Exploring the Relationship between Online Privacy on Cyber Security

Samar Fumudoh
Usha Viswanathan
2014

Master of Arts (60 credits)
Master of Science in Information Security

Luleå University of Technology
Department of Computer Science, Electrical and Space Engineering
Exploring the relationship between online privacy on cyber security

Authors: Samar Fumudoh & Usha Viswanathan

June 2014

A7007N
Magister Thesis in Information Security
Department of Computer Science, Electrical and Space Engineering
Luleå University of Technology
ABSTRACT

The aim of this research is to explore the relationship between online privacy and cyber security. With the birth of the internet and the recent revolution in technology, people have taken to the internet by storm - to do their online shopping and to connect to friends via social media. Online privacy has become a great concern to many while attitudes on security are still maturing. This thesis is based on a quantitative research methodology. The first part of the report looks into the definitions of privacy, cyber security and also the relationship between these two terms. The second part of the research incorporates the findings of a survey that was conducted as part of the thesis. The research found that while people are consciously trying to improve their online privacy, they seem to be subconsciously lowering the barriers on their privacy.

KEYWORDS

Privacy, Security, Cyber, online privacy and cyber security
TABLE OF CONTENTS

ABSTRACT ................................................................................................................................. 2
KEYWORDS ................................................................................................................................. 2

1 INTRODUCTION ..................................................................................................................... 4
  1.1 Problem Area ..................................................................................................................... 4
  1.2 Motivation .......................................................................................................................... 4
  1.3 Research Objective .......................................................................................................... 5
  1.4 Assumptions ...................................................................................................................... 5
  1.5 Limitations ......................................................................................................................... 5

2 LITERATURE REVIEW ........................................................................................................... 6
  2.1 What is privacy? .................................................................................................................. 6
  2.3 Concern for privacy ............................................................................................................ 6
  2.4 What is cyber security? ....................................................................................................... 8
  2.5 User attitude towards cyber security ................................................................................. 9
  2.6 Online privacy vs. Cyber security ...................................................................................... 9

3 METHODOLOGY ................................................................................................................... 11
  3.1 Hypothesis ......................................................................................................................... 11
  3.2 The sample and sampling procedure ............................................................................... 11
  3.3 Instrumentation .................................................................................................................. 11
  3.4 Data collection ................................................................................................................... 11
  3.5 Data analysis ..................................................................................................................... 11

4 SURVEY RESULTS ............................................................................................................... 12

5 DISCUSSION ......................................................................................................................... 16

6 CONCLUSION ......................................................................................................................... 17

REFERENCES .............................................................................................................................. 19

APPENDIX .................................................................................................................................... 21
Appendix 1 – Survey questionnaire and responses ............................................................... 21

List of Figures
Figure 1: Survey Results - Number of respondents................................................................. 12
Figure 2: Survey Results - Sharing personal information online........................................... 12
Figure 3: Survey Results - Users concern about security of information shared online .......... 13
Figure 4: Survey Results - Importance when browsing the internet........................................ 13
Figure 5: Survey Results - Respondents who read user agreements and privacy statements.... 13
Figure 7: Survey Results - User Opinion (1).......................................................................... 14
Figure 8: Survey Results - User Opinion (1).......................................................................... 14
Figure 6: Survey Results - User Opinion (1).......................................................................... 14
1. INTRODUCTION

1.1 Problem Area

Today the internet is bigger than what anyone anticipated it would ever become. Since the early 90’s the internet has had a ground-breaking impact on society in general and more importantly on businesses. What was once a mere way of sharing information has become, in a way, a database containing an extremely diverse wealth of information. There are blogs, social networking sites, discussion forums and an array of online shopping sites. Corporate organisations use the internet in a variety of ways to promote their business and individuals use social networking sites and blogs to virtually publicise their own lives.

Privacy is defined as the right to be free from surveillance and to determine whether, when, and to whom one’s personal or organisational information is to be revealed. Companies such as Facebook have privacy policies and might protect your private information from outside intruders, but what are they doing with your information and who are they sharing it with? In the same way, big corporations might have secure networks to protect from hackers and other cyber criminals, but what are they doing with your information and who are they sharing it with?

