An investigation into whether the Government have the right to monitoring networks for public safety?

A dissertation submitted in partial fulfilment of the requirements for the degree of Bachelor of Science (Honours) in Computing

By Dax Baker

Department of Computing & Information Systems Cardiff School of Management

Cardiff Metropolitan University

April 2017

Declaration

I hereby declare that this dissertation entitled as "An investigation into whether the Government have the right to monitoring networks for public safety?"

Is entirely my own work, and it has never been submitted nor is it currently being submitted for any other degree.

Candidate: Dax Baker

Signature:

Date:

Ethics Approval ID Number: 2016D0324

Abstract

This dissertation looked into how the Government monitor networks in the interest of public safety. While having a better understanding of what the public's thoughts are on the matter. After analysing the results it showed most of the participants were for the Government monitoring network but did not fully understand what network monitoring is.

The literature review provides an insight into how the Government monitor networks, looking at the laws they have to follow, the power they have on monitoring social media and looking at the success rate.

The research gathered for this dissertation was based on a python program that determines the participant's outcome, whether they were for or against the Government monitoring networks. These results would then be compared to their original opinion.

The testing had three different scenarios

1) Random selection giving participants no time to consider their opinion before taking part in the questionnaire program.

2) A detailed interview with participants giving them time to think about their own opinion. This also allowed me to get a better understand on what participants thought on the matter. After this, the participant to do the questionnaire to see if this had any impact on their outcome.

3) A participant would state their opinion on network monitoring. After this the participant will be given an information sheet on how the Government actually monitor networks. Once reading the sheet the participant will be asked to take part in the questionnaire.

The overall findings is that people are for the Government monitoring networks however the participants didn’t really understand how it worked.

Acknowledgments

I would like to thank my housemate Raphael for staying up with me on many all-night work marathons and keeping me motivated.

My family for ordering me food when things got tough

And last but not least Emma Becke who refocused me when all seemed lost and providing me with her laptop when my program wouldn’t work on my laptop. I could honestly have not got to this stage without her.

Contents

1.0 Introduction

In today’s society, the Internet takes up a large proportion of our daily life. It has actually become a vital part in running our everyday life from standard tasks, education, business and even Government surveillance. With this networks need to be more diverse and unique than ever. Specifically, networks are required to be constantly updated to keep up with technology, so that it can keep up with growing expectations of its users. The current debate over the protection of privacy is trapped within a false dichotomy between freedom and security. In this paper the purpose is to determine whether the control of networks by the Government is helping protect the wellbeing of the UK as well get a general idea of the public’s view. Over the years the Government has become more involved in monitoring networks to counter terrorism. This research investigates the perception of general public regarding networking monitoring and interfering with their private life. Furthermore, this research will investigate how social media technologies such as Facebooks APIs could be manipulated to obtain personal information about connected users.

Further research/analysis will be carried out to understand the progress into stopping terrorists getting past networks by law enforcement authorities. The debate in question is about whether the Government should have the power to monitor networks. However if the question ‘should the Government monitor networks to track terrorists’ was presented to the public, the majority of people would answer yes, with statistics showing that 56% of voters would agree to monitoring networks to track terrorists. In the book “Nothing to Hide” by Daniel Solove a quote stands out: ‘’we must give up some of our privacy in order to be more secure.” The author of this book is a civilian, illustrating that at least some of the public understand this is the best way to combat the threats to the nation.

1.1Background

In the ever inclining technology boom, networks have become vastly important to the way we communicate. The majority of organisations and people use some form of networks in everyday social interaction with friends, business colleagues and companies around the world. The biggest problem presently is that networking is becoming so powerful that groups like Al Qaeda try to intercept information from ours and other nations and communicate it to their leaders, so they can use it in their favour to attack our country. The argument in question is whether or not the government should have the power to monitor network usage so they can try to avoid any attacks coming to our country. This is a debate strongly argued with many people having an opinion. A large majority of people would argue that they are invading their right to privacy, I want to show this is not always the case and give people a better understanding on what is actually done.

The government have tried to combat terrorism for many years now using different projects, for example with a box called Deep Packet which will be explained later on. MI5 chief Jonathan Evans quotes: 'Access to communications data of one sort or another is very important indeed. It’s part of the backbone of the way in which we would approach investigations to protecting our nation. UK government plans to track ALL web use: MI5 to install 'black box' spy devices to monitor British internet traffic, Link-

1.2 Aim

The aim of this project is to investigate the current methods the government use to monitor networks. Then analyse the research the actual opinion from the general public regarding networking monitoring and interfering with their private life.

1.3 Objectives

To complete the investigation for this project, the researcher must;

1. Review the literature and identify characteristics and features of network monitoring for example what steps the Government actually do to prevent this comparing in to other countries

2. Gather a better understanding on how the Government monitor networks and have an idea how they are interacting with social media

3. Analysis the actual data gathered from participants of the study and review the actual results compared to opinion

4. Interrupt how the public actually feel towards network monitoring

5. Have a better understanding how the Facebook API actually works and what information can be gathered

1.4 Motivation for the project

Ever since being given an assignment on network communication I have been fascinated in following in up. I have structured most of my assignments in the last 2 years around this and I hope to incorporate them into this project. The more and more work that I have put into network monitoring the more I have wanted it to be a future career for me. Even before the assignment I had an interest in working with the Government, mainly the civil service. I have always been for the monitoring of networks, however I have been around a lot of people who are against it. I feel this sort of project where I get to interact with people giving them a better understanding of how the Government actually go about it and that they are not just invading people's personal space. The different ways the Government go about monitoring networks around the world is intriguing and I hope dig even deeper to have a better understanding for the future.

1.5 Structure of the project

1.5.1 Introduction

The introduction will provide an outline of what the project is all about, this will include the overall aim, with clear objectives of how to reach the aim. Included in this chapter is the background of network monitoring and reasoning of why I want to do this project.

1.5.2 Literature Review

This section introduces what is network monitoring and why it is used today. Going into detail on the advantages and disadvantages of it and why so many people have different opinion. Looking into how efficient network monitoring has been over the last few years and how it differs from country to country. A brief look into who the government actually employ to monitor networks which are the National Counter Terrorism Security Office (NCTSO).

1.5.3 Methodology

The Methodology provides a clear guideline on how the research will be carried out throughout the project, discussing how the data collection process will take place.

1.5.4 Results and Discussions

In this section I will discuss the findings of my data collection, this section will be the core of my project I want to show that what people are thinking network monitoring is about is actually the opposite to actually what goes on.

1.5.5 Conclusion

The final chapter will provide an overall review on the research gathered on this paper by evaluating whether the objectives have been met and to see if the overall aim of the project has been achieved.

1.5.6 Questionnaire Program

The questionnaire program section will provide a clear understanding on how it works with detailed information for what each page works

1.5.7 Testing

Testing of the Questionnaire program making sure the functionality works as it is meant to.

2.0 Literature review

2.1 What is network monitoring?

Network monitoring refers to the practice of overseeing the operation of a computer network using specialized management software tools. Network monitoring systems are used to ensure availability and overall performance of computers and network services. These systems are typically employed on a larger scale corporate university IT networks.

2.2 Why does the government use it?

The reason for monitoring networks by the government in the UK can be backed up by evidence in the US: on 17th October 2012 the FBI stopped an attempted bomb threat when they had the power of monitoring the American networks. The American Government gave the FBI the power to create a team which would be able to monitor any suspicious activity on the networks. They intercepted messages from a man named Quazi Nafis who flagged up on their system after he looked the parts which are used to make a certain type of bomb. The Police managed to monitor his entire network usage and monitor his location with the power to track his mobile. The NYPD Commissioner stated ‘’without this power many lives would have been lost and even though people may look at this as snooping or invading privacy the results show that it is beneficial to all the citizens in our state’’.

2.3 Laws on Network Monitoring

The laws on monitoring networks are different around the world. The UK are planning on following Australian government after the change of the Bill National Security Legislation Amendment Bill (No. 1) 2014 which gives spy agency (ASIO) the power to monitor all Australian internet. Spy agency ASIO will be given the power to monitor the entire Australian internet and journalists' ability to write about national security will be curtailed when new legislation, which was passed by the Senate on the 26th September 2014. This law enables ASIO to track and monitor any suspicious activity without the need of a warrant, which can benefit the public as waiting for a warrant can lead to other events happening in the meantime without being able to stop them.

Until recently the UK government law they have limitations on how to monitoring networks due to The UK Regulation of Investigatory Powers Act 2000 (RIPA) which states that it is prohibited to intercept communications via public telecommunication system (UK Legislation. 2000) However, the current government are trying to change this law with The Retention and Investigatory Powers Act 2014 which is ‘To Make provision, in consequence of a declaration of invalidity made by the Court of Justice of the European Union in relation to Directive 2006/24/EC, about the retention of certain communications data; to amend the grounds for issuing interception warrants, or granting or giving certain authorisations or notices, under Part 1 of the Regulation of Investigatory Powers Act 2000; to make provision about the extra-territorial application of that Part and about the meaning of “telecommunications service” for the purposes of that Act; and for connected purposes.’

This would allow the government further power to monitor public networks as long as the reason for the monitoring is justified. The power would be handed to the armed forces intelligence committee and they would have the responsibility of making sure the monitored data is handled correctly and securely

2.4 New law

Starting the beginning of 2017 - The Investigatory Powers Act 2016 (nicknamed the Snoopers' Charter or Snooper's Charter) comes into place this has now been passed by both Houses of Parliament, and the Queen signified her royal assent to the Investigatory Powers Act 2016. This has caused many mixed opinions which I will go into detail more later on in this document.

2.5 Surveillance vs privacy

The conception of privacy not only as an aspect of human life but as a human right, pinpoints the importance of protecting that right from violations, invasion of privacy is not simply an inconvenience but an important human rights issue. In modern society there are daily many violations of the right to privacy, which civil rights defenders must confront and take into consideration. This thesis aims to contribute to this field and discuss the implications of certain violations to the right to privacy. Due to limitations of scope this thesis will delimit its investigations to the field of surveillance, specifically that of video surveillance. Surveillance is an increasingly debated topic, coming to the forefront over recent years due in part to the "War on Terror" and the increasingly important role that surveillance plays in security since the events of September the 11th 2001, and partly due to the development of more sophisticated and integrated database and information gathering technology. In addition, many countries have recently altered or added legislation lending increased scope to surveillance, both with regards to the amount of surveillance available to security agencies and the intrusiveness of said surveillance in the post 9/11 era. 7 Surveillance is in a perpetual state of antagonistic contradiction to the right to privacy, as it necessarily involves an invasion and violation of the right to privacy. But most commentators argue that surveillance is necessary in many different aspects of societal life, be it health care, security against crime or terrorism or even in order to improve customer service (references). Therefore the extent to which surveillance is to be allowed or regulated in society is a current and important, although often controversial, topic. This debate is further complicated by different understandings and conceptualisations of what privacy is, and to what extent it is acceptable to derogate from the right to privacy in exchange for other societal goods. As such the issue of surveillance and its effect on the right to privacy is an important and current issue, which certainly warrants a deeper investigation. In order to achieve this, the thesis will look at two different cases where video surveillance has been used for the benefit, or protection of public security and what consequences this has for the privacy of the people under surveillance. It will also analyse the media coverage of said surveillance to understand how people and the press react to, and conceptualise such surveillance and the right to privacy in the given cases. The first case is the use of Closed Circuit Television (CCTV) by the authorities in London, arguably one of the sites under most surveillance in the world, to prevent crime and terrorism with particular focus given to the post 9/11 period. The second is the covert video surveillance use against Arne Treholt during the 1980s by the Norwegian. This covert video surveillance was of his house as part of their evidence gathering activities while he was under suspicion of treason.

2.6 Current system

In comparison with past the system, the current digital surveillance system for monitoring populations is unique in that it is not direct, but rather participatory. *By 'participatory', we mean a mutual, horizontal surveillance based on the intentional, agonistic disclosure of personal information by users of digital services, mobile applications and online platforms. It is accompanied by a loss of control over the terms of service of the infrastructure where personal data are stored and circulated. This surveillance is participatory insofar as it is mutual and involves a generalization of bottom-up moderation mechanisms and of the way online communities enforce norms within social platforms.*

2.7 Methods of network monitoring

2.7.1 (Deep packet)

One of the ways the government have planned to track terrorist movements is by using GPS tracking. The government can flag up a terrorist or potential terrorist using the Deep Packet box, which is a program that can monitor almost all communication networks on the web, searching for encrypted messages or flag up warning signs for when trigger words such as 'bomb' or 'attack' are used. Once they had received warning of a potential threat, using data surveillance they would have access to the suspect's phone number, and consequently be able to track their movements via GPS. Furthermore, a GPS tracking system can be extremely helpful in investigating and preventing bombings which are activated by a cell phone call or text message. For instance, if GPS tracking had been used in Mumbai last November, a bombing could have been avoided because law enforcement officials would have been able to identify cell phone users in the area, thus the authorities using this knowledge to cut off the primary means of communication between the terrorists, therefore avoiding the bombing. ([i]. A GPS tracking system can also protect against domestic terrorists, whether they are dangerous environmental rights activists, violent gangs or racist groups with aggressive agendas, radical civil rights or human rights supporters. While acts of domestic terrorism do not kill as many people as international terrorism such as the World Trade Center bombings, they do kill a significant number of people and cause thousands of dollars' worth of damage each year, thus making them a worthy cause to try to stop.

