“An Investigation into Students Awareness Regarding their Online Privacy and Private Information rights”

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

By Matthew Scott Holland
Department of Computing & Information Systems
Cardiff School of Management

Cardiff Metropolitan University

April 2018
Declaration

I hereby declare that this dissertation entitled “An investigation into Students awareness regarding their online privacy and private information rights” is entirely my own work, and it has never been submitted nor is it currently being submitted for any other degree.

Candidate: Matthew Holland

Signature: 

Date: 

Supervisor: Panicos Georghiades

Signature:

Date:
Acknowledgements

This dissertation would have not been possible without the guidance from the author’s supervisor. Considering this the highest praises goes to Panicos Georghiades for not only being extremely helpful throughout the process of writing this dissertation but being supportive.

The Author would also like to extend thanks to all those who participate during this research, especially those who participated in the primary research.
Abstract

In today’s society we rely on technology more than ever. Given this fact, it is right to say that our privacy and data security is being called into question. This research attempts to clear up how knowledgeable our students are, regarding their privacy, and how they deal with their online data.

The research involved secondary and primary data in the form of an online questionnaire administered to about 80 students, the questions were mainly knowledge based, attempting to gauge the knowledge levels across different genders, age groups and the group as a whole. The secondary research investigated current and proposed, future, legislation as well as case studies about recent data breaches to highlight the importance of data security and privacy and why personal knowledge regarding this topic is of particular importance.

The results show that most of the participants were well versed in terms of privacy issues, but there were some significant differences among gender and age groups, mainly how knowledge about certain tools and business practices, and what data was easier to part with.
# Table of Contents

1. **Introduction** .................................................................................................................. 1

2. **Literature Review** ........................................................................................................... 3

   2.1 Businesses .................................................................................................................... 4

   2.2 Legislation ..................................................................................................................... 5

   2.3 Data Breaches ............................................................................................................... 6

      2.3.1 Carphone Warehouse 2018 Data Breach .............................................................. 6

      2.3.2 Facebook and Cambridge Analytica Data breach ............................................... 7

   2.4 American Legislation .................................................................................................... 7

   2.5 Strava Application Breach .......................................................................................... 8

   2.6 Facebook Revenge Porn Prevention Program .............................................................. 8

   2.7 Browser Cookies .......................................................................................................... 9

   2.8 United Kingdom Spy Laws .......................................................................................... 9

   2.7 China Social Score ...................................................................................................... 10

   2.8 Right to be forgotten .................................................................................................. 10

3. **Methodology** ................................................................................................................. 11

4. **Results and Discussion** ................................................................................................ 13

   4.1 Participant Statistics ................................................................................................... 13

   4.2 Online Shopping .......................................................................................................... 19

   4.3 Social Media ............................................................................................................... 22

   4.4 Mobile Devices ......................................................................................................... 30

   4.5 Privacy tools .............................................................................................................. 34

   4.6 Internet Browsing ....................................................................................................... 36

   4.7 Police Warrants ......................................................................................................... 41

   4.8 The Right To Be Forgotten Act ................................................................................... 41

   4.9 Fraudulent Techniques ............................................................................................... 42

   4.10 Online Streaming Services ....................................................................................... 43

5. **Findings Analysis, Discussion and Conclusions** ............................................................. 45

   5.1 Participants Statistics Analysis ....................................................................................... 45

   5.2 Online Shopping Analysis ........................................................................................... 46

   5.3 Social Media Analysis ................................................................................................. 46

   5.4 Mobile Devices Analysis ............................................................................................. 47

   5.5 Privacy Software Analysis .......................................................................................... 47

   5.6 Internet Browsing Analysis ........................................................................................ 48

   5.7 Law Enforcement Analysis ......................................................................................... 49

   5.8 Right to be Forgotten Analysis .................................................................................... 50
1. Introduction

In this digital age, privacy isn’t at the forefront of concern, with us all being connected to the rest of the world via a multitude of different devices, all connected to the internet at various times. This tends to bring our private lives into the lime light. But since a lot of students these days have grown up around these platforms do they even realise that they not only can have a private life, but they have a right to it.

The topic that this research will be looking at is that of privacy, and more specifically privacy regarding the internet and our digital world in an attempt to try and understand where our students stand regarding their understanding of privacy and private information and their rights as human beings to a private life. The topic of privacy is extremely important since as it appears we are giving away our privacy a daily basis. It is also important in certain fields of work such as software engineering, as developers could be designing software in the future that could be handling a lot of privileged information. It would be good to get a general understanding on where students at Cardiff Metropolitan stand on their rights to privacy. Whether this is on social media platforms, private messaging applications or just browsing on the internet. This digital world has opened us all up to faceless intrusion into our private lives, whether we are aware of it or not.

The topic of privacy is very relevant in this day and age since we are all connected. Our privacy is at an all-time low, and those people who are growing up with this technology, knowledge of privacy laws and right to have a private life is becoming more important. People don’t seem to understand that putting something on the internet will mean it will be there for ever and a simple Google search could bring it up after years of it being dormant.

The fact that the UK is looking to leave the EU pulls our privacy into question. A lot of the laws surrounding privacy were introduced and enforced by the EU. These could now be overturned, and new UK laws brought in which could negatively affect our privacy.

“The United Kingdom does not have a written constitution that enshrines a right to privacy for individuals and there is no common law that provides for a general right to privacy. The UK has, however, incorporated the European Convention on Human
Rights into its national law, which provides for a limited right of respect towards an individual's privacy and family life" (Feikert-Ahalt, 2012) The law Clare was talking about included the Data Protection Act of 1998. This was the first act brought into the UK as National law that gave some semblance of online privacy and is one law that isn’t affected by us leaving the EU, but some others maybe are at risk.

As the UK prepares to leave the EU, new research needs to be done, to figure out where we stand. Realistically with data privacy laws changing all the time data privacy research should be done every year. It is also important for more research to be conducted as the General Data Protection Regulation (GDPR) is a new addition that will stir up the business scene in a considerable way.

With technology evolving on an almost daily basis, it comes with new methods of exploiting private and sensitive data found on the internet, such as Geo-Mapping, a method of plotting locations on a map. These locations can be found on such things as a person’s Facebook page, and with enough data someone can create a map of said person’s movements, and start to build a portfolio of their life, learn where they live and where they visit frequently. But how aware are people of this type of technology, and how susceptible are they to methods of data collection that can be seen as intrusive, and even life threatening. If data such as this gets into the wrong hands, like that of a Stalker or someone with ill intent.

The main research of this project will come from not only legislation and case studies of recent data breaches, but there will be a questionnaire sent out to students of Cardiff Metropolitan University, of the age of 18 or over. This questionnaire will contain 40+ questions, mainly of the Yes/No Variety, which will help the analysis process, and hopefully a connection can be made at the end, to see whether their age or ethnicity links to the level of knowledge regarding privacy. It could be that students understand the dangers of having their lives on display, but they may not care.

“The reality is more complex than the scare stories would have you believe; young people display a wide variety of behaviours online, while many use social networks such as Facebook and Twitter, they have an aversion to drama, and often take steps to limit the kinds of information available about themselves online. A Pew Internet research survey from 2013 revealed that 60% keep their Facebook profiles private, while 74% have deleted people from their friend’s lists” (Bradbury, 2015)
Bradbury has a point that young people display a wide variety of behaviours online, but does these behaviours connect to either their lack of knowledge regarding privacy or their lack of concern.

2. Literature Review

In a connected world, where almost everybody has a device of some form which has connection to the internet, privacy is on the forefront of concern regarding our private information. “Our lives are lived in data. Data crossing borders and connected in virtual space. Most often, it appears, we live in open and too easily accessible data networks. States and corporations are watching us through data, and we are watching each other through data. What does individual privacy mean in this saturated environment?” (Hasselbalch and Tranberg, 2016) The way Hasselbalch and Tranberg talk about our digital selves is like they are becoming our book cover, and companies and states are starting to see us and judge us by that book cover. Meaning what our data shows is how we will be perceived.

Our online data not only shows ourselves as people, but it shows much more than that, “What you and your family do online says a lot about who you are, your preferences, your socio-economic status and more.” (Wright, 2018)

So why is privacy on the internet important “Privacy is a limit on government power, as well as the power of private sector companies. The more someone knows about us, the more power they can have over us. Personal data is used to make very important decisions in our lives. Personal data can be used to affect our reputations; and it can be used to influence our decisions and shape our behaviour. It can be used as a tool to exercise control over us. And in the wrong hands, personal data can be used to cause great harm.” (Solove, 2014). When someone has access to all our personal data they can change our lives, if employers get hold of our social media they could potentially reject us from a job because of something we did years ago.