With all this information that is now openly available on the internet, the issue of privacy has made it to the frontline of many debates relating to the internet. Most websites have some sort of policy pertaining to ensure your privacy. Facebook, Yahoo, Google are just a few of the organisations that people freely sign up to trusting that their personal information will be secure. Although there appears to be numerous researches and studies in relation to individual privacy on the internet and also separately on cyber security, there appears to be little research that explores the relationship between individual privacy and cyber security. In particular, there was a lack of studies that examined whether the concern of one concept can lead to a weakness in the other.

The problem area driving the research for this thesis is the magnitude in which personal information is currently shared online and its security or lack thereof.

1.2 Motivation

Privacy makes us (those who use the internet) feel secure and safe in knowing that our personal details are in fact private. Without this concept of privacy it would be difficult to achieve any form of security. Many cyber criminals like to specifically target organisations that hold private information about individuals. Knowing this threat, businesses have taken steps to protect their networks and in particular the private information they hold on individuals.

In essence, by protecting individual’s private data, they have tried to ensure security. On the one hand it is important to protect the privacy of individuals yet on the other hand it is vital to implement security. When you share your data with a company, they can ensure it is kept private by keeping it away from the outside world yet it is still stored and kept by them.

Everyone is always focused on privacy and what is happening to their personal data. They want to be sure that it does not come out into the public domain. By constantly putting the focus on privacy, is it possible that the actual issue at hand – security – has been sidestepped? What is the relationship between online privacy and cyber security? Is it the achievement of keeping data private that entails whether security has been attained?
1.3 Research objective

This research was aimed specifically at trying to explore the relationship between individual privacy and cyber security and examine the impact (if any) online privacy has on cyber security. Simply put, this research aims to consider if privacy is possible without security and whether online privacy and cyber security are two very distinct notions.

1.4 Assumptions

This thesis is based on the assumption that people are highly concerned about the privacy of their online personal information and its security.

1.5 Limitations

This study will review mainly published academic research, in English, which is accessible through the Internet. However, as part of the research a small survey will also be carried out. The size of the respondents is expected to be small and no predefined sampling will be conducted. As such the findings of the survey will not be treated as definite and while no direct conclusion will be drawn from the findings, the findings of the survey will used in reflecting and comparing with findings of other academic research that may be found.
2. LITERATURE REVIEW

2.1 What is privacy?

The literature review provided some interesting definitions for the term privacy. In one of its oldest definitions, Warren and Brander (1890) described privacy as the ‘right to be let alone’. While this is a simple enough definition of privacy, Westin (1967) provided a slightly more elaborate definition noting that privacy was a form of individual control over disclosure and subsequent uses of one’s personal information.

Everyone likes to have some sort of privacy and we all (some more than others) have information that we like to keep to ourselves and in essence private. Posner (1978) remarked that while all people have information which they are interested in concealing, that same information is of value to others. The first group of people are concerned about “privacy” while the second group is into “prying”. One could argue that this statement is perhaps not quite accurate or perhaps no longer accurate. In this age of information and technological evolution, a third type of person has made their way to the forefront of the privacy debate. It is no longer about those who simply like to “pry”. Now, we have the cyber criminals who, pry but do so with bad intentions such as stealing your private or personal information.

A classic example of this is the recent eBay account hacking incident. Here, hackers were successful in compromising a small number of employee log-in credentials which gave them access to the company’s corporate network. Subsequently, the hackers were able to access eBay customer’s names, their encrypted passwords, email, registered addresses, phone numbers and date of birth. These were the private details provided by the consumers to a company trusting that the information will be secure (Kelly, 2014), but which were compromised by the cyber criminals who like to pry with bad intentions.

Like a lot of other research on privacy, Miyazaki & Fernandez (2001) explored risk perceptions in relation to online shopping and pointed out that the biggest concern amongst users was indeed their privacy. Almeida (2012) explains that individual privacy is largely an illusion and that in the online world, people, organizations, and governments hear not only what is public but also what should remain private. Almeida (2012) stressed that to tackle the issues relating to individual privacy, one would require a multidisciplinary approach that aligns knowledge from social sciences and humanities with computer science.

