The People have spoken: An Assessment of User Awareness and Requirements of the Security of Open Wi-Fi Networks

Rick Clement
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands
r.clement@student.utwente.nl

ABSTRACT
With open networks becoming more and more prevalent in everyday life, their lack of security too becomes more concerning. By using these open networks, many users put their privacy at risk, regardless of whether or not they are aware of the risks. To protect users from these risks, a lot of research has been conducted aiming to make open networks more secure. However, many of these studies focus purely on the technical side of the issue and leave the users out of the equation, even though users have the ability to be more secure on open networks. Currently, though, there are little to no assessments of how aware users are of these possibilities, nor of to what their requirements of open networks are. This paper describes such an assessment in the form of a survey, asking users about their open network usage, their requirements for an open network, their awareness of their own security on open networks and whether they favour quality of service over privacy and security in certain situations. The results of the survey showed that, while privacy and security were not the most important aspects to the respondents, many ways that improve both at the cost of quality of service were rated more positively than negatively.

Keywords
Open Wi-Fi networks, security, privacy, quality of service

1. INTRODUCTION
More and more open Wi-Fi networks are becoming available to the public. From fast food chains and coffee shops to libraries and university campuses, people visiting these places can expect to be able to use the Internet as always: they can browse their usual websites and use their favourite apps to check their email, various social media and even perform online banking actions. These networks should be fast and reliable enough to fit the demands of modern Internet users, and in reaching those goals, some sacrifice the security of the connection, and thus possibly compromise the user’s privacy.

As these open networks allow users to satisfy their everyday internet needs for free and with relatively high speeds, it is no surprise they are becoming more popular and more available. With the popularity of these open networks rising, so will the concern of the privacy and security risks, though, and while researchers are coming up with more and more ways to secure both networks and applications, the opinions of the actual users seem to have been mostly overlooked or seemingly disregarded. Some possible methods that might help solve the problem are getting lower priority or are even discarded because it is assumed it would negatively impact the quality of service too much, like replacing the current access point discovery system of active probing for passive scanning [13] or using a virtual private network to allow users to transmit all data through an encrypted channel [14].

This research aimed to find out if users really preferred the quality of service of the current system over the more secure ways in which privacy and security could be enhanced on networks. Overall, it was found that, while respondents said they found privacy and security less important than other aspects of an open network, almost all ways in which quality of service would be sacrificed in favour of security and privacy were rated positively than negatively. Furthermore, it was found that more traditional personal data like names, physical addresses and bank details were often named to be at risk, but data like the MAC addresses of devices and locations the user has been or is at the moment were barely named at all.

1.1 Problem Statement
With the assumption that some of these methods will impact the quality of service of open networks for users too much, potentially, solutions that not only provide open networks with better safety measures but also retain a satisfactory quality of service will be discarded.

In order to prevent this from happening, an assessment needs to be made to determine the current state of user awareness regarding open networks: how much do users know about the security? To what extent are they willing to give up quality of service in order to make these networks more secure? Who do they feel is most responsible for the security of open networks and what ways do users feel are most useful to raise awareness? Making this assessment by creating and spreading a survey is the main point of this paper.

1.2 Research Questions
Based on the problem described in the problem statement, the following research questions have been defined:

1. What do users know about their privacy and security on open networks and what are their requirements of an open network?
2. To what extent do users value their privacy and security over quality of service on open networks?

3. Who do users feel should be responsible for the privacy and security of the users on open networks?

4. What ways of raising awareness about privacy and security risks are preferred by users?

2. RELATED WORK

Starting off, an excellent overview of the problem, some of the risks of free, open Wi-Fi networks and even some solutions are laid out by Dave Mancinelli [14]. However, for a deeper analysis of current vulnerabilities of open networks, other research has been done, all focusing on different risks and threatened personal data: de-anonymisation of users based on phone requests sent by their mobile devices [7], accurately compromising location privacy [9] and even a full characterisation of private personal information [5].

Minimising these risks is of course a priority, and research has been conducted to increase the security of users in open networks. Some enhance privacy at the discovery of the access points [13] and location authentication [4] in specific stages of the message exchange, while others enhance overall security by obfuscating possible personal data [3].

