such policies | 5% |

Again, income and education level were inversely proportional to whether people reviewed these policies. 29% of lower income respondents reviewed these privacy policies, as did 28% of middle income respondents, compared to just 12% of upper income respondents, and 32% of lower and middle income respondents did not review these policies, compared to 52% of upper income respondents.

**Table 30.**

**Income**

| | Lower | Middle | Upper |
|---|---|---|---|
| Yes | 29% | 28% | 12% |
| No | 32% | 32% | 52% |
| Some of them | 30% | 34% | 30% |
| I am unaware whether I receive these privacy policies | 3% | 4% | 3% |
| I have not received any such policies | 6% | 3% | 3% |

Consistent with other reported privacy policy review, 37% of those with no college degree reviewed these policies, compared to 19% of individuals with a college or graduate degree, and 26% of those with no college degree did not review the policies, compared to 40% of those with a college or graduate degree.

**Table 31.**

**Education**

| | No College Degree | College Degree or Graduate Degree |
|---|---|---|
| Yes | 37% | 19% |
| No | 26% | 40% |
| Some of them | 27% | 34% |
| I am unaware whether I receive these privacy policies | 3% | 3% |
| I have not received any such policies | 6% | 4% |

*O. Cable Company Privacy Policies—Conclusion.*

Once again, income and education levels were inversely proportional to privacy policy review, though age did not have an impact on this question.

*P. Internet Service Provider Privacy Policy Review.*

Generally, respondents reviewed ISP privacy policies at a lower level than other privacy policies, with 32% reviewing them, 35% reporting they had not reviewed the privacy policies, and 27% reporting that they had reviewed some of them.

**Table 32.**

| | Total |
|---|---|
| Yes | 32% |
| No | 35% |
| Some of them | 27% |
| I am unaware whether I receive these privacy policies | 3% |
| I have not received any such policies | 3% |

Again, income level was inversely predictive of whether privacy policies were reviewed, with 32% of lower income respondents reviewing them, 37% of middle income respondents revering them, and only 23% of upper income respondents reviewing them.

**Table 33.**

**Income**

| | Lower | Middle | Upper |
|---|---|---|---|
| Yes | 32% | 37% | 23% |
| No | 34% | 29% | 48% |
| Some of them | 27% | 28% | 26% |
| I am unaware whether I receive these privacy policies | 4% | 3% | 1% |
| I have not received any such policies | 3% | 3% | 1% |

A similar effect was seen when one considers the negative response to this question, with 34% of lower income respondents not reviewing these policies, 29% of middle income respondents not reviewing them, and 48% of upper income respondents not reviewing them.

Education level was similarly inversely predictive of privacy policy review, with 44% of respondents with no college degree reviewing these policies and 27% of this group not reviewing the policies, compared to 26% of respondents with a college or graduate degree who reviewed the policies and 39% who did not review them.

**Table 34.**

**Education**

| | No College Degree | College Degree or Graduate Degree |
|---|---|---|
| Yes | 44% | 26% |
| No | 27% | 39% |
| Some of them | 24% | 29% |
| I am unaware whether I receive these privacy policies | 3% | 3% |
| I have not received any such policies | 2% | 3% |

In this case, age was predictive of whether these policies were reviewed. 27% of those in the under 18-25 demographic reviewed these policies, 49% did not review them, and 18% reviewed some of them, compared to much higher levels at older age ranges, including the 46-65 demographic again being the highest rate of review.

**Table 35.**

**Age**

| | Under 18-25 | 26-45 | 46-65 | 66+ |
|---|---|---|---|---|
| Yes | 27% | 27% | 38% | 33% |
| No | 49% | 32% | 32% | 38% |
| Some of them | 18% | 35% | 25% | 25% |
| I am unaware whether I receive these privacy policies | 4% | 3% | 3% | 3% |
| I have not received any such policies | 2% | 3% | 2% | 3% |

*Q. Internet Service Providers—Conclusion.*

The findings regarding ISP privacy policy review were consistent with the other data—education and income were inversely proportional to privacy policy review, and the 46-65 cohort had the highest rate of policy review.

*R. Do People Read Other Documents?*

Respondents were also asked whether they had reviewed other common documents, such as credit card agreements, leases or purchase contracts for automobiles, website terms and conditions, and their homeowners insurance policy. The results for these agreements appear below in the tables. It is important to note that certain privacy policies are reviewed at a similar level to important consumer contracts, but other privacy policies are not, which tends to support a conclusion that consumers are making active choices about which policies they want to spend time reading.

