Protecting Private Information:
Current Attitudes Concerning Privacy Policies

Therese L. Williams, Nitin Agarwal, Rolf T. Wigand
Department of Information Science
University of Arkansas at Little Rock, United States
tlwilliams8@ualr.edu, nxagarwal@ualr.edu, rtwigand@ualr.edu

Abstract

Privacy, in the modern connected world, has become a much discussed topic in society ranging from privacy concerns to impacts, attitudes, practices and technologies. Privacy policies are published by businesses and other organizations to communicate to individuals how their private information will be used. This research strives to answer the question – *What are the current attitudes of individuals towards these published privacy policies and have those attitudes changed in the last ten years?* The research in this paper is based on data collected from an online survey in spring 2014. Compared with research published by Annenberg Public Policy Center in 2005, somewhat surprisingly attitudes have not changed in the last decade.

Keywords: Privacy; Confidentiality; Privacy Policies, Information Privacy, Data Privacy, ICT, Social Media.

1. Introduction

In *Privacy and Freedom*, Alan Westin defined privacy as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others." [1, p. 7]

In contrast to this, the cyber-security concept of confidentiality, defined as the "protection of information within systems so that unauthorized people, resources, and processes cannot access that information." [2, p. 6], is clearly not concerned about individual privacy but about unauthorized access to various types of information, some of which could be some individual's private information.

And while cyber-security professionals concern themselves with encryption methods and other technical solutions to keep information confidential; information privacy concerns are managed by policy.

Recent changes in the Information and Communication Technology (ICT) landscape, including the advent and popularity of social media, have caused individual information privacy concerns to increasingly rise and claims that privacy is dead to appear in mainstream media. [3] A Pew Internet Project survey in 2007 reports that 85% of adults consider it "very important" to control access to personal information. [4]

While many people are rightly concerned about the dangers involved in the misuse of their personal identifying information; the dangers also exist with the misuse of other personal information, often in the realm of big data.

Many people are familiar with the example of Target using shopping information to determine that a teenager was in the early stages of pregnancy. [5] Other recent incidents of data-mining involved Nordstrom, using sensors from another company, obtaining shopping information from shoppers' smartphones and Urban Outfitters alleging violating laws by requiring credit card users to provide their ZIP codes. Urban Outfitters then used that information to obtain addresses. [6]

One website, www.pleaserobme.com, exists only to raise awareness of the potential risks associated with location-awareness and the over-sharing of 'private' information. [7]

Having a privacy policy on a consumer website may imply to an individual that the website offers privacy to those who visit, shop, and purchase. The research in this paper will show that some people realize that this is not always an accurate implication but also that many do not share this realization. The following are additional reasons affecting the attitudes of individuals towards privacy. Privacy policies are difficult to read and/or interpret. Policies keep evolving making it difficult for even the most tech savvy individuals to keep-up. Interfaces to configure one's privacy settings also evolve to reflect the policies and are often not the most user-friendly.

Privacy attitudes of many individuals have not evolved along with the technology and marketing practices of gathering and the use of both personally identifying information and information collected without conscious awareness of those individuals.

In this paper, we will share information gathered from an online survey about privacy and privacy policies – how it was collected and the results that were obtained. Finally, we will discuss several conclusions based on these results and offer a direction for future work in this area.

2. Literature Review

Recent research has shown that the published literature concerning privacy is abundant and covers a wide range of topics. In 2011, Bélanger and Crossler evaluated over 500 articles and categorized them into five topic areas: Information Privacy Concern, Information Privacy and E-Business Impacts, Information Privacy Attitudes, Information Privacy Practices, and Information Privacy and Technologies. [8]

Using this methodology, the research in this paper would be classified under the topic of Information Privacy Attitudes. The following literature review begins with existing US law and case studies, to the history of privacy policies and then to more recent published literature concerning attitudes.

Federal law of the United States does not require that a business or a website have a privacy policy. There are laws regarding deceptive practices [9] and laws regarding certain information, such as personal financial and health information. There is also a considerable set of laws which address the privacy of children, especially at the state level. Legislation has also been enacted for specific industries, such as telecommunications. However, with these exceptions, there are no federal laws in the United States that address what a company or an individual can do with the information of someone else [10]. There are no federal laws that require privacy policies [9].

In their landmark legal argument in 1890, Samuel Warren and Louis Brandeis broached the subject of privacy for the first time and discussed privacy as the "right to be let alone." [11, p. 195] Their argument was precipitated by the use of new photographic technology that allowed photographs without a photographic sitting. These snapshots were being published without permission of the photographed. While Warren and Brandeis' argument was based on separating the right to privacy from the physical property rights, most US privacy court cases still rested on property rights. [12]

The primary federal law regarding electronic privacy is the Privacy Act of 1974. While the Privacy Act was enacted prior to the World Wide Web, it also only deals with information collected by the federal government. It provides only four procedural and/or substantive rights for personal data collected by the US government [13].

In a 1997 survey, the Electronic Privacy Information Center (EPIC), in Washington, D.C., found that only 17 of the top 100 websites published an explicit privacy policy [14]. A follow-up survey, by EPIC, in 1998 was based on the self-regulation efforts of the Direct Marketing Association (DMA). In late 1997, the DMA announced a new policy where new members to the organization would be required to have posted privacy policies along with an opt-out option for consumers. The 1998 EPIC survey found that of 76 new members with 40 websites, only eight had privacy policies and of those only three met the DMA's own requirements [15]. EPIC consequently concluded that self-regulation was not sufficient.

In 1999, EPIC published a second follow-up based on the top 100 shopping websites [16]. In this research, EPIC looked for compliance with the Fair Information Practices published by the Federal Trade Commission in 1973. The Fair Information Practices are not legally binding but include five principles upon which the electronic collection of personal information should be based [17]. In this survey, EPIC found "that 18 of the top shopping sites did not display a privacy policy, 35 of the sites have profile-based advertisers operating on their pages, and 86 of the e-commerce operations use cookies." [16, p. 1] None of the shopping websites complied with all the principles of the Fair Information Practices. EPIC concluded that there was little meaningful privacy protection for consumers.

While these surveys are over ten years old, there has been no additional legislation enacted at the federal level. There is some privacy regulation at the state level, but it varies from state to state. Most recently, California has been enacting legislation on privacy in several different forms [18]. One measure enacts the ability for children to request that their online posts be deleted. Another forbids anyone from posting indecent or pornographic images of ex-lovers online. In California, websites are now required to tell consumers how the site responds to the "Do Not Track" signals sent from browsers. Further legislation adds additional notifications in the event of data breaches; for user names and passwords and for other personal information. Various federal legislation provides that consumers be notified for specific personal information primarily financial and health [19], but the California notification laws add a promising layer to this existing legislation.

In 2004, Milne and Culnan published results of a study investigating why (or why not) consumers read privacy notices and found that while a concern for privacy had a positive impact on the tendency to read online privacy notices, consumers also rely on other signs that indicate a reliable experience such as privacy seals and reputation or brand of the company. [20]

A more recent survey by the Annenberg Public Policy Center of the University of Pennsylvania in 2005/2008, examines consumers' understanding of privacy rules and regulations. This research notes that while the majority of consumers knew that the regulation of privacy was dependent on the type of information collected; they were confused about which types have which rules [21]. This same survey showed that 75% of the respondents believed that because a website had a privacy policy, they would not sell the information. In other words, 75% believed that a privacy policy meant and implied that their information would be kept private.