Research also exists on user security and privacy awareness. A study by Dodge et al. showed that phishing remains an effective way of illegitimately obtained private user information [8]. Krasser et al. propose the use of honeynets, networks of purposely vulnerable computer systems intended to be compromised, to help teach users more about cyber security risks [12]. However, both studies are aimed at very specific groups and are not related to open Wi-Fi networks.

Efforts have been made to increase awareness and give a possible way for users to increase their privacy and safety. BonnAl' et al. [2] not only proposed but also implemented and tested a system they called SASQUATCH that would draw the attention of smartphone users by showing anonymised information on a screen, offering a more in-depth and personal component, including several solutions users can employ to increase their safety and privacy. One of these solutions is an app they created themselves called PrivacyPolice that protects smartphone users against some of the attacks described in their work.

Ackerman et al. [1] held a survey pertaining users’ online privacy concerns, particularly in e-commerce. However, as of writing, this paper is 17 years old, and thus may no longer be accurate. The study found that overall, the respondents had a high level of privacy concern. A more recent survey was held in 2005 by Govani and Pashley [11]. Students of a university were asked about their reasons for joining the social network Facebook and if they were aware of its privacy settings or the privacy risks involved in using the service. Perhaps the most interesting finding of the study was that while the survey increased the awareness about online privacy of the students and identity theft and stalking were named as the primary privacy concerns, very little change in behaviour was noticed when the researchers revisited the accounts of those who had partaken in the survey.

3. METHODOLOGY

Before the research questions can be answered, we need a proper way to assess user awareness and knowledge. In order to reach that goal, several options are available: in order to see how users behave in open networks, observation could be useful. However, this method brings with it several problems. Firstly, this method is quite slow, and with the relatively short amount of time available to collect data, this method might not allow us to collect a sufficient amount of data that will allow us to make a proper assessment. Additionally, there are two ways in which users could be observed: either with or without their knowledge or even consent. Both methods have their own issues: clearly, observing people’s behaviour without their knowledge or consent is quite invasive of their privacy, especially when it involves them performing actions that they might want to remain private.

On the other hand, if observations are made with their knowledge and consent, their actions may change, as the users in question are now aware of the fact that they are being observed. On top of that, there is still the time constraint to consider: observations take considerably more time to carry out than spreading a survey that can yield multiple results simultaneously. For the reasons stated above, this method, in all of its possible instances, has been discarded.

The other methods involve asking several questions to users, either through direct interviews or a digital survey. Once again, both methods have their advantages and disadvantages. Like the observation method, interviews take a lot more time than some of the other proposed alternatives, but with the subject possibly involving several technical terms and concepts that some users might not be familiar with, having an interviewer with sufficient knowledge present to give deeper explanations might help the users give answers more in line with their thoughts.

The main advantage of the survey is that, unlike the earlier proposed methods, the entire recording of data is done by a single person: the user taking the survey. Without a researcher necessary to obtain the data directly, this method is by far the one with the highest collection potential. Not only that, the only necessity for people to take part in the survey is that they are able to connect to the internet, so a more varied set of users can be reached.

However, while the survey has the potential of reaching a lot more users simultaneously, it has the drawback of not being able to provide many answers users might have while taking the survey, meaning that all the questions asked in the survey must be defined as clearly as possible to prevent these confusions from popping up as much as possible. After consideration, it was decided that the benefits of the survey outweigh the downsides, and was ultimately chosen as the preferred option of collecting the data.

3.1 Creating the survey

With the survey chosen as the method of obtaining the necessary data, a plan needed to be made for its creation and spreading. As mentioned earlier, it is important that the questions and their introductions are as clear as possible to prevent any confusion. The structure of the survey is also important, and the order of questions will have to be defined in such a way that they approximately follow the order in which the research questions have been posed. To test that both of these issues were properly addressed, a draft of the survey was created prior to the spreading. This draft was then sent to several potential users, who were asked if they found the questions understandable and if there was any confusion while taking the survey. After this round of reviewing, the questions of the survey were finalised. The final survey was made using Google Forms [10], which automatically creates graphs for the answers of
multiple choice questions. This is highly desirable for the analysing stage of the research. A link to the full survey is provided in the references [6].