Students were chosen as the focus of this research because they are the ones in the coming years that are going to be judged the harshest, most of them will be unproven in the work place, and only have a slip of paper from university and their first impression to help them secure a future, which is why they will need to be completely aware of how their data is used online, and how much someone can find out about a
person just by looking at their social media accounts. “If you think your Facebook and Twitter profiles won’t be looked at when you’re applying for a job, think again. The vast majority of employers are now searching through candidates’ social media accounts as part of the hiring process, new research finds. A study from CareerBuilder revealed that 70 percent of employers now use social media to screen job candidates before hiring them, up from 60 percent a year ago and 11 percent in 2006” (Brooks, 2017) What is worrying is that students will leave university after having an amazing experience and documenting it all on Social Media and then after they have passed their exams and coursework to earn that bit of paper that says they are able to competently perform a certain skill, they will be judged on their social media, by the actions they performed on the journey to obtain that piece of paper.

2.1 Businesses

Why are businesses and corporations interested in our data, if there wasn’t a use for it, it would be valueless, so there must be a reason why data is being collected. The answer is almost certainly profit. As explained by an article in New Scientist Magazine Issue 3151. “If somebody from a shop you occasionally visited phoned and asked what you had been doing for the past month, would you tell them? Almost certainly not. Yet often without thinking we allow technology companies to track and collect such data. Everything from your movements to what you have been buying, watching, reading and listening to gets scooped up and filed, ostensibly to help tailor services to your needs and sell you things you want. But this data is so valuable that it is often sold to third parties.

None of this happens without your consent, but consent is often obtained by sleight-of-click, via lengthy and impenetrable service agreements. The terms and conditions for an Amazon Kindle e-book reader, for example, are longer than many novels. Has any ordinary punter ever read them? Does Amazon actually expect us to? Both parties know it is easier to simply click “accept”. “ (New Scientist, 2017) The reason businesses are collecting data is to sell onto third parties, this can be seen through companies such as Google. Before Google procured Android and YouTube it was just a search engine, so how did they stay afloat during those years.

One of the biggest uses for data for such companies as Amazon or eBay is targeted advertisements, this happens, when someone buys something. A built-in algorithm looks at the purchase history or search history on their websites and then will often
show ads for products on similar to those that have already been purchased in hopes to get that person’s interest and in the end, their money. This is admitted to by Amazon themselves on their websites, and it reads, “personalized or targeted ads, are displayed to you based on information from activities such as purchasing on our sites, visiting sites that contain Amazon content or ads, interacting with Amazon tools, or using our payment services.” (Amazon, No Date)

2.2 Legislation

There is a lot of legislation currently in place to help protect customer data, the main one is the Data Protection Act of 1998, which originally came into UK law with the Human Rights Act of the same year, it was adopted from European Legislation, the Data Protection Act was under Article 8 of the Human Right Act. The Data Protection Act allows a person to control how their information is used by organisations, businesses or the Government. This being said anyone who is responsible for controlling the data, must follow a strict rule set, to make sure it is handled, processed and stored in correlation to the Act. The rules that are in place for these controllers are, the Information must be used fairly and lawfully, the data can only be used for a limited specific purpose, this meaning that they can only use the data for the reason they collected it, the data should be up to date and accurate and should be kept safe and secure. Certain items of data require higher security because they are usually sensitive, data such as Ethnic Background, political Opinions, sexual health and criminal records.

The controller in charge of the data, is also known as the data controller which is “a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed” (ICO, No Date) This person oversees processing the data and making sure it is used in accordance with DPA.

For businesses or any organisation that breaches the DPA there are a set of penalties in place that can be issued by the Information Commissioners Office or ICO, some of these being they can “Serve enforcement notices and ‘Stop Now’ Orders where there has being a breach” ICO can also “issue monetary penalty notices, requiring the organisation to pay up to £500,000 for serious breaches of the Data Protection Act occurring on or after 6 April 2010” (ICO, No Date), these penalties and rules should help deter businesses and organisations from being irresponsible with customer data,
but there are cases of blatant disregard for customer data protection, such as the recent Carphone warehouse data breach in January of 2018.

2.3 Data Breaches

2.3.1 Carphone Warehouse 2018 Data Breach

In January 2018 Carphone warehouse was subject to a data breach, attackers extracted the data of more than three million customers and 1,000 employees. This attack affected their online stores which OneStopPhoneShop.com, Mobiles.co.uk and e2save.com the compromised data was names, addresses, phone numbers, data of birth marital status and unfortunately for 18,000 of those customers, their historical payment details.

The attackers managed to breach Carphone Warehouse via an outdated piece of WordPress software, and for this the ICO fined Carphone Warehouse £400,000 which was reduced to £320,000 because they paid in the first month of issue.

Fortunately there is another set of laws passing that should make DPA more formidable this new piece of legislation known as GDPR or General Data Protection Regulation, should hopefully bolster DPA with higher penalties and new, stricter regulations and principles, there are reasons why GDPR is being introduced, “The biggest one is the EU’s desire to bring, data protection law in line with how people’s data is being used, especially considering that firms like Amazon, Google, Twitter and Facebook offer their services for free, as long as people offer their data to these tech giants.” (Curtis, 2018). Most of the principles of GDPR are similar to DPA, just more extensive, one of the biggest changes coming with GDPR is the increased territorial scope, according to EUGDPR.org the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company’s location.” (eugdpr.org, No Date)

The territorial change is very much welcomed, as it helps bring those companies such as Equifax to justice. Equifax is an American company specialising in credit ratings, if someone wants to borrow money, the lender will contact Equifax for the details, to check the persons score. In September 2017, Equifax had a data breach, affecting not only millions of Americans but hundreds of thousands UK residents, although according to their website “UK systems were not breached, the attack compromised
the personal information of some UK customers” (Equifax, 2017). Since GDPR hasn’t arrived yet, Equifax isn’t liable for the loss of the UK data, but under GDPR that will change. The penalty for neglecting the responsibility of protecting the data and conforming the Data protection standards, is going up considerably, into two tiers in fact, tier one being, a fine of 10 Million Euros or 2% of the organisation’s annual income, whichever is higher, and the second tier which is 20 Million Euros or 4% of the annual income, this should deter businesses considerably more than the old penalties.

2.3.2 Facebook and Cambridge Analytica Data breach

The most recent and shocking data related story was surrounding Facebook and them sharing data with Cambridge Analytica, where “Around 87 Million individuals, including more than 1 Million people in the UK” (Hern, 2018) data was shared. Cambridge Analytica is “a company that offers services to businesses and political parties who want to “change audience behaviour””(Osborne, 2018) this happened because, of a third party application that was on Facebook, called “This Is Your Digital Life” which is a personality quiz used by Cambridge Analytica to gather the data, but in this instant it seems like the users who was just looking for a quick 5 minute break, didn’t realise what those answers would be used for, and if you used this app not only did your answers from that quiz be gathered but if you had a public profile then “page likes, birthday and current city were likely shared with the company, as well as potentially the contents of their news feed at the time” reports Alex Hern Under GDPR, both companies would be liable for the data that was lost from the EU, and this could have been avoided to an extent if people read what permissions the “This is your digital life” quiz was asking for.

2.4 American Legislation

In America they have similar guidelines when it comes to data security, one of their main pieces of legislation is the is The Federal Trade Commission Act, this act is a federal consumer protection law that “prohibits unfair or deceptive practices and has been applied to offline privacy and data security policies. The FTC has brought many enforcement actions against companies failing to comply with posted privacy policies and for the unauthorised disclosure of personal data.” (Jolly, 2017) America is a good
case study for trying to understand what direction the UK is heading in regards to data privacy, in recent memory the US house of Representatives approved a set of rules that gives Internet Service Providers over in the USA the right to sell consumers internet history to the highest bidder, which is not something we would like to see appear in the UK, this sort of data selling, could lead to residents being profiled on their internet behaviour, and potentially losing out on such things as job opportunities.

2.5 Strava Application Breach

Another example of recent data security flaws is with Strava, based in San Francisco, they are the developers of an application, which acts as a social network for athletes, it works by using satellite navigation to track the runners, cyclers and swimmers, but in early 2018 there was a leak at Strava Headquarters. Which resulted in Heat Maps being leaked, a Heat Map being a “tool for representing complex statistical data. Doctors, engineers, marketers, sociologists, researchers of every kind, use heatmaps to make complex data sets comprehensible and actionable.” (Hall, 2016) It basically created maps of everybody who used the app, the route they ran, their heart rates and in some cases their names, this unfortunately led to covert US military bases being revealed, because of the soldiers using this application, but that isn’t the point, if they can track everyday use and monitor where you go, when you exercise they can create a digital map of your life, they could potentially find out where you live, your daily routine, and if the data is released to the internet like in the case of Strava, then everybody else can find that data.

2.6 Facebook Revenge Porn Prevention Program

One of the most curious cases of a business asking their users to trust them with even more data comes from Facebook, back in late 2017, before the Cambridge Analytica breach, their idea was to try and combat revenge porn. “Revenge Porn is the sharing of private, sexual materials, either photos or videos, of another person, without their consent and with the purpose of causing embarrassment or distress.” (GOV.uk, 2015). The way Facebook wanted to tackle this, was to allow users to upload their nude images to Facebook servers in order to stop those certain pictures being reuploaded by somebody else. Essentially you send your nudes to Facebook, and they run the
pictures through an algorithm in order to detect when those images are reuploaded, these pictures are then said to be deleted. That is putting a lot of trust into a company.