A different 2005 study compares the self-reported behavior of users concerning privacy versus what they actually do and finds that "in many cases it is that the presence of a policy has a positive effect on users." [22, p. 217] This is consistent with the 2004 results of Milne and Culnan mentioned earlier.

A 2007 article by James Nehf cites research that Internet users rarely read privacy policies and provides reasons why the author believes this is so [23]. Nehf states that it is too difficult for consumers to truly evaluate a privacy policy based on obtuse and difficult wording. He also writes that consumers reduce their perceived privacy risk when they feel a sense of trust with the website owner/company. Such trust can be achieved in a number of ways not related to a privacy policy.

A 2008 report discusses the roots of online privacy in the offline realm (as it pertains to California.) This report shows that while online privacy has become a visible point of contention; it has also exposed the same practices common in the offline venues for many years. [24]

On April 1, 2010, GameStation, a British computer game retailer, inserted a clause into its End User License Agreement that gave it ownership of the users' immortal soul. While this was an April Fools' Day joke, the retailer found that 88% of the customers that day failed to notice the clause even though there was an opt-out clause (which also earned the observant customer a £5 voucher). [25]

Toysmart was primarily an online retailer that filed for bankruptcy in 2000. While the retailer promised its online customers that they would never sell customer information to a third-party, the bankruptcy trustees offered to sell the customer database as an asset during debt recovery. [26] The US Federal Trade Commission sued Toysmart to block the sale of the database and ultimately approved the sale to a major stockholder who agreed to destroy the information.

Possibly in reaction to the issues raised by the Toysmart events, several bills were introduced in the US Congress in 2000-2001. These included the Consumer Privacy Protection Act, the Consumer Internet Privacy Enhancement Act, the Privacy Commission Act, the Consumer Online Privacy and Disclosure Act, the Online Privacy Protection Act of 2001, the Electronic Privacy Protection Act, the Identity Theft Protection Act of 2001, the Social Security Online Privacy Protection Act, the Consumer Internet Privacy Protection Act, the Financial Information Privacy Protection Act of 2001, the Spyware Control and Privacy Protection Act of 2001, the Wireless Privacy Protection Act of 2001,the Student Privacy Protection Act, the Social Security Number Privacy Act of 2001, the Financial Institution Privacy Protection Act of 2001, the Citizen's Privacy Commission Act of 2001, the Social Security Number Privacy and Identity Theft Prevention Act of 2001, the Consumer Credit Report Accuracy and Privacy Act of 2001, the Privacy Act of 2001, the Location Privacy Protection Act of 2001, the Patient Privacy Act of 2001, the National Consumer Privacy Act, and the Consumer's Right to Financial Privacy Act. [27]

These twenty three bills all died in committee in the US Congress. While privacy bills were introduced with some regularity in the 2000-2001 time-period, after September 11, 2001, they ceased to be introduced for the remainder of 2001. In October, 2001, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 was passed into law. [28] Beginning almost immediately, many privacy advocates believed that this Act infringed on many facets of individual privacy rights. [29]

While Warren and Brandeis argued that the right to privacy was the right to be let alone and the right to not have one's unsolicited photograph published in the newspaper, a new argument in the European Union is the right to be forgotten. Most interpretations call for search engines to cease including certain information in search results. Realizing that personal information and photographs will be published, the European Commissioner for Justice, Fundamental Rights and Citizenship has proposed that the right to be forgotten become a new regulation. [30] While the intention is to allow some information to become past information, Jeffrey Rosen, among others, has written that this could harm the balance between privacy and free speech. [30]

An even more recent research paper asks the question "Who is entitled to privacy?" [31, p. 1] and develops a model to determine the influences on an individual's opinion as to the answer to this question.

McDonald and Cranor estimated that the annual time spent reading privacy policies (if everyone read all of them) would be 53.8 billion hours per year in the United States. They further estimated the cost of this time as $781 billion per year; much more than estimates of completing federal income tax forms and more than half of the total time spent using the Internet. [32]

It is clear that privacy is and continues to be a consistent concern and that current privacy policies and practices are not allaying those concerns.

3. Data Collection And Methods

Institutional Review Board approval for this research was obtained in March, 2014 for an online survey to determine the current frequency of users' reading of privacy policies, their reasoning for not reading them if not, and their attitudes towards and knowledge of Internet privacy policies.

In March and April of 2014, this survey was made available online with an unrestricted public link. It was distributed directly to a personal contact list of 175 individuals and also published publicly on Facebook and LinkedIn. In addition, the link was circulated to the membership of local InfraGard (www.infragard.org) and ISACA (www.isaca.org) chapters. The link was open for responses for forty-five (45) days with reminders posted on Facebook approximately once per week. There were a total of 151 respondents; one, however, was eliminated because the survey was not completed.

Ideally, the sample size for this survey would have a minimum of 377 respondents for a 95% confidence level with a 5% margin of error. With 150 respondents, there is a 95% confidence level with a 7.97% margin of error [33].

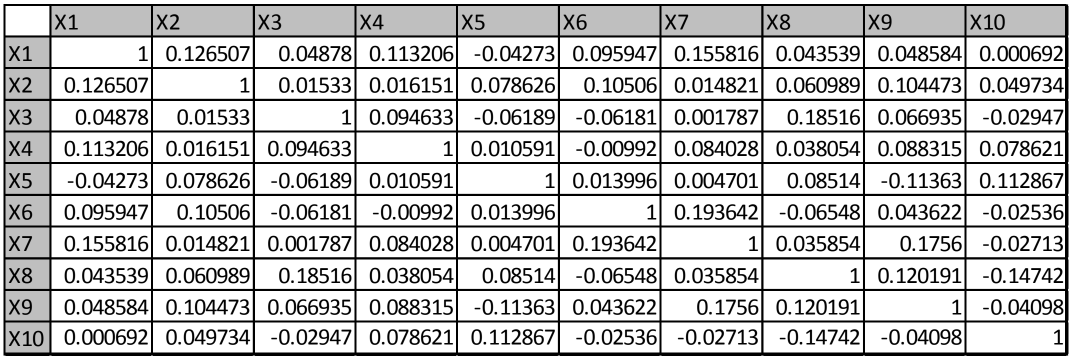
The survey includes a total of ten questions along with four demographic questions and the opportunity to submit other open comments, totaling to 15 questions. Two of the ten questions were based on a Likert scale in order to assess qualitative attitudes regarding the subject. The remaining eight questions were multiple-choice with "I prefer not to answer." as one of the choices. The four demographic questions captured age, gender, education level and residence (state) with a final chance to add any free-form comments, opinions, strong beliefs or suggestions. The questions included on the survey are provided in Figure 1 and as screenshots in Appendix A.