2.7.3 SMISC

One of the government's investments was a program called "Social Media Strategic Communications" (SMISC), which is a tool that tracks social media and weeds out information which can be deemed dangerous. The program has set four goals for the project: to detect, classify and measure the development of ideas, concepts in hidden social media messages; specify the structure of the campaign and influence the social media sites and the community they create; identify the participants and their intentions by conducting a social media campaign of persuasion and measure its effect; and develop an effective counter-message to an identified campaign carried out against the enemy. One example of the program might be a closed social media network of 2,000 to 5,000 people who have agreed to conduct social media-based activities in this network and agree to participate in required data collection and experiments. This network might be formed within a single organization, or span over several.

2.8 Cyber warfare and cyberterrorism

There are two types of social networking issues in our current day lives: Cyberterrorism and Cyber warfare. I shall define what they are and explain why the government can benefit from monitoring networks.

‘’Cyber warfare is internet-based conflict involving politically motivated attacks on information and information systems. Cyber warfare attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems -- among many other possibilities’’. Tim Godwin stated that without the extra monitoring from the government these crimes would continue to happen without any clear evidence to charge people. Cyberterrorism does not have an actual definition, however the United States Department of State prescribes the following definition of terrorism: “…premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents.” (Title 22 of the U.S. Code, Section 2656 f(d)).

2.10 Efficiency? (Results before and after London bombing)

Since then the government has invested in the world’s biggest Data Centre, code-named Bumblehive, which is the first Intelligence Community Comprehensive National Cyber-security Initiative (IC CNCI). The data centre is designed to support the Intelligence Community's efforts to monitor, strengthen and protect the nation. Since the opening of Bumblehive in 2013 the NSA announced that 215 terrorists have been stopped. Gen. Keith B. Alexander stated ‘without this technology in place the lives of many would have been lost and I can sleep peacefully at night that we have done everything we can to protect the nation.’

2.11 Cost

Looking at the cost for the government to run fully functional network monitoring system (ICRs) – databases which has been the plan since the Investigatory Powers Bill 2016 had been passed. The original cost was estimated to cost £170 Million, however a recent study coming of Denmark has shown the head-per-head cost for this system would be £19. So the overall start up would be an investment of £1.2bn, as well as annual running costs

2.12 Advantages

Reason for the government monitoring networks

- Government surveillance will make the world safer and hold criminals more accountable for their actions.

- People should have nothing that they are hiding so they should be fine with the government searching through their information
- It causes no physical harm or crosses any boundaries, yet keeps us safe and protected.
- Government spying programs help in the fight against terrorists and ensure that Americans stay safe

2.13 Disadvantages

- Too much surveillance can be detrimental and leave people without any privacy. Critics like Representative James Sensenbrenner argue that surveillance can go too far. Sensenbrenner has compared today's government surveillance to "Big Brother" from the George Orwell's "Nineteen Eighty-Four."
- Increasing political surveillance in the name of protection against war or an enemy fuels the never-ending excuse to monitor innocent people's lives. In 2013 Ami Stepanovich, director of the Domestic Surveillance Project at the Electronic Privacy Information Center, argued that unregulated surveillance could potentially "strip us of our privacy rights, and by extension, restrict association, assembly, organization in such a widespread manner that would have the most oppressive regimes in history foaming at the mouth.

2.14 Power of social media

Social networking has grown and grown over the years and has become the key way to communicate, with many functions of businesses relying on it. There have been key events in the world in recent years which have occurred due to the power of the internet, from the protests in China set up by students organising meets in the square over the social networking site Facebook, to the more well-known London riots. The Riots went from a peaceful protest to complete anarchy and this, in the government's eyes, was worsened by social sites such as Twitter, Facebook and BBM. These riots were spread across the networks and people found excuses to get involved. Before this, there was no monitoring situation in place, so a lot of people were unable to be tracked for their crimes. With the government having the power to monitor networks, they could give information to the police service which gives them the power to watch out for any planned gatherings and targeted areas the user has planned to hit. Even if the user hasn't been caught in the act, there would be significant evidence from monitoring the network to prosecute the user. Since these actions the government have given police action to stop riots and in December 2011 the police intercepted BBM messages on a planned mall riot so that gang members were stopped from stealing thousands of pounds of goods.

2.1.5 Third party companies

The government recently started paying third companies to help monitor social media and a wider range. In an announcement issued by the Crown Commercial Service, the names of companies that have won government contracts were made public, along with the details of what they are expected to provide. The agreement with the companies replaces a previous agreement, which employed companies solely to monitor the press. It has now been expanded to incorporate multiple forms of media, and cast the net more widely than professional journalists. This power has been given to seven companies such as Gorkana Group Ltd, LexisNexis (Reed Elsevier UK Ltd T/A LexisNexis) and Meltwater (UK) Ltd. Each company has a similar role. However some will be responsible for scanning social media, including Facebook, Twitter, LinkedIn and others will be responsible for news articles, blogs and other platforms, looking for keywords and following conversations that matter to the general public.

2.1.6 Facebook Api

The Facebook API is a platform for building applications that are available to the members of the social network of Facebook. The API allows applications to use the social connections and profile information to make applications more involving, and to publish activities to the news feed and profile pages of Facebook, subject to individual users privacy settings. With the API, users can add social context to their applications by utilizing profile, friend, Page, group, photo, and event data. The API uses RESTful protocol and responses are in JSON format.

3.0 Methodology

3.1 Introduction

When it comes to looking at the opinions the public have on the Government monitoring networks, a methodology is needed so that the report can investigate the results. To start the investigation on should the Government monitor networks, an interpretative research philosophy will be adopted involving an inductive research strategy and qualitative data gathering for this dissertation. The qualitative research methods will be employed together information related to Network monitoring by authorities. There will be three definite stages to this research these are an interviewing section, a random selection questionnaire and an information first followed by a questionnaire. This section will go into further detail on why these methods are selected for gathering this data, why certain methods were debated and why certain parts were changed to meet ethical approval.

3.2 Sample size

The sample size for each questionnaire test will be kept to 20 participants, however each test will vary a little. This shall be explained in each of the sections below

The interviews will have 15 participants with each answering in detail the questions asked before taking part in the questionnaire.

3.3 Questionnaire part 1 (random selection)

For this section the aim is to use the random selection technique and to get participants to fill the program out without having time to think about the topic. The participants would be sat down and just before they started the questionnaire the participant will ask them the question whether they are for or against the Government monitoring questions. From the participant would go onto to answer the ten questions on the program which is designed to weight each answer differently to give an overall result to see if the results matched their opinions or not. The random selection test will be available to see if rash decisions really match the participant's opinion. The aim of this is to see

1) To see if rash decisions match the actual belief of the participant
2) To see if age has any difference is participants opinion
3) To have a rough scale on rash decisions to actual outcomes

3.4 Interview

When it comes to the interview, this will require the participant to sit down with me and spend time answering ten questions in detail. Giving the participant time to think about their answers gives them time to actually think whether they are for or against the Government monitoring networks. Once the interview is done the participants will be asked to do the same as participants who just do the questionnaire part 1, the aim of this is to learn different things

1) To have a bet understanding what the general public think of the Government and how they run it and how network monitoring actually works.
2) To see if the participant given more time to think about their opinion will vary from participants given no time to think about their decision.
3) To see even when given more time the participant's opinion matches the outcome of the computer program.
4) To look at comparisons between age and awareness. This can be looked at in many different ways

3.5 Questionnaire part two

This part of the testing will look whether if given actual information on network monitoring to the participant will it give any influence to their outcome. So the Participant will give their opinion then be given the information about what the about network monitoring such as what it actually is, how it work and the costs of running it.

1) See if actual facts can influence the participants opinion
2) Give participants a better understanding on what the Government actually do when monitoring networks
3) Compare the age vs awareness, by this I mean does a younger mind get influenced by the facts more than the older generation.

3.6 Ethics Approval

As the data collected is sensitive information ethical issues had to be considered. This required approval from the ethics committee, who required certain documents. This included sample questions for the interview and questionnaire section, a consent form giving me the power to use their data for my research and an information sheet to allow the participant to know exactly what the test is for. Upon a couple of changes had been made the ethics form has been approved. All these documents with be found at the end of the document in the appendix.

3.6.1 Protection

As required in the ethics form all the data collected from the program from participants is protected file this can only be accessed from a user name and password when running the program this will be explained later in the how the program works. Once all the data is used the information will be deleted as detailed in the consent form.

4.0 Questionnaire system

The program so as mentioned above participants will be answering the questions on a program I have designed. The reason for the program will help determine the participments overall view on network monitoring. This is done by how they answer the questions each answer will score them one point to the for or against outcome unless they select the third option of Not bothered which will score them 0 for both outcomes (this will demonstrate this diagrams later on).

In the Appendix you can see the testing that went on with the questionnaire and an image by image of how the program ran.

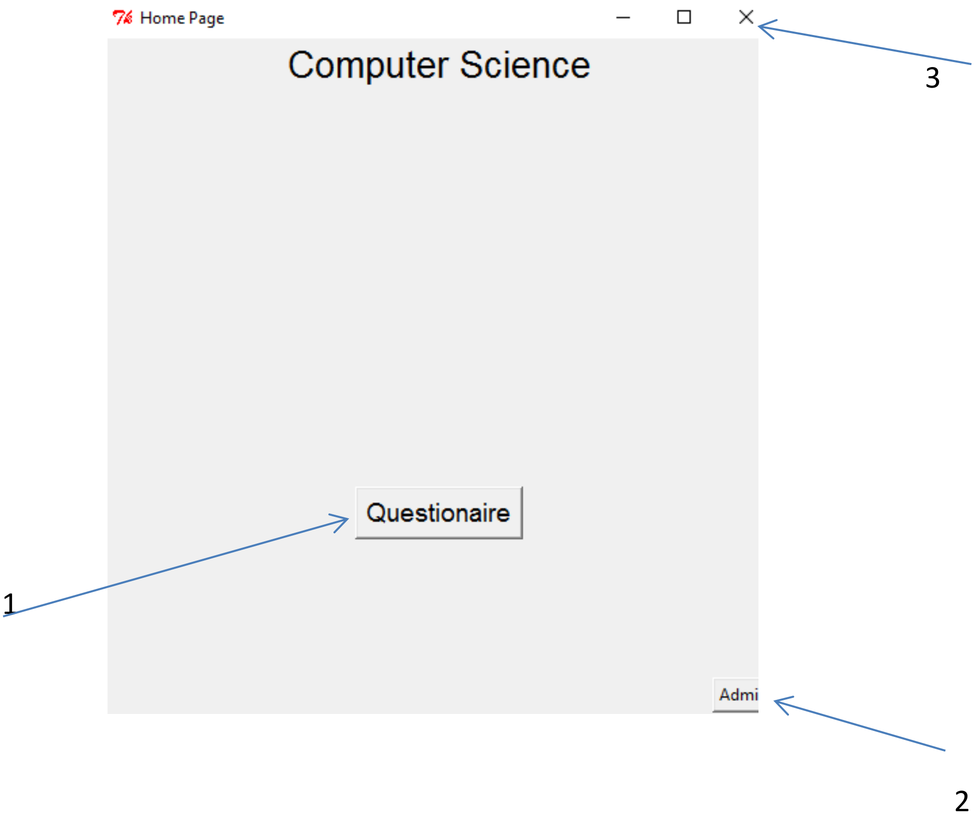
4.1 Home Page

Once the program is running there will three possible functions

1) The questionnaire button this allows the Participant to open the questionnaire and start the test

2) The admin button is for the interviewers use only this will prompt another separate screen and closer the current screen

3) End the program

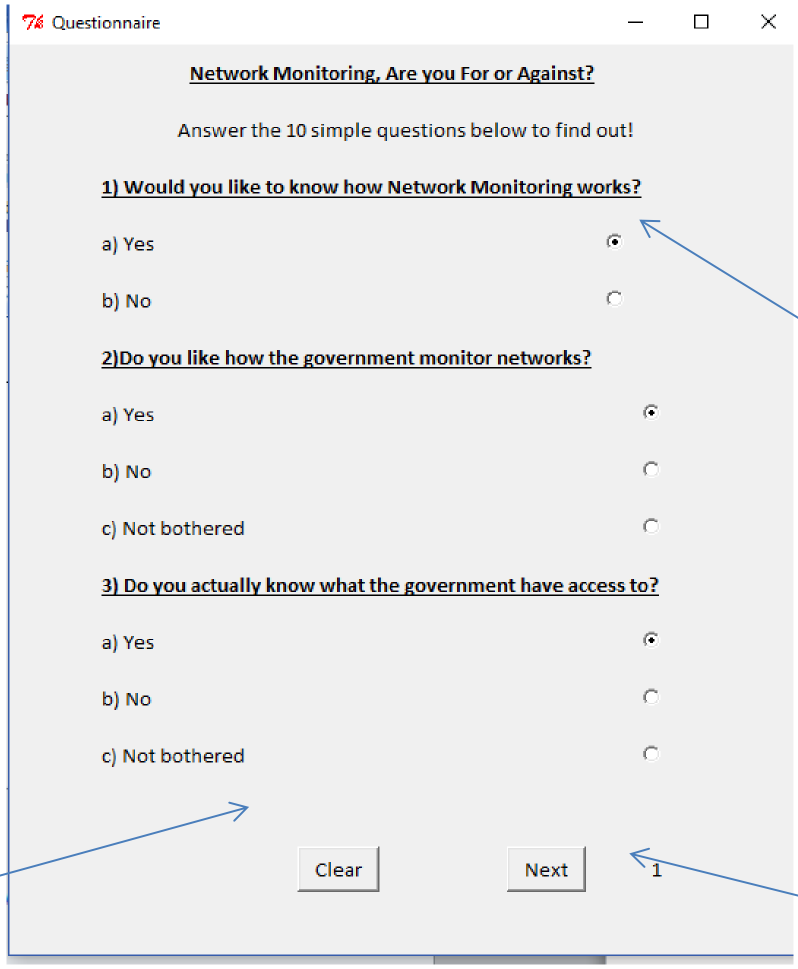


Looking at the questionnaire part prompt first

4.2 Questions 1-10

There are ten questions altogether each question must be answered in order to move onto the next page, if the participant does not answer all the questions an error message will pop up and the participant will not be able to move forward. There is a total of three questions on pages one and two.