2.2 Concern for privacy

Plenty of studies have been carried out looking into people’s concerns in relation to online privacy, particularly with regards to personal information. For instance, a research done by Hoffman et.al (1999) revealed that online consumers are concerned about whether web providers sell their personal information to third parties without their consent or knowledge. Over 80 percent of consumers simply did not want their information to be resold to other businesses.

Similarly, in 2002, a survey conducted by Harris Interactive found that the majority of consumers are concerned about losing control over how personal information is collected and used by companies. Around 75 percent of respondents were concerned about the threat of
their personal information falling into the hands of third parties (individuals or companies). Interestingly, a study by Westin (1997) found that consumers were willing and felt comfortable in providing information to a web site, but only if the site provided notice about how the information collected would be used prior to disclosure. Acquisti and Grosslags (2005) suggest that mostly consumers do not have enough information to make privacy sensitive decisions and even when they have information, they are likely to ignore long term privacy concerns for short term gains.

White et. al (2008) carried out a study to determine if confidence in using computer technology related to the four information privacy components. The two most relevant to this research are unauthorized secondary use, and improper access. The findings of this study support the idea that internet users can walk away if inappropriate information is requested and although they are most concerned about unauthorized access and secondary use of personal information, their judgment of their ability to control the computer is not a consideration. That is to say that although privacy is an issue to us, we fail to realise that we are indeed in control of the data that we share, and, if something seems good now, we are more likely to want to enjoy the current buzz than to worry about the future implications of our personal information.

Furthermore, a study conducted by Park et al. (2012) revealed that privacy concerns did not directly play a meaningful role in guiding users’ information behaviour. They found that interplay between knowledge, concern and reward played a significant role in determining information behaviour. So, while White et.al (2007) argue that we are in fact in control of the information we share, Park et. al (2012) mean that companies can manage people’s behaviour by offering them some form of reward and hence making them more willing to share their personal information.

Klve & Mulder (2008) argued that privacy, as a constitutional right, is subject to changing norms as a result of the advent of information society. In considering all the above research findings, it could be argued that the best practice for ensuring control over ones’ personal information is to read the privacy notices or policies of websites and to learn about the organization’s information practices.

Studies done by Culnan & Milberg (1998) claimed that this information can help the consumer decide whether or not to disclose personal information to the website. This can also reduce the risk of exchange of information to third party. Furthermore, in a rather recent study conducted by Lin (2012) it was concluded that privacy policies should be designed with the user's viewpoint in mind.

It is fair to say that most privacy policies usually have the users interests at heart simply by ensuring that the personal data will remain safe and out of the public domain. The remainder of the policy is actually there to support the company rather than the user. In fact, some social networking sites will only let you join if you agree for them to share at least some of your personal data with third parties e.g. Facebook.
2.3 What is Cyber Security?

Cyber security can be defined as the protection of the systems, networks and the data that is held in cyber space. It refers to the set of technological mechanisms that mediate the requests for access or control of the data that is held within a system (Bambauer, 2013). Simply put, cyber security consists of the process and the procedures that keep the information, in this case – personal information – protected.

Key to the field of cyber security is the rapid development in new technologies. These have been revolutionary and if anything extraordinary, however, with these new technologies, new unprecedented threats and risks have emerged, particularly in relation to online privacy. These threats are manifold but for the purpose of this review we will be looking at general cyber crime particularly amongst online retailers and social networking sites.

While cyber security has evolved over the years, it is not new and has been the subject of discussion in government, industry and academia for some time (Rowe et. al 2011). Several studies have been conducted within the field of cyber security with regards to privacy and one of the risks identified is in relation to retailers onwards distribution of personal information. Such onward distribution of personal information is normally done as a form of online behavioral targeting. This form of targeting is a marketing practice of collecting and compiling a record of individual consumers’ online activities, interests, preferences, and/or communications over time and across websites in order to deliver personalized advertising.

In 2013, Jai et.al conducted a study into behavioral targeting of consumers. This study found that although consumers may initially share personal information with online retailers to either complete purchase transactions or participate in a consumer loyalty programs, retailers also use, sell, or share such information for secondary marketing purposes. It is worth nothing that the term behavioral tracking refers to tracking that has not been expressly authorized by the consumer after the consumer has been given adequate notice of the information privacy practices of the company doing the tracking.