3.1.1 Defining the questions
In order to allow the survey to both properly follow the order of the research questions and to prevent users taking the survey to change their earlier answers based on questions asked during the process, the survey was split up into five sections, each of which will be described in more detail below.

Section 1: Personal information
The answers to the questions of the first section were mainly used to determine whether the entire group of people who took part in the survey are diverse in terms of their age and especially their field of education; the research aims to determine what a section of the general populace knows about open networks and the security concerns surrounding them, and a high amount of people with for instance a computer science background could imply skewed results. Furthermore, the subjects were asked how often they used open networks as well.

Section 2: Open network preferences
The second section of the survey asked the users about their preferences and behaviour when using open networks. First, users were given four aspects of networks and were asked to indicate how important these aspects were to them when using open networks. These aspects are connection speed, connection stability, service access (as in, no services are blocked or otherwise inaccessible) and privacy/security.

Next, users were asked about whether their behaviour changes or would change depending on the provider of the network, and if so, why. Finally, the respondents were given a selection of possible providers and were asked whether they would trust each provider to have provide a secure network and whether they had ever used a network provided by each of them.

Section 3: Data at risk
Section 3 consisted of a single, open question asking users what data they believe is at risk from adversaries while using open networks. This was included not just to determine whether or not people are aware of the safety and privacy risks while using an open network, but also what kinds of personal data are stored on their devices. The main reason for choosing a single question was that the goal of this particular question was an assessment on the knowledge of the respondents. Any additional questions regarding the same subject may have provided answers to the first question in the section, which would be counterproductive.

Section 4: Security/Privacy versus Quality of service
This section was made in order to help answer one of the main research questions: to what extent do users prefer their security and privacy over the quality of service of open networks? In order to test this, users were given a total of four situations in which the security of open networks could be improved and were asked to indicate whether they preferred the security of the new system or the quality of service of the old one on a five point semantic differential scale. These methods were the usage of Virtual Private Networks (VPNs), the blocking of unsafe websites and services by the network provider and two ways of changing the way in which devices discover access points of a network. One of these involves having devices scan for access points instead of sending broadcast messages, the other proposes decreasing the amount of information in the broadcast messages sent out by devices. The main challenge with this section was that the descriptions of each proposition had to be clear and complete, as not all users might be familiar with the inner workings of networks in general, but also short, as Google Forms places all questions in a very narrow space. Additionally, users taking the survey should not feel intimidated by very long and large blocks of text.

Section 5: Final Questions
The survey was ended with several general questions regarding open networks and network security. Firstly, users were given the buttons that are involved in creating, maintaining and using an open network. Then, they were asked to indicate how responsible they feel each actor is for the security of a user of an open network. Finally, the users were presented with several measures which are used to try and raise awareness. Then, the users were asked if they ever encountered the measure in question, and if so, rate how effective they felt it was. Once again, a five point scale was used, with the middle option being used to allow users to indicate that they have never encountered the method in question.

3.2 Spreading the survey
After the survey was finished and reviewed, the link to the survey was spread using several social media outlets like Facebook and Twitter. With Google Forms automatically recording survey results, the choice was made not to print any surveys to allow the usage of the statistics kept by Google Forms, as obviously external results would render parts of these statistics useless. In the end, fifty-six people filled out the survey.

3.3 Processing the data
Once the data was collected, it needed to be visualised and analysed in order to answer the research questions. Using the statistics gathered through the survey in Google Forms, the visualisation part was mostly completed automatically. Only the answers to the open questions need additional interpretation and visualisation.

4. RESULTS
After the data was collected the research questions could be answered by analysing the results. This section describes the results from each section of the survey in detail.

4.1 Section 1: Personal information
The main purpose of the first section was determining whether the group of users that had taken the survey was diverse in age and field of education. In figure 1, we can see that most respondents are aged between 18 and 25 years old, with two-thirds of them falling in this age range. Twenty percent of the respondents fell into the age range of 26 and 35 years old. The rest of the respondents fell into the ranges younger than 18 years old, older than 55 years old and between 36 and 45 years old.