2.7 Browser Cookies
One of the big data types to be mined is browsing history, this is very common, and it involves something called cookies which are “very small text files placed on your computer by a web server when you view some sites online (not all websites place cookies). They’re used to store data about you and your preferences.” (Collins, 2017) Collins goes onto to say that “Some web sites and search engines use them to track users as they browse the web, collecting highly personal information and often surreptitiously transferring that information to other web sites without permission or warning.” This is a common cause for alarm, but can easily be negated by using certain programs, such as Virtual Private Networks and Incognito Mode, which is built into most web browsers.

2.8 United Kingdom Spy Laws
With the new Prime Minister, Theresa May comes uncertainty with how things will change, in the case of prime minister May, an idea of how data protection laws could change comes from an article back in 2015 an article details new “Spy laws” that will “Allows ministers to retain the power to sign off warrants for intrusive surveillance” and “Force internet and communications companies to retain customer usage data for up to a year” (Wilkinson, 2015) at the time of this article Theresa May was not the Prime minister she was the Home Secretary, which means if she still thinking about using this new set of laws, now that she has more power as the Prime Minister? We are already seeing new laws such as this coming into power, with little to no opposition, the new law that was brought in around 2016, “will force internet providers to record every internet customer’s top-level web history in real-time for up to a year, which can be accessed by numerous government departments; force companies to decrypt data on demand” (Whittaker, 2016) it will also allow “security services and police with new powers to hack into computers and phones and to collect communications data in bulk. The law requires judges to sign off police requests to view journalists’ call and web records, but the measure has been described as “a death sentence for investigative journalism” in the UK” (Travis, 2016), this is very similar to what May proposed back when she was working with the home office, with the exception that ministers do not
have the power to signoff warrants for intrusive surveillance, but it has been dubbed by Edward Snowden, the ex-CIA Whistle blower as “The most extreme surveillance in the history of western democracy”

2.7 China Social Score
Where endless amounts of information is available about a person, whether this be through social media or other aspects of the internet, there could come a time of governments profiling their citizens based on their social interactions on the internet, to find out how trust worthy they are, this isn’t as farfetched as it may sound as it may become a reality in China as early as 2020, “A high-level policy document released in September listed the sanctions that could be imposed on any person or company deemed to have fallen short. The overriding principle: “If trust is broken in one place, restrictions are imposed everywhere”. A whole range of privileges would be denied, while people and companies breaking social trust would be subject to expanded daily supervision and random inspections” (Denyer, 2016) the way this works is with a score that is allocated by the Chinese government and it “follows you wherever you go. A high score allows you access to faster internet service or a fast-tracked visa to Europe. If you make political posts online without a permit, or question or contradict the government’s official narrative on current events, however, your score decreases.” (Mitchell and Diamond, 2018) this is alarming, as it could be used to create ideas in western culture to follow suit, we could see a dystopian future similar to that of Phillip K Dick’s Minority Report, where crimes could be predicted before they happen, but this could also be used to create a further divide in society where basic amenities are denied because of something said online, or the wrong person not likely what you have said.

2.8 Right to be forgotten
The Right To Be Forgotten is something that has been around since 2006, a method in which a person can requested the removal of their data from the internet, but with the General Data Protection Regulation just around the corner, this act is being revamped and updated with the new EU legislation, the new act will be name “Right to Erasure” (ICO, 2016) according to the Information Commissioners office, individuals will be able to have their personal data erased if “the personal data is no longer necessary for the purpose which you originally collected or processed it for?”
You are relying on consent as your lawful basis for holding the data.

You have processed the personal data unlawfully.” This means that the data can only be erased as part of breaking principles set out by the General Data Protection Regulation or the Data Protection Act. According to the same site on the information Commissioners office website, this act does not apply in cases of “to exercise the right of freedom of expression and information. To comply with legal obligation. For the performance of a task carried out in the public interest or in the exercise of official authority.” A person cannot just ask for their data to be removed unless they have legitimate concerns that the GDPR has been breached with use of the data in question.

3. Methodology

With Research comes the need for an appropriate research philosophy and methodology, the onion model created by Saunders et al helps researchers plan their research model. This model by Saunders et al, is called the onion model because it’s built up with layers. The first layer being philosophical stances, the second layer being research approaches, layer 3 is strategies, layer 4 is choices, layer 5 is time horizons and layer 6 is techniques and procedures, this is all shown in the diagram below.

Fig 1. Research Onion Diagram (Based upon Saunders et al’s diagram, 2009)
This research will be using this model to develop the research philosophy that will be used when researching.

The First layer of the onion model is philosophy stances, which contain six stances, positivism, realism, interpretivism, objectivism, constructivism, pragmatism. In the research that will be conducted the stance will be positivism which “depends on quantifiable observations that lead to statistical analyses” (Research Methodology, No Date) the way positivism will be implemented is through a questionnaire, as the only data that will be received will be statistical.

Looking at layer two of the onion model, we need to pick our research approach, which we have the choice between inductive research and deductive research, deductive being “a basic form of valid reasoning. Deductive reasoning, or deduction, starts out with a general statement, or hypothesis” (Bradford, 2017) seeing as we are using a questionnaire to figure out a pattern or trend in knowledge, there isn't really a hypothesis to prove, in that case we will be using the Inductive Method, which according to Bradford in the same article is “inductive reasoning makes broad generalizations from specific observations. Basically, there is data, then conclusions are drawn from the data.” Which is how the questionnaire will work.

There are two data types we can extrapolate from research, these are quantitative and qualitative, qualitative being “drawn from the constructivist paradigm (Bryman & Allen, 2011). This approach requires the researcher to avoid imposing their own perception of the meaning of social phenomena upon the respondent (Banister et al., 2011)” (UK Essays, 2013) and in the same essay it explains that quantitative data is “It holds a number of accepted statistical standards for the validity of the approach, such as the number of respondents that are required to establish a statistically significant result (Goddard & Melville, 2004)” since the questionnaire will be pulling mainly statistical data then the data will be quantitative.

The next layer is the research strategy, which is how the researcher intends to carry out the work. In the onion model there is 7 different research strategies, Experiment, Survey, Case Study, Action Research, Grounded Theory, Ethnography, Archival Research. Since the research that will conducted is a questionnaire the research strategy will be a survey which involves “sampling a representative proportion of the population (Bryman & Bell 2011). The surveys produce Quantitative data that can be analysed empirically” (UK Essays, 2013)
The fifth layer of the onion model is Time Horizons, which is the “time framework within which project is intended for completion (Saunders et al., 2007).” (UK Essays, 2013) There are two types of time horizon specified in the onion model, there is the cross sectional and the longitudinal, the cross sectional is whereby the data must be collected at a certain point. This is used when the investigation is concerned with studying a topic that occurs at a certain time. Longitudinal refers to data collection that occurs over a time period, which is how questionnaires work since researchers cannot control when participants complete questionnaires or surveys.

After the data is collected it needs to be analysed, but first the type of data we collected needs to be identified as either, primary or secondary, the difference being, primary research is collected by the researcher and is first hand data, secondary data is work or opinions derived from other researchers. This research will be using a mix of both the primary data will be derived from the questionnaire that will be distributed, and the secondary data, will be research of legislation such as the data protection act, the General Data Protection Regulation, and case studies such as the Cambridge analytical data breach.

In conclusion, the methodology of this research will focus around deriving numerical and statistical data from a survey that will be sent out, the data retrieved from this survey will be of the primary type and secondary data will be present in the literature review in the form of legislation and case studies.

4. Results and Discussion

The research that was done was in the form of a questionnaire, that was distributed to Cardiff Metropolitan Students, the questionnaire contained around 40 Questions, the first job to analysing the data received was removing any responses that was not 100% complete, there were 15 incomplete responses, which were removed from the final data set. The results will be broken down into their individual questions.

4.1 Participant Statistics

This first sub section we will look at is the overall statistics of the participants, their genders, their age and ethnicity, all participants were anonymous, with all the unfinished results filtered out, we had 53 completed responses, of which 25 were male and 28 were female as shown in the diagram below.
Fig 2. Results of question What is your gender? from online questionnaire

Even though in the questionnaire the participant could enter their age rather than selecting from a specified grouping, the data has been grouped into easier to read and easier to quantify groups. The groups chosen, are 18-24, 25-39, 40-60, and no answer, the participants have been grouped and is shown in the chart below.

Fig 3. Result of question What is your age? From questionnaire

As expected and as mentioned in section 1 the majority of my participants are of the normal age range of students.

The Ethnicity of the participants, were mostly white, as shown below.
This is unfortunate, and if this research was repeated a wider ethnic group would be ideal and sought after.

The first question that was asked of the participants was, how concerned were they in regard to their own privacy on the internet, the results, weren’t as expected.