Another risk to the security of personal information is the regular use by retailers of small text files called ‘cookies’. Research by Miyazaki (2008) in stated that many online retailers allow third party advertisers to put cookies into the Internet browser programs on consumers’ computer drives. These cookies allow the third parties to track the browsing behaviors of the users and provide enough knowledge which helps them to provide personalized advertisements.

While cookies were not so common in the early years of the internet, it has now become common practice for websites (most of whom rely on cookies) to notify you that they are indeed using cookies to track your online behaviors. Although cookies do not track your personal identifiable information such as your name and address, they do track your internet browsing with the hope of customizing your user experience.

One example for this can be found in a CNN.com report (2005) which talks about the variable prices offered to the customers by Amazon.com. In 2000, one Amazon.com customer deleted the cookies on his computer and the website identified him as a regular user. The result was that the price of a DVD offered to him for sale drop from $26.24 to $22.74. Ultimately, Amazon.com ended up publicly apologizing and refunding all customers.
who had paid the higher prices. Another report by New York Times (2010), talks about retargeting advertisements. These are advertisements which are customized for a particular user based on his or her browsing history. The FTC Report (2012) stated that the browsing habits of consumers both online and offline are tracked analyzed and then shared and used instantaneously without the user knowledge. All the above discussions of course have sparked a lot of research interests in user attitude towards cyber security.

### 2.4 User attitude towards cyber security

A study by Berendt et al. (2005) exploring user behaviors found that there is disparity between the concern for privacy and the disclosure of information. Users, when given the right circumstances, completely forget the concerns of privacy and disclose even the most personal details without any compelling reasons. This is true when the online exchange is entertaining and appropriate benefits are offered to the users. Research has also found that people perform a simple risk-benefit calculation in deciding whether or not to disclose their personal information.

A study by Jarvenpaa & Tractinsky (1999) found that trust had a negative influence on risk perceptions that is the trust the users have on a vendor will reduce the amount of anticipated risk. A study by Malhotra et al. (2004) found that this trust can mitigate the customer’s reluctance in releasing personal information. Another study by Dommermeyer & Gross (2003) showed that while consumers were well informed on privacy-protection strategies, their use of these strategies was quite low. Weber (2010) argued that actions to remain secure and private are often passive and a secondary task in the situation. For example, some social networking sites will only let you join if you agree for them to share at least some of your personal data with third parties. Here the users have clearly overlooked the need for privacy.

All the above concerns have resulted in a number of recommendations. The foremost among these is the FTC (2010) recommendation which asks the behavioral advertising industry to offer consumers a “do not track” mechanism which asks the consumer whether his browsing habits can be tracked or not. Subsequently, companies like Microsoft, Mozilla and Google have announced the plans to modify their Internet browsers to include “do not track” features that will enable users to limit online tracking (Bradley, 2011).

### 2.5 Online Privacy vs. Cyber Security

The terms online privacy and cyber security are two different entities that are quiet often intertwined with each other. However, it is important to note that privacy relates to keeping personal information private and away from the prying eyes while cyber security is about keeping the systems in which information is held safe and protected. This has been noted by Rombel (2001) who nicely pointed out that though interrelated, privacy and security are really separate issues with different dynamic subtleties. Similarly, Bambauer (2013) mentions that privacy and security can and should be treated as distinct matters.

Although plenty of information is available about online privacy and separately about cyber security, little research is available in relation to the link between privacy and security. Even so, it has been found that there is a significant overlap in the research on privacy and
that of security. Perhaps this is not surprising given that security mechanisms are in place to protect systems which contain the information that we want to keep private. As such, it is difficult to study the one without mentioning the other. Bambauer (2013) states that security is an interface layer between information and privacy. While privacy, as mentioned earlier is about keeping the information away from prying eyes, security helps mediate those rights to privacy and helps put them into effect.