If the participant changes there mind at any point they will be able to go back at any point by click the previous page button. If the participant wants to start the page again then all they need to do is press the clear button. Once the participant has completed the page, to move on they just need to click on the next button. I will highlight below when a function can be used



Network Monitoring, Are you For or Against?

Answer the 10 simple questions below to find out!

1) Would you like to know how Network Monitoring works?

a) Yes ●

b) No ○

2)Do you like how the government monitor networks?

a) Yes ●

b) No ○

c) Not bothered ○

3) Do you actually know what the government have access to?

a) Yes ●

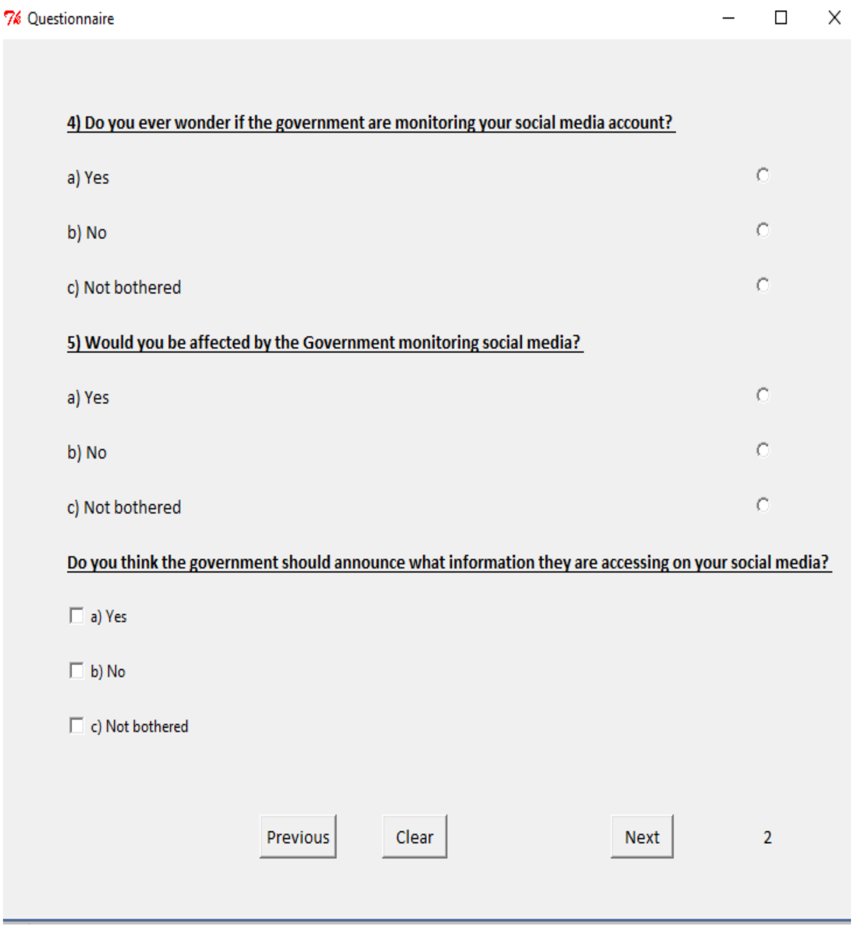
b) No ○

c) Not bothered ○

Box must be selected

To **CLEAR** selected answers

To press to **NEXT** page



4) Do you ever wonder if the government are monitoring your social media account?

a) Yes ○

b) No ○

c) Not bothered ○

5) Would you be affected by the Government monitoring social media?

a) Yes ○

b) No ○

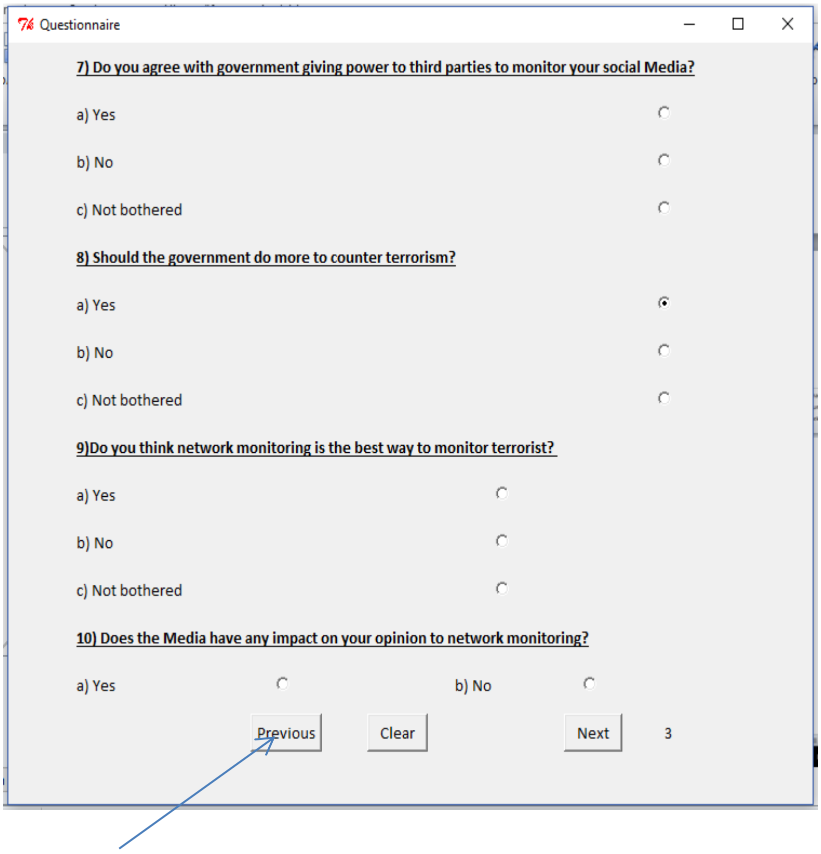
c) Not bothered ○

Do you think the government should announce what information they are accessing on your social media?

□ a) Yes

□ b) No

□ c) Not bothered



7) Do you agree with government giving power to third parties to monitor your social Media?

a) Yes ○

b) No ○

c) Not bothered ○

8) Should the government do more to counter terrorism?

a) Yes ●

b) No ○

c) Not bothered ○

9)Do you think network monitoring is the best way to monitor terrorist?

a) Yes ○

b) No ○

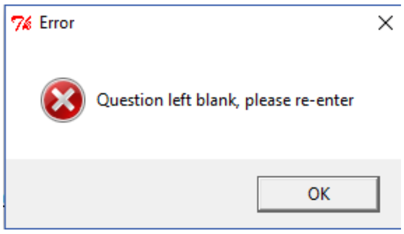
c) Not bothered ○

10) Does the Media have any impact on your opinion to network monitoring?

a) Yes ○ b) No ○

To go back to the **Previous** screen

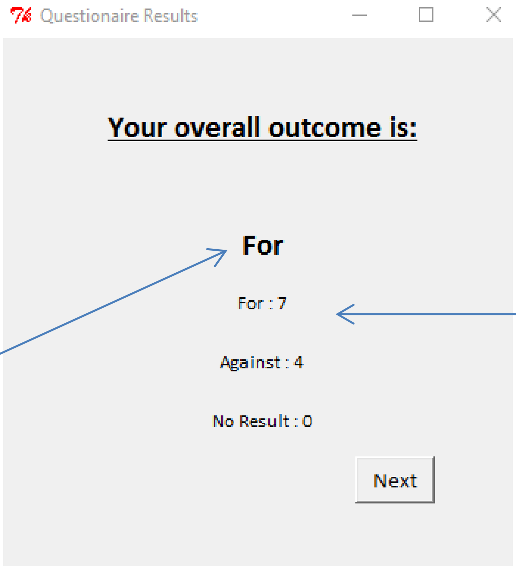
4.3 Error Prevention


Error

Question left blank, please re-enter

4.4 Questionnaire Results

Once the Questionnaire is complete the participant will be able to see their results. Originally this was not the case however after a little feedback many people wanted to see if their opinion matched their outcome. Each answer is weighted so that the participant will score a point towards for or against or even No result if applicable. The results will show the pariticant the overall outcome and how heavily they were for or against the governemnt montoring networks. Once the participant had reviewed their results they would move onto the next page for their person details


Questionaire Results

Your overall outcome is:

For

For : 7

Against : 4

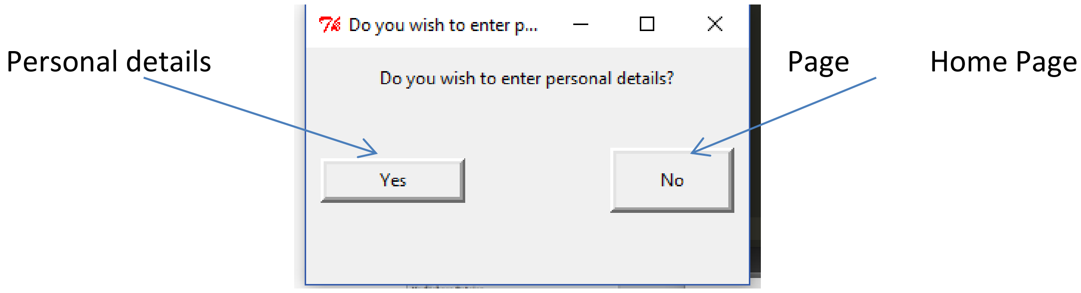
No Result : 0

How the results came out

Overall **Outcome**

4.5 Approval page

This prompt was added due too not everyone wanting to enter personal details. As can be read from the methodology some of the test did not require consent. All outcomes would be sorted but not all personal information will. The need for personal information is mainly for age so along as I receive a variety of different ranges, I could still analyse the results-



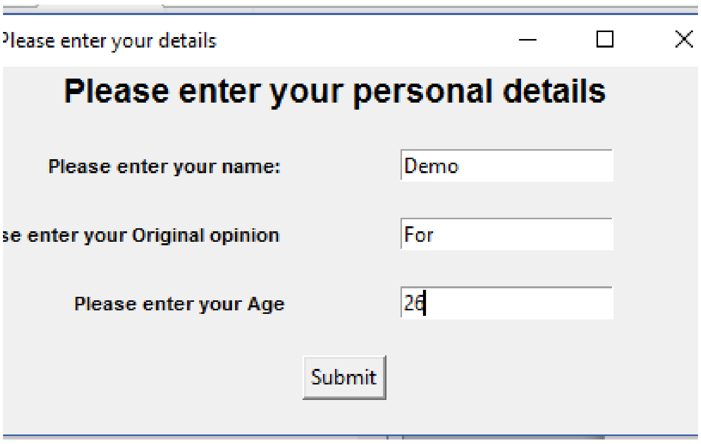
Do you wish to enter personal details?

4.6 Personal details

On the personal details page the participant will be asked three personal questions

1) Their Name
2) Their original opinion
3) Their age

They must enter all three bits of information for the form to be submitted if one part of the information is missing then an error prompt will pop up and inform them of their error. Once the information is all entered the participant can enter submit and a new prompt will open up to confirm the participants information is stored.



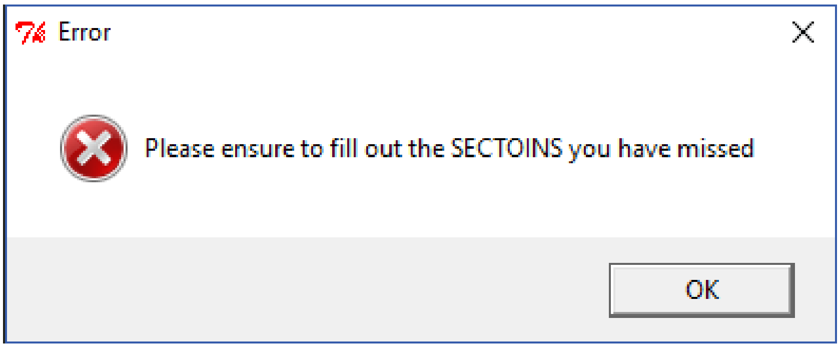
Please enter your personal details

Please enter your name: Demo

se enter your Original opinion For

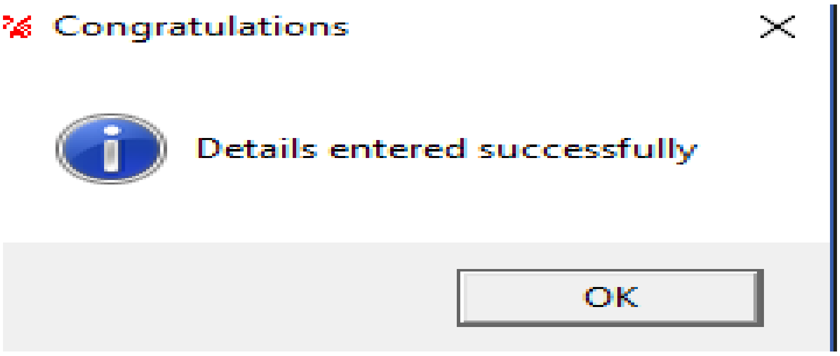
Please enter your Age 26

Personal details error prevention message



Please ensure to fill out the SECTOINS you have missed

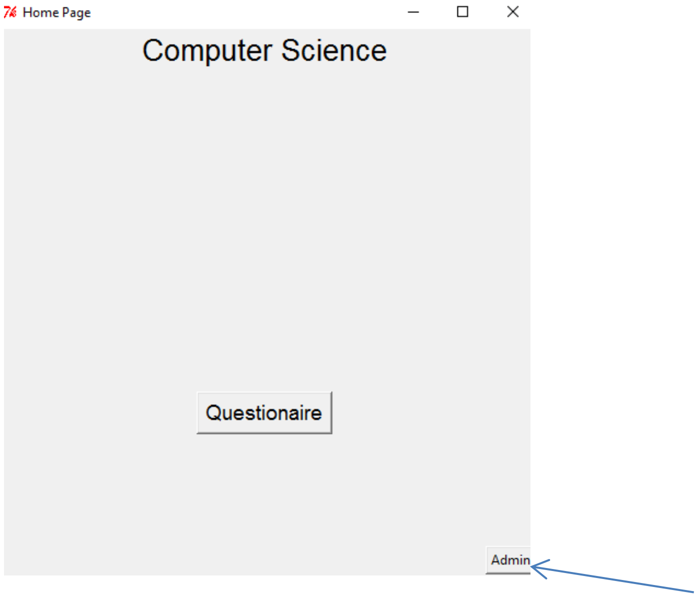
Confirmation message


Congratulations

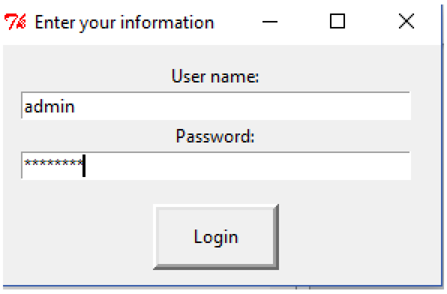
Details entered successfully

4.7 Administration Page

Considering pariticipments will be giving out personal information it was aggreed that a private admin page will be needed. To access this you will need to click on the button based at the bottom of the page. This application has to be password protceted so this functionality was added. This stopped anyone other that the owner accessing perosnal details of the participants.