As for the field of education, with the open nature of the question, the answers were quite varied, with some respondents citing more in-depth degrees. It was decided that, to properly show the diversity of the respondents’ educational backgrounds, all results were categorised into broader educational fields. These fields and the number of respondents fitting in each field can be found in table 4.1.
Some of the respondents had multiple educational backgrounds, explaining why the total in the table is higher than fifty-six, the total amount of respondents.

### Table 1. Fields of education of the respondents

<table>
<thead>
<tr>
<th>Field of education</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Science</td>
<td>20</td>
</tr>
<tr>
<td>Economics/Business</td>
<td>7</td>
</tr>
<tr>
<td>History</td>
<td>4</td>
</tr>
<tr>
<td>Engineering</td>
<td>3</td>
</tr>
<tr>
<td>Law</td>
<td>3</td>
</tr>
<tr>
<td>Applied physics</td>
<td>2</td>
</tr>
<tr>
<td>(Bio)chemistry</td>
<td>2</td>
</tr>
<tr>
<td>Medicine</td>
<td>1</td>
</tr>
<tr>
<td>Electrical Engineering</td>
<td>1</td>
</tr>
<tr>
<td>Mathematics</td>
<td>1</td>
</tr>
<tr>
<td>Philosophy</td>
<td>1</td>
</tr>
<tr>
<td>Energy/environmental engineering</td>
<td>1</td>
</tr>
<tr>
<td>Linguistics</td>
<td>1</td>
</tr>
<tr>
<td>Political science</td>
<td>1</td>
</tr>
<tr>
<td>Graphical design</td>
<td>1</td>
</tr>
<tr>
<td>None</td>
<td>1</td>
</tr>
<tr>
<td>Unknown</td>
<td>7</td>
</tr>
</tbody>
</table>

We can see several interesting occurrences in the table: while over half of the respondents have a relatively diverse educational background, there is a large group with a computer science background. Furthermore, several respondents entered a level of education instead of a field, and thus their background is unknown. The assumption was made that the question as posed was not clear enough in its intention, with the term “field of education” being too vague. However, it has to be said that some of the respondents that fall into this category had not chosen a specific field of education to pursue yet as of writing this paper. With the high number of respondents with a computer science background, expectations of the answers to later questions needed to be altered, especially the answers to section 3, which asked respondents about their knowledge regarding privacy and security on networks, which on average people with a computer science background would have more knowledge of.

Lastly, this section asked users about the frequency at which they use open networks. The results can be found in section 4.2.

From the figure, we can conclude that around just over half of the respondents use open networks at least monthly, with almost nine percent never using them at all.

While it could be said that overall, the group of respondents is somewhat diverse, a possible addition of several more users would greatly diversify the results, especially those in the fields with only one respondent. The vast majority of respondents also fell in the lower age categories, so there definitely is another option of diversification there.

### 4.2 Section 2: Open network preferences

The second section gave several aspects of networks and asked the users to indicate how important they found them on a five-point scale. A score of 1 indicated a very low perceived importance and a score of 5 indicated a high perceived importance. Figures 3 and 4 show the results regarding the physical quality of the network, in speed and stability, respectively.

While some of the respondents do not mind a slower network, many do find speed important. The opinion on connection stability is a lot less divided: only five respondents were neutral on the issue, whereas the rest found it an important aspect of an open network.

Next, the users were asked about security and privacy related aspects: in addition to security and privacy in general (as seen in figure 5), service access was also mentioned (as seen in figure 6).

Out of these two aspects, full access to online services was found to be more important than the privacy and security, though the amount of respondents who found privacy and security to be very important is higher.

Additionally, users were asked if there were other aspects of open networks they found important, on top of the ones that were already named. As this question was optional, it got a lot less answers than the other questions. These additional aspects were the duration of the connection (the Dutch railway company, the NS, was mentioned, as their network automatically disconnects after fifteen minutes), the ability to allow virtual private networks (VPNs) to
be set up, the provider being known to the user and user friendliness and clarity with regards to agreements and explanations before the connection is made.