1.	How often do you read privacy policies on websites?
2.	If you did not answer "Always" on the previous question, why don't you always read them?
3.	Have you ever taken the advice of a friend or acquaintance regarding a privacy policy rather than reading it?
4.	Based on your knowledge, if a website or company has a privacy policy, may they sell your information?
5.	Have you ever chosen not to provide personal information after reading a privacy policy on a website?
6.	Have you ever provided incorrect information on a website because of privacy concerns?
7.	In your opinion, what is the value of a privacy policy on a website?
8.	Choose the appropriate category for your Internet Usage. Business Only / Personal Only / Business and Personal /
9.	What is the PRIMARY reason you use the Internet? For Business / Social Networking / Shopping, Research / Entertainment / Email / News and Weather / All of the Above
10.	Have you ever posted a photograph on a social networking site?
11.	What is your age? ______________ (You must be at least 13 to submit this survey.)
12.	What is your gender?
13.	What is the highest level of education you have achieved?
14.	Where do you live? (*Choose from a list of US States and a choice for International)*
15.	If you would like to add any comments, opinions, strong beliefs or suggestions, please do so. ____________________

Figure 1– Questions included on the survey

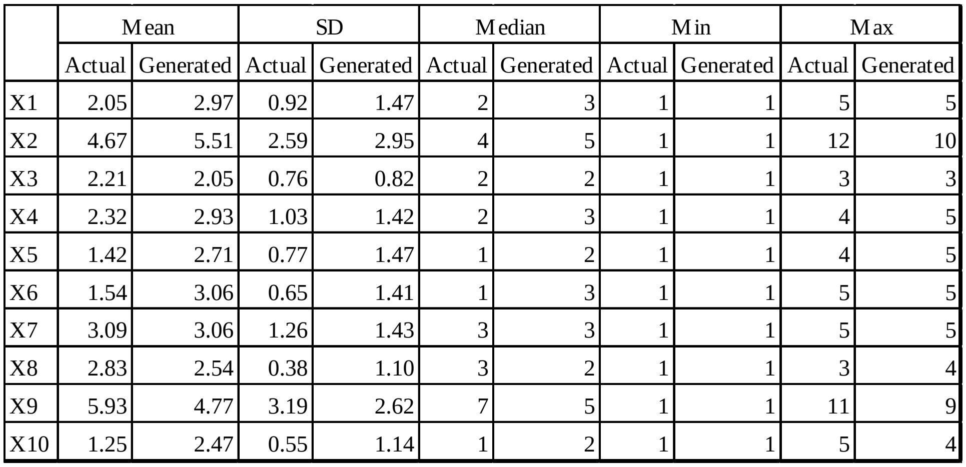
To ensure that the results from this study are statistically significantly different from random responses, an R script was used to generate a completely random sample (available in Appendix B). This involved generating numbers in the appropriate range for each question for 150 respondents. Once generated, a correlation matrix was calculated for all questions. This matrix, shown in figure 2, is clear that there is no correlation between any of the questions with the randomly-generated answers. Additionally, several statistical calculations were compiled for comparing the two samples. These can be seen in figure 3.

In reviewing the calculations in figure 3, for all survey questions, each of the calculations vary between the actual responses and the generated responses. This shows a statistical difference between the actual responses and the randomly-generated answers.



	X1	X2	X3	X4	X5	X6	X7	X8	X9	X10
X1	1	0.126507	0.04878	0.113206	-0.04273	0.095947	0.155816	0.043539	0.048584	0.000692
X2	0.126507	1	0.01533	0.016151	0.078626	0.10506	0.014821	0.060989	0.104473	0.049734
X3	0.04878	0.01533	1	0.094633	-0.06189	-0.06181	0.001787	0.18516	0.066935	-0.02947
X4	0.113206	0.016151	0.094633	1	0.010591	-0.00992	0.084028	0.038054	0.088315	0.078621
X5	-0.04273	0.078626	-0.06189	0.010591	1	0.013996	0.004701	0.08514	-0.11363	0.112867
X6	0.095947	0.10506	-0.06181	-0.00992	0.013996	1	0.193642	-0.06548	0.043622	-0.02536
X7	0.155816	0.014821	0.001787	0.084028	0.004701	0.193642	1	0.035854	0.1756	-0.02713
X8	0.043539	0.060989	0.18516	0.038054	0.08514	-0.06548	0.035854	1	0.120191	-0.14742
X9	0.048584	0.104473	0.066935	0.088315	-0.11363	0.043622	0.1756	0.120191	1	-0.04098
X10	0.000692	0.049734	-0.02947	0.078621	0.112867	-0.02536	-0.02713	-0.14742	-0.04098	1

Figure 2– Correlation matrix for generated sample



	Mean		SD		Median		Min		Max	
	Actual	Generated	Actual	Generated	Actual	Generated	Actual	Generated	Actual	Generated
X1	2.05	2.97	0.92	1.47	2	3	1	1	5	5
X2	4.67	5.51	2.59	2.95	4	5	1	1	12	10
X3	2.21	2.05	0.76	0.82	2	2	1	1	3	3
X4	2.32	2.93	1.03	1.42	2	3	1	1	4	5
X5	1.42	2.71	0.77	1.47	1	2	1	1	4	5
X6	1.54	3.06	0.65	1.41	1	3	1	1	5	5
X7	3.09	3.06	1.26	1.43	3	3	1	1	5	5
X8	2.83	2.54	0.38	1.10	3	2	1	1	3	4
X9	5.93	4.77	3.19	2.62	7	5	1	1	11	9
X10	1.25	2.47	0.55	1.14	1	2	1	1	5	4

Figure 3 – Statistical calculations comparing both samples

4. Results and Findings

There were 150 complete responses to the survey. The respondents were 52% female, and 45% male with 3% declining to provide this information. Two thirds of the respondents were from the home state of the authors with the remaining third from 15 other US states and 3% reporting international locations. Age was measured by the year of age with the average age of the respondents being 45.9. Education was measured by eight categories ranging from "Currently in high school" to "Terminal Degree". The median value for each category was used to convert each value to years of education. The average education level was 16.25 years or the level of a 4-year college degree with some graduate classes.

This sample is not a true random sample and is not representative of the US population. Using information from the US Census bureau and the same median value for each category, the average educational level of the US population, in 2013, was 13.1 or the level of a high school degree with some college. [34] It is expected that this bias will have some impact on the results.

The first question asked was "How often do you read privacy policies on websites?" See Figure 4. This question utilized a Likert scale with values from 1 (Never) to 5 (Always). Only 7% of the respondents answered with Almost Always or Always (4/5), while 70% Never or Almost Never (1/2) read privacy policies.

When asked why they didn't read privacy policies, 74% of the respondents answered that the policies were too long and/or too complex while only 8% thought that the policies didn't matter. In response to another question, shown in figure 5, utilizing a Likert scale, 37% of the respondents thought that the privacy policies on websites were valuable or extremely valuable with a comparable 33% having an opinion that they are worthless. Another third of the respondents felt that they are neither valuable nor worthless. According to this survey, the majority of the respondents agree that privacy policies matter but that they are too complex and difficult to understand. Interestingly, 70% of the respondents have a four-year college degree or a higher education level.