Fig 4. Results of question What is your ethnicity? From questionnaire

Fig 5. Results of Question How concerned are you about your privacy and private information? From the questionnaire
In section 1 it was theorised that people may already understand that their privacy was at stake and they may not care. That doesn’t seem to be the full truth. There are a lot of participants who are indifferent about their privacy but quite a few are slightly concerned or even very concerned. Whilst there are only a few that are not concerned, maybe this means they understand that their privacy is important but are unable to do anything about it and have become complacent about it. This can be broken down into age and gender groups, first off gender, the graphs have been split so it is easier to read and understand.

![Male Breakdown of question How concerned are you about your privacy and private information results](image)

The chart for the males shows that the majority of them are very concerned about their privacy while another large set are slightly concerned, there are a few which are indifferent, and a couple that are not concerned or not that concerned.

Next graph is for females.
Fig. 7 Female Breakdown of question How concerned are you about your privacy and private information results

For the females a vast majority of the participants are slightly concerned, a smaller majority is very concerned, there were no participants that said they were indifferent, and there are a few that are not that concerned and a few that are not concerned at all.

The next break down will be for age group, this will be again split down into 3 groups, 18-24, 20-39, 40-60, this will be done because a pie chart with 15 sections will be difficult to see. The first graph is for the age group 18-24
The majority of the 18-24 year olds, are very concerned with quite a few slightly concerned, and then a few that are indifferent, not concerned and not that concerned. The next graph will be for the age group 25-39.

![Pie chart showing concern levels for ages 25-39](image)

**Fig 9. Age group 25-39 breakdown of question how concerned are you about your privacy**

For the ages 25-39 there were no participants who were not concerned, a few with are not that concerned, 5% of them are indifferent, the vast majority sit at slightly concerned and just over a quarter are very concerned. The last graph is for the 11 participants that are in the age group 40-60.
As is clear from the graph there were not participants from this age range that was either not concerned, not that concerned or indifferent.

4.2 Online Shopping

This second subsection will be interested in the participants online shopping habits, what data they store on these websites, such as Amazon and eBay, and how much they know about how the business uses their data.

The second question that was asked of the participants was if they did shopping online using retailers such as Amazon or eBay, in this day and age you would be hard pressed to find someone who didn’t do some shopping on the internet, and that is especially true within the student community, as the results from the questions came back as 100 percent yes.
Fig 11. Results from question do you do online shopping? From questionnaire

The next two questions asked were about what data they stored on these websites. There was a question for delivery address and a question about their credit/debit card information. The question for delivery address was met with 100% of participants answering yes, but over a quarter of the participants didn’t store their credit/debit card details. These questions were asked on the basis, that websites such as Amazon and eBay will be able to access this data at any point and if there is a data breach this data could be lost.

Fig 12. Results from do you store your delivery address on these websites? From questionnaire regarding online shopping
Fig 13. Results from question Do you store your credit/debit card details on these websites? Regarding online shopping, question from questionnaire.

The Participants storing their delivery address on these websites is most likely due to convenience sake, but it seems like some of them, well over a quarter of them value their payment information higher than their delivery address, for good reason. But a full breach of Amazon systems could lead to this data being leaked. The next question regarding these websites, was regarding the algorithms in place on these websites used to track a person’s purchase history and advertise products similar to their purchasing habits in hopes of enticing them into buying more.

Fig 14. Results from question asking participants about targeted advertisements.
This result is interesting as it shows that most of them do understand that this sort of business practices happens. This is elaborated in the literature review, in section 2.1 Businesses paragraph 3, in hindsight, this sort of result should have been foreseen as targeted ads are very commonplace and easy to spot, most people will realise that if they have bought a DVD online, then they see ads for more DVDs this is targeted because of their purchase.

The next question that was asked was, do you understand that these companies and their websites can access the data you have stored on their websites?

Are you aware that websites such as these can access all your data you have stored on their website? such as card details recent purchases and delivery address?

![Pie chart showing 72% Yes and 28% No](image)

Fig 15. Results from question asking participants if they understood websites like amazon could access their data

With the hefty result of people storing their credit/debit card and delivery address details on the websites, this result wasn’t as expected, the fact that they understand their details can be accessed by the websites storing them, but they still decide to store the data.

4.3 Social Media

The next topic that was asked of the participants, was whether they use social media, whether this be Facebook, Twitter or other websites such as Reddit. This topic is especially interesting, as a lot of people post to their accounts on these websites
without realising the impact it could be having on their lives, “whatever you put into the internet can be found within minutes. This has resulted in the fact that, for many candidates their social media profile has become their new CV.” (Smejkal, 2017) whether this be employers or the security of data. Since social media is a social requirement currently the results were as expected.

Do you use social media websites such as Facebook, Twitter or Reddit?

![Pie chart showing 87% Yes and 13% No]

Fig 16. Results from question about who out of the participants uses social media

That is only 7 participants who do not use social media out of the 53 completed questionnaires.

The next couple of questions were about social media, so the seven participants that answer no to the last question were not privy to the next couple. The next couple of questions are regarding the ability for companies to Geo-Map locations using the social media activity of the user, which again is expanded in the Literature review: section 2.0.

The first question was just to gauge how many of the remaining 46 used features on these social media platforms, sometimes known as location services, which allow you friends to see where you are when you post to these platforms, for example when you take a picture it will automatically, use your phones GPS to tell you friends where you took that photo.
Most people, over two thirds of the participants don't use these services, meaning they will most likely not be victim to Geo-Mapping. Again, with the next question anyone who answered no will not be taking part in the next question, that means there will only be 15 participants answering the next question.
Do you know that by consistently posting your location on social media, people, not just the website provider can create a map detailing your whereabouts on certain times and days and use that to estimate your movement patterns and even where you live?

![Pie chart showing 53% Yes and 47% No responses.](image)

Fig 18. Results from question detailing dangers of using location services on social media sites

The answers to this question was 8 No and 7 Yes, meaning people are more knowledgeable about this subject than first thought, the next question was for every who used social media, and that was whether they had posted their home address directly to their social media accounts.
Fig 19. Results from question about posting home address to social media

Only 1 person had openly admitted to this, which shows some understanding to safeguarding their information and the potential dangers they may face by posting such information.

The next question which also was only for users of social media, was a sensitive question, which hopefully was answered honestly, and that was the topic of whether or not the users had sent nude images to other users of social media, this is particularly dangerous as you are essentially sending very sensitive data over the internet to someone, without considering, how secure your network is, where these pictures are being stored, and how trustworthy the person on the other end is.

Out of the participants that responded to this question only 5 participants admitted to sending nude images of themselves while 41 participants said no.
Given the fact that we have the gender of the people who answered these questions we can see that of the 5 who answered yes to this question 4 out the 5 were Male, leaving the last 1 as Female as shown in the below graph.

This could allure to males being less caring about sending their image, or it could be lack of data, which is an improvement that could be made, if these tests were redone, get a larger population base to answer these questions.
The next question asked was whether or not the participants who had sent nude images of themselves to other users, understood that those pictures are not just stored on the senders and recipient’s devices and are actually stored on a server somewhere.

![Pie chart](image)

**Fig 22.** Results from question regarding the storage of those nude images on the social media providers servers

Four out of the five responses eluded to the fact that they knew that their images would be stored in a place that they had no control over, again the people who knew about this was the four male participants, and the person who didn’t know was the female participant.

The next question was reopened to all participants, and it was regarding, the Facebook program that is supposed to combat Revenge Porn, this is expanded on in the Literature review, but the idea of it was for users to send nude images to Facebook, this would allow Facebook systems to identify when those pictures were getting uploaded by a different source, and it would allow them to stop the upload. The question asked was how much you agree with this program.
Fig 23. Results from question about participants feelings towards Facebook’s Revenge porn prevention program

This question was poorly timed due to the mistrust around the Facebook-Cambridge Analytica controversy recently, as some answers may be going on the idea that this information maybe leaked. The next question was for the people that agreed on some level with this program, whether that the strongly agree, agree or indifferent, the assumption was made that if the participant disagreed with this program the answer would be no for the next question which is, whether the participant would use...
this program in the future if it was implemented.

![Pie chart showing responses](image)

**Do you think you will use this service provided by Facebook?**

- Yes: 83%
- No: 17%

**Fig 24. Results from question whether or not the participant would use this service**

It's strange that the people who have agreed with the program would not use the program, this could be because if they haven’t sent nudes before they may not see the need for this as they may never send nudes in the future.

### 4.4 Mobile Devices

We rely on mobile devices on a day to day basis, it’s how we stay in contact with friends, family our employers, and how we get our daily news and information about the weather and so on. But this sort of device opens us up to intrusion. So, the next question that was asked was what sort of device the participant owns and use.