Next, another open question was asked with regards to different providers of open networks and if respondents feel their behaviour changes depending on the provider of the network, and if so, why. The results of these can be found in table 2.

Important to note is that several of the "no" responses also contained a reason describing ways in which the respondents themselves made sure the connection was as safe as possible through the use of VPNs and HTTPS. Many of the respondents who answered "yes" often named banking as a service they do not use on open networks, and university networks were often perceived as safer.

Finally, the respondents were given several possible providers and were asked to indicate which ones they would trust to provide a secure network and which ones they have ever used. These results can be found in figures 7 and 8. The providers were, from top to bottom: fast food restaurants, coffee shops, universities, cities and public services.

Interestingly, every single provider is used much more often than it is trusted, which seems to imply that the respondents prefer quality of service and convenience over privacy and security. These results are in line with results found earlier in the section where respondents were asked if their behaviour on open networks changes depending on the provider of the network. Several respondents claimed to trust university networks more than other open networks, which is in line with the results as seen in figure 7, where university networks are almost unanimously perceived as trustworthy.

In the end, it was decided that the best way to discuss these outliers separately in smaller sections, which can be found below. It is worth noting that one of the respondents admitted they did not know any specifics, but assumed a large portion of data could be intercepted. Additionally, they supported the idea of raising awareness on the issue.

**4.3 Section 3: Data at risk**

The third section contained a single, open question asking respondents about the personal data they thought was at risk on open networks. Initially, the goal of this section was to compare the kinds of personal data the respondents felt was at risk to the kinds of personal data that were found to be vulnerable in the literature study done prior to this research. However, when reviewing the answers it became clear that this method was too shallow: with the large amount of personal data available on devices that could be intercepted on open networks, it is unlikely that respondents would be able to give a complete list of data, meaning a table with data and frequencies like the tables shown earlier would most likely be unable to give a proper representation of the general knowledge about what data is generally perceived to be at risk.

Supporting the idea that the question itself was too broad are several answers that simple stated that all information was at risk, especially if the connection itself was insecure. While that statement is certainly true, the main goal of this question was to determine whether there were certain kinds of personal data that the respondents would name either often or not often at all to see if where current awareness levels stand.

In the end, it was decided that the best way to discuss these outliers separately in smaller sections, which can be found below. It is worth noting that one of the respondents admitted they did not know any specifics, but assumed a large portion of data could be intercepted. Additionally, they supported the idea of raising awareness on the issue.

**"Traditional" personal data**

Most respondents named the more traditional personal data as being at risk, like names, addresses, phone numbers, contacts and email addresses. More concerning data like credit card numbers and login credentials, especially those used for online banking were mentioned. Interestingly, there was even a single mention of medical data. With electronic health systems rising in prevalence, and thus this kind of data possibly being present on mobile devices like smartphones and laptops more often, it could become a more popular target for cyber criminality in the near future.

**Location**

The location of the user was mentioned five times, even though it is quite an issue, with methods to accurately determine a user’s location based on broadcast information [9].
**MAC addresses**

Interestingly, while there was a mention of personal device information and IP addresses, not a single mention of MAC addresses of the used device was mentioned. This is an interesting occurrence, as MAC addresses are regarded as sensitive personal data, and ways such as randomised MAC addresses are researched to anonymise this data to protect users from adversaries.

**Metadata**

Perhaps more obscure than most personal information, metadata and data that could be obtained by it were rarely mentioned. Browsing history, preferences or personal interests and the like were rarely found to be at risk, indicating there might be a lack of knowledge in consequences of data leaks.

### 4.4 Section 4: Security/Privacy versus Quality of service

One of the main goals of the research was trying to find out whether users of open networks preferred quality of service or security and privacy in the networks they use. This section proposed four ways in which networks could be made more secure at the possible cost of quality of service. Then, the respondents were asked to indicate if they were in favour of each system's added security (and thus increased privacy) or the quality of service of the current system. In each of the figures, the leftmost options denote privacy whereas the rightmost options denote quality of service.