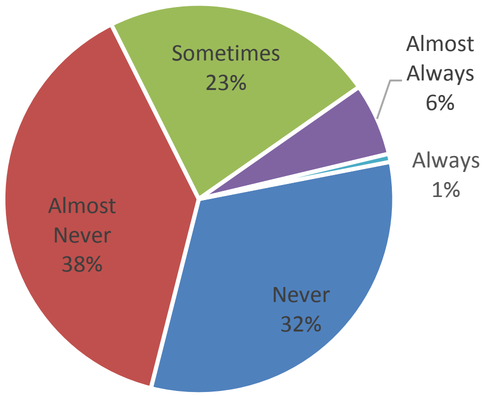


Figure 4 - How often do you read privacy policies on websites?

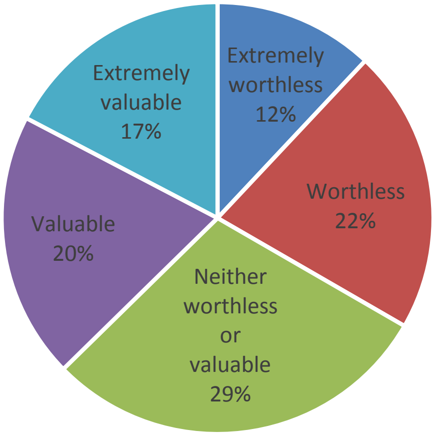


Figure 5 - In your opinion, what is the value of a privacy policy on a website?

Following that the majority of respondents feel that privacy policies are important, 71% answered that they have chosen not to provide personal information after reading a privacy policy (figure 6).

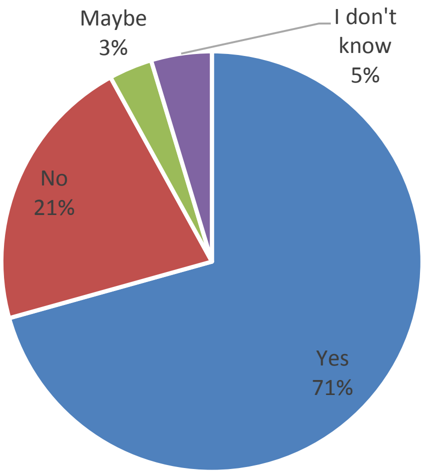


Figure 6 – Have you ever chosen not to provide personal information after reading a privacy policy on a website?

Concerns about privacy also lead individuals to provide inaccurate personal information. (figure 7) According to this survey, 55% of the respondents probably provided incorrect personal information after reading a privacy policy. This could present an information quality issue to the business requesting the information. The severity of the issue would be dependent on the type of information that is being provided incorrectly. One respondent noted "I usually give information that is close to the truth, such as changing my birth date by a few days, months and years."

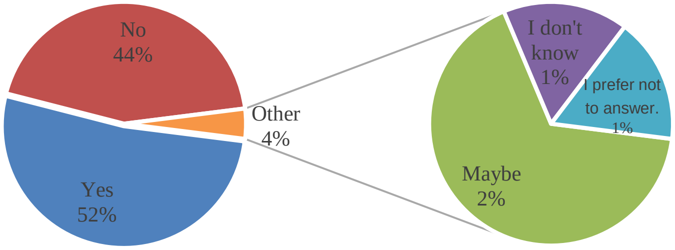


Figure 7 – Have you ever provided incorrect information on a website because of privacy concerns?

Nehf wrote that users can feel a sense of trust with some businesses or organizations, which decreases the importance of a privacy policy [23]. This is reflected in this study by one respondent who added the comment "I only agree to the privacy terms (which I haven't read - they are too long, too complex and a waste of my time) from companies that are well established and whom I consider are probably trustworthy."

The Annenberg Public Policy Center study mentioned earlier reported that 75% of the respondents believed that a privacy policy meant that their information would not be sold [21]. A similar question on this study revealed that 72% believed, or didn't know, that their information could not be sold (see figure 8). With a margin of error for the 2005 study of ±2.5% and a margin of error for this study of ±8%, there is, at most 7.5% difference between the 2005 study and this 2014 study. This is a small difference and points out that **there has been no real change in consumer awareness in the last nine years**.

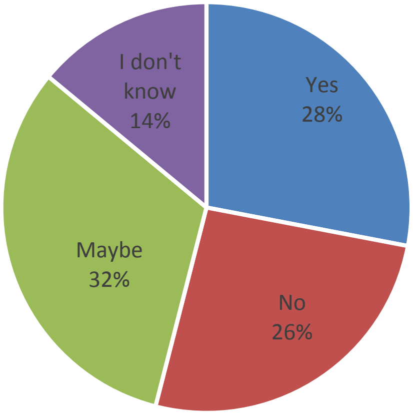


Figure 8 - Based on your knowledge, if a website or company has a privacy policy, may they sell your information?

While the 2005 study provided overall demographic information, correlations were not provided on specific questions. That study showed a correlation between overall knowledge and both educational levels and age but the comparison of current responses to this specific item “Based on your knowledge, if a website or company has a privacy policy, may they sell your information?” across both educational levels and age groups does not show a correlation associated to either demographic. For age the correlation coefficient is 0.003 and for education it is 0.051. These numbers are very near zero, which indicates very little, if any, correlation. The results for this question are shown across education levels in figure 9.

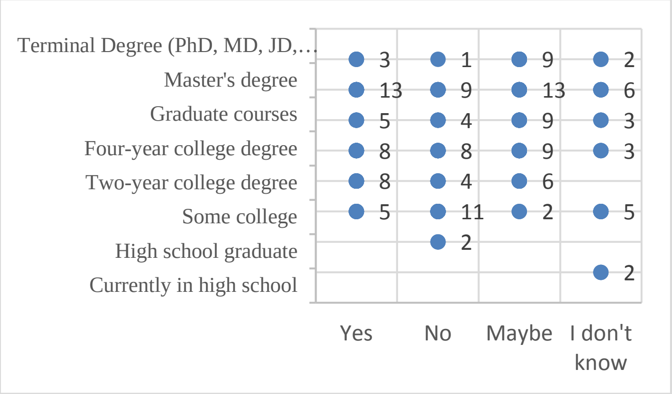


Figure 9 - Based on your knowledge, if a website or company has a privacy policy, may they sell your information? (By Education)

In figure 10, the results for the question “Based on your knowledge, if a website or company has a privacy policy, may they sell your information?” are shown by age group.

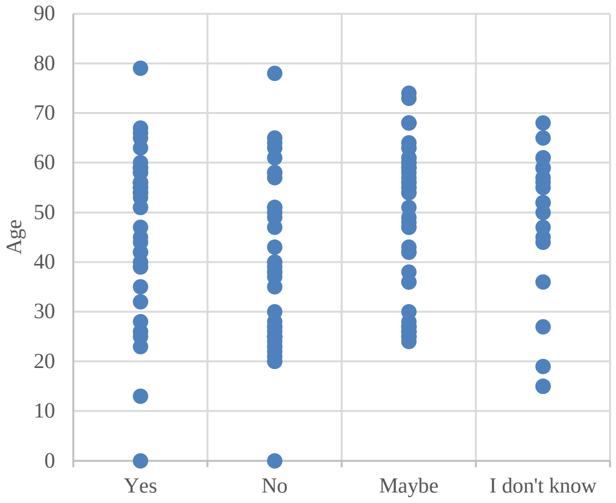


Figure 10 - Based on your knowledge, if a website or company has a privacy policy, may they sell your information? (By Age)

A larger sample size would provide a lower margin of error; however, it is possible to see the percentage of those who erroneously believe that a privacy policy means that an organization is keeping your information private has stayed approximately the same since 2005 and that this particular belief is not directly related to age or education level, but rather distributed across all ages and all education levels. Other studies, and in particular, the 2005 Anneberg study, show a correlation between education and similar questions. [21] This paradoxical finding is indeed puzzling and worthy of further study and analysis.