![Pie chart showing device usage](image)

**Which of devices do you own and currently use?**

- Android: 62%
- Kindle Fire: 36%
- Iphone: 2%

**Fig 25. Results from what devices the participants use on a regular basis**
The majority owns an iPhone, with Android users coming in second and a single person who stated that they own a kindle fire, but every participant owns a device of some form that’s connected to the internet. This next question is for all device owners, and its regarding whether or not they store important information on their device, whether this be Nude Photos, Credit Card details or home address.

This result is not really what was expected as you’d expect everyone to store something like payment details on their phone, whether that’s an amazon account or some other account information. But 55% of people did responded with yes, they store this sort of information on their mobile device. The next question is regarding applications on mobile phones, and the permissions they ask for, but first a question to ascertain how many of the participants regularly install new applications on their mobile devices.
Fig 27. Results from the question whether the participant regularly installs new applications on their device

The majority of them do, whilst a good portion of them do not. The next questions as mentioned is regarding the permissions these applications ask for and how vigilant the participants are when it comes to reading what permissions these apps are asking for. This next question is exclusive to those participants who said yes to installing new applications regularly.

Fig 28. Results from whether the participant reads the permissions from the applications

So, half of the people who install applications regularly on their mobile device do not read the permissions the application is asking for before accepting, and half of them do. This question can be used in conjunction with one of the previous questions specifically the one about storing sensitive information on their mobile device,
depending on if they store this sort of information, does it change whether or not they read application permissions.

![Pie chart showing Do you read application permission? (Sensitive Information Breakdown)](#)

Fig 29. Results from sensitive information against reading permissions

In regards the whether the participants with sensitive information on their device reads the permissions, the majority of them do, while a lot of them do not, but the people who do not have a lot of sensitive information on their device are the most vigilant. The next question all the participants and it is a knowledge question regarding what these application developers do with some of the permissions they ask for, which is mainly selling the data onto third party companies.

![Pie chart showing Did you know that a lot of these applications request the use of such things as contacts, phone records and access to your photo album without even needing it, this is done so that they can build a portfolio of your life and social activities to help them](#)

Fig 30. Results from question regarding the dangers of giving certain permissions to applications
This seems to be common knowledge amongst the majority of the participants.

4.5 Privacy tools
The next section of questions revolves around privacy tools such as Incognito Mode, virtual private networks (VPNs) and proxies, and if the participants use them. The first question asked them whether they are aware of these tools.

Fig 31. Results from question asking about knowledge regarding privacy services

58% of participants, have at least heard of these tools, this question could be broken down for us to see if knowledge of these services is known primarily by a certain age group.
Fig 32. Results from age split, whether or not age changes knowledge regarding privacy services

As the results show, the majority of the age group 18-24 shown in dark blue and orange are aware of these services that can mask privacy, the participants that are in the 24-39 age range are split in half regarding the knowledge of these services, and the majority of the 40-60 age group are not aware of these services. The next question was for those who answered yes, this is was a multiple-choice question to find out which of these services the participants use, or if they have just heard of these tools.
Fig 33. Results regarding the privacy services used by the participants

Quite a good range of different services being used, the most common being Incognito mode, though that is most likely due to its availability and the fact that it is built into most pieces of browsing software.

4.6 Internet Browsing
This next section is all about internet browsing, it is common place that without proper protection, privacy can be compromised on the internet. All the participants are asked these questions. The first section in this question is regarding IP addresses and the fact that you can be tracked back to your home with it.
Are you aware that by just the act of accessing a website you have just given away your IP Address of your computer/device which allows you to be tracked back to your home or your connection point?

![Pie chart showing 70% Yes and 30% No]

**Fig 34. Results from question regarding IP address tracking**

Most of the participants understand this, but a few did not, hopefully after the questionnaire they did start to understand. The next question was regarding cookies, which are small packets of data that are stored on your computer's hard drive when you access a website, which can track your browsing history.

Did you know that when you access a website they will often ask you to "enable cookies" on your website. These cookies allow the website provider to compile and see your browsing history

![Pie chart showing 62% Yes and 38% No]

**Fig 35. Results from question regarding cookies on websites and how they can affect somebody**
The majority of the participants knew about this, whilst just over a third did not. The next question is regarding a new development, that hasn’t been properly implemented as of yet, but can be read about in the literature review, in short, it allows Wi-Fi enabled devices to be tracked, and that is what the next question is about, how much the participants agree with this sort of technology.

**How much do you agree with a recent development in this technology that allows websites to use analytics to collect data regarding contacts, friends, family and associates when using your mobile phone to access the internet?**

![Pie chart showing the distribution of responses to the question.](image)

*Fig 36. Results from question regarding the participants agreement with technological advancements that allow mobile tracking of contacts.*

The majority of people do disagree with this technology, but it is interesting to see that some people are in agreement with it. The next question is whether or not participants access pornographic materials on the internet, a lot of websites that offer these sorts of services are still highly populated by viruses that can infect your devices and aim to steal something of value from you.
**Fig 37.** Results of question regarding the use of pornographic material on the internet

This question is almost 50/50, there are multiple ways we can break this question down with the data we have, that’s by gender and by privacy software the participant has admitted to using, first is gender.

**Fig 38.** Results from participants broken down into gender, whether they access porn on the internet

The majority of participants who said yes were Male and the majority of the females said no. The next theory that needs to be tested is if the people using certain privacy enabling tools such as incognito mode, are these the people who are watching porn on the internet.
The majority of people who watch pornography on the internet use incognito mode, or VPN while a smaller amount use proxies and TOR browser, and a small percentage use nothing.

The next question is regarding the use of incognito mode, and the fact that even though it stops data showing up on your browsing history it doesn’t stop your internet service provider from being able to see what sites you browse.

Did you know that even using Incognito features provided by many browsers these days does not stop your internet provider from being able to see what sites you have been browsing whilst in incognito mode?
This should be relatively common knowledge as most browsers such as chrome warn about this when incognito mode is started up.

4.7 Police Warrants
This next section comprises of a single question and it is regarding whether or not police need a warrant to access personal information regarding a person on the internet, this was included as in recent memory Theresa May, the Prime Minister of the United Kingdom was looking to make it, so the police do not need a warrant, this can be read about in the Literature Review. The question was yes or no, should law enforcement be required to seek a warrant for this information.

![Figure 41](image)

**Should Law enforcement be required to seek a warrant before accessing personal information on the internet about you? i.e. Emails, Texts, social media messages**

[Pie chart showing 94% Yes, 6% No]

Fig 41. Results from question regarding whether law enforcement should seek a warrant to access personal information on the internet

The vast majority of the participants believe the police should seek a warrant before accessing personal data on the internet about a person, whether that be Emails, Texts, or Social media messages.

4.8 The Right To Be Forgotten Act
The basis for this question was to understand whether or not the participants understood that there was a way of removing one’s self from the internet and that is through the right to be forgotten which is covered again in the literature review.
Fig 42. Results from question regarding the knowledge about the right to be forgotten

Quite a lot of the participants knew about this but quite a few didn’t.

**4.9 Fraudulent Techniques**
This section will contain only one question and it is regarding whether or not the participant has been targeted by any fraudulent activities which are generally out to steal bank details, or just money, this can be done through phone calls, email scams, private messages.
4.10 Online Streaming Services
This section will be about controversial online streaming services such as Kodi which allow unauthorised upload of such things as movies to be streamed by the general public, these websites are a hive of viruses that can infect your devices.
Nearly a third of the participants do use streaming services such as these, the next two questions will be for them, one will be do they realise that their internet service provider (ISP) can see when they have accessed these streaming services, and the second question being, do they realise that the links that takes them to the videos are usually downloading other pieces of potentially harmful data onto their machines and not just the video that they want to watch.

![Pie chart showing the results of the knowledge question about internet service providers and their ability to identify when streaming services are being used.](image)

**Fig 45.** Results from knowledge question about internet service providers and their ability to identify when streaming services are being used.

Did you know that when you access a "mirror" using these websites, you are not just accessing the data you clicked on but a whole host of potentially infected data that could infect your device with such things as viruses, Trojan Horses or Keylogging programs.

![Pie chart showing the results of the knowledge question about accessing mirrors.](image)
The majority of them know that they can be seen watching these potentially illegal programs, and they realise that the videos they watch and the links they click could potentially compromise their information and devices.