Password protected


Enter your information

User name:

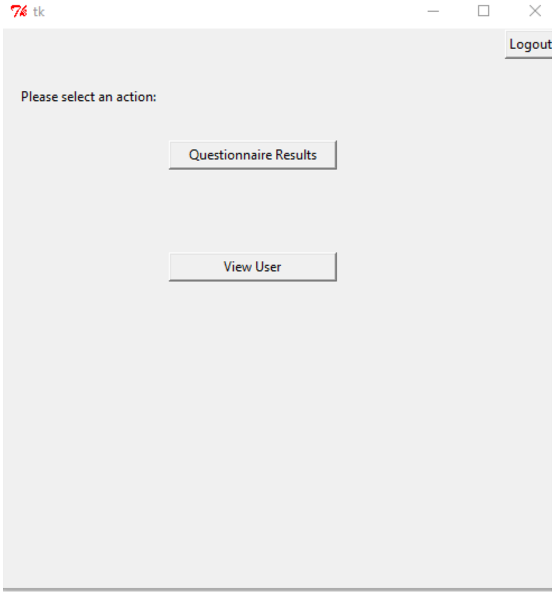
admin

Password:

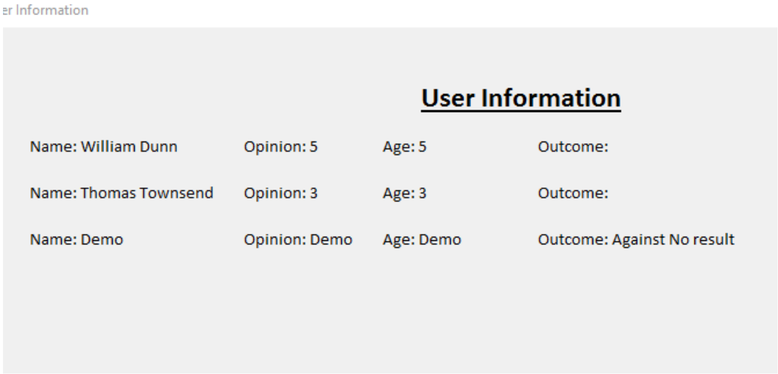
****

4.9 Admin information questionnaire results and participant information

Once the access has been gained the admin has access to to the overall questionnaire results which will be used for analying the data later as well as all the participant personal data. Once finioshed the admin has the functionality to log out and return to the home screen

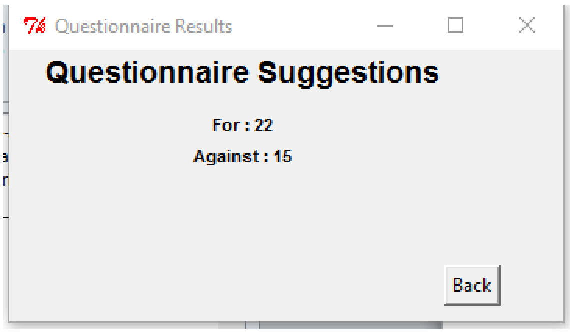


Please select an action:



User Information

Name: William Dunn	Opinion: 5	Age: 5	Outcome:
Name: Thomas Townsend	Opinion: 3	Age: 3	Outcome:
Name: Demo	Opinion: Demo	Age: Demo	Outcome: Against No result



Questionnaire Suggestions

For : 22

Against : 15

4.10 Excel Csv file

Finally the last part of this application has the functionality to back up all personal information to an excel spread sheet this is so that the data can be separated from each test for analysing. As well as this each participants answer is saved so that I can look at the answers individually to analyse the overall condenses for each question.

5.0 Questionnaire testing

To make sure the program worked properly a test case will be devised to make sure all the functions and outcomes were corrected.

Test case :1	**Test Purpose: Submit answers for the Questionnaire**		
Tested on a Windows 8			
Test case steps:			
Step	Procedure	Response	Pass/fail
1	Click the ‘Questionnaire’	Moves to the ‘Question’ page	Pass
2	Select ‘Yes’ for Question 1		
3	Select ‘Yes’ for Question 2		
4	Select ‘Yes’ for Question 3		
5	Click the ‘Next’’ button	Move to page two of the questions	Pass
6	Select ‘Yes’ for Question 4		
7	Select ‘Yes’ for Question 5		
8	Select ‘Yes’ for Question 6		
9	Click the ‘Next’’ button	Move to page two of the questions	Pass
10	Select ‘Yes’ for Question 7		
11	Select ‘Yes’ for Question 8		
12	Select ‘Yes’ for Question 9		
13	Select ‘Yes’ for Question 10		
14	Click the ‘Submit’’ button	Move to the ‘Moves to results page’ or the Questionnaire.	Pass
15	Check Overall Outcome	Main Outcome ‘For	Pass
		For – 6	Pass
		Against – 5	Pass
		No Result – 0	Pass
Comments : The error for missing out questions was tested and pop up box displayed – Pass The clear all answer was tested and cleated all answers – Pass The Previous page button was tested and returned to past page – Pass			
Checked 10th February 2017			

Test case :2	**Test Purpose: Entering Participants details**		
Tested on a Windows 8			
Test case steps:			
Step	Procedure	Response	Pass/fail
1	Click the ‘Next’ after Questionnaire results	Moves to the ‘Participants Detail’	Pass
2	Input ‘Dax Baker’ Into Name section		
3	Input ‘For’ Into Original Opinion section		
4	Input ‘Name’ Into Age section		
5	Click the ‘Submit’ button to save your details into the system	If all the information is imputed correctly a confirmation pop up will appear	Pass
Comments: Fall backs in place in case information is missing error message showed when personal information was missing. - Pass			
Related to test: 1			
Checked 10th February 2017			

Test case :3	**Test Purpose: Admin Page (Login, Show Personal Details, Questionnaire overall results**		
Tested on a Windows 8			
Test case steps:			
Step	Procedure	Response	Pass/fail
1	Click the ‘Admin’ button	Moves to the ‘To Log in’ page	Pass
2	Input ‘Admin’ into username section		
3	Input ‘Password’ into password section		
4	Click Log In’ Button to log into Admin page	Moves to ‘Admin’ page	Pass
5	Click ‘View Users’	Moves ‘Participants details’ page	Pass
6	View Personal details of Participant	The inputted name will read ‘ Dax Baker’	Pass
		The inputted Opinion will read ‘For’	Pass
		The Inputted Age will read ‘26’	Pass

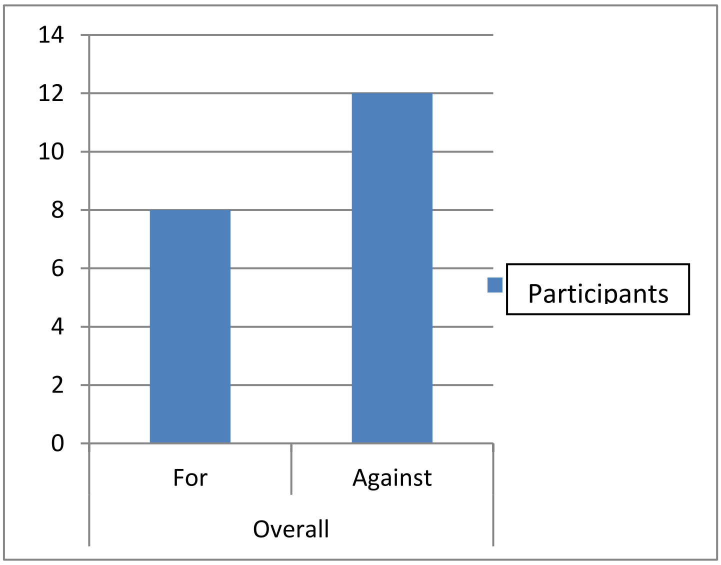
7	Click ‘Back’ Button	Moves Back to the ‘Admin’ page	Pass
8	Click ‘Questionnaire Results’ Button	Moves to ‘Questionnaire Results’ page	Pass
9	Click ‘Log Out’ button	Moves to ‘Home’ page	Pass
Comments: Checked if data was being saved to student.csv file for participant information- Pass Checked if all participant answers were being stored to Questionnaire.csv file- Pass			
Related to test: 2			
Checked 10th February 2017			

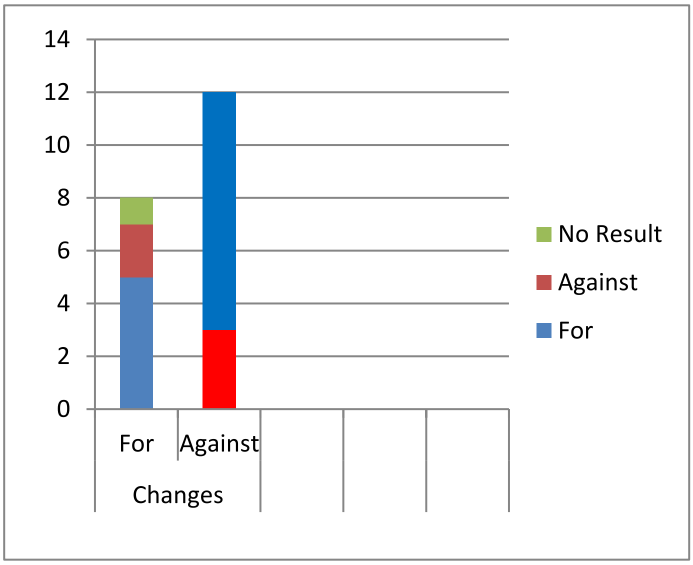
6.0 Findings and analysation

This section of the document will analyse and discuss your answers provided from all three test. Each test will be analysed individually allowing results to be broken down, this will help have a better understanding on whether participants were four or against network manager about the Government.

6.1 Questionnaire part 1

The overall opinion of the participants when first asked if they were for or against network monitoring by the Government was 8 for and 12 against as displayed in the graph below. However as predicted when participants were made to make a rash decision the outcome often changed. Looking at graph two 8 of the participants how said they were for 3 of them of the results had changed. This is a comparison to the participants who were against which was miner as 9 of the 12 participants had an outcome of for. This really showed an in consistency to participant's opinions this was expected when running this test. A lot of the participants when asked showed desire to have more time to think of their answer as many of them expressed it was not a black and white answer, the tests later on will hopefully give better clarity of this and see if there is any impact in the results.





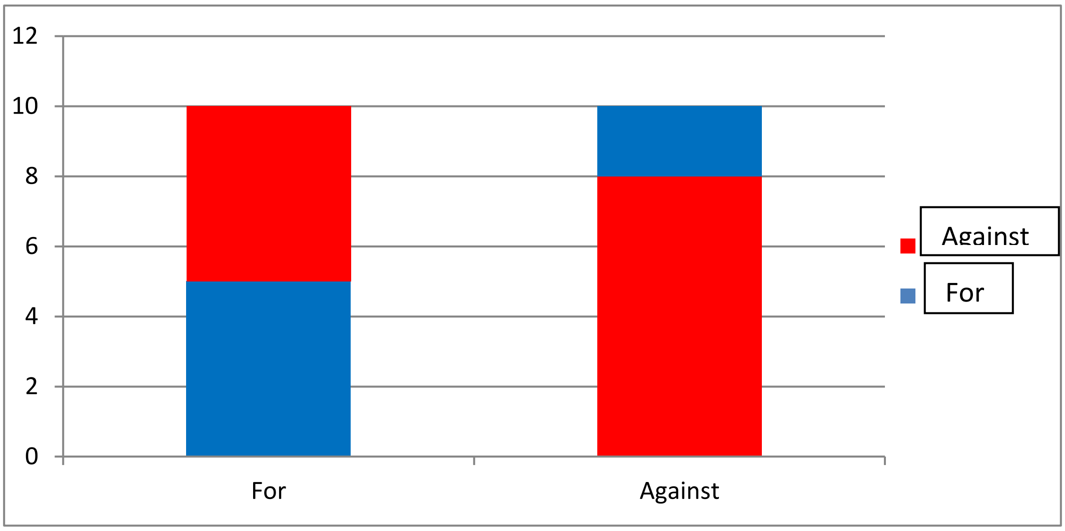
Graph 1

Graph 2

6.1.1 18-26

Another factor having to be consider was age vs awesness, this will looked at further in the interview stages. With technolgy growing vastly over the last decage the younger generation should have a better understaind how how computers and the internet work. In these results it showed that participants not only had their opinions often stay the same the majority were for network montoring. When it came to the 18-26 year olds results showed that the opinions were split 50/50. However whe looking at the changed to ther outcome only three results changed. Looking at the participants answers 80% of participants had a general idea what networking is and 100% of the participants did not have an issue with the Government monitoring social media. Graph 3 show the the changes made in this age bracket going from 50/50 to 80/20 for the montoring of networks.