**Table 36.**

Have you read your homeowners insurance policy?

| | Total |
|---|---|
| Yes | 55% |
| No | 18% |
| I don't have one | 27% |

**Table 37.**

Websites—Do you read the terms and conditions for websites you visit?

| | Total |
|---|---|
| Yes | 54% |
| No | 46% |

**Table 38.**

Have you read the agreement (lease or contract) you entered when you purchased or leased your most recent car?

| | Total |
|---|---|
| Yes | 66% |
| No | 34% |

**Table 39.**

Have you read the agreement for any credit cards you have?

| | Total |
|---|---|
| Yes | 58% |
| No | 21% |
| I do not have credit cards | 21% |

This data presents some interesting benchmarks for assessing the relative review of privacy policies. When review of certain agreements is compared as a matter of percentages, a relative ranking of document review can be created.

**Table 40.**

| | |
|---|---|
| Have you read the agreement (lease or contract) you entered when you purchased or leased your most recent car? | 66% |
| Have you read the agreement for any credit cards you have? | 58% |
| Do you read the terms and conditions for websites you visit | 54% |
| Health Care Privacy Policy Review | 52% |
| Review of Financial Privacy Policies | 44% |
| Internet Service Provider Privacy Policy Review | 32% |
| Cable Company Privacy Policies | 25% |

One challenge with the data is that it is based upon respondents' self-reporting of conduct, and not a measurement of the conduct itself, and thus these results could be higher than if we measured actual conduct. One could conclude that the overall self-reporting bias, if any, was consistent across the categories, and therefore this table permits us to assess the relative review of all of these very common consumer-facing agreements and policies. Two conclusions can be drawn based upon this data, even assuming some self-reporting bias. First, with certain exceptions, privacy policies are generally reviewed as often as some very standard agreements—credit card and insurance agreements—that are routinely enforced. In other words, not everyone may review privacy policies, but they generally review them almost as often as some routinely enforced agreements in our society.

Second, consumers are making clear choices about their policy review, which seem at least in part based upon their level of concern about the data at issue. Television viewing history was the second least sensitive data element, and the finding that people reviewed cable company privacy policies less than other privacy policies is consistent with a conclusion that consumers are less concerned about this type of data, and thus choosing not to review these policies as often as they review other policies.

## VI. Conclusions.

When respondents' self-reported sensitivity, as well as privacy protective behaviors are examined, some clear patterns emerge. Age is one of the most relevant factors to predict both privacy sensitivity, as well as privacy protective behavior, but it is not a linear relationship, and the 46-65 age range is consistently the most privacy sensitive and protective group. Education levels were, where relevant to sensitivity, inversely related, and clearly inversely related to privacy protective behavior. Income overall was not that significant in predicting sensitivity, but had relevance to predicting privacy protective behavior in the sense that higher income individuals were generally less likely to read privacy policies. Consumers also appear to be making choices about what agreements or policies they review, and it appears that the sensitivity of the information covered by the policy appears to influence the level of consumer review of these policies.

One main question to consider is how this information can help companies and consumers better understand privacy issues. It is a question that will require further analysis, but there are certain conclusions that are apparent. It seems clear from the data, particularly the data regarding privacy policy review and the inverse relationship between education level and policy review, that consumers are actively making choices about what privacy policies they review. While many may claim that "consumers do not read privacy policies", a categorical statement that does not appear to be accurate, a more accurate statement may be that consumers make active choices about what policies to review. It may be that consumers make value judgments about what they choose to spend their time reviewing, based upon their level of concern, but the general conclusions that consumers' refusal to read polices undercuts their effectiveness does not appear to be accurate.

A second conclusion is that companies can likely impact their brand in a positive way if they examine their customer base on a demographic basis and try and promote privacy in a positive way. As shown above, certain demographic segments are more concerned about certain forms of privacy, and this data can serve as the beginning of a roadmap to brand improvement on privacy.

A third conclusion is that consumers are likely not as careful as many would hope regarding their own privacy practices, particularly regarding carrying their Social Security cards and the failure to shred PII. While this does not directly correlate to companies' obligations, that data may be relevant in assessing businesses risk judgments regarding data disclosure and data destruction.

Fourth, and finally, whether a company is choosing to implement an information governance program, or PbD, this research represents the beginning of a roadmap for both types of programs. It is not the complete picture, and more research will be released by the Lares Institute regarding these issues, but consumers' attitudes and patterns regarding privacy protective behavior offer important insights as companies attempt to design privacy into their products and services, or implement governance regimes that implement best practices.