In a study by Pirim et al (2008) an instrument was developed and tested to measure an individual’s perceived need for security and perceived need for privacy. The instrument was found to be highly reliable and a significant relationship was found between the perceived need for privacy and perceived need for security constructs. So, while it is evident that people require both privacy and security, not much is mentioned in relation to the link between privacy and security. Does giving more information mean better security or does better security mean giving less information?

An interesting find in this research was the work of Kleve and Mulder. Kleve and Mulder (2008) looked into the relationship between safety and privacy and observed that privacy and safety do not have to be opposites per se and that the one can indeed affect the other. Furthermore, they argue that safety is not in opposition to privacy, but an aspect of it. That is to say that while privacy and security are two different notions, security helps make what privacy is. While security keeps personal information private, online privacy could not be achieved without adequate security.

A good example of just how one helps make up the other is the case of the Acxiom data breach that took place between 2002 and 2003. In this data breach Acxiom exposed sensitive consumer data three times. The first breach was carried out by contractor that was working with Acxiom and the other two by outsider threats. Here, security was inadequate, and as a result personal customer data was accessed. So, while security could be a standalone entity, privacy cannot be achieved without ample security.
3. METHODOLOGY

3.1 Hypothesis

In carrying out this research, a quantitative study was carried out. In doing so, the following hypotheses were used.

1. Online privacy strengthens cyber security.
2. Online privacy weakens cyber security.

3.2 The Sample and Sampling Procedure

Given the scope and the time frame that was available to carry out this study, the chosen sample for the research was small. Our main focus in selecting the sample was that the chosen individuals were IT literate and regularly used the internet. Consequently, the primary target was fellow students and a few staff members at Lulea University of Technology (LTU), while the secondary target were our friends, family, co-workers and their onward networks. In total, 100 LTU students and staff were invited to partake in the study and an estimated 30 friends, family and co-works were selected.

3.3 Instrumentation

To carry out the quantitative study, we chose to conduct an online survey. This was deemed to be the most straightforward and perhaps most trouble-free for the chosen participants. An online questionnaire was created with 10 compulsory questions for the participants to complete. 9 of the questions were multiple choices while 1 allowed for an open answer. The questions chosen for the questionnaire were aimed at gathering views and insights of people perceptions of online privacy and cyber security and also their online habits in terms of privacy. A list of the questions and the answers received can be found in Appendix 1.

3.4 Data Collection

Respondents were given 1 week to complete the survey. To ensure accuracy in the data collection and to avoid duplicate responses, the online questionnaire was restricted to one response per machine. Also, to avoid blank responses, all the 10 questions were made compulsory. That is to say, the questionnaire could not have been submitted unless all 10 questions were answered.

3.5 Data Analysis

Once the survey closed and the respondents were no longer able to submit their responses, the data was analysed. To analyse the data a descriptive approach was used. A descriptive approach is used when the researcher has no control over the variables and the researcher only reports what is happening or has happened. As the sample size was small and the aim of our study was to understand the present state of affairs, the descriptive research approach was well suited for our study.
4. SURVEY RESULTS

Approximately 130 participants were provided with the link to complete the online questionnaire. The survey was open for 1 week and then closed automatically and no further submissions were allowed. In total, 33 completed surveys were received. Given the time scale and the number of individuals invited to complete the survey, it was found to be a reasonable amount of responses, but, it also meant that the results could not provide a definite conclusion as to the findings. They could however be used together with the results of the qualitative study to get a more comprehensive view of people’s perception of online privacy and cyber security. Not surprisingly, 75% of the respondents were aged between 30 and 49. This is perhaps a reflection of the chosen sample which was mainly fellow students at LTU.

When asked about how they felt about sharing their personal information online, 18 of respondents felt fine about it but tried to keep it to a minimum while 14 would rather not share any information online.

Furthermore, when questioned about how concerned they were about the security of the information that they had actually shared online, 17 were very concerned, 11 were slightly concerned, while 5 were not bothered by it.
Exploring the relationship between online privacy on cyber security

Respondents were further questioned about their preferences when browsing the internet. They were given 3 choices and asked to choose which of the 3 were more important to them when browsing the internet. Here, 19 felt that ensuring their details remained private and secure and not shared with third parties or the general public was the most important while 12 felt that ensuring their personal information remained private so only they could see it was the most important.