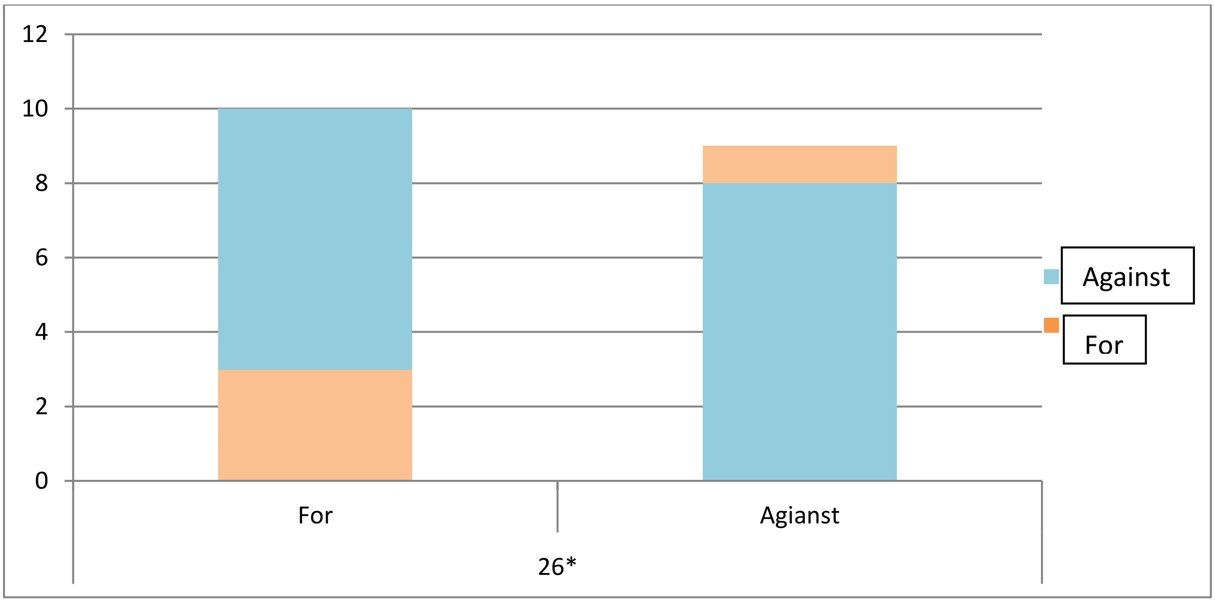
Graph 3 **18-26**



6.1.2 26+

The results for the 26+ however had significantly changes to the outcomes. Looking at the graph below the majority of opinions changed 8 of the 10 participants had a different outcome. When looking at the answers from the participants theirs main concern was social media privacy as 90% of participants wanted the Government not to monitor social media. A surprising result is 70% of participants had no idea what the Government actually monitor. When it comes to opinions on the matter it showed 100% of participants were swayed by the media. More data will be collected in the interview stage of testing to back this theory up.

26*



6.1.3 Conclude

For the first stage of testing it has shown people's opinions aren't often what they think when given no time to think about the decision rash choices are made. Also the results so far are that even though many people think they are against the network monitoring results actually show they might actually be for. It seems age has an impact as well as younger participants seemed to have the same outcome throughout, where the older participants seemed to change. To gain a better understanding of why this is this report will have to look into each question of the interview stage in more detail

6.2 Interview findings

6.2.1 General consensus

The overall opinion when conducting the interviews for each question is seen below

Why do you think Government monitor networks?

The majority of the participants found that the overall use for network monitoring was to monitor the movements of terrorists and try have an understanding of what they are planning?

Do you think the Government go too far on motoring peoples personal information and why?

This answer was split down the middle some participants saying the Government are doing enough where others are saying they are doing too much. Looking into it further it seemed the participants who decided the Government were doing too much all seemed to have answers related to the news this seemed to indicate that they were easily influenced by social media, this also was backed up in the questionnaire as most of the participants stated they were.

What do you think is the best way to monitor networks? E.g. (letting the public know exactly what they access)

The overall consensus with this question was contradicting to most of the participant's questionnaire results as most answered no to the Government monitoring social media. However the overall opinion was for the Government to monitoring social media with programs that pick up key words, as well as doing this let the public know exactly what sort of thing will be flagged up. The other opinions were that the Government shouldn't monitor networks as it just invades the privacy laws that are in place.

How Success do you feel think network monitoring has been to counter terrorism?

Participants found even though network monitoring works it is not the answer and terrorists will always just find another way to communicate. Even though this was the majority of the answer not one participant came up with another idea on how to combat the issue.

Can you think of any other organisations having access to your social media accounts?

This question was more designed to see if participants were aware of the new deal the Government have come up with for third parties to have access to their social media to help the Government. Ironically the overall opinion was based around marketing and advertising companies using participant's personal data to sell them products. Ideally similar to the powers of a Facebook API

Would the Government giving access to third parties monitoring your social media have any impact on how you use social media?

This question was quite a sensitive subject participants were really against the Government giving powers to third parties. Most of the participants suggesting if they knew, then they would probably move to a more secure way of communicating. This is an interesting outcome as they are comfortable with advertising and marketing companies having access with no concern, however as soon as you mention anything to do with the Government giving access to Companies they refuse to accept it.

What sort of information do you think the Government want from you when looking into your accounts?

The Overall opinion from the participants here was key words and certain information to be flagged up on social media. Such as certain videos being liked and shared and likes to certain pages. A system which was discussed would be a traffic light system so that depending on the chats and the content being talked about then you would be graded a colour. E.g. green friendly chat, amber minor chats like Drugs and red for terrorist conversations.

What is your opinion in the best way in countering terrorism?

This question had been the only one not to have any real similarities to the participant's answers. It seems everyone had their own opinion on the matter, most agreed networking was the best way to counter terrorism however there are better ways about it. Such as not getting involved in other countries issues.

Could you tell me anything About Facebooks API?

This was an interesting outcome, throughout the interviews every participant gave me information on what a Facebook API could do but didn't actually know what it was called.

Which protect your information better companies or the Government and why?

Like one of the questions earlier this split participant's opinion, however they all gave very valid reasons. Participants who believed the Government were better, argued that they were not aiming to make profit from their personal information where companies were only accessing personal information so that they could make a profit. Where participants who thought companies were better believed that personal information is protected by laws and companies would face huge fines if breached that they would put in extra measures to protect information.

6.2.2 Interview Results

The results for this test showed that overall the participants opinion seemed to match their outcome with just two changes out the whole results. This seemed to show that when the participants had time to think of their opinion through discussing the matter seemed so give them enough time to gather if they were for or against network monitoring. Of the 15 participants for took part in the Interview stages eight choose for the monitoring of networks with just one change and seven were against the monitoring of networks and against one changing to for.

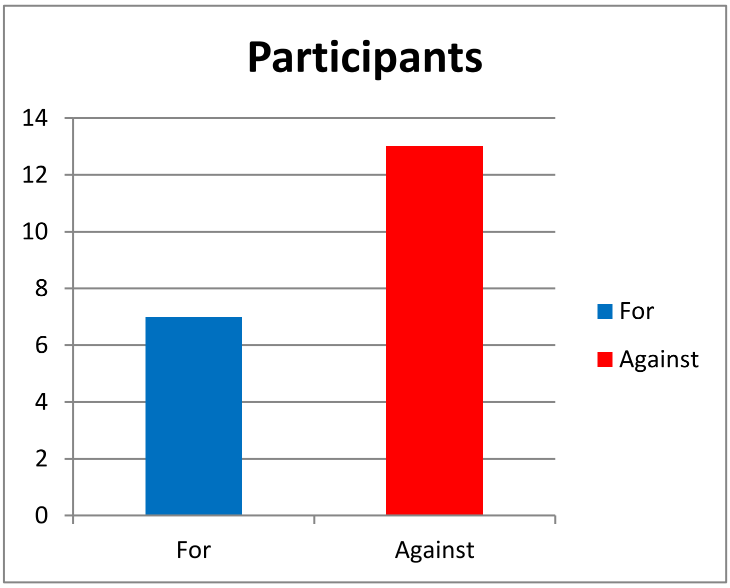
6.2.3 Age Vs Awareness

Similar to the first test results showed that the younger generation (18-26) were generally for the Government monitoring networks with 6 of the 7 being for it. Where the older generation (26+) showed the 7 of the 8 participants were against the monitoring of networks. This does seem to back up that the younger generation are more aware what is going on with the monitoring of networks.

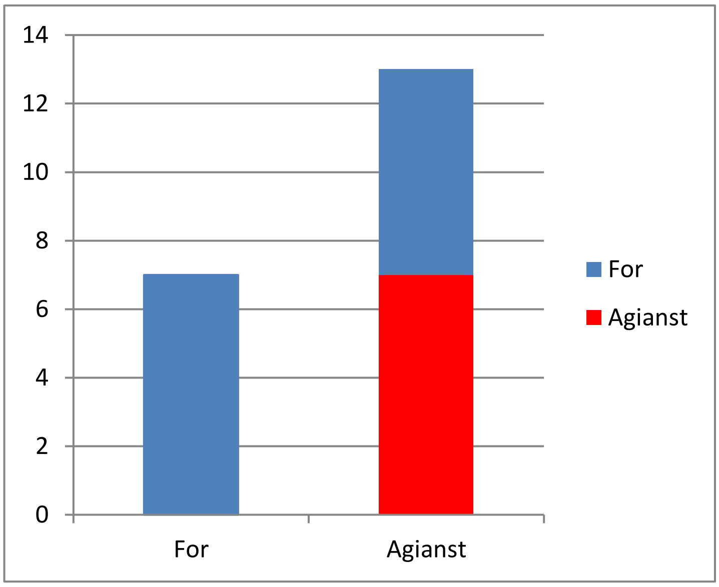
6.3 Questionnaire part 2

The overall opinion of the participants when first asked if they were for or against network monitoring by the Government was 7 for and 13 against as displayed in the graph below. However results for this drastically changed, as explained once the participant made an opinion on the monitoring of networks they were given an information sheet on what network monitoring actually is. Participants who opted for the monitoring of networks none of the outcomes had changed. However of the 13 participants who were against the monitoring of networks 7 of the results changed to for the monitoring of networks, as you can see in the graph below

Graph 1



Graph 2

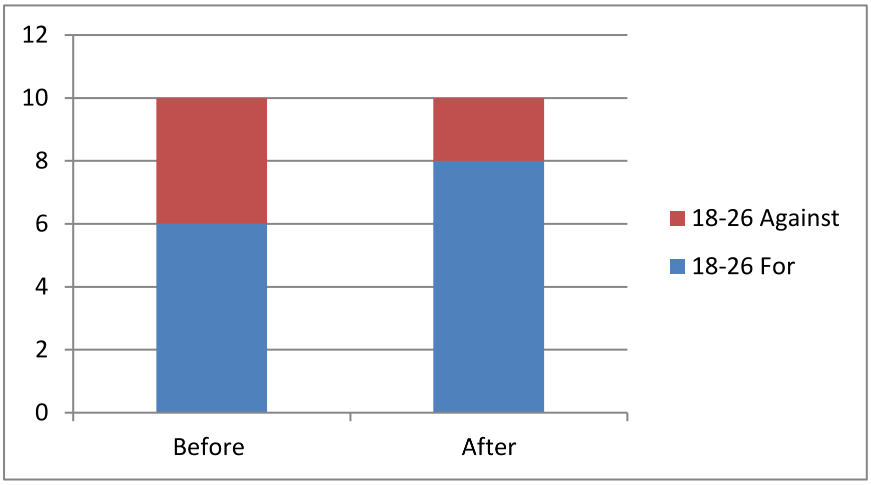


18-26

18-26

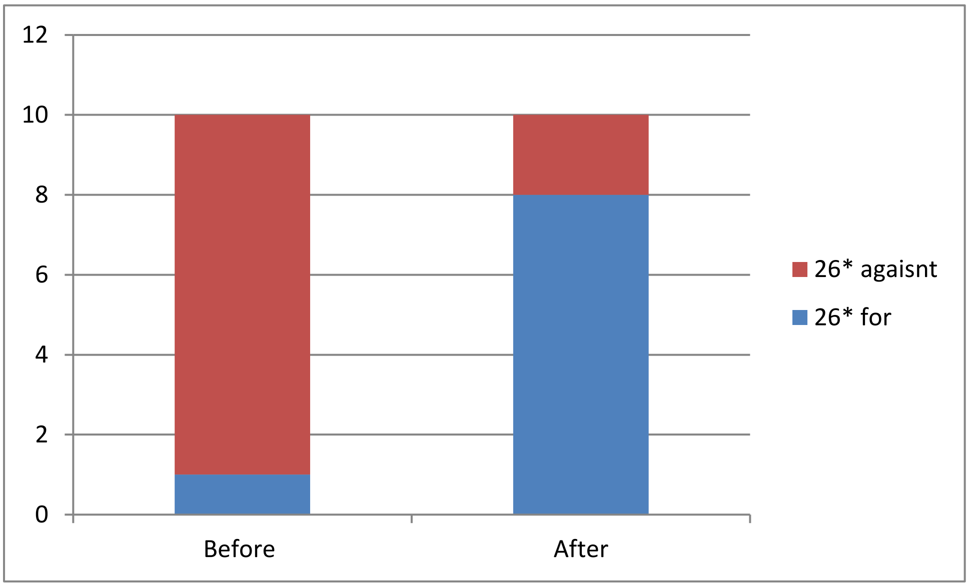
When lookng at the overall opinion of the younger generation the majority was for the monitoring of networks, even before the information sheet was handed too them. The results show once the participants took the questionniare the results swayed more towards the for monitoring of networks. There wasn’t much as a change in these results as expected with the younger generation being more awere of what going on in the world of technology.