When asked to choose the appropriate category for their Internet use, an overwhelming majority, 83%, indicated that it was for both Business and Personal use.

An additional question asked “What is the PRIMARY reason you use the Internet?” as a multiple-choice question with eight (8) choices, including **All of the Above**. **All of the Above** was chosen by 36% of the respondents. The next primary reason was **For Business** with 19%. The only other choices with double-digit responses were **Email** and **Research** with 15% and 11% respectively.

While the correlation of both Age and Education to the question “Based on Your Knowledge, if a website or company has a privacy policy, may they sell your information: was discussed earlier, a complete correlation of all the questions to each other was calculated. The only strong correlation (0.98) was between Age and Education: the older one is, the more likely it is to have higher levels of education.

Respondents to this survey were 52% female, and 45% male with 3% not answering the question. The absence of correlation between this information and any other question is a strong indication that the results of this survey are not gender-specific. Privacy is a gender-neutral issue.

5. Conclusions and Future Work

One conclusion is that, as supported by a majority of respondents, most privacy policies are too long, too complex and do not get their points across well. As written, they serve only to protect organizations from sharing or selling consumers’ private information to other organizations. This makes one wonder if the *readability* of this text would need to be examined and simplified or rewritten for consumers. In conjunction with identity issues that are prominent in today’s technological world [35], perhaps a new social contract about individuals’ private, and supposedly confidential, information should be developed to protect this information while still allowing the spread of technology and online commerce.

There continues to be significant misconception concerning the purpose of online privacy policies. While many online marketing practices duplicate those in the offline world, it has been shown that consumers also have misconceptions concerning these offline practices. [24] These misconceptions, along with the degree to which technology allows these practices to evolve in an online setting is cause for concern. Future work may provide different avenues to explore to further consumer knowledge.

A recent article suggests that the focus of privacy efforts should not be as much about the collection of personal data but the use of that data. [36] Realizing that many consumers do not necessarily have the total picture of personal information that is aggregated and shared by the many collectors of such data, perhaps a study into the sources and types of data available would be enlightening.

Another potential future focus is to inquire into the characteristics of a policy that would lead someone to not provide information and what effects this could potentially have on participation and data collection.

Without any specific US federal laws to mandate the use of privacy policies nor to specify the specifics of those policies or how they are written, these policies are self-regulated within multiple industries. From this research, it is clear that effective self-regulation for consumer privacy has yet to emerge.

Minimally, organizations should strive to make the specifics of how they handle private information clear and obvious to their users, without (a) hiding behind words such as share when in reality they mean sell and (b) merely meeting legal requirements satisfying the expectations of lawyers. The information that will be shared should also be clear and specific instead of grouping all data under personal information.

Acknowledgement

This material is based upon work supported in part by the U.S. Air Force Research Lab and the U.S. Office of Naval Research under award number: N000141410489.

References

[1] A. F. Westin, Privacy and freedom, New York: Atheneum, 1967.

[2] S. Hansche, J. Berti and C. Hare, Official (ISC)2 Guide to the CISSP Exam, Boca Raton, FL: Auerbach Publications, 2004.

[3] P. Cashmore, "Privacy is dead, and social media hold smoking gun," CNN.com, 28 October 2009. [Online]. Available: http://edition.cnn.com/2009/OPINION/10/28/cashmore.online.privacy/. [Accessed 16 June 2014].

[4] M. Madden, S. Fox, A. Smith and J. Vitak, "Digital Footprints: Online identity management and search in the age of transparency," Pew Internet & American Life Project, Washington, DC, 2007.

[5] K. Hill, "How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did," Forbes, 16 Feb 2012. [Online]. Available: http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/print/. [Accessed 1 Sept 2014].

[6] C. Waxer, "Big data blues: The dangers of data mining," Computerworld, 4 Nov 2013. [Online]. Available: http://www.computerworld.com/article/2485493/enterprise-applications/big-data-blues--the-dangers-of-data-mining.html. [Accessed 1 Sept 2014].

[7] F. Groeneveld, B. Borsboom and B. v. Amstel, "Over-sharing and Location Awareness," Center for Democracy & Technology, 24 Feb 2010. [Online]. Available: https://cdt.org/blog/over-sharing-and-location-awareness/. [Accessed 1 Sept 2014].

[8] F. Belanger and R. E. Crossler, "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly,* vol. 35, no. 4, pp. 1017-1042, 2011.

[9] "Privacy Law," [Online]. Available: http://www.sba.gov/content/privacy-law. [Accessed 10 10 2013].

[10] "Federal Trade Commission," [Online]. Available: http://epic.org/privacy/internet/ftc/. [Accessed 10 10 2013].

[11] S. D. Warren and L. D. Brandeis, "The Right To Privacy," *Harvard Law Review,* pp. 193-220, 1890.

[12] R. C. Post, "Rereading Warren and Brandeis: Privacy, Property, and Appropriation," *Faculty Scholarship Series,* p. Paper 206, 1991.

[13] "The Privacy Act of 1974," [Online]. Available: The Privacy Act of 1974. [Accessed 10 10 2013].

[14] "Surfer Beware: Personal Privacy and the Internet," [Online]. Available: http://epic.org/reports/surfer-beware.html. [Accessed 10 10 2013].

[15] "Surfer Beware II: Notice Is Not Enough," [Online]. Available: http://epic.org/reports/surfer-beware2.html. [Accessed 10 10 2013].

[16] "Surfer Beware III: Privacy Policies without Privacy Protection," [Online]. Available: http://epic.org/reports/surfer-beware3.html. [Accessed 10 10 2013].

[17] U.S. Department of Health, Education and Welfare, "Fair Information Practices," Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens VIII, 1973.

[18] Politico, "California driving Internet privacy policy," 2013. [Online]. Available: http://www.politico.com/story/2013/10/california-internet-privacy-policy-97964.html. [Accessed 10 10 2013].

[19] "Data breach notification laws," [Online]. Available: http://itlaw.wikia.com/wiki/Data_breach_notification_laws. [Accessed 12 10 2013].

[20] G. R. Milne and M. J. Culnan, "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices," *Journal of Interactive Marketing,* vol. 18, no. 3, pp. 15-29, 2004.

[21] J. Turow, M. Hennessy and A. Bleakley, "Consumers' Understanding of Privacy Rules in the Marketplace," *The Journal of Consumer Affairs,* vol. 42, no. 3, pp. 411-424, 2008.

[22] C. Jensen, C. Potts and C. Jensen, "Privacy Practices of Internet users: Self-reports versus observed behavior," *International Journal of Human-Computer Studies,* vol. 63, no. 1, pp. 203-227, 2005.