It was clear to see from the responses received, that the majority of participants felt strongly in relation to the privacy of their information, and while they had strong views as to what should and should not be done with their information, only a very small percentage actually read the privacy statement and user agreements before downloading files from the internet. While this is not enough to draw a particular conclusion, one could argue that while people have tough boundaries in regards to their online privacy, they are not being proactive in ensuring its security. Also, the survey found that more than have of respondents hardly ever or never read the user agreements and privacy statements before downloading or installing programs or files from the internet.
The remainder of the questionnaire was used to establish people’s perception on a number of different statements in relation to online privacy and cyber security. The majority of respondents seemed to agree in that whether or not they kept their personal information online private, it would still not be secure.

Similarly, the majority of people questioned did not feel that keeping their personal information private would make it less secure. There seemed to be an equal dispersal of agreement and disagreement with the final statement “If I keep my online personal information totally private then my information will be totally secure?”.

Finally, the last portion on the survey set out to gain peoples understanding in relation to the concept of online privacy and cyber security. Here, participants were asked to, describe their understanding of the difference between online privacy and cyber Security. While some responses were one worded, others were insightful. For instance, some respondents wrote the following:

“Cyber security involves using available solutions to protect networks and anything linked to the network from being attacked to gain unauthorized access or to cause damage. Online privacy depends on information you have provided about yourself on the internet. The more you give, the more you would be
concerned about online privacy and the more information a hacker would get if they bypass cyber security.”

“On-line privacy is about keeping your on-line presence secure, not having what you do interfered with or tracked by cookies etc. Cyber security deals more keeping the data you do make available on-line safe. this may include keeping it safe from hackers”

“Privacy doesn't necessarily mean security while the other around is usually true - security almost always includes privacy.”
5. DISCUSSION

The key question that was guiding the research for this thesis was how the concern for privacy impacted on the concern for security. A wealth of information was available in relation to online privacy and then again in relation to cyber security, but when searching for research that compares or explores the link between the two, it was limited. As such, with the help of the quantitative study we were able to add depth to this research.

It is fair to say that the research found a great deal of focus is being put on privacy, more so about people’s concern in relation to their online privacy. However, in this endeavour, is it possible that the actual issue at hand – security – has been sidestepped? By looking separately into the issue of cyber security in regards to online personal information, a number of different studies have been conducted. As mentioned earlier, a study by Berendt et al. (2005) explored user behaviors and found that there is disparity between the concern for privacy and the disclosure of information. Users, when given the right circumstances, completely forget the concerns of privacy and disclose even the most personal details without any compelling reasons.

This is an interesting finding, especially if it coupled together with the findings of the survey conducted. It was clear to see from the responses received, that the majority of participants felt strongly in relation to the privacy of their information, and while they had strong views as to what should and should not be done with their information, only a very small percentage actually read the privacy statement and user agreements before downloading files from the internet.

That is to say, while users have voiced great concern about the privacy of their online information, they too are partly to blame for the lack of it. While privacy statements and user agreements are available for them to read, they tend ignore them. Even if they choose to read them, and if the risk to the privacy of their personal information is high but they are somehow provided with a reward for accepting the user agreement, they tend to ignore the risk.

In terms of privacy, it is apparent from the research that people are willing to sacrifice some part of their online privacy. They are willing to do this in order to achieve a greater freedom. To be able to register with web sites, do their online shopping and connect with friends through social media. With this sacrifice comes the increased risk in relation to the privacy of their online personal information and also the security of it.

One could argue that it appears that people are consciously voicing concern about their online privacy, yet subconsciously they are agreeing to less online privacy. By allowing web site and other third parties access their data, they are inevitable creating greater security risks for themselves. Hence, by unconsciously weakening their concern for privacy, they are also weakening their concern for security.
6. CONCLUSION

This thesis was aimed specifically at trying to explore the relationship between online privacy and cyber security and to examine the impact the concern for privacy has on security.

Privacy can be defined as the right to be free from surveillance and to determine whether, when, and to whom one’s personal or organisational information is to be revealed. Cyber security can be defined as the protection of the systems, networks and the data that is held in cyber space. The terms online privacy and cyber security are two different entities that are quiet often intertwined with each other. However, it is important to note that privacy relates to keeping personal information private and away from the prying eyes while cyber security is about keeping the systems in which information is held safe and protected.