5. Findings Analysis, Discussion and Conclusions

5.1 Participants Statistics Analysis
This section will look at all the data shown so far and try to create an average stance that will include all the participants, the first section of questions was regarding the participant statistics, we had a fair split of male and female participants, which was good for the research as gender related knowledge will be covered later. The age range was good, quite a few people over the usual age of a student, but most of them were in the normal range. The first set of questions after the participant statistics was how concerned the participants were with their privacy online, we will be using this as a comparison for the rest of the data. The majority of the participants said they was concerned or very concerned, with a small portion saying they were indifferent, but not many of them saying they were not concerned, this data was broken down into groups, gender and age group, on the gender side of things, the males had more participants that were indifferent, which could show some form of indecisiveness or lack of caring, but there were more of them that had said they are very concerned about their privacy than the females, who had more people in the not concerned part. In terms of age groups, there was a clear pattern, the 18-24 year olds had the most participants out of the three groups who answered, either indifferent, not that concerned and not concerned, this could be a result of being brought up around this technology, the 25-39 year olds, had a few that were not concerned and the majority fell into the category of slightly concerned and very concerned, whereas with the 40-60 age range, there wasn’t a single participant that was not concerned with their privacy, eluding to the fact that since they was not brought up with the internet and social media, they understand how important privacy is. Now how does this hold up to their answers in the questionnaire.
5.2 Online Shopping Analysis
The first section of the questionnaire was about Online shopping, where 100% of the participants admitted to doing their shopping on such online retailers as Amazon or eBay, in this day and age you would be hard pressed to find someone who doesn’t do their shopping online, the next two questions of that section were about what data do they store on these websites, the expected answer would be at minimum home address, as that isn’t as detrimental as credit and debit card details, but again the majority verdict was that they store both credit/debit card details and home address on these websites which can be accessed by these retailers, but that could be just for convenience sake alone. One of the biggest tactics used by these retailers is targeted advertising, which is essentially reviewing what you purchased and advertising similar products to try and sell more to you, the majority of people knew about this and the majority of people knew that these websites can access the data you store on their website including purchase history and buying habits. Overall when it comes to online shopping, the participants showed good knowledge of how their private information was used.

5.3 Social Media Analysis
The next section was regarding social media, one of the biggest uses for smart phones and one of the most used communication techniques in this day and age, privacy knowledge is extremely important on these websites, 46 of the participants admitted to using these platforms in some capacity. The first question was regarding the use of location services, which essentially allows your friends to see where you are posting from, whether that be your house or somewhere in public, this is an optional feature on the majority of social media platforms, only 15 out of the 46 agreed to using these features, meaning their friends will know where they are when they post, out of the 15 that used location services 8 of them knew about Geo-mapping, a method of mapping someone movements using online data that is readily available. Returning back to the 46 that answered yes to using social media, the question “have you ever posted your home address” was asked where only 1 admitted to actually doing so, which is amazing. 5 people admitted to sending nudes over social media platforms of which 4 knew that the social media provider stored these images on their servers and the images were not exclusive the sender and receiver. The results of the questions revolving around the preventative program to combat revenge porn that was planned
by Facebook was met with an indifference from nearly a half of the participants, this is probably due to the fact that there are only 5 participants that admitted to sending lude images of themselves, a large participant base could help clarify the position on this subject.

5.4 Mobile Devices Analysis
For the mobile device section, there was a majority verdict in favour of the iPhone platform, with android coming in second and kindle fire having a 2% share, this section was mainly revolving around applications that are installed on these devices, and the idea that they could be using data on the phone that they do not need to operate, when the participants were asked whether or not they install applications regularly on their phone or device, there was just more than 50% that said yes they do, this is surprising in the fact that there wasn’t more people who install applications regularly as that is one of the main features of these devices. The next couple of questions were exclusive to those that said they installed apps regularly on their mobile phone. The first being, does the participant read the permission the application requests before installing and operating the software. This data was broken down into those who have sensitive information on their device against those who read the permissions that applications ask for, and it seems like if a participant does have sensitive information on their phone they are more likely to read the application permission description before they install the software, which shows some either conscious or subconscious effort to protect the data on their device.

5.5 Privacy Software Analysis
The next section of the findings revolved around the use and knowledge of privacy masking tools such as TOR browser, Virtual private networks, proxies and incognito mode, the first question asked was is the participant aware of these pieces of software? 31 out of 53 participants said yes, they were aware of these tools and a further 22 of the participants said they were unaware of these tools, this data was then used to try and see if the level of awareness was age related, this proved to be absolutely the case, as in the age group 18-24, 18 of the participants out of the 22 in this age range were aware of this technology, whereas in the 25-39 age group just over half the population for this age range had knowledge of this sort of technology. Finally, in the age group 40-60 just under 75% of the participants were not aware of this sort of software, this shows that the older the participants, the more likely a
participant would be unaware of privacy masking tools. The next question was for the participants that had answered yes, to the question of are you aware of these privacy masking tools, and it was to find out which of these tools were the most popular. Out of the 5 offered, them being TOR, virtual private networks, incognito mode, proxies or none of the above, incognito mode was the most popular with 15 participants admitting to the use of this software, the second most popular was virtual private networks with none of the above coming in third, proxies in fourth and TOR browser in last with only 3 participants. Incognito mode is most likely going to be the first in any question of this calibre as it is the most readily available, being offered as standard in most web browsers.

5.6 Internet Browsing Analysis
Section 4.6 revolved around the use of the internet, and how it is used by the participants. The first question was a knowledge question regarding internet protocol (IP) addresses and the idea that these addresses can allow someone to track back to your home address, 70% knew about this and 30% did not know about this, this is could have been split up into the participants profession or degree course if the question had been asked, this will be mentioned in improvements. The next question of this section is regarding cookies and the idea that these can access and compile browsing history, although strictly these cookies are restricted to the websites they were sent from, it is still a big privacy matter that the participants need to be aware of. 62% of the participants were aware of these cookies, where as 38% were not, it’s not a surprise that a lot of the participants were aware of these as most websites give a popup or in-site notification asking the user to enable cookies on their browser for the “best experience”. The next question from section 4.6 is about a new development in mobile tracking and data mining technology, which allows websites to analyse mobile users and find their contact information and other sensitive information stored on their devices, the vast majority of the participants, a whole 81% were either strongly disagree or disagree , which 7% indifferent and the last 12% agreeing and strongly agree, this shows that people do not want to be tracked and they don’t want to see technology like this coming to the mainstream. The next 3 graphs from this section were all about the same topic, whether or not the participants accessed porn on the internet, this data was combined with gender and also a question asked in the privacy tools section, specifically which of these tools do you use, but first the question for all
the participants, which is do you access porn on the internet. The results came back as nearly a 50/50 split, with no edging just slightly into the lead, this was then broken down into gender, where the results were, 41% out of the 45% males asked this question admitted to accessing porn on the internet, with just 4% saying they do not, on the other hand the females is the complete opposite, with 49% out of the 55% asked the question do you watch porn on the internet only 6% said yes they do, showing that males are more likely to access these sorts of websites than females. The next combination was to do with privacy masking tools, to see if there was a correlation with using privacy tools and access this sort of material on the internet. The data was limited to those who do access porn, and another column was added for those who access porn but do not use privacy masking tools, this doesn’t necessarily mean they use these tools whilst accessing porn, but it could be one of the reason they have these tools in the first place. First up was incognito mode, as mentioned in the last section this is the favourite amongst the participants due to its availability, 32% of the people who access porn use incognito mode, a small portion of the users who access porn also use the TOR browser, a much larger portion comparable to the incognito mode results use virtual private networks, 19% use proxies and 11% don’t use any of these whilst accessing this material. It is assumed that if these participants have these tools at their disposal they will be using them to access porn to be on the safe side of privacy, especially since some websites that offer services such as porn can be on the unsafe side, what is interesting is that there were 11% that do not using any privacy masking tools whilst accessing porn even the most readily available one, incognito mode, this shows some form of effort to protect data or at least privacy, whereas the 11% might just not care about their privacy.

5.7 Law Enforcement Analysis
The next section comprised of a single question and that was whether or not the police would require a warrant to access online information about someone, whether this be social media messages, emails and so on, the participants responded with a resounding yes as 97% of them believe the police should need a warrant before accessing this sort of data, and 3% believe they shouldn’t, which just shows that they don’t want faceless intrusion into their lives for no reason.
5.8 Right to be Forgotten Analysis
The next question was regarding the right to be forgotten act of 2006 which allows a person to request the removal of information regarding themselves from the internet, this is a very useful tool as it allows someone to essentially remove their data from the internet without creating a big hassle out of it, but just only a third of the participants knew about it, which is surprising.

5.9 Fraudulent Technique Analysis
The next question was about fraudulent emails, phone calls, texts that sort of thing, this question works well on multiple levels, for one it shows how wide spread these sort of emails are, but it also shows how knowledgeable the participants are and how vigilant they are, 87% of the participants said they had been targeted by these techniques, which means 87% of them know how to spot this sort of impersonation, which is a key step in keeping data secure.

5.10 Streaming Services
The next section is regarding streaming services, the example used in the section was a platform called Kodi, a streaming service that offers a multitude of movies, uploaded by users, Kodi itself is not an illegal service, but the movies uploaded by the users are illegal. Out of the participants who answered this question 30% admitted to using these services, leaving 70% who do not use these services, this question was there to ascertain how many of the participants use this service, but it was to help filter the participants for the next couple of questions. The question after was did you know your ISP can identify when you are using this sort of service, this question was asked of only the 30% that had said they used Kodi, 77% of the participants involved in this question said yes, they understood that the internet service provider could identify when this service was being used. The next question is about the potential dangers when using these services, when a link is clicked that is supposed to load a movie, that’s not the only thing which is loaded, access to the source is given to the user which could potentially be infected with a whole host of nasty infections such as keyloggers (programs that monitor key strokes) viruses and so on, this question was asked of the participants that use these services, because if they knew about it, it would be strange that they continued their use of it. 77% of the participants knew about these dangers, so they know their internet service provider can identify when they are
using it, and they understand that clicking these links could potentially infect or damage their device, but they still do it, it’s probably because it is free.