Graph 3



6.4.1 26+

The results for the 26+ however had dramatically changed. Looking at the graph below before only 1 participant was for the monitoring of networks before reading the information sheet and taking part in the questionnaire. The outcomes showed a dramatic change in opinion with seven participant's outcome changing to for the monitoring of networks. When looking into this there was a possibility that most of the participants not actually knowing anything about network monitoring this showed in the way they answered some of the questionnaire.



7.0 Conclusion

After going into depth on how the Government monitor networks in the interest in public safety. It was found that the general consensus is the public is that they are for the use of network monitoring, however the public have no actual idea how the Government go about doing it. There is no clear solution on how the Government can make the public aware of the information being gathered without giving away this knowledge to terrorists or criminals.

The research carried out for this dissertation was an interpretative research philosophy which allowed the report to gather information and opinions on the matter of network monitoring. The literature review allowed this report to understand the amount of work the Government go into to when monitoring networks looking at the costs for effective it is and how they are using social media to combat terrorism,

7.1 Objectives

'Review the literature and identify characteristics and features of network monitoring for example what steps the Government actually do to prevent this comparing in to other countries'

This objective is completed in the research gathered in the literature review, which gives a clear understanding on how the Government monitor networks and how they are trying to combat terrorism,

'Gather a better understanding on how the Government monitor networks and have an idea how they are interacting with social media'

This is also gathered in the literature review looking at how the Government are giving power to third parties to monitor the public's social media. Looking into the Facebooks API in the literature review to understand how anyone can access your personal details with just a simple program.

'Analysis the actual data gathered from participants of the study and review the actual results compared to opinion'

This is completed in the analysis and findings section, each section is separated so that the data can be reviewed in more detail to have a better understanding on what the public think on the matter and actually see if they are for or against the monitoring of networks.

'Interrupt how the public actually feel towards network monitoring'

Understanding how the public feel and what they actually know about network monitoring was key to the report. The findings and analysis section shows a general consensus of what the public actually think on each matter.

'Have a better Understanding how the Facebook API actually works and what information can be gathered'

The research gathered in this report demonstrates the power the Facebook API has. It enabled the participants taking part in the information test to have some knowledge on what it can do.

7.2 Age

Throughout the testing stage participants knowledge had a clear difference, the generation factor really had an influence on the results. The younger generation generally seemed to have better understanding on what the Government were doing as well as understanding what network monitoring was. They also seemed to have the same outcome as their opinions. Where the older generation seemed to be unaware on what the Government were doing and how they did it, a lot of the older generation seemed to be against the idea of network monitoring however when answering the survey their outcomes were often for the monitoring of works.

7.3 Awareness

This dissertation has showed that the general public has no real idea how the Government monitor networks and it seems the majority of people are really influenced by the media. Most participants were against the idea of third parties having access to their social media but had no Idea that anyone who knew how to use the Facebook API would have the same access as the third party companies.

7.4 Future research

To gather an even better understanding of the power people have on gaining personal information this report could further go into the power of the Facebook API. However not only with this platform, the research could use other social Medias such as Twitters API as well as Googles. Future tests such demonstrating to the public what information can be gathered with a simple API program. Making the public more aware on how easy sensitive information can be accessed and that they would need to do more in order to protect their information.

Another path this research could take is to directly work with the Governments organisations such as The MOD or GCHQ. This would allow research to be gathered directly from a company that directly deals with network monitoring. Allowing this report to possibly give the public a better understanding on what information is taken and why this information might be gathered.

8.0 Bibliography

http://www.alternet.org/story/155764/6_Government_surveillance_programs_designed_to_watch_what_you_do_online

https://arstechnica.co.uk/tech-policy/2016/11/investigatory-powers-act-privacy-disaster-waiting-to-happen/

http://www.computerweekly.com/news/4500279596/Britain-to-pay-billions-for-monster-internet-surveillance-network

http://www.economist.com/node/10808502

https://en.wikipedia.org/wiki/List_of_government_mass_surveillance_projects#United_Kingdom

https://en.wikipedia.org/wiki/List_of_government_mass_surveillance_projects

https://en.wikipedia.org/wiki/Interception_Modernisation_Programme

Link- http://en.wikipedia.org/wiki/Fiber_optic_splitter

Rosen.D. 6 Government Surveillance Programs Designed to Watch What You Do Online Link-

https://www.gov.uk/government/organisations/national-counter-terrorism-security-office/about

https://www.gov.uk/government/statistics?keywords=ter&topics%5B%5D=all&departments%5B%5D=all&from_date=&to_date=

http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted/data.htm

http://www.legislation.gov.uk/ukpga/2015/6/contents/enacted

http://www.independent.co.uk/news/uk/politics/government-awards-contracts-to-monitor-social-media-and-give-whitehall-real-time-updates-on-public-10298255.html

https://medium.com/@AntonioCasilli/four-theses-on-digital-mass-surveillance-and-the-negotiation-of-privacy-7254cd3cdee6 Link- https://nsa.gov1.info/utah-data-center/

Hughes.S, Goodwin.S. NSA Director Says Data Programs Foiled Plots Link- http://online.wsj.com/articles/SB10001424127887324688404578541582428920860

Grubb.B.http://online.wsj.com/articles/SB10001424127887324688404578541582428920860

https://www.programmableweb.com/api/facebook

https://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/231.pdf

Link- http://resources.infosecinstitute.com/cyberterrorism-distinct-from-cybercrime/

https://www.rt.com/uk/337759-surveillance-powers-bill-cost/

Barlett.G. (Apr 2009) GPS Tracking System and Terrorism Link- http://www.rmtracking.com/blog/2009/04/20/gps-tracking-system-and-terrorism/

Link- searchsecurity.techtarget.com/definition/cyberwarfare

Purvis.C. Network Monitoring Could Help Detect State-Sponsored Cyberattacks Link- http://www.securitymanagement.com/news/network-monitoring-could-help-detect-state-sponsored-cyberattacks-0010176

http://www.telegraph.co.uk/technology/2016/11/29/investigatory-powers-bill-does-mean-privacy/

https://www.theguardian.com/uk-news/2016/oct/28/britain-foiled-terror-attacks-plots-police-counter-terrorism-security-services

http://www.wired.co.uk/article/government-pays-companies-to-monitor-social-media-use

Laws

Data Retention and Investigatory Powers Act 2014 Link- http://online.wsj.com/articles/SB1000142412788732468840457854158242892086

Books

[1] *Solove,D, Harlan.M. (2011)* Nothing to Hide

George Washington University Law School: Yale University Press.p46.

9.0 Append

9.1 Ethics Form

PART ONE

Name of applicant:	Dax Baker
Supervisor (if student project):	Dr. Hewage, Chaminda
School / Unit:	Cardiff School of Management
Student number (if applicable):	ST20093283
Programme enrolled on (if applicable):	BSc. (Hons) Computing
Project Title:	Does the Government have the right to monitoring networks for public safely?
Expected start date of data collection:	15/01/2017
Approximate duration of data collection:	2 months
Funding Body (if applicable):	N/A
Other researcher(s) working on the project:	N/A
Will the study involve NHS patients or staff?	No
Will the study involve human samples and/or human cell lines?	No

Does your project fall entirely within one of the following categories:	
Paper based, involving only documents in the public domain	No
Laboratory based, not involving human participants or human samples	No

Practice based not involving human participants (eg curatorial, practice audit)	No
Compulsory projects in professional practice (eg Initial Teacher Education)	No
A project for which external approval has been obtained (e.g., NHS)	No
If you have answered YES to any of these questions, expand on your answer in the non-technical summary. No further information regarding your project is required. If you have answered NO to all of these questions, you must complete Part 2 of this form	

In no more than 150 words, give a non-technical summary of the project
The main aim of this project is to determine whether the control of networks by the government is helping protect the wellbeing of the UK. Over the years the governments have become more involved in monitoring networks to counter terrorism. This research investigates the perception of general public regarding networking monitoring and interfering with their private life. Furthermore, this research will investigate how social media technologies such as Facebooks APIs could be manipulated to obtain personal information about connected users. Further research/analysis would be carried out to understand the effect of decrypting cryptic messages used by Terrorist networks by law enforcement authorities.

DECLARATION: **I confirm that this project conforms with the Cardiff Met Research Governance Framework** **I confirm that I will abide by the Cardiff Met requirements regarding confidentiality and anonymity when conducting this project.** **STUDENTS: I confirm that I will not disclose any information about this project without the prior approval of my supervisor.**	
Signature of the applicant: D Baker	Date: 18/11/2016
FOR STUDENT PROJECTS ONLY	
Name of supervisor: Dr. Chaminda Hewage	Date: 18/11/2016
Signature of supervisor:	

Research Ethics Committee use only
Decision reached: Project approved □ Project approved in principle □ Decision deferred □ Project not approved □ Project rejected □

Project reference number: Click here to enter text.	
Name: Click here to enter text.	Date: Click here to enter a date.
Signature:	
Details of any conditions upon which approval is dependant: Click here to enter text.	

PART TWO

A RESEARCH DESIGN	
A1 Will you be using an approved protocol in your project?	No
A2 If yes, please state the name and code of the approved protocol to be used[1]	
N/A	
A3 Describe the research design to be used in your project	

An interpretative research philosophy will be adopted involving an inductive research strategy and qualitative data gathering for this dissertation. The qualitative research methods will be employed to gather information related to Network monitoring by authorities.

Questionnaire

- The researcher aims to gather a variety of data from the questionnaires created – with the anticipation that age has a significant impact on what people think of the monitoring or networks.
- The researcher will hand out data to the Cardiff MET students and staff on two different dates. One before gathered to see what they think they know and how they feel towards it. Then again after I have gathered some of the facts. See if results will change after.
- The timing of the questionnaire should take no longer than 5 mins

Detailed interviews/questionnaire

- The idea behind this project is to see whether the participants actually understand the idea behind what the government do when monitoring networks

  For this:-

- The researcher would arrange some detailed interviews with students and staff of Cardiff MET. Each interviewee will be selected randomly and get an opportunity to answer 10 questions. An email confirmation will be obtained from each participant before the interview.
- After this the researcher would ask the participant their opinion on the government monitoring networks.
- The researcher will then devise a questionnaire that participants would answer. The follow on analysis will determine the participants view on network monitoring.

[1] An Approved Protocol is one which has been approved by Cardiff Met to be used under supervision of designated members of staff; a list of approved protocols can be found on the Cardiff Met website here

- The participants will be asked beforehand their opinion on the matter and I am hoping the results of the survey will alter their thought on government control

Sample

The random sampling technique will be used in order to capture more general views about network monitoring. The sample size will be moderate in size as described below. The participants will be voluntary people replying to the questionnaire/interviews.

- The age (awareness vs. age) will be a main factor in this research design. Therefore, an extra effort would be made to find a good balance of participants (from different age groups) for the study. I want to determine if experience and awareness of threats with technology is a factor.
- An even range of participants will be needed for both interview and questionnaires, a range of 20 from each category will be sufficient to find an average outcome of opinion

Participants:

- All participants will be over the age 18 (Mainly staff and students from Cardiff MET)
- The researcher will only record age

The collected primary data will then be analysed to draw final conclusions. Thematic analysis will be used to identify different awareness groups and patterns of usage of Network monitoring.

The anonymity of all the participants will be maintained throughout the research. Furthermore, all collected data will be remained confidential and will be stored securely (i.e. encrypted data) in a password protected computer system. All data will also be deleted securely at the end of the project.

A4 Will the project involve deceptive or covert research?	No
A5 If yes, give a rationale for the use of deceptive or covert research	
No	
A6 Will the project have security sensitive implications?	No
A7 If yes, please explain what they are and the measures that are proposed to address them	
N/A	

B PREVIOUS EXPERIENCE
B1 What previous experience of research involving human participants relevant to this project do you have?
None
B2 **Student project only** What previous experience of research involving human participants relevant to this project does your supervisor have?

Dr. Chaminda Hewage has more than 10 years of experience in conducting subjective tests involving human participants.

C POTENTIAL RISKS

C1 What potential risks do you foresee?

Two major issues I can foresee are

- Not all the details regarding decrypting cryptic messages used by terrorist cells will be available from public sources.

- I would investigate how Facebooks API could be used to gather information about its users. However, if Facebooks privacy settings are changed, I won’t be able to demonstrate all the possibilities which could be possible with the current version of the API.

C2 How will you deal with the potential risks?

- The latest news bulletins and white papers will be referred to obtain information regarding latest tools and approaches for cryptic message decryption by law enforcement authorities.
- For the API of the project I will constantly keep checking whether the privacy settings are changed and make sure that I am following all the rules set by which ever social media API I am using.