In carrying out the research, the following hypotheses were used:

1. Online privacy strengthens cyber security.
2. Online privacy weakens cyber security.

The research found that although privacy is an issue to us, we fail to realise that we are indeed in control of the data that we share, and, if something seems good now, we are more likely to want to enjoy the current buzz than to worry about the future implications of our personal information. It was clear to see that the people feel strongly in relation to the privacy of their information, and while they had strong views as to what should and should not be done with their information, the survey found that only a very small percentage actually read the privacy statement and user agreements before downloading files from the internet.

Therefore, in relation to whether online privacy strengthens cyber security, one could argue that although in theory this could seem true, the reality is that while people are consciously trying to improve their online privacy, they seem to be subconsciously lowering the barriers on their privacy. As such, it is more likely that online privacy is leading to weaker cyber security. That is to say, while more and more personal information is being released to third parties, the risks in terms of the security surrounding that data is likely to be increasing.

In considering the research findings, it could be argued that the best practice for ensuring control over ones’ personal information is to read the privacy notices or policies of websites and to learn about the organization’s information practices.

In view of the findings of this research, further studies into the relationship between online privacy and cyber security are urged. As mentioned earlier, with more and more personal information entering cyber space, it is evident that should data breaches take place, more private data would be at risk.
REFERENCES

Exploring the relationship between online privacy on cyber security

- Harris Interactive, 2002. First major post-9-11 privacy survey finds consumers demanding companies do more to protect privacy; public wants company privacy policies to be independently verified.
- Patel, V., Juric, R., "Internet users and online privacy: a study assessing whether

Appendix 1

Survey Results
Privacy vs. Cyber Security

Total number of respondents = 33
Timeframe: 22/05/2014 – 28/05/2014

1. What is your age?

<table>
<thead>
<tr>
<th>Answer choices</th>
<th>under 20</th>
<th>20-29</th>
<th>30-39</th>
<th>40-49</th>
<th>50-59</th>
<th>60-69</th>
<th>70-80</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responses</td>
<td>0</td>
<td>6</td>
<td>20</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

2. How do you feel about sharing your personal information online?

<table>
<thead>
<tr>
<th>Answer choices</th>
<th>Fine by me</th>
<th>Fine by me but I try to keep it to a minimum</th>
<th>I'd rather not</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responses</td>
<td>2</td>
<td>18</td>
<td>14</td>
</tr>
</tbody>
</table>

3. How concerned are you about the security of the information you have shared online?

<table>
<thead>
<tr>
<th>Answer choices</th>
<th>Very concerned</th>
<th>Slightly concerned</th>
<th>It doesn't bother me</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responses</td>
<td>17</td>
<td>11</td>
<td>5</td>
</tr>
</tbody>
</table>

4. When browsing the internet which is more important: (a) Your personal information remains private and only you can see it (b) Your personal information remains secure but the companies or social networking sites you have registered with can share your details with third parties without leaking it into the public domain OR (c) Your details remain private and secure and are not shared with third parties or the general public

<table>
<thead>
<tr>
<th>Answer choices</th>
<th>(a)</th>
<th>(b)</th>
<th>(c)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responses</td>
<td>12</td>
<td>2</td>
<td>19</td>
</tr>
</tbody>
</table>

5. Do you read user agreements and privacy statements before downloading or installing programs or files from the Internet?

<table>
<thead>
<tr>
<th>Answer choices</th>
<th>Always</th>
<th>Sometimes</th>
<th>Hardly ever</th>
<th>Never</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responses</td>
<td>2</td>
<td>8</td>
<td>14</td>
<td>10</td>
</tr>
</tbody>
</table>
6. What is your opinion on the following statement: If I keep my online personal information totally private then my information will be totally secure.