![Figure 9. Virtual Private Networks](image)

Figure 9 shows the results of the first proposed method in which security on open networks could be improved by allowing VPNs to be used. The two highest scoring options were the neutral one and the one slightly in favour of the quality of service. As this method would still leave the choice to the user and as it involves extra steps and third-party software on the user’s side, the neutral option could also imply that, if the option would be implemented, these respondents would not use the method. Then, with merely seventeen out of the fifty-six respondents preferring the added privacy and security benefits, it could be concluded that many users are less willing to take action to increase their online safety and privacy themselves, which is in line with what was found in earlier research [11].

![Figure 10. Service blocking](image)

Even though earlier results shown in section 2 showed that the respondents were not too keen on the idea of services and websites being blocked, figure 10 shows a different picture: all options got quite similar amounts of respondents voting for them, with the leftmost option denoting a high preference towards privacy coming out on top, closely followed by the option slightly preferring quality of service and the neutral option.

One possible explanation for the difference between the results found in sections 2 and 4 of the survey (which also applies to further discrepancies) could be that section 4 of the survey contains more detailed descriptions, giving the respondents additional information regarding open networks they might not have had before. This extra information may have changed their minds in favour of privacy and security.

Another explanation might be that the question as posed in section 4 specifically states blocking unsafe services and websites whereas the question in section 2 names blocking in general, which would include services that might be properly secured, but are not desired by the provider and thus blocked. Examples include the Dutch railway company NS being allowed to block streaming services, as these services could substantially lower the quality of service if they are being used often and simultaneously across the network by a large amount of users.

![Figure 11. Passive scanning](image)

Once again, the results collected in this section seem to contradict what was found in section 2. Figure 11 shows that the opinion on passive scanning to replace active probing is rather divided: twenty-two respondents voted in favour of the added security, while twenty preferred the current quality of service. However, figure 4 showed that nearly all respondents found connection stability an important aspect of open networks, the same aspect this method would impede.

The explanation for the shift towards safety and privacy might be the explanation of the access point discovery algorithm placed before the question, and especially its main drawback: an interceptable list of preferred networks a user connects to contains a lot of information about a user, and this perhaps not being well known to the respondents until this point may have caused a portion of them to reconsider their opinion.

Another explanation might be much simpler: while the respondents found a stable connection very important over-all, they are willing to sacrifice it if it means an increase of their online safety and privacy.

Finally, figure 12 shows the results of the final question regarding a change to the current broadcast message devices send out. This method reduces the amount of information contained in these broadcast messages, resulting in less potentially sensitive information being sent out with the drawback of receiving answers from all access points in range, which could result in a slower connection. With
twenty-three respondents in favour of the system’s benefits against thirteen who preferred the current quality of service and twenty-one voting neutral, this option is quite popular among the respondents.

One explanation might lie in the conditions of the setbacks named in the description of this method: when not many networks and therefore access points are in range, the speed of the connection would not be impeded too much, resulting in the same heightened security and privacy at a relatively low cost in quality of service.

4.5 Section 5: Final Questions

The final section consisted of two parts. Firstly, respondents were given several actors affiliated with creating and using open networks. Then, the respondents were asked to indicate how responsible they felt each actor was on a five-point scale. The results can be found in figures 13 through 17.

These figures show an interesting pattern: on average, each actor’s responsibility was rated very similarly, with the curves in the graphs being near identical, edging towards a relatively high degree of responsibility, indicating that the respondents feel that protecting the users’ personal and private information is an effort to be shared by all involved parties. However, section 4 found that the method that involved the users themselves the most, the addition of VPN support, was shown to be the least favourite. This seems to imply that while the respondents do feel the users are partially responsible for their own safety, many are not willing to take the action of installing the necessary software to allow the usage of VPNs.

Lastly, respondents were given several methods in which users are made more aware of security risks and were asked how effective they felt each of these methods were. However, where the middle option would normally indicate a neutral stance towards the subject, this time, this option was used to indicate that the respondent had never encountered the method in the first place. The results can be found in figures 18 through 22.