[23] J. P. Nehf, "Shopping for Privacy on the Internet," *The Journal of Consumer Affairs,* vol. 41, no. 2, pp. 351-375, 2007.

[24] C. J. Hoofnagle and J. King, "Research Report: What Californians Understand About Privacy Offline," University of California-Berkeley School of Law, Berkeley, 2008.

[25] Fox News, "7,500 Online Shoppers Unknowingly Sold Their Souls," [Online]. Available: http://www.foxnews.com/tech/2010/04/15/online-shoppers-unknowingly-sold-souls/. [Accessed 28 July 2014].

[26] D. Bronski, C. Chen, M. Rosenthal and R. Pluscec, "FTC vs. Toysmart," *Duke Law and Technology Review*, 2001.

[27] "www.govtrack.us," [Online]. Available: https://www.govtrack.us/congress/bills/browse?congress=__ALL__&text=2001%20privacy#sort=introduced_date. [Accessed 24 Aug 2014].

[28] "USA Patriot Act," [Online]. Available: https://www.govtrack.us/congress/bills/107/hr3162. [Accessed 24 Aug 2014].

[29] "USA Patriot Act," www.EPIC.org, [Online]. Available: http://epic.org/privacy/terrorism/usapatriot/. [Accessed 24 Aug 2014].

[30] J. Rosen, "The Right To Be Forgotten," *Stanford Law Review Online,* vol. 64, pp. 88-92, 2012.

[31] J. S. Giboney, D. Wilson and A. Durcikova, "An Individual's Views of the Right to Privacy of Other Individuals, Companies, and Governments: A Theoretical Perspective," in *Twentieth Americas Conference on Information Systems*, Savannah, GA, 2014.

[32] A. M. McDonald and L. F. Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society,* vol. 4, no. 3, pp. 540-565, 2008.

[33] "Sample Size Calculator," [Online]. Available: http://www.raosoft.com/samplesize.html. [Accessed 13 July 2014].

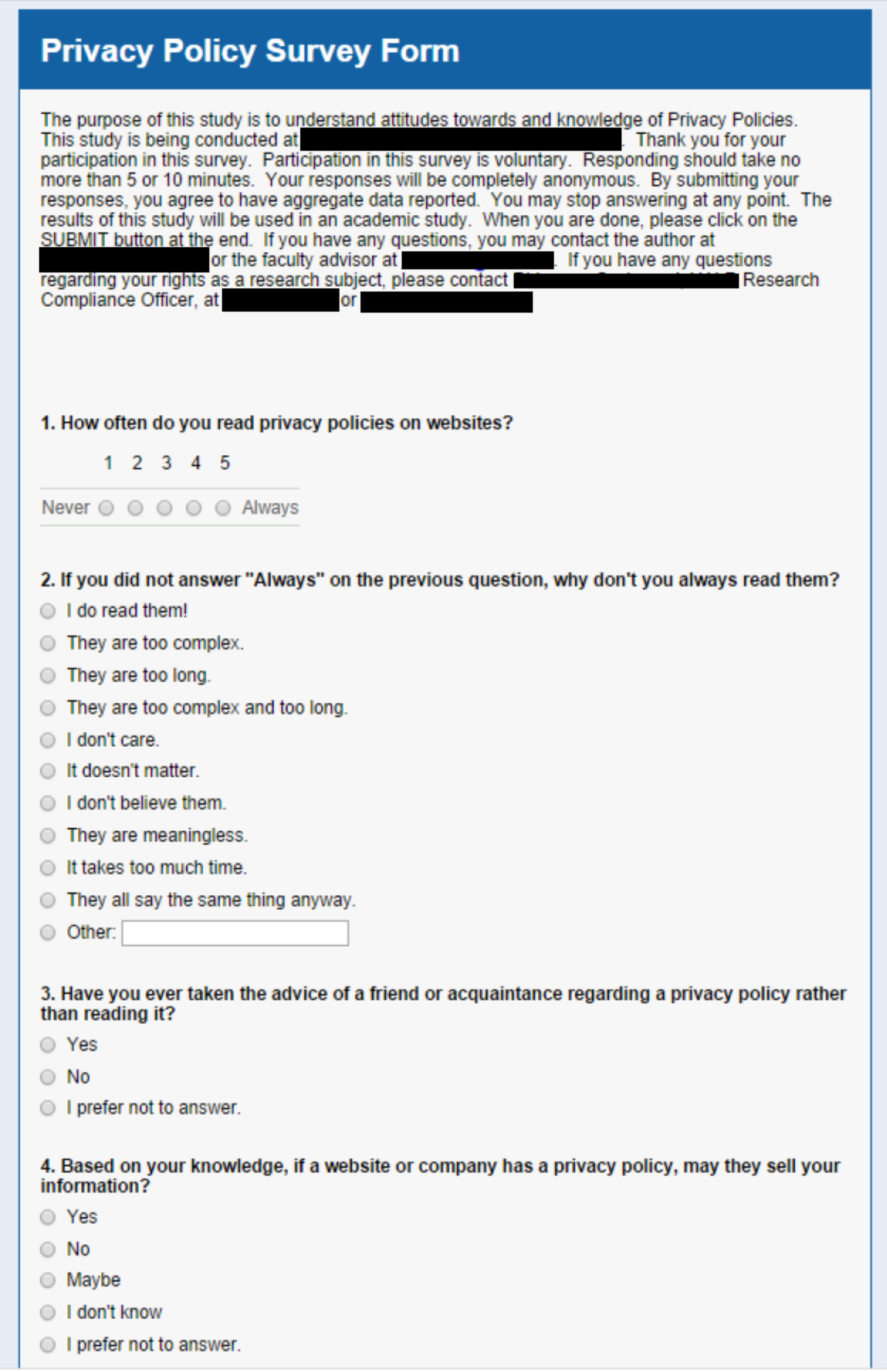
[34] "US Census," 2013. [Online]. Available: http://www.census.gov/hhes/socdemo/education/data/cps/2013/tables.html. [Accessed 14 Oct 2014].

[35] J. Harper, Identity Crisis: How Identification is Overused and Misunderstood, Washington, DC: Cato Institute, 2006.

[36] C. Mundie, "Privacy Pragmatism: Focus on Data Use, Not Data Collection," *Foreign Affairs,* pp. 28-38, March/April 2014.

[37] C. Hoback, Director, *Terms And Conditions May Apply*. [Film]. United States: Hyrax Films, 2013.

APPENDIX A



Privacy Policy Survey Form

The purpose of this study is to understand attitudes towards and knowledge of Privacy Policies. This study is being conducted at [redacted]. Thank you for your participation in this survey. Participation in this survey is voluntary. Responding should take no more than 5 or 10 minutes. Your responses will be completely anonymous. By submitting your responses, you agree to have aggregate data reported. You may stop answering at any point. The results of this study will be used in an academic study. When you are done, please click on the SUBMIT button at the end. If you have any questions, you may contact the author at [redacted] or the faculty advisor at [redacted]. If you have any questions regarding your rights as a research subject, please contact [redacted] Research Compliance Officer, at [redacted] or [redacted]

1. How often do you read privacy policies on websites?

	1	2	3	4	5	
Never	○	○	○	○	○	Always

2. If you did not answer "Always" on the previous question, why don't you always read them?

○ I do read them!