<table>
<thead>
<tr>
<th>Answer choices</th>
<th>Strongly Agree</th>
<th>Agree</th>
<th>Strongly disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responses</td>
<td>3</td>
<td>13</td>
<td>17</td>
</tr>
</tbody>
</table>

7. What is your opinion on the following statement: Keeping my online information private will make it less secure?

<table>
<thead>
<tr>
<th>Answer choices</th>
<th>Strongly Agree</th>
<th>Agree</th>
<th>Strongly disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responses</td>
<td>3</td>
<td>6</td>
<td>24</td>
</tr>
</tbody>
</table>

8. What is your opinion on the following statement: Whether or not I keep my personal information online private it is still not secure?

<table>
<thead>
<tr>
<th>Answer choices</th>
<th>Strongly Agree</th>
<th>Agree</th>
<th>Strongly disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responses</td>
<td>14</td>
<td>15</td>
<td>7</td>
</tr>
</tbody>
</table>

9. How comfortable are you in sharing your personal details while creating an online account?

<table>
<thead>
<tr>
<th>Answer choices</th>
<th>Very much concerned</th>
<th>Worried a little</th>
<th>I'm cool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responses</td>
<td>7</td>
<td>18</td>
<td>8</td>
</tr>
</tbody>
</table>

10. In a few words, please describe your understanding of the difference between online privacy and cyber Security.

*Online privacy refers to personal information to be safe but cyber security relates to safeguarding the computers exposed to internet.*

*Privacy doesn’t necessarily mean security while the other around is usually true - security almost always includes privacy.*

*Online Security concerns the individual and their interests. cyber security has to do with a bigger scale and not only with information.*

*Online privacy means your information isn't shared with others other than the intended website. Cyber security is about security measures the website has to take so that unauthorised access is revoked.*
**Online privacy means that my details are not shared to a third party by the company. Online privacy nowadays does not mean you are foolproof from cybercrimes. Online privacy does not guarantee cyber security.**

**Online privacy are not under your own control**

**Online privacy is keeping information private and secure cyber security can mean sharing private information across secure channels.**

**Privacy is for the individual cyber security is for the network. Cyber security has no effect or correlation to privacy.**

**Even if my information is private, meaning "it is not shared with the general public", it may not be secure, because organizations, firms, intelligence agencies, governments, etc. may still have access to it.**

**On-line privacy is about keeping your on-line presence secure, not having what you do interfered with or tracked by cookies etc. Cyber security deals more keeping the data you do make available on-line safe. this may include keeping it safe from hackers.**

**Online privacy is important for individuals, cyber security is important to companies.**

**Security to my understanding refers to viruses as well, it is a broader term.**

**Cyber security involves using available solutions to protect networks and anything linked to the network from being attacked to gain unauthorized access or to cause damage. Online privacy depends on information you have provided about yourself on the internet. The more you give, the more you would be concerned about online privacy and the more information a hacker would get if they bypass cyber security.**

**Cyber security is when ur info is not safe, such as ssi and passwords etc ..**

**I don't really understand it which now makes me worried on how easily I do give personal details**

**Privacy is sharing my info when I want to, cyber security is online companies keeping the info I have shared secure and protects it as I protect my own info.**

**I am just guessing but I imagine online privacy to be about what happens to information I share voluntary. Is it then sold on to third parties etc? Cyber security I imagine to be about the technical side of things. Ie when I am doing online banking or buying something - how secure is that information? But I don't know the right answer to this!**

**Online privacy controls what can be seen by third parties on purpose while Cyber security's job is to make sure it can't be seen by third parties who are not intended to see it.**

**The terms are to different to compare**
In my View online privacy is which iam agreed to shared and hide ..where as cyber security is a global things..for suppose example :if im having an account on gmail..i can do my best to secure my information but how far and how much gmail is potential in providing me security to my data..

Security tries to ensure that privacy is not compromised

Online privacy refers to the ability of being in "stealth mode" while browsing the internet sharing zero data or personal info eg. cookies, forms etc.

online privacy is for me to choose what i want to share. cyber security is for others to handle that service such as antivirus firewalls etc

I think online privacy is how to policy and roles of how to share your information, who can see it and so on , while cyper security is chronology to protect your information like firewall , antivirus ,..etc

Privacy means keeping information to yourself and private while security ensures no other person has access to it.
Exploring the relationship between online privacy on cyber security