9.2 Consent Form

Cardiff Metropolitan University

Ethics Committee

PARTICIPANT CONSENT FORM

Cardiff University Ethics Reference Number:

Participant name:

Title of Project: Does the Government have the right to monitoring networks for public safely

Name of Researcher: Dax Baker

____

Participant to complete this section: **Please initial each box.**

1. I confirm that I have read and understand the information sheet for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily. □

2. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving any reason. □

3. I agree to take part in the above study. □

____ ____________________

Signature of Participant Date

____ ____________________

Name of person taking consent Date

____

9.3 Information Sheet

Signature of person taking consent

PARTICIPANT INFORMATION SHEET

Does the Government have the right to monitoring networks for public safely?

Project summary

The purpose of this research project is to establish whether you think the control of networks by the government is helping protect the wellbeing of the UK. Over the years the governments has become more involved in monitoring networks to counter terrorism. Your participation will enable the collection of data which will form part of a study being undertaken at Cardiff Metropolitan University.

Why have you been asked to participate?

You have been asked to participate because you fit in one of the profile of the population being studied; that is you are between the ages of

18 and 25

26-65

The reasoning between the different age groups to so get an even range of opinion of government control, as well as the knowledge of what network control actually is.

You will be agreeing to one of the following

The interview will involve a range of audio questions for the researcher to listen back and analyse. After this you will be asked a certain question before being given some facts. Once the facts have been given you will be required to fill in a multiple choice questionnaire on a computer this will give me an answer available to you if requested however it will only be relevant to my study.

Project risks

The research involves the completion of a questionnaire and participation in audio interview which will be recorded for later analysis. There will be no sensitive information taken from this study this is only based on your personal opinion and no answer can be viewed as wrong. Furthermore, if you don’t feel comfortable with any of the questions due to person views (Government can be a sensitive subject) –I will completely respect your decision.

How we protect your privacy

All the information you provide will be held in confidence. We have taken careful steps to make sure that you cannot be directly identified from the information given by you. Your personal details (e.g. signature on the consent form) will be kept in a secure location by the research team. When we have finished the study and analysed all the information, the documentation used to gather the raw data will be destroyed except your signed consent form which will be held securely for 5 years. The recordings of the focus interview will also be held in a secure and confidential environment during the study and destroyed after 5 years.

YOU WILL BE OFFERED A COPY OF THIS INFORMATION SHEET TO KEEP

If you require any further information about this project then please contact:

Dax Baker Cardiff Metropolitan University

Cardiff Metropolitan University email: St20093283@cardiffmet.ac.uk

9.4 Fact Sheet

Participants Fact Sheet

What is computer networking?

Computer and network surveillance is the monitoring of computer activity and data stored on a hard drive, or data being transferred over computer networks such as the Internet. The monitoring is often carried out covertly and may be completed by governments, corporations, criminal organizations, or individuals. It may or may not be legal and may or may not require authorization from a court or other independent government agencies

Why does the Government do it?

Surveillance allows governments and other agencies to maintain social control, recognize and monitor threats, and prevent and investigate criminal activity. With the advent of programs such as the Total Information Awareness program, technologies such as high speed surveillance computers and biometrics software, and laws such as the Communications Assistance For Law Enforcement Act, governments now possess an unprecedented ability to monitor the activities of citizens.

Costs

Looking at the cost for the government to run fully functional network monitoring system (ICRs) – databases which has been the plan since the Investigatory Powers Bill 2016 had been passed. The original cost was estimated to cost £170 Million, however a recent study coming of Denmark has shown the head-per-head cost for this system would be £19. So the overall start up would be an investment of £1.2bn, as well as annual running costs

Third parties

The government recently started paying third companies to help monitor social media and a wider range. In an announcement issued by the Crown Commercial Service, the names of companies that have won government contracts were made public, along with the details of what they are expected to provide. The agreement with the companies replaces a previous agreement, which employed companies solely to monitor the press. It has now been expanded to incorporate multiple forms of media, and cast the net more widely than professional journalists

Facebook API

The Facebook API is a platform for building applications that are available to the members of the social network of Facebook. The API allows applications to use the social connections and profile information to make applications more involving, and to publish activities to the news feed and profile pages of Facebook, subject to individual users privacy settings. With the API, users can add social context to their applications by utilizing profile, friend, Page, group, photo, and event data. The API uses RESTful protocol and responses are in JSON format.

9.5 Interviews

Interview 1

Participant interview

Name- Raphaël (23)

1. Why do you think Government monitor networks?

 In order to be more efficient in fighting criminality and protecting people.

2. Do you think the Government go too far on motoring peoples personal information and why?

 According to the latest news, the British Government has indeed gone too far concerning the collection and the use of personal information's. Even in a difficult context due to counter terrorism, the Government overstepped its rights to collect personal information's about non-concerned citizens.

3. What do you think is the best way to monitor networks? E.g. (letting the public know exactly what they access)

Letting the public to know exactly what type of data has been collected about them seems to be the most adapted and fair way to do it. However, it can obviously also present disadvantages due to the people with bad intentions about the society that will try to focus on hiding these information's, resulting on a more difficult access by the Government to collect it.

4. How Success do you feel think network monitoring has been to counter terrorism?

However, the paradox is that network monitoring has clearly been crucial and efficient concerning counter terrorism, not only in UK but all over Europe as well.

5. Can you think of any other organisations having access to your social media accounts?

The today's problem is that people's personal data isn't always kept for the organisation that collected it at the beginning. These organisations might sell it to others, sometimes in an illegal way, resulting on a general loss of control and understanding of who has personal information's about us and what they will do with it.

6. Would the Government giving access to third parties monitoring your social media have any impact on how you use social media?

This could have a negative impact on how I use social media (e.g.: a mistrust and lower use of it). It only depends on what type or third parties are concerned (companies, public organisations, other Governments…) and if we are correctly informed of the use of it.

7. What sort of information do you think the Government want from you when looking into your accounts?

Depending on the type of account they have access to, they are probably focusing on the personal data in order to have a very precise idea of each profile of people.

8. What is your opinion in the best way in countering terrorism?

Germany, France and some Scandinavian countries has demonstrated quit good effectiveness in countering terrorism, particular through a really close monitoring to suspected people (e.g.: giving a huge attention of their network connections with people).

9. Could you tell me anything About Facebooks API?

   /

10. Which protect your information better companies or the Government and why?

Some companies showed a real willingness to protect their user's personal information's against the Government (e.g.: WhatsApp). On the other hand, others has for example been convicted for not offering, voluntarily or not, enough security or information's about what they do with these information's.
Concerning the British Government, it is said to be one of the world's foremost surveillance state, with a global following of its citizens, no mattering if they represent or could represent a danger.

Interview 2

Participant interview

Name- Richard (54)

1. Why do you think Government monitor networks?

To monitor the movements of terrorists

2. Do you think the Government goes too far on monitoring peoples personal information and why?

No, not at all I feel that in recent times the Government has to keep up with what people are doing to prevent any future terrorist attacks

3. What do you think is the best way to monitor networks? E.g. (letting the public know exactly what they access)

Via social media the whole world is using the web these days

4. How Success do you feel think network monitoring has been to counter terrorism?

I feel that not enough is being done to prevent this

5. Can you think of any other organisations having access to your social media accounts?

Not that I am aware of

6. Would the Government giving access to third parties monitoring your social media have any impact on how you use social media?

No more needs to be done

7. What sort of information do you think the Government want from you when looking into your accounts?

I am not too sure this sort of thing is not my area of expertise

8. What is your opinion in the best way in countering terrorism?

Application programming interface on Facebook

9. Could you tell me anything About Facebooks API?

No sounds like what I just said though

10. Which protect your information better companies or the Government and why?

Unsure

Interview 3

Participant interview

Name- Harry (26)

1. Why do you think Government monitor networks?

To combat tourists, grooming, Paedophiles, traf0ficking, highly illegal stuff and for use in criminal investigations.

2. Do you think the Government goes too far on monitoring peoples personal information and why?

I don't think they go too far although I don't know exactly what they monitor but I don't believe they are looking at everything only specifics

3. What do you think is the best way to monitor networks? E.g. (letting the public know exactly what they access)

Yeah they should notify the public what they monitor or this could alert criminals of what not to do or how they should avoid being detected. They could just say general stuff not specifics what they monitor

4. How Success do you feel think network monitoring has been to counter terrorism?

Very effective although more could be done with social network companies to target terrorists. Better links with the police/ Government could prevent radicalism

5. Can you think of any other organisations having access to your social media accounts?

Mi5, Government, social networks themselves

6. Would the Government giving access to third parties monitoring your social media have any impact on how you use social media?

Yes massively, might even delete it because can already see links to different sites selling or passing info over about my google searches. IL be more careful even though nothing to hide. That company may be hacked and my info breached

7. What sort of information do you think the Government want from you when looking into your accounts?

I don't think they are looking in to my account but imagine if I shared a lot of terrorist material, videos that should be deleted, or whats app conversations linked with isis they will be monitored. I might even be monitored for writing this over messenger. Or if I've had a criminal background

8. What is your opinion in the best way in countering terrorism?

To counter terrorism I think more monitoring of accounts. Closer relationship with social media companies like apple, Whats app, Facebook, Reddit, twitter to help. Remodel and build better prisons where people become radicalised, shut Syria off from the rest of the would, if they can cut their internet signal, remove Assad, build Syrian army and kill Isis

9. Could you tell me anything About Facebooks API?

Not sure what API is.

10. Which protect your information better companies or the Government and why?

The Government because they put laws in place to partly protect us from companies abusing their freedom to profit and benefit from out information. Just saying but many people's passwords will be known by the social networking companies which usually are the same as say a bank account. Information like this could be used illegally. More needs to be done to protect our identity and information as there's been a lot more hacking stories happening. I don't want to be a victim.

Interview 4

Participant interview

Name- Tom Hannigan (23)

1. Why do you think Government monitor networks?

To collect data that could be used in several capacities such as internal and external security, as well as for research on how populations can be influenced for capital and political gain, and ideological changes.

2. Do you think the Government go too far on motoring peoples personal information and why?

Yes, as increasing invasions into individuals' privacy comes under the guise of national security, when in reality I suspect there is significant action by political and corporate bodies on how to influence people. In the aftermath of several terrorist attacks, it has come to light that they were organised over unencrypted and known to be monitored communication channels such as sms, which has not been picked up by Government monitoring. Yet further more invasive methods are being used. There are currently plans to make giving the password to your Facebook account compulsory when entering the USA and I'm sure that this will continue to spread across the western world. The Government also has a poor track record of data protection which will lead to regular scandals as leaked data will have the potential to ruin people's lives even if they have not broken the law, such as extra-marital affairs, pornography use, inappropriate jokes etc.

With the addition of smart home tools such as Alexa and Google home, voice recording from the home is recorded and kept for an undefined length of time with will add another dimension to Government invasiveness, and the first case is in courts at the minute as far as I am aware that is using information captured and recorded in this way, without the direct consent of the homeowner.

3. What do you think is the best way to monitor networks? E.g. (letting the public know exactly what they access)

I think there should be end to end encryption as a right for any individual if they choose without Government access, and if networks are being monitored, then it should be required by law to make it clear, similar to how the EU has made it a requirement for websites to show cookie tracking.

4. How successful do you feel think network monitoring has been to counter terrorism?

Somewhat successful. However there is simply too much data to be used to effectively monitor for terrorism and I believe it will ultimately be used for other purposes.

5. Can you think of any other organisations having access to your social media accounts?

Information is sold and distributed widely between social networks and various businesses. I would assume nearly any company could do significant checks on my personal data assuming they were willing to spend enough money and buy the information from the organisation that originally obtained it, despite data protection laws.

6. Would the Government giving access to third parties monitoring your social media have any impact on how you use social media?

Yes, I would make efforts to communicate through more secure mediums on principle alone.

7. What sort of information do you think the Government want from you when looking into your accounts?

They monitor for key words that pertain to illegal activities, and I think they probably look at language use very carefully and how that relates to various demographics I am in. A recent study used machine learning applied to social media statuses and could diagnose depression with greater accuracy than experienced clinical psychologists.

8. What is your opinion in the best way in countering terrorism?

The best way I believe is through real life monitoring of high risk groups and areas. Network monitoring can be a useful tool, but should be treated with the same respect and need the same justification as monitoring people in real life, including more thorough data protection and destruction of collected data after an investigation is finished.

9. Could you tell me anything About Facebooks API?

I don't know what API stands for.

10. Which protect your information better companies or the Government and why?

I think both don't have significant motivation or a high enough stake in protecting mine or other members of the population's information.

Interview 5

<u>Participant interview</u>

Name- Sherri (24)

1. Why do you think Government monitor networks?

Terrorist activities/ treason

2. Do you think the Government goes too far on monitoring peoples personal information and why?

At times I feel like there is too much data for them to find it useful and I feel that they may share it with unnecessary parties

3. What do you think is the best way to monitor networks? E.g. (letting the public know exactly what they access)

Pinging keywords or suspicious activity

4. How Success do you feel think network monitoring has been to counter terrorism?

Not very. Once again I think there is too much data.

5. Can you think of any other organisations having access to your social media accounts?

Many unnecessary sections of the Government have access. The department of health for example…why?

6. Would the Government giving access to third parties monitoring your social media have any impact on how you use social media?

Yes I believe so. Anything I google is already causing a variety of ads to be thrown at me if the ads where tailors to my private conversations things could get weird.

7. What sort of information do you think the Government want from you when looking into your accounts?

The idea is that they are looking for threats. I think there could be additional motives. Governments are often funded by large corporations which could use the information for marketing research.