○ They are too complex.

○ They are too long.

○ They are too complex and too long.

○ I don't care.

○ It doesn't matter.

○ I don't believe them.

○ They are meaningless.

○ It takes too much time.

○ They all say the same thing anyway.

○ Other: □

3. Have you ever taken the advice of a friend or acquaintance regarding a privacy policy rather than reading it?

○ Yes

○ No

○ I prefer not to answer.

4. Based on your knowledge, if a website or company has a privacy policy, may they sell your information?

○ Yes

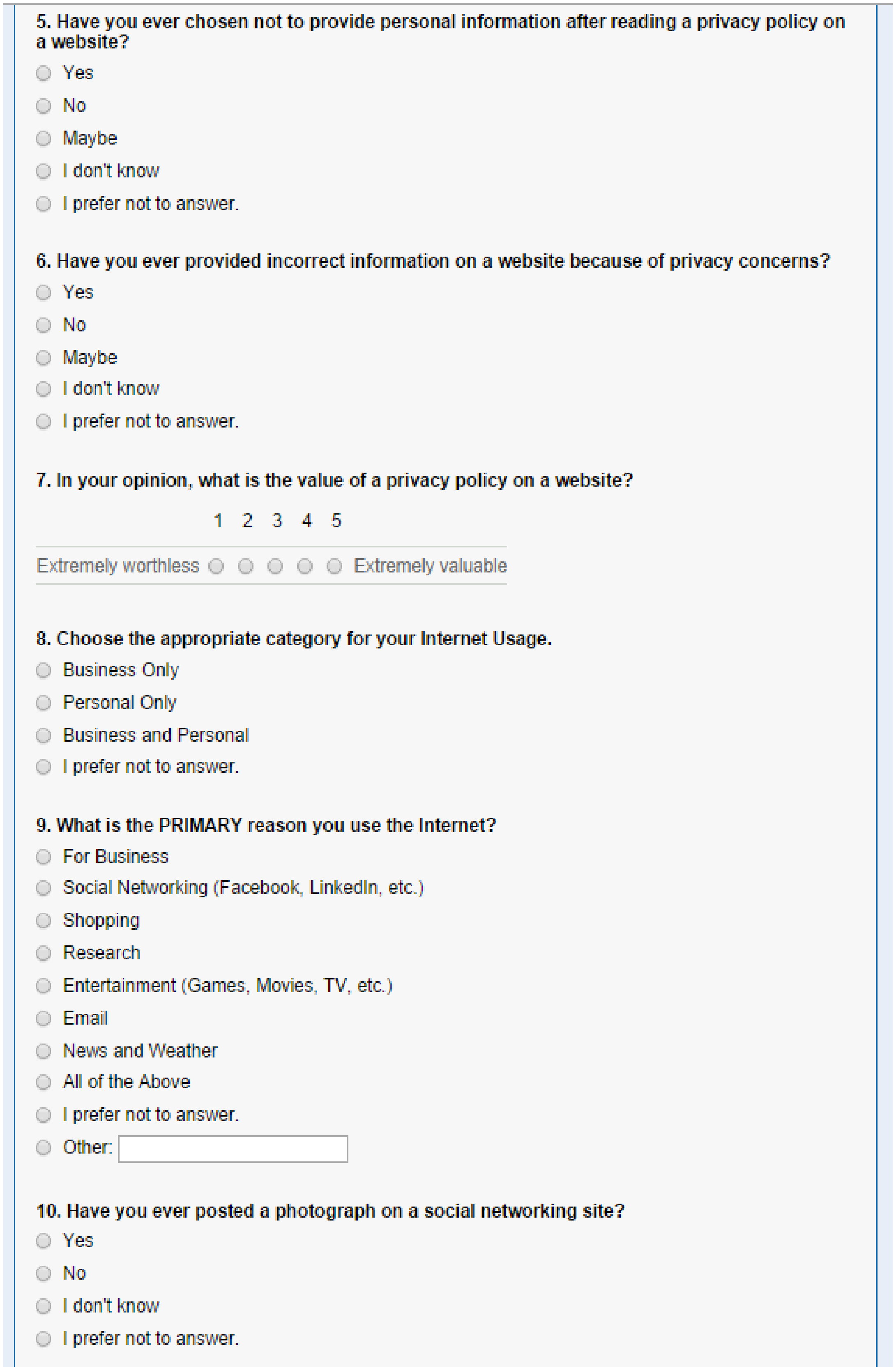
○ No

○ Maybe

○ I don't know

○ I prefer not to answer.

Screenshot 1- Survey Questions 1 – 4



5. Have you ever chosen not to provide personal information after reading a privacy policy on a website?

○ Yes

○ No

○ Maybe

○ I don't know

○ I prefer not to answer.

6. Have you ever provided incorrect information on a website because of privacy concerns?

○ Yes

○ No

○ Maybe

○ I don't know

○ I prefer not to answer.

7. In your opinion, what is the value of a privacy policy on a website?

	1	2	3	4	5	
Extremely worthless	○	○	○	○	○	Extremely valuable

8. Choose the appropriate category for your Internet Usage.

○ Business Only

○ Personal Only

○ Business and Personal

○ I prefer not to answer.

9. What is the PRIMARY reason you use the Internet?

○ For Business

○ Social Networking (Facebook, LinkedIn, etc.)

○ Shopping

○ Research

○ Entertainment (Games, Movies, TV, etc.)

○ Email

○ News and Weather

○ All of the Above

○ I prefer not to answer.

○ Other:

10. Have you ever posted a photograph on a social networking site?

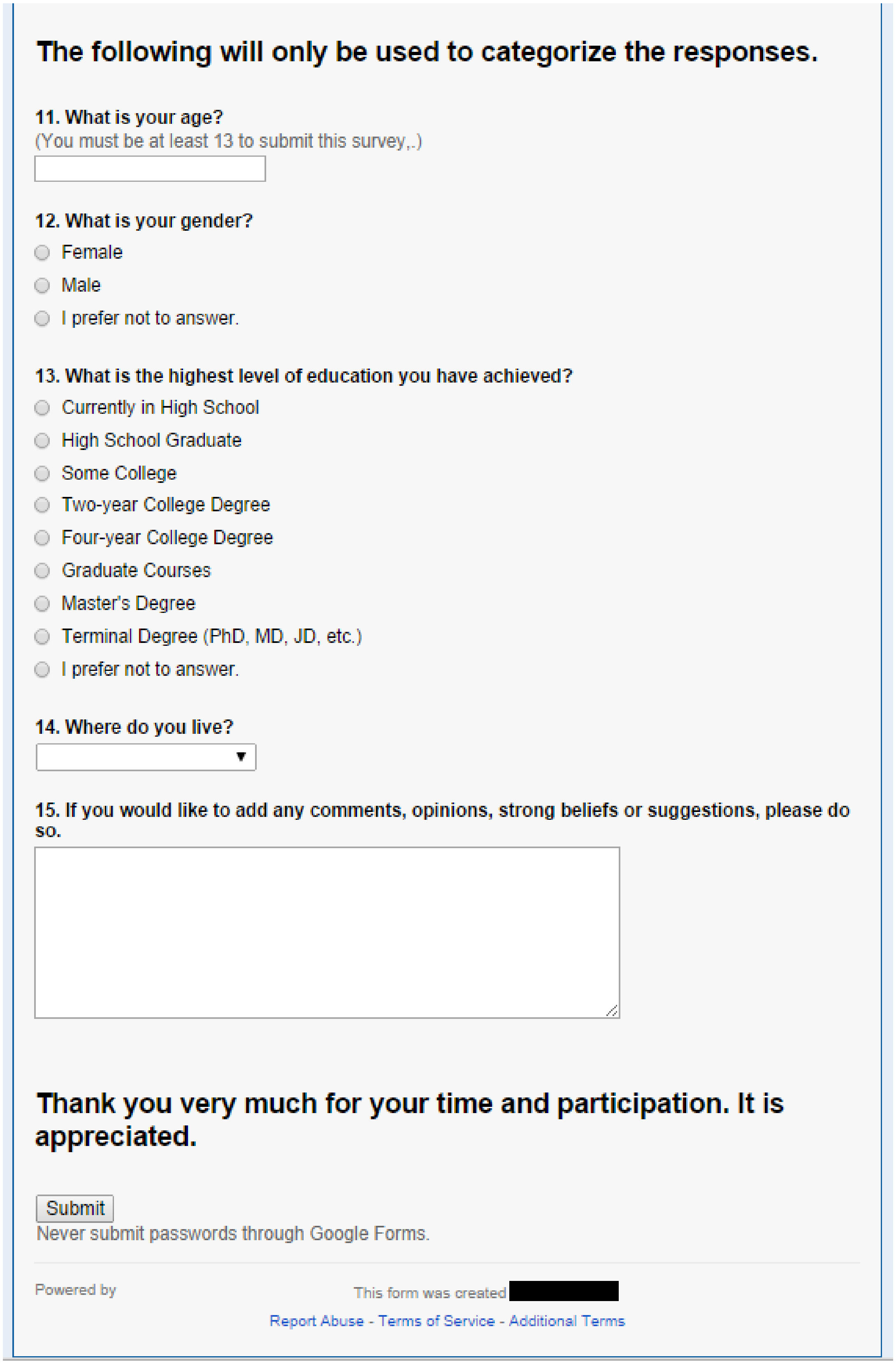
○ Yes

○ No

○ I don't know

○ I prefer not to answer.

Screenshot 2 - Survey Questions 5 -10



The following will only be used to categorize the responses.

11. What is your age?
(You must be at least 13 to submit this survey,.)

12. What is your gender?

○ Female
○ Male
○ I prefer not to answer.

13. What is the highest level of education you have achieved?

○ Currently in High School
○ High School Graduate
○ Some College
○ Two-year College Degree
○ Four-year College Degree
○ Graduate Courses
○ Master's Degree
○ Terminal Degree (PhD, MD, JD, etc.)
○ I prefer not to answer.

14. Where do you live?

▼

15. If you would like to add any comments, opinions, strong beliefs or suggestions, please do so.

Thank you very much for your time and participation. It is appreciated.

Submit

Never submit passwords through Google Forms.

Powered by

This form was created [redacted]

Report Abuse - Terms of Service - Additional Terms

Screenshot 3- Survey Questions 11 – 14

APPENDIX B

R Script used to generate random sample

```
library(XLConnect)
library(psych)
GenerateRandomAnswer <- function(x) sample(1:x,1,replace=TRUE)
# rows needed to match actual/real sample
TotalRowsNeeded <- 150
# import spreadsheet with question columns and range of answers
data.df = readWorksheetFromFile("privacyTemplate.xlsx", sheet=1)
TotalColumns <- length(data.df)
# initialize answers.df
answers.df <- data.frame (0,0,0,0,0,0,0,0,0,0)
# copy column names from template spreadsheet
names(answers.df) <- names(data.df)
# change column names in the dataframe to shorter names for ease in working
for (i in 1:TotalColumns) {
  names(data.df)[i] <- paste('X',i,sep="")}
# generate random answers for each question (hardcoded qty) for total number of rows
for (r in 1:TotalRowsNeeded){
  result1 <- GenerateRandomAnswer(data.df[1,paste('X',1,sep="")])
  result2 <- GenerateRandomAnswer(data.df[1,paste('X',2,sep="")])
  result3 <- GenerateRandomAnswer(data.df[1,paste('X',3,sep="")])
  result4 <- GenerateRandomAnswer(data.df[1,paste('X',4,sep="")])
  result5 <- GenerateRandomAnswer(data.df[1,paste('X',5,sep="")])
  result6 <- GenerateRandomAnswer(data.df[1,paste('X',6,sep="")])
  result7 <- GenerateRandomAnswer(data.df[1,paste('X',7,sep="")])
  result8 <- GenerateRandomAnswer(data.df[1,paste('X',8,sep="")])
  result9 <- GenerateRandomAnswer(data.df[1,paste('X',9,sep="")])
  result10 <- GenerateRandomAnswer(data.df[1,paste('X',10,sep="")])
  newrow = c(result1,result2,result3,result4,result5,result6,result7,result8,result9,result10)
# add random answers to dataframe
  answers.df <- rbind(answers.df,newrow)
}
# remove initial row of all 0s
answers.df <- answers.df[-1, ]
# calculate correlation matrix for generated answers and copy to dataframe
random.cor = cor(answers.df)
random.df <- data.frame(random.cor)
# open new spreadsheet and create a sheet with generated responses and correlation matrix
wb <- loadWorkbook("PrivacyRandomize.xlsx", create=TRUE)
createSheet(wb, name="RandomResponses")
createSheet(wb, name="Correlation")
writeWorksheet(wb,answers.df,sheet="RandomResponses")
writeWorksheet(wb,random.df,sheet="Correlation")
saveWorkbook(wb)
# after saving spreadsheet, change column names to shorter version for convenience
names(answers.df) <- names(data.df)
# read actual responses from spreadsheet into dataframe
real.df = readWorksheetFromFile("Privacy Survey 201405.xlsx",sheet="Form Responses")
# spreadsheet contains extraneous information (Answer literals / demographics)
# remove extraneous information from real.df so that it matches format of generated responses
real.df[27] <- NULL
real.df[26] <- NULL
real.df[18] <- NULL
real.df[17] <- NULL
real.df[16] <- NULL
real.df[14] <- NULL
real.df[13] <- NULL
real.df[12] <- NULL
real.df[11] <- NULL
real.df[2] <- NULL
real.df[2] <- NULL
real.df[2] <- NULL
real.df[2] <- NULL
real.df[2] <- NULL
real.df[3] <- NULL
real.df[3] <- NULL
real.df[3] <- NULL
# remove rows that don't contain data
real.df <- real.df[complete.cases(real.df), ]
# reorder columns in real.df so that it matches answers.df (generated)
real.df <- real.df[c(1,4,5,3,6,7,2,8,9,10)]
# change column names to match answers.df (generated) (short version)
names(real.df) <- names(answers.df)
# use the describe function from the psych library to calculate mean/median/sd/etc.
describe(real.df)
describe(answers.df)
```