5.11 Research Improvements
If the research was to be conducted again there are a few things that could be improved on, namely getting a larger population base to answer the questions, this could be done in multiple ways; either advertise the questionnaire more and let it run for longer before pulling the data, or expand the population criteria to other universities, this could help diversify the ethnicity, as the majority of the population for this questionnaire conducted in the research was primarily of white background.

More data could have been collected about the participants such as what profession they were involved in, or what course they are studying, this could have provided some better comparisons when it came to questions such as are you aware of privacy masking services.

Some questions regarding Facebook especially one which asked whether the participant agreed with a program they were rolling out to attempt to combat revenge porn could have been poorly timed due to Facebook being in the spotlight in regards the Cambridge analytical breach a few months ago.

The data that was received was good but not extensive enough especially for questions like which of these services do you use (TOR, VPN, Proxies, etc.) this question could have done with a follow up, in the form of why you use these services, or what do you use them for, this could’ve helped give more background on why people were moving towards these forms of services.

The questions could have been structured differently, instead of yes or no knowledge-based questions, the questions could have been true or false, giving the participant more chance to think about it, rather than plaining saying if they know something or not.
5.12 Summary of Conclusions

5.12.1
The main conclusion that can be derived from the findings is, on the surface, the majority of the participants are well versed in terms of privacy especially in the areas of internet browsing, as discussed in section 5.6

5.12.2
When the data was broken down into age groups or gender there is a serious split between the younger participants and the older ones. The younger participants fared better in the questions that was more knowledge based, for example the question regarding if they had heard about privacy software such as incognito mode and VPNs. Whereas the older participants were more vigilant when it came to their security, more likely to read permissions, or to not store certain pieces of data online, as discussed in section 5.5

5.12.3
There also seemed to be differences between male and female participants. There was a significant difference when it came to gender regarding porn or illicit images, where it seems like the males were more likely watch pornographic material on the internet as well as more likely to send illicit images of themselves to other users on the social media sites, which could show a lack of caring on the male’s side, or a more protective side from the females. This topic was discussed and expanded on in section 5.6

5.12.4
When it comes to the use of privacy software, there was a lack of people using such pieces of software such as incognito mode, even though it is readily available, but those who use it made up the majority of the participants who accessed pornographic material on the internet, showing that maybe, the more secure a person is feeling, the more likely they are to venture into the territory of porn. We like to think that we are safe with our data, especially important data such as credit card details and our home address, but nearly everybody that was asked, stored their details on websites such as amazon or eBay, the only reasoning that can be behind this is convenience. Data security is well known, but we only see application of it when it is convenient, storing
data such as credit card and debit card numbers can be dangerous, but not storing them is inconvenient.
References


Amazon. No Date *Interest-Based Ads* [ONLINE] Available at: https://www.amazon.com/b/?ie=UTF8&node=5160028011 [Accessed 19th April 2018]


Eugdpr, No Date. *GDPR Key Changes* [ONLINE] Available at: [https://www.eugdpr.org/key-changes.html] (Accessed 11th April 2018)

Equifax, 2017. *Cybersecurity Incident – Information for UK Consumers* [ONLINE] Available at: [https://www.equifax.co.uk/incident.html?gclid=Cj0KCQjw5LbWBDRDCARI5ALAbcOdddUBTe9X35G0rsAGRL18j6Z6kgyvHZNm72EuW0x92tUNT5wSAnGznkaAtD3EALw_wcB&gclsrc=aw.ds] (Accessed 12th April 2018)


Denyer, S. 2016 *China wants to give all of its citizens a score – and their rating could affect every area of their lives* [ONLINE] Available at: https://www.independent.co.uk/news/world/asia/china-surveillance-big-data-score-censorship-a7375221.html [Accessed 27th April 2018]


**Appendix**

Fig 47. Ethics Form, the form submitted before initiation of this research project

**DEVOLVED ETHICS APPROVAL APPLICATION SUMMARY**

Student Name: Matthew Holland
Student Number: ST20064644

Module Name: Software Development Project Y17
Module Number: BCO6010_Y17_17

Programme Name: BSc (Hons) Software Engineering
Supervisor Name: Supervisor Dr Panicos Georghiades

<table>
<thead>
<tr>
<th>To be completed by student and supervisor before submission to Ethics Approval Panel</th>
<th>Student Signature</th>
<th>Supervisor Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application for ethics approval</td>
<td>[ X ]</td>
<td>[ X ]</td>
</tr>
<tr>
<td>Participant information sheet</td>
<td>[ X ]</td>
<td>[ X ]</td>
</tr>
<tr>
<td>Participant consent form</td>
<td>[ X ]</td>
<td>[ X ]</td>
</tr>
<tr>
<td>Pilot interview/s (where applicable)</td>
<td>[ ]</td>
<td>[ X ]</td>
</tr>
<tr>
<td>Pilot questionnaire/s (where applicable)</td>
<td>[X ]</td>
<td>[ ]</td>
</tr>
<tr>
<td>Letter/s to participating organisation/s (where applicable)</td>
<td>[ ]</td>
<td>[ X ]</td>
</tr>
<tr>
<td>Confirmation of interviewee participation (where applicable)</td>
<td>[ ]</td>
<td>[ X ]</td>
</tr>
</tbody>
</table>

First Submission   [X ]    Resubmission   [ ]

Date: ____________________________

For use by the devolved ethics approval panel:

<table>
<thead>
<tr>
<th>Panel Members</th>
<th>Name</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module Leader, Chair:</td>
<td>____________________________</td>
<td>________________</td>
</tr>
<tr>
<td>Supervisor:</td>
<td>____________________________</td>
<td>________________</td>
</tr>
</tbody>
</table>

CSM Ethics Committee Representative:
Date: ______________ Date of Reassessment: ____________

**Outcome:**

Project Approved [ ] Reference number issued: ______________
Chair’s Action [ ]
Application Not Approved [ ]

Comments for projects not fully approved:

The original to be retained by the module leader and a copy given to
When undertaking a research or enterprise project, Cardiff Met staff and students are obliged to complete this form in order that the ethics implications of that project may be considered.

If the project requires ethics approval from an external agency (e.g., NHS), you will not need to seek additional ethics approval from Cardiff Met. You should however complete Part One of this form and attach a copy of your ethics letter(s) of approval in order that your School has a record of the project.

The document Ethics application guidance notes will help you complete this form. It is available from the Cardiff Met website. The School or Unit in which you are based may also have produced some guidance documents, please consult your supervisor or School Ethics Coordinator.

Once you have completed the form, sign the declaration and forward to the appropriate person(s) in your School or Unit.

PLEASE NOTE:
Participant recruitment or data collection MUST NOT commence until ethics approval has been obtained.

PART ONE

<table>
<thead>
<tr>
<th>Name of applicant:</th>
<th>Matthew Holland</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisor (if student project):</td>
<td>Dr Panicos Georghiades</td>
</tr>
<tr>
<td>School / Unit:</td>
<td>Cardiff Metropolitan School of Management</td>
</tr>
<tr>
<td>Student number (if applicable):</td>
<td>ST20064644</td>
</tr>
<tr>
<td>Programme enrolled on (if applicable):</td>
<td>BSc (Hons) Software Engineering</td>
</tr>
<tr>
<td>Project Title:</td>
<td>An Investigation into Students awareness regarding their online privacy and private information rights</td>
</tr>
<tr>
<td>Expected start date of data collection:</td>
<td>20/02/2018</td>
</tr>
<tr>
<td>Approximate duration of data collection:</td>
<td>6 Weeks</td>
</tr>
<tr>
<td>Funding Body (if applicable):</td>
<td>N/A</td>
</tr>
<tr>
<td>Other researcher(s) working on the project:</td>
<td>N/A</td>
</tr>
<tr>
<td>Will the study involve NHS patients or staff?</td>
<td>No</td>
</tr>
<tr>
<td>Will the study involve human samples and/or human cell lines?</td>
<td>No</td>
</tr>
</tbody>
</table>

Does your project fall entirely within one of the following categories:

<p>| Paper based, involving only documents in the public domain | No |
| Laborotary based, not involving human participants or human samples | No |</p>
<table>
<thead>
<tr>
<th>Practice based not involving human participants (eg curatorial, practice audit)</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compulsory projects in professional practice (eg Initial Teacher Education)</td>
<td>No</td>
</tr>
<tr>
<td>A project for which external approval has been obtained (e.g., NHS)</td>
<td>No</td>
</tr>
</tbody>
</table>

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

This research project aims to identify the awareness levels of students (18+) regarding their privacy rights in respect to their confidential information and how it is handled within the confines of the internet. I will then be using current legislation and laws such as the Data protection act to research the reality of privacy on the internet and what can be done to keep ourselves secure. I will be using primary research methods such as questionnaires to gauge what the current popular idea is regarding privacy as a collective. I will be looking into different aspects of the internet where private information is used and where privacy can be essential such as Social Media and online shopping. I will also be analysing the effect the Brexit movement will have on legislation brought in by the EU such as the data protection act which was included within the human rights act of 1998.