Out of all methods, there is clearly one that the respondents found useful and one that was regarded as less impactful: the web browser intervening and showing a large warning screen to the user was rated as highly effective in raising awareness regarding online safety, and flyers and posters were seen as the least effective, with only four respondents giving a positive response towards them. The more subtle security warnings in the form of icons and address bar colour changes were rated quite positively as well with regards to effectiveness, with fourteen respondents not finding them very effective and almost double that, with twenty-seven, finding them effective. In total, fifteen never encountered or noticed them, which, given their more subtle nature, is understandable.

Infomercials were not often encountered, and most respondents who encountered them did not found them very effective, with sixteen out of the twenty-three negative ratings being the lowest option. Even out of the eleven positive ratings, only a single respondent found the method very effective.

Trainings were rated more positively, with the fifteen negative scores being divided as evenly as possible and a total of twenty-one positive ratings, with a third of those being highly positive.

5. DISCUSSION AND RECOMMENDATIONS

5.1 Discussion

This research was carried out to create an assessment on user knowledge, awareness and requirements of free, open networks. The main reason behind the creation of the research and this survey was the notion observed in several research papers that most users of (open) network would not have a positive attitude to many methods that could be deployed to increase the safety of the networks,
making the user experience of open networks more privacy oriented, as many of these methods would have an adverse effect on the quality of service currently provided by the network.

The research questions that were defined to help create this assessment were aimed at four main aspects: what do users know about their privacy and security on open networks, to what extent value users their privacy and security over quality of service on open networks, who do users feel is responsible for the privacy and security and what ways in which awareness regarding privacy and security used now are seen as most effective by users?

The latter two questions are answered the easiest. From figures 13 to 22 it is clear that the respondents found all given actors in open networks, from the users themselves to government legislation, nearly equally responsible for the security and privacy of users of open networks. Furthermore, the methods of icons and changing colours in address bars and warning pages in web browsers were regarded as highly effective measures to raise awareness of network security in general, with flyers being regarded as ineffective and trainings and infomercials not often being encountered in the first place.

The third question is a lot more ambiguous. While early on in the survey quality of service aspects were shown to be highly desirable in open networks, only the addition of VPN support was shown to have a somewhat strong bias towards quality of service by the respondents in a later section detailing some possible methods that could improve security on open networks. A possible explanation for this is the extra descriptions and explanations in the fourth section that gave the respondents more information about how open networks work and how their safety can be improved.

Another explanation is that the questions as posed in section 4 were more detailed, whereas the aspects of section 2 covered more broad terms. For instance, as mentioned in the results of section 4, respondents were much more inclined to support the blocking of unsafe services and websites (figure 10), in contrast to section 2, where the blocking of websites and services in general not being very popular (figure 6).

The final explanation is that users are simply willing to sacrifice some of the quality of service aspects if it means an increase in safety and privacy. This is supported by the results as shown in figure 5, where safety and privacy were overall found to be another important aspect of an open network.

Finally, regarding what personal data the respondents felt are at risk, several conclusions can be drawn: while certainly, traditional personal data like names, addresses, contacts and login credentials are known to be at risk by most users, there are still several kinds of data at risk like locations and metadata that a lot of users are not aware of.

The lack of some data being named could have several explanations. One is that the respondents simply do not regard this data as particularly important, or do not realise that this data can be used to make deductions that are more concerning, like a person’s shopping habits or visited locations. Another is that the respondents were not aware that the data could be intercepted, or that the data even exists to begin with.

5.2 Recommendations

As mentioned earlier in this paper, the target audience could be greatly expanded to reach a broader public. Especially focusing on some of the underrepresented studies as seen in table 4.1 could be a great help in diversifying the results.

While section 3 of the survey fulfilled its purpose by showing what data the respondents found to be at risk and its open nature did not help the respondents by giving answers they might not have come up with themselves, it was also very broad, leading to some respondents filling in that all data was at risk without going into details what kinds of data that might be. A more direct question might deliver more detailed results.

The addition of more propositions of ways to improve the security and therefore the privacy of users of open networks would give a deeper insight into user preferences regarding open networks, and therefore would help develop more user friendly ways in which networks could be im-
proved regarding safety and security.

6. REFERENCES