8. What is your opinion in the best way in countering terrorism?

Abolishing all forms of religion…but since that isn't going to happen. Stop getting involved in other countries wars and bombing people you have no business bombing. I'm all for taking in refugees.

9. Could you tell me anything About Facebooks API?

Mark Zuckerberg

10. Which protect your information better companies or the Government and why?

That's vague as hell. Some companies maybe? Banks. But Facebook sucks

Interview 6

Participant interview

Name- Angel (29)

1. Why do you think Government monitor networks?

In order to gain knowledge of any threat, whether that be towards the general public or those with vested interest to maintain the status quo

2. Do you think the Government go too far on motoring peoples personal information and why?

Yes. All electronic information is now monitored. Like it or not Governments have access to all private online details.

3. What do you think is the best way to monitor networks? E.g. (letting the public know exactly what they access)

AI program that have been tested prior to use, as this will prevent humans using sensitive information for personal ago.

4. How Success do you feel think network monitoring has been to counter terrorism?

Fairly but network monitoring will not stop terrorism and its importance is way over thought of

5. Can you think of any other organisations having access to your social media accounts?

The ones that have full access, we never hear about.

6. Would the Government giving access to third parties monitoring your social media have any impact on how you use social media?

Yes, reduce private I formation posted.

7. What sort of information do you think the Government want from you when looking into your accounts?

All info, as algorithm is used to determine a threat.

8. What is your opinion in the best way in countering terrorism?

First by accepting responsibility for decades of exploitation via colonialism and then neo-colonialism in the Middle East. Then talks can begin. Although this will never happen and the alternative is to bomb them all or at least that is what our leaders believe.

9. Could you tell me anything About Facebooks API?

Unfortunately no. Will be looking it up now though.

10. Which protect your information better companies or the Government and why?

Government as no profit based mentality that companies maintains.

Interview 7

Participant interview

Name- Warren (21)

1. Why do you think Government monitor networks?

Terrorism and to make sure they have information on vulnerable individuals

2. Do you think the Government goes too far on monitoring peoples personal information and why?

I think it is safer that it is monitored properly so that more people can be caught before they do any harm to the community

3. What do you think is the best way to monitor networks? E.g. (letting the public know exactly what they access)

I think personally the best way to monitor everything is to make sure nothing is encrypted as this will stop people using encrypted services to arran

4. How Success do you feel think network monitoring has been to counter terrorism?

I think it is working in some cases but I think that there will never be a way to completely stop them as not every situation is the same so people will always find a way around it.

5. Can you think of any other organisations having access to your social media accounts?

I believe that if someone wanted to monitor your activity hard enough that it is possible for them. All they need is the right tools

6. Would the Government giving access to third parties monitoring your social media have any impact on how you use social media?

No If they feel the need to check all my personal information I would be fine with it as I have nothing to hide and would not change how I act on social media.

7. What sort of information do you think the Government want from you when looking into your accounts?

I think they would be looking into anything to show a pattern in behaviour that may be leading towards a threat to our community

8. What is your opinion in the best way in countering terrorism?

There will never be a right or wrong way to ever completely stop terrorism but the best way would be to keep doing what they're doing be more ruthless in cracking down on the suspected terrorists.

9. Could you tell me anything About Facebooks API?

I have never heard of that at all.

10. Which protect your information better companies or the Government and why?

Think the companies play a better part at protecting you as they have more to lose as if someone uses them to commit a crime they are the ones named and shamed and they do not want to be put in the public eye for helping criminals

Interview 8

<u>Participant interview</u>

Name- Beccy

1. Why do you think Government monitor networks?
   In order to remove indecent images on the internet which are unsuitable for public viewing
   to monitor individuals who are a danger or threat to society
   to have a better grasp on current issues in the world

2. Do you think the Government go too far on motoring peoples personal information and why?
   To a certain degree. I believe that individuals have a right to privacy which the Government goes against. However, I understand in some cases that it's done with the best intentions to keep society safe.

3. What do you think is the best way to monitor networks? E.g. (letting the public know exactly what they access)
   I have no idea because I don't know how they monitor them in the first place

4. How Success do you feel think network monitoring has been to counter terrorism?
   I'm not sure because the only information we get is from the media when terrorist attacks have occurred. However I do think a lot of things happen behind the scenes which we don't know about. My dad had mentions that he knew of someone who worked in that field who said there are loads of terrorist plots which are stopped by police which the public don't know about, so I'm assuming since the UK has only had a few terrorist attacks in recent years that network monitoring is doing well to counteract terrorism.

5. Can you think of any other organisations having access to your social media accounts?
   Advertising or marketing companies like Asos

6. Would the Government giving access to third parties monitoring your social media have any impact on how you use social media?
   Not sure. They most probably do anyway

7. What sort of information do you think the Government want from you when looking into your accounts?
   Everything

8. What is your opinion in the best way in countering terrorism?

Uniting and working together as a team. Shutting down their access to social media or technology devices which enable them to communicate. Not reporting issues such as their attacks to the extent that they do as it's the reaction that they want.

9. Could you tell me anything About Facebooks API?
   Account personal information? No idea…

10. Which protect your information better companies or the Government and why?
    Government, as they don't gain any profit from selling or passing your information on.

Interview 9

Participant interview

Name-Terri (42)

1. Why do you think Government monitor networks?
   I didn't realise they monitored networks

2. Do you think the Government go too far on motoring peoples personal information and why?
   Unsure

3. What do you think is the best way to monitor networks? E.g. (letting the public know exactly what they access?
   Warnings when letting know if somethings being monitored so it not such an invasion of privacy.

4. How Success do you feel think network monitoring has been to counter terrorism?

Not very, I feel that if the monitored everyone there may be an easier way of finding terrorists.

5. Can you think of any other organisations having access to your social media accounts?
   Companies used for marketing when using sites

6. Would the Government giving access to third parties monitoring your social media have any impact on how you use social media?
   Not sure. They most probably do anyway

7. What sort of information do you think the Government want from you when looking into your accounts?
   Everything

8. What is your opinion in the best way in countering terrorism?
   Blocking their use of the internet

9. Could you tell me anything About Facebooks API?
   Not a clue

10. Which protect your information better companies or the Government and why?
    Companies, simply because the Government shares information with everyone

Participant interview

Interview 10

Name- Mike (19)

1) I personally think that the Government monitor networks not only for our safety but also for their own interests. While they might want to protect us it also gives them a good opportunity to monitor individuals without their permission.

2) I'm not sure to what extent they monitor our personal information but based on things like the extensive usage of CCTV cameras and other monitoring devices it seems reasonable to assume there is high level of monitoring personal information.

3) It would be useful to inform people when joining a network that they may be monitored by the Government although this may defy the point as people may not be their true selves if they know they're being monitored.

4) It may be hard to judge this because of the media sensationalism of the ineffectiveness of the Government trying to tackle it, however, I feel like if the Government didn't monitor networks there might be a lot more terrorism happening.

5) Advertisement agencies, for example the use of cookies online.

6) Yes, based on the fact I already try not to share anything potentially risky or damaging as I think it could affect things like job chances if it was shared with third parties

7) Anything threatening, possible links with people of interest and clear signs you're breaking the law.

8) Monitoring suspects online, increased security in high risk places, aiding integration between cultures and religions, reducing tensions in communities.

9) I'm not sure what that is.

10) I guess Government because companies do share your details based on the fact that when you do sign up for things, you do seem to get a lot of emails which you didn't sign up for, however, I don't know to which extent Government protect our information as I'm not sure how much information they do have.

Interview 11

<u>Participant interview</u>

Name- Annabel Jardine – Blake (22)

1. Why do you think Government monitor networks?
   To alert Government of security risks

2. Do you think the Government go too far with motoring people’s personal information and why?

I’m not really sure how far the Government actually go with it so this is a difficult question to answer, however I’m sure that whatever they are monitoring is for the best in the interests of public safety.

3. What do you think is the best way to monitor networks? E.g. (letting the public know exactly what they access)
   I definitely think we should be told more about what is accessed. It would stop conspiracy and enable people to understand more about why it is needed. Also to protect people – in case they send things they shouldn’t or whatever.

4. How successful do you feel think network monitoring has been to counter terrorism?
   I have no idea. I feel like everything we are told is skewed by the media and we are protected from information that may scare us.

5. Can you think of any organisations having access to your social media accounts?
   I feel like a lot more organisations have access than I realise, such as for targeted advertising and such.

6. Would the Government giving access to third parties monitoring your social media have any impact on how you use social media?
   I don’t think so – I’m relatively careful about what I put on there anyway.

7. What sort of information do you think the Government want from you when looking into your accounts?
   I feel like the Government don’t really care about what I buy on amazon etc. (like ad companies would) but I think they’re more looking to keep the public safe.

8. What is your opinion in the best way in countering terrorism?
   I feel like I’m uneducated on this question, however I think monitoring networks definitely helps in this situation. Being able to know when/where terrorists are planning and meeting is useful.

9. Could you tell me anything About Facebooks API?
   No.

10. Which protect your information better: companies or the Government, and why?
    The Government, as companies are constantly trying to one-up each other in any way they can and will do whatever they can get away with, whereas the Government has the welfare of the public more in mind and has more responsibility with that data.

Interview 12

Participant interview

Name- James (36)

1. Why do you think Government monitor networks?
   National Security (e.g. terrorism)
   Safeguarding networks (e.g. removing indecent material)

2. Do you think the Government go too far on motoring peoples personal information and why?
   No, I have never seen evidence of the Govt. unnecessarily monitoring people's accounts unless they have a good reason. I don't believe they read my chats…

3. What do you think is the best way to monitor networks? E.g. (letting the public know exactly what they access)
   I don't know, probably adverts

4. How Success do you feel think network monitoring has been to counter terrorism?
   Relatively, there has been lower levels of terrorism within in the UK compared to Europe at the current time, so they must be doing something right

5. Can you think of any other organisations having access to your social media accounts?
   Games do sometimes ask to post (candy crush)
   Spotify is linked to my Facebook

6. Would the Government giving access to third parties monitoring your social media have any impact on how you use social media?
   No, I tend to use social media to read other posts rather than make them.

7. What sort of information do you think the Government want from you when looking into your accounts?
   Any evidence of suspicious behaviour or illegal activities, e.g. conversations to other known or potential targets

8. What is your opinion in the best way in countering terrorism?
   Combined approach of cyber methods and physical methods, education is important too, to prevent future terrorism.

9. Could you tell me anything About Facebooks API?
   I do not know what that stands for

10. Which protect your information better companies or the Government and why?
    Companies, they have legal requirements to protect their customers from any form of cybercrime, the company would be liable if your information gets sold or hacked.

Interview 13

Participant interview

Name- Tony (49)

1. Why do you think Government monitor networks?
   To monitor those who are a risk to others.
   Regulate indecent websites/images
   Detect threats

2. Do you think the Government go too far on motoring peoples personal information and why?
   It's done with good intentions but many may find it too invasive.

3. What do you think is the best way to monitor networks? E.g. (letting the public know exactly what they access)
   N/A

4. How Success do you feel think network monitoring has been to counter terrorism?
   I have no idea. The media does not cover the 'full' stories in term of terrorism so we do not get a clear understanding of what is really going on.

5. Can you think of any other organisations having access to your social media accounts?
   Adverts on Facebook, clothing websites etc.

6. Would the Government giving access to third parties monitoring your social media have any impact on how you use social media?
   Not sure.

7. What sort of information do you think the Government want from you when looking into your accounts?
   Looking for information that may cause a threat or harm to others e.g. involved with radical groups, indecent images etc.

8. What is your opinion in the best way in countering terrorism?
   Educate others on radicalisation and radical religious groups in areas that are under threat/ at a higher risk.
   Understand that Islamic terrorist groups do not account for all Muslims – decrease racial violence – unity as a nation.

9. Could you tell me anything About Facebooks API?
   N/A

10. Which protect your information better companies or the Government and why?
    Government - companies can sell your information on – less regulation.

Interview 14

Participant interview

Name- Zoe (27)

1. Why do you think government monitor networks?
   To guard against or monitor illegal or inappropriate usage such as terrorist activity and paedophilia

2. Do you think the government go too far on motoring peoples personal information and why?

I’m not particularly confident about what is monitored and why but, as long as my personal information is used to keep me safe and isn’t passed on to third parties for profit I don’t mind

3. What do you think is the best way to monitor networks? Eg (letting the public know exactly what they access)
   I have no idea because I don’t know how they monitor them in the first place. I do think that we should be told what is being monitored and why

4. How Success do you feel think network monitoring has been to counter terrorism?
   I can only assume that it has been successful as I don’t know what has been done or how successful it has been. I am happy not to know if that would compromise its success. I do think that the government should do more to ensure that social messaging networks such as facebook and wassap have to allow access to information as, if terrorists know that these cannot be monitored, it seems obvious that they are going to use them

5. Can you think of any other organisations having access to your social media accounts?
   No, although I’m aware that some do as advertisements related to my browsing history regularly pop up

6. Would the government giving access to third parties monitoring your social media have any impact on how you use social media?
   I would not be happy about third parties monitoring my social media so yes, although maybe they do?!

7. What sort of information do you think the government want from you when looking into your accounts?

8. What is your opinion in the best way in countering terrorism?

Uniting and working together as a team. Shutting down their access to social media or technology devices which enable them to communicate. Not reporting issues such as their attacks to the extent that they do as it’s the reaction that they want.

9. Could you tell me anything About Facebooks API?
   Account personal information? No idea…

10. Which protect your information better companies or the Government and why?
    Government, as they don’t gain any profit from selling or passing your information on.