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: M S Holland  Date: 13th December 2017

FOR STUDENT PROJECTS ONLY

Name of supervisor: Dr. Panicos Georghiades  Date: 15 Jan 2018

Signature of supervisor: PGeorghiades

Research Ethics Committee use only

Decision reached:  Project approved x
                      Project approved in principle
                      Decision deferred
                      Project not approved
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

My research involves a Positivist philosophy as I will be using case studies such as the United States of America to make predictions on what will happen in the United Kingdom. My Research will be a mix of Inductive and Deductive research methods, Inductive because my private information is stored on the internet and deductive because I will be using quantitative data by ways of analysing behaviours and opinions regarding the private information and privacy on the internet.

Questionnaire:
- I intend to create an online questionnaire to be completed by at least 50 people and comprising of around 30 questions per questionnaire. This will allow a solid assumption to be made about the consensus regarding privacy and confidential information on the internet, and will aid in my research regarding awareness overall.
- There will be a consent document and tick box at the beginning of the online questionnaire to make sure all participants are happy to fill out the questionnaire
- Approximately it will take a participant around 10 minutes to complete the questionnaire
- The sample will start off confined to Cardiff metropolitan students.

Participant Sample:
- I will be looking for primarily students of the age range of 18+ to take part in the questionnaire, since this questionnaire will be on the internet I can’t stop people above or below the age range from participating but there will be a message at the beginning of the questionnaire asking that only students above the age participate. This will also allow me to hypothesise a correlation between age and behavioural patterns regarding sharing private information on the internet.

\(^1\) 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
To maximise my chances of having a large sample size I will be asking at the end of the questionnaire that the link for the questionnaire be sent to participants friends that fit into the category of 18-25-year-old student.

Consent:  
The consent form terms will be present on the website before any of the questionnaire takes place and before an information gathering happens, after they have read through the form a tick box that will be at the bottom will be used so that the participant can give consent.

Sample security:  
All participants will be answering the questions on the internet I will be asking for age, gender and ethnicity and they will be stored securely (Encrypted Memory Stick), they will not be used outside of the project bounds and will be destroyed after the research project is complete. The names of the participants will not be present during the final write up of the project and theirs ages will only be used by being grouped with others of similar ages to create correlation between age and behaviour.

Secondary Research:  
- Analysing legislation regarding data protection act, such as the data protection act and what changes leaving the EU will have on our rights.

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

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?  
More than 30 years experience in academic research.

C POTENTIAL RISKS

C1 What potential risks do you foresee?  
Questionnaires:  
- There might not be many responses, limiting the sample size.
• There may be the possibility of people doing the questionnaire and using a different age.
• There may be concerns regarding the security of the information.

C2 How will you deal with the potential risks?

If there is only a small amount of questionnaires that haven’t being returned then I will continue the research as planned, otherwise if a large portion of them haven’t been returned or if not many have been given out then I will expand the sample to include other universities.

When submitting your application you **MUST** attach a copy of the following:

• All information sheets
• Consent/assent form(s)

An exemplar information sheet and participant consent form are available from the Research section of the Cardiff Met website.
Questionnaire

Title
An Investigation into Students awareness regarding their online privacy and private information rights

Summary

The purpose of this project is to work out how our private information is used by companies on the internet and what legislation and laws in the United Kingdom are in place to protect it, your participation with this questionnaire will enable collection of data that will allow a correlation between age and personal use of private data.

1. Please tick the box to acknowledge that you have read and signed the consent form at the beginning of this questionnaire and are willing to take part in this project by filling in this questionnaire and that you are 18 years old and over?

2. What is your age? (Years 18 or over)

3. What is your gender(Choose one)

   Male
   Female

4. What is your Ethnicity (Choose one)?

   White
   Black – Caribbean
   Black – African
   Black – Other
   Indian
   Pakistani
   Chinese
   State other
5. In regards to privacy and private information on the internet how concerned are you (1 being the least concerned and 5 being very concerned)?

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
</table>

6. Do you do shopping online using retailers such as Amazon and eBay?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

7. (Follow on from Question 6) Do you store your delivery address on these websites?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

8. (Follow on from Question 6) Do you store you debit/credit card details on these websites?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

9. (Follow on from Question 6) Are you aware algorithms embedded in the websites of the online retailers learn your spending patterns in order to try and sell you other stuff in the future?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

10. (Follow on from Question 6) Are you aware that websites such as these can access all your data that you have stored on their website? Such as card details recent purchases and delivery address.

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

11. Do you use social media websites such as Facebook, Twitter or Reddit?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

12. (Follow on from Question 11) Do you have your location posting along side your posts, pictures or videos, or if you use the “Check in feature” that lets your friends know where you are?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

13. (Follow on from Question 12) Do you know that by consistently posting your location on social media, people, not just the website provider can create a map detailing your whereabouts on certain times and days and use that to estimate your movement patterns and even where you live?

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

14. (Follow on from Question 11) Have you ever posted your home address to your social media account?

| Yes | No |
15. (Follow on from Question 11) Have you ever sent nude images of yourself over a social media platform to another user?

| Yes | No |

16. (Follow on from Question 15) Do you realise that just by sending a photo over a social media platform that photo has to be stored somewhere on that social media platforms servers?

| Yes | No |

17. Have you ever received nude images of someone else on a social media platform?

| Yes | No |

18. On what level do you agree with Facebook’s choice to roll out a program that allows you to send Facebook your nude photos in order to help combat Revenge porn? (They will use algorithms that look for your photos and make sure they cannot be re-uploaded) (1 – least concerned/5 – Most concerned)

| 1 | 2 | 3 | 4 | 5 |

19. (Follow on from Question 18) Do you think you will use this service?

| Yes | No |

20. Do you own an iPhone or Android device?

| iPhone | Android | Neither |

21. (Follow on from Question 20) Do you store sensitive information on your mobile device I.E Nude photos, credit/debit card information, home address?

| Yes | No |

22. Are you aware of privacy masking services such as TOR Browser, Incognito Mode, proxies or VPNs(Virtual Private Networks)

| Yes | No |

23. Do you use any of these services? (Select all that apply)

| TOR | Incognito Mode | Proxy | VPN |

24. Are you aware that by just the act of accessing a website you just given away the IP address of your computer which allows you to be tracked back to your home?

| Yes | No |
25. Did you know that when you access a website they will often ask you to enable “Cookies” on your browser these cookies allow the website provider to compile and see your browsing history.

| Yes | No |

26. How much do you agree with a recent development in this technology that allows websites to use analytics to collect data regarding contacts, friends, family and associates when using your mobile phone to access the internet?

| 1 | 2 | 3 | 4 | 5 |

27. Do you often install new applications on your mobile phone?

| Yes | No |

28. (Follow on from Question 27) Do you automatically grant permissions requested by these applications without reading what they are asking for?

| Yes | No |

29. Did you know that a lot of these applications request the use of such things as contacts, phone records and access to your photo album without even needing it, this is done so that they can build a portfolio of your life and social activities to help them sell to you or even sell that data onto third party companies?

| Yes | No |

30. Should law enforcement be required to seek a warrant before accessing personal information on the internet about you? I.E Emails, texts, social media messages

| Yes | No |

31. Are you aware of the concept of “The Right to be Forgotten” which has been in practice since 2006, which allows you to retract your information from the internet, in the hopes of ‘being forgotten’?

| Yes | No |

32. Have you ever been targeted by fraudulent techniques such as phone scams or phishing emails which aim to steal your information?

| Yes | No |

33. Do you use illegal streaming platforms such as Kodi?

| Yes | No |
34. (Follow on from Question 33) Do you realise that your internet service provider can recognise when you are using these services?

| Yes | No |

35. (Follow on from Question 33) Did you know that when accessing a “Mirror” using these sites, you are not just accessing the data you are looking for but a whole host of information that could potentially infect your machine with viruses such as trojans or keyloggers.

| Yes | No |

36. Do you access pornographic material on the internet?

| Yes | No |

37. Did you know that even using Incognito features provided by many browsers these days do not stop your internet provider from being able to see what sites you have been browsing?

| Yes | No |

**END OF QUESTIONNAIRE**

Thank you for being part of my research, if you have any concerns regarding the information gathered today or if you want to retract your answers, you may contact either me or my supervisor using the contact details below.

Cardiff Metropolitan University email: ST20064644@cardiffmet.ac.uk

Supervisor: Panicos Georghiades, email: pgeorghiades@cardiffmet.ac.uk